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

MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

Las políticas de Seguridad Informática tienen como objetivo principal, establecer reglas sobre el uso de los sistemas informáticos y de comunicaciones de la Unidad Administrativa Especial de Servicios Públicos - UAESP, por parte de usuarios, administradores o terceros, proteger los recursos de información de la Entidad y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Las políticas de Seguridad Informática buscan establecer controles administrativos y operativos, que regulen de manera efectiva el acceso de los usuarios a los sistemas a nivel de aplicación, sistema operativo, base de datos, red y acceso físico; asegurar la implementación de las medidas de seguridad comprendidas en estas Políticas, identificando los recursos y las partidas presupuestarias correspondientes.

2. OBJETIVOS ESPECIFICOS

La Unidad Administrativa Especial de Servicios Públicos - UAESP, para el cumplimiento de su misión, visión, objetivos estratégicos y alineados a sus valores corporativos, establece la función de Seguridad de la Información en la entidad, con el objetivo de:

- Mantener la confianza de los ciudadanos en general y el compromiso de todos los funcionarios, contratistas respecto al correcto manejo y protección de la información que es gestionada y resguardada en la Unidad Administrativa Especial de Servicios Públicos - UAESP
- Identificar e implementar las tecnologías necesarias para fortalecer la función de la seguridad de la información.
- Implementar el Sistema de Gestión de Seguridad de la Información.
- Proteger la información y los activos de la información de la entidad.
- Asegurar la identificación y gestión de los riegos a los cuales se expone los activos de información de la entidad.
- Cumplir con los principios de seguridad de la información: disponibilidad, integridad y confidencialidad de la información.
- Concientizar a los funcionarios, contratistas sobre el uso adecuado de los activos de información puestos a su disposición para la realización de las funciones y actividades diarias, garantizando la confidencialidad, la privacidad y la integridad de la información
- Dar cumplimiento a los lineamientos establecidos en la Estrategia de Gobierno en Línea respecto a la Seguridad de la Información.

• Dar las pautas generales para la protección de los datos personales y sensibles, brindando herramientas que garanticen la autenticidad, confidencialidad e integridad de la información.

• Regular la recolección, tratamiento, almacenamiento, protección y administración de los datos personales legalmente obtenidos de sus funcionarios, contratistas, usuarios, proveedores, terceros y ciudadanos en general, que puedan involucrarse en virtud del desarrollo de sus actividades misionales, captados a través de los diferentes canales de información y almacenados en bases de datos de la entidad, sujetos a tratamiento y protección de datos personales.

3. ALCANCE

Este Manual aplica a todo el ámbito de la UAESP, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad, así como a los datos e información, sin diferenciar la presentación o formato de almacenamiento; tales como papel, discos magnéticos (fijos y removibles), terminales y dispositivos de almacenamiento óptico, memorias USB y discos externos, así como a todos los elementos del ambiente de cómputo, independientemente de su localización, propósito, consideraciones de custodia o uso original.

El ambiente de cómputo de la UAESP contiene los siguientes componentes:

- Computadores internos y externos
- Equipos de oficina (escáner, impresoras, entre otros)
- Datacenter
- Elementos WAN y equipo asociado
- Routers, Firewalls y Switches
- Access Point y elementos de Red Inalámbrica
- Terminales VolP
- Proveedores externos de datos e información
- Todos los dispositivos terminales
- Líneas de comunicaciones de datos
- Equipos de prueba
- Administración mantenimiento y monitoreo de computadores/redes
- Servicios Internet

Todos los computadores, sistemas de cómputo y activos de información son críticos para el desarrollo y cumplimiento de las funciones, y deben ser protegidos a un nivel acorde con su valor, sensibilidad e importancia.

La violación del presente manual será motivo para adelantar acciones disciplinarias, civiles y penales según aplique. La UAESP también llevará a cabo acciones judiciales donde lo considere apropiado a algún funcionario de planta, en provisionalidad o contratista que acceda, utilice, intente acceder a algún computador, sistema de cómputo, aplicación, sistema de comunicaciones o redes de la entidad, sin autorización.

4. REFERENCIA NORMATIVA

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: Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014. 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 1150 de 2007: Seguridad de la información electrónica en contratación en línea.

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 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 de 2009: Por la cual se definen 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 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión 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 2693 de 2012: Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.

Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

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.

Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

5. TÉRMINOS Y DEFINICIONES

- **Activo:** cualquier cosa que tenga valor para la organización.
- **Administración de Riesgos:** Conjunto de Elementos de Control que al interrelacionarse permiten a la Entidad Pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función.
- **Auditabilidad:** Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Confidencialidad:** la propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados
- **Data Center:** Un “centro de datos” o “Centro de Procesamiento de Datos” (CPD). Es una instalación empleada para albergar los sistemas de información y sus componentes asociados, como las telecomunicaciones y los sistemas de almacenamiento. Generalmente incluye fuentes de alimentación redundantes o de respaldo, conexiones redundantes de comunicaciones, controles de ambiente (por ejemplo, aire acondicionado) y otros dispositivos de seguridad.
- **Disponibilidad:** la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.
- **Evaluación del Riesgo:** Permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la entidad al riesgo; de esta forma es posible distinguir entre los riesgos ubicados en los niveles: Nivel bajo, moderado, alto y extremo y fijar prioridades de las acciones requeridas para su tratamiento.
- **Evento de seguridad de la información:** 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 las salvaguardas, o una situación

previamente desconocida que puede ser relevante para la seguridad.

- **Firewalls:** Son dispositivos de seguridad, que permiten filtrar contenidos y proteger las aplicaciones de accesos no autorizados o ataques externos.

- **Incidente de seguridad de la información:** un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Integridad:** la propiedad de salvaguardar la exactitud e integridad de los activos.

- **Seguridad de información:** preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad

- **Legalidad:** Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto la Unidad.

- **Sistema de Gestión de Seguridad de la Información SGSI:** Esa parte del sistema gerencial general, basado en un enfoque de riesgo comercial; para establecer. implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

- **No Repudio:** Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

- **Protección a la Duplicación:** Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se registre una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- **Router:** Dispositivo de hardware o software para interconexión de redes internas y/o externas que opera en la capa tres (nivel de red) del modelo OSI (Open Systems Interconnection - Interconexión de Sistemas Abiertos). El router toma decisiones basadas en diversos parámetros con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuados.

- **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.

- **Tecnología de la Información:** Se refiere al hardware y software operados por la Unidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Unidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

- **Tercero:** Contratistas que prestan servicios directos o indirectos, 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 UAESP.

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

6. ESTRUCTURA DEL DOCUMENTO

Este documento de políticas está estructurado de acuerdo a los Objetivos de Control y Controles establecidos en la norma NTC- ISO-IEC 27001: 2013. El documento se encuentra directamente relacionado con el anexo A de la norma, iniciando desde el dominio de Aspectos Organizativos de Seguridad de la Información y finalizando en el dominio de Cumplimiento de los Requisitos Legales; por ello, sus títulos están alineados con dicho anexo en los objetivos de control y controles para los cuales la entidad ha fijado políticas de seguridad de la información.

7. RESPONSABILIDAD Y AUTORIDAD

7.1. Asignación de Responsabilidades en Materia de Seguridad Informática.

- El/La directora (a) de la UAESP, asigna las funciones relativas a la Seguridad Informática de la UAESP al Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones (en su defecto a quien él proponga y tenga las capacidades para tal tarea), en adelante el "Responsable de Seguridad Informática", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en las presentes Políticas.

- El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación la definición y asignación de las responsabilidades que surjan del presente manual.
- Todo el personal, sea cual fuere su nivel jerárquico es responsable de la implementación de estas Políticas de Seguridad de la Información dentro de sus dependencias, así como del cumplimiento de dichas Políticas por parte de su equipo de trabajo.

- Las Políticas de Seguridad de la Información son de aplicación obligatoria para todo el personal de la UAESP, cualquiera sea su situación, vinculación, dependencia y nivel de las tareas que desempeñe.

- Las máximas autoridades de la UAESP deben aprobar estas Políticas y son responsables de la autorización de sus modificaciones.

- El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, podrá designar las responsabilidades del personal que apoya la gestión, de acuerdo con las necesidades de la Entidad.

Comité de Seguridad de la Información o en su defecto el Comité de Sistemas de la UAESP. La seguridad de la información es una responsabilidad de la Entidad por tal razón se debe crear el Comité de Seguridad de la Información, integrado por representantes designados de la Dirección, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. El mismo contará con un responsable, quien cumplirá la función de impulsar la implementación de la presente Política, y cumplirá con las siguientes funciones:

- Revisar y proponer a la máxima autoridad de la entidad las Políticas de Seguridad de la Información y las funciones generales en materia de seguridad de la información para su aprobación.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro de la UAESP.
- Coordinar el proceso de administración de la continuidad de las actividades de la Unidad.
- Revisar y proponer a la máxima autoridad de la UAESP para su aprobación, las Políticas y las funciones generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.

El Responsable del Comité de Seguridad de la Información será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

Los Propietarios de la Información son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de esta, documentar y mantener actualizada la clasificación efectuada, y definir que usuarios deberán tener permisos de acceso a la información de acuerdo con sus funciones y competencia.

El Responsable de Talento Humano o quién desempeñe esas funciones, deberá notificar a todo el personal que ingresa, sus obligaciones respecto del cumplimiento de las Políticas de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de las presentes Políticas a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad.

El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones (Oficina TIC), cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la UAESP. Por otra parte, tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

El responsable de la Subdirección de Asuntos Legales verificará el cumplimiento de las presentes Políticas en la gestión de todos los contratos, acuerdos u otra documentación de la UAESP con sus funcionarios y con terceros.

El responsable de Seguridad informática: cumplirá funciones relativas a la seguridad de los sistemas de información de la UAESP, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en las presentes Políticas, tiene a cargo las siguientes responsabilidades:

- Revisar y monitorear regularmente los incidentes de seguridad que se presenten.
- Generar informes de los diferentes incidentes de seguridad que se presenten.
- Analizar los accesos a los recursos informáticos sensibles de la compañía y realizar un seguimiento y monitoreo de estos.
- Garantizar la operación de los sistemas de comunicaciones y de su instalación y configuración de acuerdo con los estándares de seguridad informática.
- Comunicar a la Oficina de TIC la intención de implantar nuevas versiones y/o productos de software o hardware.
- Informar a la Oficina de TIC sobre las modificaciones a realizar sobre los sistemas e infraestructura.
- Informar a la Oficina de TIC sobre cualquier utilización no apropiada de los sistemas de información, equipos de red, servidores o cualquier otro evento que pueda convertirse en un incidente de seguridad informática.
- Colaborar y trabajar en la implantación de estándares de seguridad informática en los sistemas de información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir las Políticas de

Seguridad de la Información vigente.

8. LINEAMIENTOS O POLÍTICAS DE OPERACIÓN

- La violación de las políticas serán motivo para emprender acciones disciplinarias, civiles y/o penales según aplique.
- Los funcionarios de planta, provisional o contratista que utilice las herramientas de tecnología informática para acceso a direcciones en Internet que contengan pornografía, juegos o salas de conversación será sancionado administrativamente.
- La Subdirección de Asuntos Legales, adelantará los procesos disciplinarios para los funcionarios que incurran en cualquiera de los siguientes delitos informáticos a través de Internet o de acceso físico, así como analizar cómo afectarían dichos sucesos a la Organización:

- Acceso no autorizado a la red de datos de la entidad.
- Acceso no autorizado al centro de datos de la entidad.
- Acceso no autorizado a equipos no asignados para su labor.
- Destrucción de Datos, archivos e informes.
- Infracción de los derechos de autor.
- Infracción de Copyright de Bases de Datos.
- Interceptación de e-mail.
- Estafas electrónicas.
- Transferencias de Fondos en forma ilegal.
- Delitos convencionales como extorsión, espionaje, terrorismo, narcotráfico, proselitismo de sectas, propaganda de grupos extremistas.
- Mal uso, como: Usos comerciales no éticos, agresión moral, cyber bullying.
- Accesos a páginas de contenido restringido y/o promueva su uso.
- Participar de juegos en línea a través de la red.

- El Comité de Seguridad de la Información o quien sea designado, revisará como mínimo cada año el presente Manual a efectos de mantenerla actualizada. Asimismo, efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como pueden ser, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, entre otros.

9. POLÍTICAS DE SEGURIDAD INFORMÁTICA

La UAESP, establece una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

9.1. ORGANIZACIÓN DE LA SEGURIDAD

Orientado a administrar la seguridad de la información dentro de la Unidad y establecer un marco gerencial para controlar su implementación.

9.1.1. Generalidades

Se establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la Entidad. Por ello se define formalmente un ámbito de gestión para efectuar tareas tales como, la aprobación de la Política, la coordinación de su implementación, la asignación de funciones y responsabilidades, así como, la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Por otro lado, debe tenerse en cuenta que ciertas actividades de la Entidad pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones y/o responsabilidades relacionadas con el procesamiento de la información. En estos casos, se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

9.1.2. Objetivos

- Administrar la seguridad de la información dentro de la Entidad, estableciendo un marco gerencial para iniciar y controlar su implementación, así como para la definición de funciones y responsabilidades.

- Fomentar la consulta y cooperación con organismos especializados para la obtención de asesoría en materia de seguridad de la información.

- Garantizar la aplicación de medios de seguridad adecuadas en el acceso de terceros a la información de la Entidad.

9.1.3. Responsabilidad

El responsable del Comité de Seguridad de la Información o quien sea designado será el responsable de impulsar la implementación de la presente Política.

El Comité de Seguridad de la Información tendrá a cargo el mantenimiento y la presentación de estas Políticas para su aprobación, ante la máxima autoridad de la UAESP, el seguimiento de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad de operaciones, impulso de procesos de concienciación, etc.), de acuerdo a las competencias propias de cada área y la proposición de asignación de funciones.

El Responsable de Seguridad Informática asistirá al personal de la UAESP en materia

de seguridad de la información y coordinará la interacción con entidades especializadas. Así mismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información de la UAESP y verificará la aplicación de las medidas de seguridad necesarias para la protección de esta.

Los responsables de las Oficinas y Subdirecciones cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su competencia.

La Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información o el comité designado, será responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de las presentes Políticas.

El responsable de la Subdirección de Asuntos Legales cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de las Políticas de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

9.1.4. Políticas

9.1.4.1 Infraestructura de la Seguridad de la Información

Para la organización de la seguridad de la información en la entidad se tienen en cuenta las siguientes actividades a saber:

ACTIVIDADES	RESPONSABLE
Seguridad del Personal	Tercero
Seguridad Física y Ambiental	Tercero
Seguridad en las Comunicaciones y las Operaciones	Jefe de la Oficina de Tecnología y las comunicaciones - Personal de apoyo
Control de Accesos	Jefe de la Oficina de Tecnología y las comunicaciones - Personal de apoyo
Seguridad en el Desarrollo y Mantenimiento de Sistemas	Jefe de la Oficina de Tecnología y las comunicaciones - Personal de apoyo
Planificación de la Continuidad de Operaciones	Jefe de la Oficina de Tecnología y las comunicaciones

Es de precisar, que las actividades descritas podrán ser asignadas para su administración a personal capacitado e idóneo, no obstante, el Jefe de la Oficina de Tecnología y las comunicaciones será el veedor del cumplimiento de las mismas. Se dejarán los registros de la designación para el cumplimiento de las actividades.

- **Proceso de Autorización para instalaciones de Procesamiento de Información**

Los nuevos recursos de procesamiento de información serán autorizados por los subdirectores o Jefes de oficina que lo requieran, considerando su propósito y uso, conjuntamente con el Jefe de la Oficina de Tecnología y las Comunicaciones, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de la Entidad.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades, por lo cual, su uso será evaluado en cada caso por el personal de apoyo y deberá ser autorizado por el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones y por el responsable del área al que se destinen los recursos.

- **Asesoramiento Especializado en Materia de Seguridad de la Información**

El Responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en la entidad a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otras Entidades. Con el objeto de optimizar su gestión, se habilitará al Responsable de Seguridad Informática el contacto con todas las Áreas de la UAESP.

- **Cooperación entre Organismos**

En los intercambios de información de seguridad, no se divulgará información confidencial perteneciente a la UAESP a personas no autorizadas.

El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, sólo se permite cuando se haya firmado un Compromiso de Confidencialidad previo o con aquellas Organizaciones especializadas en temas relativos a la seguridad informática cuyo personal está obligado a mantener la confidencialidad de los temas que trata.

- **Revisión independiente de la Seguridad de la Información**

La Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, realizará revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas de la UAESP reflejan adecuadamente sus disposiciones.

9.1.4.2 Seguridad frente al Acceso por parte de terceros

- **Identificación de Riesgos del Acceso de Terceras Partes**

Cuando exista la necesidad de otorgar acceso a terceras partes de la información de la UAESP, el Responsable de Seguridad Informática y el Propietario de la Información de

que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la seguridad de la información de la Unidad.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la Unidad, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

Se cita a modo de ejemplo:

- Personal de mantenimiento y soporte de hardware y software.
- Limpieza, guardia de seguridad y otros servicios de soporte tercerizados.
- Pasantías y otras designaciones de corto plazo.
- Consultores.

En ningún caso se otorgará acceso de terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

- **Requerimientos de Seguridad en Contratos o Acuerdo con Terceros**

Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

a) Cumplimiento de la Política de seguridad de la información de la Entidad.
b) Protección de los activos de la UAESP, incluyendo:
- Procedimientos para proteger los bienes de la UAESP, abarcando los activos físicos, la información y el software.
- Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
- Restricciones a la copia y divulgación de información.

c) Nivel de servicio esperado y niveles de servicio aceptables.
d) Descripción de los servicios disponibles.
e) Permiso para la transferencia de personal cuando sea necesario.
f) Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
g) Existencia de Derechos de Propiedad Intelectual.
h) Definiciones relacionadas con la protección de datos.
i) Acuerdos de control de accesos que contemplen:

- Métodos de acceso permitidos, el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
- Proceso de autorización de accesos y privilegios de usuarios.
- Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse, sus derechos y privilegios con respecto a dicho uso.

j) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
k) Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
l) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
m) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
n) Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de estos.
o) Proceso claro y detallado de administración de cambios.
p) Controles de protección física requeridos y los mecanismos que aseguren la implementación de estos.
q) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
r) Controles que garanticen la protección contra software malicioso.
s) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
t) Relación entre proveedores y subcontratistas.

9.1.4.3 Tercerización

- **Requerimientos de Seguridad en Contratos de Tercerización**

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de escritorio de la UAESP, contemplarán además de los puntos especificados en “Requerimientos de Seguridad en Contratos o Acuerdos con Terceros”, los siguientes aspectos:

a) Forma en que se cumplirán los requisitos legales aplicables.
b) Medios para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.
c) Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos de la entidad.
d) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible de la entidad.
e) Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
f) Niveles de seguridad física que se asignarán al equipamiento tercerizado.
g) Derecho a la auditoría por parte de la Entidad sobre los aspectos tercerizados en forma directa o a través de la contratación de servicios.

9.2. CLASIFICACIÓN Y CONTROL DE ACTIVOS

Destinado a mantener una adecuada protección de los activos de la Unidad.

9.2.1. Identificación de Activos de Información

De acuerdo con la norma ISO/IEC 27000, “activo de información” se define como cualquier elemento que tenga valor para la organización y, en consecuencia, deba ser protegido. Por consiguiente, la primera actividad en la Gestión de Riesgos es identificar los activos de información bajo las consideraciones que la Entidad defina, actividad que debe realizarse sin perder de vista el alcance definido y aprobado por la alta dirección para el Sistema de Gestión de Seguridad de la Información (SGSI) o en el caso de la UAESP el Modelo de Seguridad y Privacidad de Información - MSPI.

En este sentido, las actividades necesarias para la identificación de los activos de información y su formalización dentro de la entidad son:

1. Definir el instrumento de captura de información identificando las variables que se deben capturar.
2. Identificar los procesos y agendar las entrevistas con sus responsables.
3. Recolectar la información necesaria bajo las consideraciones definidas por la Entidad.
4. Realizar los cruces necesarios con otras fuentes de información como inventarios, Tablas de Retención Documental, entre otros, para completar información.
5. Consolidar la información.

Para adelantar esta primera etapa se debe tener en cuenta la definición de la siguiente información, con el fin de poder tener parámetros precisos frente a la captura y consolidación de la herramienta de trabajo.

9.2.2. Identificación de Propietario, Custodio, Responsable y Ubicación

Los activos de información previamente identificados en el paso anterior deben tener su respectivo propietario, definido como la dependencia o proceso donde se crea o custodia dicho activo. Así mismo, definir el custodio de la información el cual, puede ser el mismo propietario o en su defecto el proceso o la persona que la Entidad haya definido para adelantar dicha tarea.

El responsable es el jefe y/o subdirector de cada dependencia o proceso de uno o un grupo de activos de información y es quien debe velar porque los controles de seguridad sean implementados de manera satisfactoria.

En esta medida la tipología de activos de información está definida en la siguiente tabla:

Tabla I. Tipología del Activo

Tipo de activo	Propiedad del activo	Descripción
Activos de Información Puros	Información digital	Bases de datos y archivos, documentos de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, entre otros
	Información física	
	Activos de Información intangibles	
Activos de Tecnologías de Información	Servicios de información	Equipamiento informático, servicios informáticos y de comunicaciones, utilitarios generales (aire acondicionado, iluminación, energía eléctrica, entre otros), software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, entre otros.
	Software	
	Hardware de TI	
	Controles ambientales	
Activos de Información Recurso Humano	Funcionarios y servidores públicos	recursos humanos, funcionarios de la entidad, contratistas.
	Terceros	

9.2.3 Categorización de la Información

Se cuenta con una categorización para el etiquetado de la información, la cual se ha establecido al interior de la entidad con los siguientes criterios:

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de Entidad y debe estar a disposición de cualquier persona natural o jurídica del estado colombiano.

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

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 18 de la ley 1712 del 2014.

Datos Personales: Cualquier información vinculada o que pueda asociarse con los datos públicos y no públicos de una o varias personas naturales o jurídicas, de acuerdo a la ley estatutaria 1581 de 2012.

9.2.4 Valoración de los Activos de Información

Los activos de información deben ser valorados de acuerdo a su impacto en términos de la pérdida de las tres (3) propiedades básicas de la seguridad de la información que son la confidencialidad, integridad y disponibilidad, definidos a partir de la norma ISO/IEC 27000:2013.

Confidencialidad: Es la propiedad de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Integridad: Es la propiedad de salvaguardar la exactitud y estado completo de los activos de información.

Disponibilidad: Es la propiedad de que la información sea accesible y utilizable por solicitud de un individuo o entidad autorizada cuando se requiera.

Dada las anteriores definiciones, se establecen las escalas para la confidencialidad, integridad y disponibilidad respectivamente.

- **Confidencialidad**
  - ✓ Muy Alta - Acceso exclusivo para el Director(a) y Subdirectores
  - ✓ Alta - Solo es posible el acceso por el personal que preparo la información, subdirectores, Jefes de oficina y/o Dirección General
  - ✓ Medio - Se puede acceder por subdirecciones específicas, proveedores y/o contratistas directamente definidos
  - ✓ Baja - Se puede acceder solo por personal de la Entidad
  - ✓ Muy baja - Se puede acceder por cualquier usuario dentro y fuera de la Entidad

- **Integridad**
  - ✓ Alta - Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad
  - ✓ Media - Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad
  - ✓ Baja - Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos
  - ✓ No clasificada - Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA

- **Disponibilidad**
  - ✓ Alta - La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos
  - ✓ Media - La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad
  - ✓ Baja - La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen

- ✓ No clasificada - Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA

9.2.5 Rotulado de la Información

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo con el esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia.
- Almacenamiento.
- Transmisión por correo, fax, correo electrónico, ftp, etc.
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, entre otros.)

9.3 SEGURIDAD DEL PERSONAL

Orientado a reducir los riesgos de error humano, comisión de ilícitos contra la Unidad o uso inadecuado de instalaciones.

9.3.1 Generalidades

La seguridad de la información se basa en la capacidad para preservar su integridad. confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de Talento Humano que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.
La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por esto que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea, a fin de subsanarlos y evitar eventuales réplicas. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

9.3.2 Objetivo

- Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.
- Explicitar las responsabilidades en materia de seguridad en la etapa de

reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

- Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Entidad en el transcurso de sus tareas normales.
- Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

9.3.3 Responsabilidad

El Responsable de Seguridad Informática tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al Comité de Seguridad de la Información y a los propietarios de la información.

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad Informática maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El responsable de la Subdirección de Asuntos Legales participará en la elaboración del Compromiso de Confidencialidad a firmar por los funcionarios, contratistas y terceros que desarrollen funciones en la UAESP, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal de la UAESP es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

9.3.4 Políticas

9.3.4.1 Seguridad en la definición de puestos de trabajo v la asignación de Recursos

- **Incorporación de la Seguridad en los Puestos de Trabajo**

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los perfiles de cargo.

Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

- **Compromiso de Confidencialidad**

Como parte de sus términos y condiciones iniciales de empleo, los funcionarios, cualquiera sea su situación, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la Entidad. La copia firmada del Compromiso deberá ser conservada de forma segura cumpliendo con lo establecido en el Proceso de Gestión Documental en la dependencia competente.

Así mismo, mediante el Compromiso de Confidencialidad el funcionario declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del funcionario.

Se desarrollará un procedimiento, instructivo o protocolo para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre:

- Suscripción inicial del Compromiso por parte de la totalidad del personal.
- Revisión del contenido del Compromiso cada año.
- Método de re-suscripción en caso de modificación del texto del Compromiso.

9.3.4.2 Capacitación del Usuario

- **Formación y Capacitación en Materia de Seguridad de la Información**

Todos los funcionarios y cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la Entidad recibirán una adecuada capacitación, socialización y actualización periódica en materia de la política, normas y procedimientos de la Entidad.

Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y de los recursos en general, como por ejemplo su estación de trabajo.

El responsable de la Subdirección Administrativa y Financiera será el encargado de coordinar las acciones de capacitación y/o socialización que surjan de la presente Política. Cada seis meses se revisará el material correspondiente a la capacitación y/o socialización, a fin de evaluar la pertinencia de su actualización, de acuerdo con el estado del arte de ese momento.

Las siguientes dependencias serán encargadas de producir el material de capacitación y/o socialización:

- Subdirección Administrativa y Financiera
- Oficina de Tecnologías de la Información y las Comunicaciones
- Oficina Asesora de Comunicaciones y Relaciones Interinstitucionales

El personal que ingrese a la Unidad recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan. Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

9.3.4.3 Respuesta a incidentes y anomalías en materia de seguridad

- **Comunicación de Incidentes Relativos a la Seguridad**

Los incidentes relativos a la seguridad serán comunicados a través de canales dispuestos y apropiados tan pronto como sea posible.

Se establecerá un instrumento de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes. Dicho documento deberá contemplar que, ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad Informática sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo.

Asimismo, mantendrá al Comité de Seguridad de la Información al tanto de la ocurrencia de incidentes de seguridad, para lo cual todos los funcionarios y contratistas conocerán el documento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

- **Comunicación de Debilidades en Materia de Seguridad**

Los usuarios de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática. Se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

- **Comunicación de Anomalías del Software**

Se establecerán procedimientos, instructivos o protocolos para la comunicación de anomalías de software, los cuales deberán contemplar:

- Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
- Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
- Alertar inmediatamente al Responsable de Seguridad Informática o del Activo de que se trate.

Se prohíbe a los usuarios quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. La recuperación será realizada por personal experimentado, adecuadamente habilitado.

- **Aprendiendo de los Incidentes**

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

- **Procesos disciplinarios**

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias y convencionales que rigen al personal de la Administración Pública Nacional, para los empleados que violen la Política, Normas y Procedimientos de Seguridad de la Entidad.

9.4 SEGURIDAD FÍSICA Y AMBIENTAL

Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información de la Unidad.

9.4.1 Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones de la Entidad. Pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen los siguientes conceptos para tener en cuenta; la protección física de accesos, la protección ambiental, el transporte, protección y mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible de la Entidad, de accesos físicos no autorizados. El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones de la Entidad como en instalaciones próximas a la sede de este que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas la UAESP. Estas actividades deben ser ejecutadas bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así, se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente a la UAESP, pero situado físicamente fuera del mismo, así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información a la UAESP.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser

recuperadas mientras no están siendo utilizados. Es por lo que el transporte y la disposición final presentan riesgos que deben ser evaluados.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación.

9.4.2 Objetivo

- Prevenir e impedir accesos no autorizados, daños e interferencia a instalaciones e información de la UAESP.

- Proteger el equipamiento de procesamiento de información crítica de la UAESP, ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Así mismo, contemplar la protección en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

- Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información la UAESP.

- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

- Proporcionar protección proporcional a los riesgos identificados.

9.4.3 Responsabilidad

El Responsable de Seguridad Informática definirá junto con el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente numeral.

El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones asistirá al Responsable de Seguridad Informática en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación; a su vez controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones la Entidad.

Los Responsables de Oficinas y Subdirecciones definirán los niveles de acceso físico del personal la UAESP a las a las áreas restringidas bajo su responsabilidad.

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su interés a los funcionarios, cuando lo crean conveniente.

La Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información revisará los registros de acceso a las áreas protegidas.

Todo el personal la UAESP es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

9.4.4 Política

9.4.4.1 Perímetro De Seguridad Física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las instalaciones de procesamiento de información. La UAESP utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidos por el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones con el asesoramiento del Responsable de Seguridad Informática, de acuerdo a la evaluación de riesgos efectuada.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

a) Definir y documentar claramente el perímetro de seguridad.
b) Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, alarmas, cerraduras, entre otros.
c) Verificar la existencia de un área de recepción atendida por personal. El acceso a dicha área estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.
d) Extender las barreras físicas necesarias desde el piso hasta el techo, a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, por incendio, humedad e inundación.
e) Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

El Responsable de Seguridad Informática llevará un registro actualizado de los sitios protegidos, indicando:

- Identificación del Edificio y Área.
- Principales elementos que proteger.
- Medidas de protección física.

9.4.4.2 Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad Informática junto con el jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se mantendrá un registro protegido para permitir auditar todos los accesos.
c) Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.
d) Revisar y actualizar cada 6 meses los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Jefe de Oficina y Subdirecciones de la que dependa.
e) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Oficina de control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

9.4.4.3 Protección de oficinas, recintos e instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegidas de la Entidad:

AREAS PROTEGIDAS

- Datacenter
- Encerramiento de planta eléctrica y UPS
- Racks de comunicaciones

Se establecen las siguientes medidas de protección para áreas protegidas:

a) Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.

b) Establecer que los sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
c) Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.
d) Separar las instalaciones de procesamiento de información administradas por la Entidad de aquellas administradas por terceros.
e) Almacenar los materiales peligrosos o combustibles en lugares seguros a una distancia prudencial de las áreas protegidas de la Entidad.
f) Almacenar los equipos redundantes y la información de resguardo (backup) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

9.4.4.4 Desarrollo de tareas en áreas protegidas

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
b) Evitar la ejecución de trabajos por parte de terceros sin supervisión.
c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.
d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.
e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
f) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicha área o el Responsable de la Oficina de Tecnologías de la Información y las Comunicaciones y el Responsable de Seguridad Informática.
g) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

9.4.4.5 Aislamiento de las áreas de recepción y distribución

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:

a) Limitar el acceso a las áreas de almacén, desde el exterior de la sede la Entidad, sólo al personal previamente identificado y autorizado.
b) Diseñar el área de almacén de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.
c) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.
d) Registrar el material entrante al ingresar al sitio pertinente.

9.4.4.6 Ubicación y protección del equipamiento y copias de seguridad

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
d) Adoptar controles adecuados para minimizar el riesgo de amenazas como: amenazas potenciales, Robo o hurto, incendio, explosivos, humo, inundaciones, filtraciones de agua o falta de suministro, polvo, vibraciones, efectos químicos. Interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión). Radiación electromagnética.
e) Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento la información. Esta revisión se realizará cada seis meses.
f) Considerar así mismo el impacto de las amenazas citadas en el punto (d) que tengan lugar en zonas próximas a la sede principal.
g) Respaldo externo del 100% de la información sistemas y datos.

9.4.4.7 Suministros de energía

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de

control:

a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
b) Contar con un suministro de energía ininterrumpido (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la UAESP. La determinación de dichas operaciones críticas será el resultado del análisis de impacto realizado por el Responsable de Seguridad Informática conjuntamente con los Propietarios de la Información. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
c) Montar una planta eléctrica de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa. Dicho análisis será realizado por el Responsable de Seguridad Informática juntamente con los Propietarios de la Información. Se dispondrá de un adecuado suministro de combustible para garantizar que la planta eléctrica pueda funcionar por un período prolongado. Cuando el encendido de la planta eléctrica no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. La planta eléctrica será inspeccionada y probada periódicamente para asegurar que funcione según lo previsto.
d) Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo con las normativas vigentes.

9.4.4.8 Seguridad del cableado

El cableado estructurado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, mediante las siguientes acciones:

a) Cumplir con los requisitos técnicos vigentes dictados por las normas ICONTEC.
b) Utilizar piso ducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información.
c) Proteger el cableado de red contra intercepción no autorizada o daño mediante los siguientes controles: (el uso de conductos o evitando trayectos que atraviesen áreas públicas).
d) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.
e) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.

Para el cumplimiento de las especificaciones técnicas de ensamble y montaje se deben tener en cuenta las siguientes normas existentes en la industria, con las cuales se garantiza un nivel óptimo de seguridad, confiabilidad y eficiencia de las redes:

Redes Eléctricas

a) ICONTEC 2050, Código Eléctrico Colombiano.

b) NEC Aplicables Código Eléctrico Nacional EEUU 2017.

c) RETIE - Reglamento Técnico De Instalaciones Eléctricas.

Red de Comunicaciones

a) EIA/TIA 568A: Estándar de Cableado para Telecomunicaciones de Edificios Comerciales.

b) EIA/TIA 568B: Estándar de Cableado. Este estándar especifica los requisitos de componentes y de transmisión según los medios.

c) EIA/TIA 568B.1: Sistema de cableado de telecomunicaciones genérico para edificios comerciales que soporta un entorno de varios productos y proveedores.

d) EIA/TIA 568B.1.1: enmienda que se aplica al radio de curvatura de los cables de conexión UTP, unshielded twisted-pair y ScTP, screened twisted-pair)

e) EIA/TIA 568B.2: Estándar que especifica los componentes de cableado, de transmisión, los modelos de sistemas y los procedimientos de medición necesarios para la verificación del cableado de par trenzado.

f) EIA/TIA 568B.3: Estándar para los componentes y requisitos de transmisión para un sistema de cableado de fibra óptica.

g) EIA/TIA 569C: Estándares que rigen los espacios y ductos para el cableado.

h) EIA/TIA 542: Criterios y consideraciones en relación al diseño y construcción de data center y/o centros de cableado de telecomunicaciones a continuación se relaciona los artículos aplicables a este tipo de instalaciones

i) EIA/TIA 606A: Estándares que rigen la Administración (etiquetado).

j) EIA/TIA 607: Estándares que rigen el aterrizamiento y el anclaje para el cableado.

k) NFPA 101: Código de seguridad Humana

9.4.4.9 Mantenimiento de equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del jefe de la Oficina. La Oficina de TIC mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
d) Registrar el retiro de equipamiento de la sede correspondiente de la UAESP para su mantenimiento.
e) Eliminar la información confidencial que contenga cualquier equipo que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

9.4.4.10 Seguridad de los equipos fuera de las instalaciones.

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la UAESP, será autorizado por el responsable de este. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de esta. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la UAESP para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito la UAESP, cuando sea conveniente.

9.4.4.11 Desafectación o reutilización segura de los equipos.

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo, discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

9.4.4.12 Políticas de escritorios y pantallas limpias.

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, durante el horario normal de trabajo

como fuera del mismo.

Se aplicarán los siguientes lineamientos:

a) El bloqueo estándar debe activarse máximo con una espera de cinco minutos de inactividad en los equipos de cómputo. Además, es necesario cerrar aplicaciones y bloquear la pantalla cuando se aleje de su escritorio. (Cerrar sesión de inicio de Windows y bloquear el equipo con comandos como Control + Alt + Supr, o la tecla de Windows +L).
b) Los usuarios de los sistemas de información y comunicaciones de la UAESP deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.
c) Se realizará un borrado automático de iconos inactivos en la pantalla ya que la información debe ser almacenada por los usuarios solo en la carpeta “Mis Documentos” para salvaguardar la información.
d) Se establecerá un fondo de pantalla institucional aleatorio que será elegido por la Oficina Asesora de Comunicaciones y no podrá ser modificado por los usuarios de la Entidad.
e) Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
f) Guardar bajo llave la información sensible o crítica de la UAESP (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
g) Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.
h) Retirar inmediatamente la información sensible o confidencial, una vez impresa.

9.4.4.13 Retiro de los bienes

El equipamiento, la información y el software no serán retirados de cualquiera de las sedes la UAESP sin autorización formal.

9.5 GESTIÓN DE LAS COMUNICACIONES Y LAS OPERACIONES

Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

9.5.1 Generalidades

La proliferación de software malicioso, como virus, troyanos, entre otros., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

Es conveniente separar los ambientes de desarrollo, prueba y operaciones de otros sistemas de información de la UAESP, estableciendo procedimientos que aseguren la calidad de las actividades que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Los sistemas de información de la Entidad están comunicados entre sí, como con terceros fuera de ella. Por lo tanto, es necesario implementar criterios de seguridad en las comunicaciones que se establezcan. Las comunicaciones establecidas permiten el intercambio de información, que debe estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

9.5.2 Objetivo

- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

- Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes.

9.5.3 Responsabilidad

El Responsable de Seguridad Informática tendrá a su cargo, entre otros:

- Definir en documentos el control de cambios a las actividades operativas documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.

- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos documentos de aprobación de software incluyan aspectos de seguridad para las aplicaciones de Gobierno Electrónico.

- Definir en documentos el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.

- Definir y documentar una norma clara con respecto al uso del correo electrónico.

- Controlar los mecanismos de distribución y difusión de información dentro de la Unidad.

- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes de la Unidad.

- Desarrollar documentos adecuados de concientización de usuarios en materia de Seguridad, controles de acceso al sistema y administración de cambios.

- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones tendrá a su cargo lo siguiente:

- Controlar la existencia de documentación actualizada relacionada con las comunicaciones y operaciones.

- Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.

- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.

- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.

- Controlar la realización de las copias de respaldo de información, así como la prueba periódica de su restauración.

- Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.

- Desarrollar y verificar el cumplimiento de documentos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

- Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).

- Definir e implementar documentos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.

- Participar en el tratamiento de los incidentes de seguridad, de acuerdo con los documentos establecidos.

El Responsable de Seguridad Informática junto con el jefe de la Oficina de Tecnologías de la Información y las Comunicaciones y el Responsable de la Subdirección de Asuntos Legales, evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

9.5.4 Políticas

9.5.4.1 Documentación y Responsabilidades Operativas

9.5.4.1.1 Documentación Operativa

Se evidenciarán y mantendrán actualizados los documentos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad Informática.

Los documentos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

a) Procesamiento y manejo de la información.
b) Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
c) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
d) Restricciones en el uso de utilitarios del sistema.
e) Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
f) Instrucciones especiales para el manejo de “salidas”, como el uso de papelería especial o la administración de salidas confidenciales, incluyendo documentos para la eliminación segura de salidas fallidas de tareas.
g) Reinicio del sistema y documentos de recuperación en caso de producirse fallas en el sistema.

Se preparará adicionalmente documentación de las siguientes actividades:

a) Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
b) Instalación y mantenimiento de las plataformas de procesamiento.
c) Monitoreo del procesamiento y las comunicaciones.
d) Inicio y finalización de la ejecución de los sistemas.
e) Programación y ejecución de procesos.
f) Gestión de servicios.
g) Resguardo de Información
h) Gestión de Incidentes de seguridad en el ambiente de procesamiento y comunicaciones
i) Remplazo o cambio de componentes del ambiente de procesamiento y comunicaciones
j) Uso del correo electrónico.
k) Uso de Internet

9.5.4.2 Control de Cambios en las Operaciones

Se definirán documentos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El Responsable de Seguridad Informática, controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de estos ni de la información que soportan. El Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Los documentos de control de cambios contemplarán los siguientes puntos:

a) Identificación y registro de cambios significativos.
b) Evaluación del posible impacto de dichos cambios.
c) Aprobación formal de los cambios propuestos.
d) Planificación del proceso de cambio.
e) Prueba del nuevo escenario.
f) Comunicación de detalles de cambios a todas las personas pertinentes.
g) Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de estos.

9.5.4.3 Gestión y Manejo de Incidentes

Se establecerán los documentos que se requieran conforme a los lineamientos establecidos en el Sistema Integrado de Gestión.

Se establecerán funciones, roles, responsabilidades, autoridades y documentación de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad. Se deben considerar los siguientes ítems:

a) Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo: Fallas operativas. Código malicioso. Intrusiones, Fraude informático. Error humano, catástrofes naturales.
b) Comunicar los incidentes a través de canales gerenciales apropiados tan pronto como sea posible.
c) Contemplar los siguientes puntos en los documentos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):

    - Definición de las primeras medidas a implementar.
    - Análisis e identificación de la causa del incidente.
    - Planificación e implementación de soluciones para evitar la repetición de este, si fuera necesario.
    - Comunicación con las personas afectadas o involucradas con la recuperación, del incidente.
    - Notificación de la acción a la autoridad pertinente.

d) Registrar pistas de auditoría y evidencia similar para:

- Análisis de problemas internos.
- Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial.

e) Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:

- Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
- Documentación de todas las acciones de emergencia emprendidas en forma detallada.
- Comunicación de las acciones de emergencia al titular de la Oficina y/o Subdirección y revisión de su cumplimiento.
- Constatación de la integridad de los controles y sistemas de la UAESP en un plazo mínimo.

9.5.4.4 Separación entre Instalaciones de Desarrollo e Instalaciones Operativas

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán 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:

a) Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios.
b) Separar las actividades de desarrollo y prueba, en entornos diferentes.
c) Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.
d) 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.
e) Definir propietarios de la información para cada uno de los ambientes de procesamientos existentes.
f) 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.

9.5.4.5 Gestión de Instalaciones Externas

En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio y se incluirán en el contrato,

contemplando las siguientes cuestiones específicas:

a) Identificar las aplicaciones sensibles o críticas que convenga retener en la Entidad.
b) Obtener la aprobación de los propietarios de aplicaciones específicas.
c) Identificar las implicaciones para la continuidad de operaciones de la Entidad.
d) Definir las funciones y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

Dichas consideraciones deberán ser acordadas entre el Responsable de Seguridad Informática, el jefe de la Oficina de TIC y el Subdirector de Asuntos Legales.

9.5.4.6 Planificación y Aprobación de Sistemas

9.5.4.6.1 Planificación de la Capacidad

El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones o el personal que éste 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 adecuados. 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.

Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad de operaciones y del procesamiento, y puedan planificar una adecuada acción correctiva.

9.5.4.6.2 Aprobación del Sistema

El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones y el Responsable de Seguridad Informática sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Se deben considerar los siguientes puntos:

a) Verificar el impacto en el desempeño y los requerimientos de capacidad de los computadores.
b) Garantizar la recuperación ante errores.
c) Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.
d) Garantizar la implementación de un conjunto acordado de controles de seguridad
e) Desarrollar disposiciones relativas a la continuidad de operaciones de la UAESP.
f) Asegurar que la instalación del nuevo sistema no afectará negativamente los

sistemas existentes, especialmente en los períodos pico de procesamiento.
g) Considerar el efecto que tiene el nuevo sistema en la seguridad global.
h) Disponer la realización de entrenamiento en la operación y/o uso de nuevos sistemas.

9.5.4.7 Protección Contra Software Malicioso

9.5.4.7.1 Controles Contra Software Malicioso

El Responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. El Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, o el personal designado por éste, implementarán dichos controles.

El Responsable de Seguridad Informática desarrollará documentos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

a) Prohibir el uso de software no autorizado por la Unidad
b) Redactar documentos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadores y medios informáticos, como medida de precaución y rutinaria.
d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Entidad, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
f) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
g) Concienciar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a los mismos.

9.5.4.8 Mantenimiento

9.5.4.8.1 Backup y Resguardo de la Información

El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones y el Responsable de Seguridad Informática determinarán los requerimientos para resguardar cada software o datos en función de su criticidad. Con base a esto, se

definirá y documentará un esquema de resguardo y respaldo de la información.

El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración de acuerdo a las políticas en los aplicativos utilizados. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico de la Unidad. Los sistemas de resguardo deberán probarse periódicamente asegurándose que cumplen con los requerimientos de los planes de continuidad de operaciones de la UAESP.

Se definirán documentos para el respaldo y resguardo de la información, que deberán considerar los siguientes puntos:

a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.

b) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.
c) Almacenar en una ubicación remota (ya sea física o virtual) copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los documentos de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para la Entidad. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad y requisitos legales a los que se encuentre sujeta.
d) Será posible almacenar los diferentes Backups en línea (en la nube) por medio de un tercero, que mantendrá disponible la información para su descarga inmediata después de ocurrido algún incidente que no permita el acceso a los almacenamientos físicos.
e) Asignar a la información de resguardo (Backups) un nivel de protección física y ambiental según las normas. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
f) Probar periódicamente los medios de resguardo de acuerdo a las políticas de los aplicativos utilizados en la Entidad.
g) Verificar y probar periódicamente los documentos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

9.5.4.8.2 Registro de Actividades del Personal Operativo

El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

a) Errores del sistema y medidas correctivas tomadas.
b) Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas
c) Ejecución de operaciones críticas
d) Cambios a información crítica

9.5.4.8.3 Registro de Fallas

El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones desarrollará y verificará el cumplimiento de documentos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

Se registrarán las fallas comunicadas, debiendo existir reglas claras para el manejo de las mismas, con inclusión de:

a) Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
b) Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.
c) Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

9.5.4.8.4 Sincronización de Reloj

El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones debe garantizar que la infraestructura de procesamiento de información y los sistemas de comunicaciones estén sincronizados con la hora legal Colombiana.

9.5.4.9 Administración de la Red

El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Unidad, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Establecer los documentos para la administración de los equipos servidores, incluyendo los equipos en las áreas usuarias.
b) 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.
c) Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.
d) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones implementará dichos controles.

9.5.4.10 Administración y Seguridad de los Medios de Almacenamiento

9.5.4.10.1 Administración de Medios Informáticos Removibles

El responsable de la Oficina de Tecnologías de la Información y las Comunicaciones, con la asistencia del Responsable de Seguridad Informática, implementará documentos para la administración de medios informáticos removibles (USB, discos externos, cintas entre otros).

Se deberán considerar las siguientes acciones para la implementación de los documentos:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio re-utilizable que ha de ser retirado o reutilizado por la Entidad.
b) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

9.5.4.10.2 Eliminación de Medios de Información

El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, junto con el Responsable de Seguridad Informática definirán documentos para la eliminación segura de los medios de información.

Los documentos deberán considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

a) Documentos en papel.
b) Cintas magnéticas.
c) Memorias USB, Discos externos y fijos.
d) Medios de almacenamiento óptico (Todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor)
e) Datos de prueba.
f) Documentación del sistema.

9.5.4.10.3 Manejo de Información

Se definirán documentos para el manejo y almacenamiento de la información de acuerdo con la clasificación establecida en la Clasificación y Control de Activos.

En los documentos se contemplarán las siguientes acciones:

a) Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, comunicaciones de voz en general, multimedia y cualquier otro ítem potencialmente sensible.
b) Restringir el acceso solo al personal debidamente autorizado.
c) Mantener un registro formal de los receptores autorizados de datos.
d) Garantizar que los datos de entrada son completos, que el procesamiento se

lleva a cabo correctamente y que se validan las salidas.
e) Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores

9.5.4.10.4 Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se considerarán los siguientes puntos para su protección:

a) Almacenar la documentación del sistema en forma segura.
b) Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

9.5.4.11 Intercambios de información y software

9.5.4.11.1 Acuerdo de Intercambio de Información y Software

Cuando se realicen acuerdos entre entidades para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de la entidad involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

a) Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
b) Documentos de notificación de emisión, transmisión, envío y recepción.
c) Normas técnicas para el empaquetado y la transmisión.
d) Pautas para la identificación del prestador del servicio intercambio.
e) Responsabilidades y obligaciones en caso de pérdida de datos.
f) Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.
g) Términos y condiciones de la licencia bajo la cual se suministra el software.
h) Información sobre la propiedad de la información suministrada y las condiciones de su uso.
i) Controles especiales que puedan requerirse para proteger ítems sensibles, (claves o información encriptada, entre otras).

La Entidad asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. La Entidad propenderá por el uso de tecnologías informáticas y de telecomunicaciones seguras para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de la misma en medio físico o lógico.

10 En los contratos que se suscriban con terceras partes, el Grupo de Contratación debe incluir los Acuerdos de Confidencialidad o Acuerdos de intercambio, dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de beneficiarios de la Entidad que les ha sido entregada en razón del cumplimiento de los objetivos.

11 La Dirección de Tecnología debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de la misma, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de brindar protección contra divulgación o modificaciones no autorizadas.

12 La Dirección de Tecnología debe autorizar el establecimiento del vínculo de transmisión de información con terceras partes, para que posteriormente las áreas funcionales realicen las actividades de transmisión requeridas en cada caso.

13 Los propietarios de los activos de información deben velar porque la información de la Entidad o de sus beneficiarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las cláusulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

Se deben definir protocolos de seguridad, cifrado de información y/o algún otro tipo de procedimiento tecnológico, con el fin de crear confidencialidad, integridad y disponibilidad de la información suministrada.

9.5.4.11.2 Seguridad del Gobierno Electrónico

El Responsable de Seguridad Informática verificará que los documentos de aprobación de Software recibido (Aprobación del Sistema) incluyan los siguientes aspectos para las aplicaciones de Gobierno Electrónico:

a) **Autenticación:** Nivel de confianza recíproca suficiente sobre la identidad del usuario y la entidad.
b) **Autorización:** Niveles de Autorización adecuados para establecer disposiciones y emitir datos y/o documentos clave, entre otros. Forma de comunicarlo al otro participante de la transacción electrónica.
c) **Procesos de oferta y contratación pública;** Requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos.
d) **Trámites en línea:** Confidencialidad, integridad y no repudio de los datos suministrados con respecto a trámites y presentaciones ante el Estado y confirmación de recepción.
e) **Verificación:** Grado de verificación apropiado para constatar la información suministrada por los usuarios.
f) **Cierre de la transacción:** Forma de interacción más adecuada para evitar

fraudes.

g) **Protección a la duplicación:** Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.
h) **No repudio:** Manera de evitar que una entidad que haya enviado o recibido información alegue que no la envió o recibió.
i) **Responsabilidad:** Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.

9.5.4.11.3 Seguridad del Correo Electrónico

Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

a) La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.
b) La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
c) Las posibles vulnerabilidades a errores, por ejemplo, digitación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.
d) La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad del equipo receptor o de la red a la que se encuentra conectada.
e) El impacto de un cambio en el medio de comunicación en los procesos de la Unidad.
f) Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
g) El acceso de usuarios remotos a las cuentas de correo electrónico.
h) El uso inadecuado por parte del personal.

Política de Correo Electrónico

El Responsable de Seguridad Informática junto con el jefe de la Oficina de Tecnologías de la Información y las Comunicaciones definirán y documentarán aspectos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

a) Protección contra ataques al correo electrónico, por ejemplo, virus, interceptación, entre otros.
b) Protección de archivos adjuntos de correo electrónico.
c) Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de
prueba jurídica.
d) Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
e) Aspectos operativos para garantizar el correcto funcionamiento del servicio

(Ejemplo: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, entre otros.).

f) Definición de los alcances del uso del correo electrónico por parte del personal de la Unidad.

g) Potestad de la Entidad, para auditar los mensajes recibidos o emitidos por los servidores de la entidad, lo cual se incluirá en el "Compromiso o Acuerdo de Confidencialidad".

Estos dos últimos puntos deben ser tenidos en cuenta bajo las normas vigentes que no sólo prohíben a los empleados a hacer uso indebido o con fines particulares del patrimonio estatal, sino que también imponen la obligación de usar los bienes y recursos del estado con los fines autorizados y de manera racional, evitando su abuso, derroche o desaprovechamiento.

Entender el correo electrónico como una herramienta más de trabajo que se entrega al funcionario con el fin de ser utilizada conforme al uso al cual está destinada, y que faculta a la UAESP a implementar sistemas de control destinados a velar por la protección y el buen uso de sus recursos.

Adicionalmente deben tenerse en cuenta las siguientes normas para el buen uso del correo electrónico:

- 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 bloqueen el servicio de correo electrónico de la UAESP.
- Cuando un empleado requiera el uso de correo electrónico debe solicitarlo formalmente mediante un requerimiento de solicitud de acceso debidamente diligenciado y autorizado por el jefe inmediato del usuario, especificando las necesidades del uso de este servicio.
- Cualquier usuario que haga uso de la infraestructura de correo electrónico implícitamente autoriza a la Unidad a evaluar en cualquier momento el contenido de la información que intercambie.
- Ningún usuario 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.
- Salvo con aprobación previa, ningún empleado puede usar cuentas gratuitas de correo electrónico en Internet para el envío de mensajes corporativos de la entidad. Todos los mensajes de carácter corporativo deberán ser enviados a través del sistema de correo electrónico corporativo y designado.
- Salvo que exista una autorización, ningún empleado está autorizado para interceptar, revelar o contribuir en la intercepción de mensajes de correo electrónico a través de herramientas de escaneo.
- El SPAM o correo "basura" es una modalidad de envío indiscriminado de mensajes de correo electrónico no solicitados y que por lo general es masivo. Los usuarios del servicio del correo electrónico de la UAESP no deben contestar mensajes SPAM, ya que al hacerlo confirmarán su dirección de correo y si le llegan mensajes de un mismo remitente se debe notificar a la Oficina de TIC - Responsable de Seguridad Informática.

- Ningún usuario del servicio de correo electrónico debe prestar atención a mensajes con falsos contenidos de virus (Hoaxes), ofertas de premios, dinero, solicitudes de ayuda caritativa, venta de bienes (hardware o software) o financiamiento a muy bajo costo, productos medicinales, acceso gratuito a portales, advertencia de virus de fuentes desconocidas, entre otros.
- Para todos los funcionarios o usuarios del servicio de correo electrónico, está prohibido brindar servicios que, de manera directa o indirecta, faciliten la proliferación de spam, en esto se incluye casillas de correo, software para realizar spam, hosting de sitios de Web para realizar SPAM o que realicen SPAM, o bien que realicen Hoaxes o bromas de mal gusto y/o fraudes, éstos últimos definidos como un correo electrónico que atrae el interés del usuario y que esconde una maniobra deshonesta. Brindar servicios que, de manera directa o indirecta, faciliten la proliferación de Software malicioso o Malware, Software espía o Spyware o Phishing.
- El servicio de correo electrónico de la UAESP debe usarse única y exclusivamente para actividades relacionadas directamente con la funciones propias de la entidad y está restringido únicamente para el uso de las personas que determine la entidad.

Declaración de rectificación

A cada correo saliente de e-mail por Internet se le debe asociar un “aviso” como se detalla a continuación:

“La Unidad Administrativa Especial de Servicios Públicos, no garantiza de alguna forma, expresada o implícita, por el servicio de e-mail que se suministra. La Entidad no es responsable por cualquier daño sufrido mientras los mensajes estén en su sistema. Estos daños incluyen pérdida de datos como un resultado de demoras, no entregas, malas entregas, o interrupciones de servicio causadas por el sistema o errores de usuario u omisiones. La utilización de cualquier información obtenida vía e-mail de Internet es bajo su propio riesgo. La UAESP, específicamente niega cualquier responsabilidad por la veracidad de la información obtenida a través de estos servicios.”

La Unidad Administrativa Especial de Servicios Públicos, anexará la siguiente declaración a cada e-mail entregado por alguno de sus funcionarios: “Los puntos de vista expresados aquí son de mí propiedad y no Constituyen pronunciamientos oficiales u opiniones de la Unidad Administrativa Especial de Servicios Públicos”.

9.5.4.11.4 Seguridad para el uso de elementos, servicios de Red y Comunicaciones

Las redes de comunicación de datos proveen múltiples puntos de entrada al ambiente de cómputo de la Unidad Administrativa Especial de Servicios Públicos, y a la información almacenada directa y periféricamente en este ambiente. En consecuencia, las comunicaciones entre equipos de cómputo y usuarios son crítica para la operación de la UAESP, también incrementa las amenazas de conexiones no autorizadas para acceder los datos e información de la entidad.

Acceso de red

- El acceso a las redes de comunicaciones por parte de los usuarios debe ser controlado.
- Está totalmente prohibido que personas ajenas a la entidad utilicen los computadores y/o terminales de la entidad, si no es autorizado por el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones.

Caminos de acceso no estándar

- Para proteger el ambiente de cómputo, de accesos por caminos no estándar, los accesos (conexión directa y telefónica) al ambiente, deben de estar de acuerdo con las conexiones autorizadas, aprobadas y establecidas.
- Todos los caminos de acceso deben ser planeados, diseñados e instalados para no evadir la seguridad.
- Ningún empleado o asociado instalará, hará operable u otra cosa que permita un camino de acceso el cual no ha sido aprobado por los responsables de seguridad.
- No se permitirán puertas traseras las cuales pretendan evitar los métodos y seguridad de acceso aprobados.

Monitoreo de red

- Las herramientas de monitoreo, equipos, hardware y software, tales como analizadores de protocolo y sniffers, pueden ser únicamente utilizados por empleados específicos para realizar actividades autorizadas. Se requiere autorización especifica escrita de los responsables de seguridad para utilizar este tipo de facilidades y herramientas de diagnóstico.

Conexión a redes externas

- La conexión a redes externas tales como Internet y proveedores de servicios de información deberán ser controlada para prevenir el que se revele sin autorización alguna información, el ingreso de código malévolo y otros eventos que afecten el servicio.

Comunicaciones electrónicas

Las comunicaciones electrónicas son necesarias para desarrollar el portafolio de servicios de la Unidad Administrativa Especial de Servicios Públicos y se reconoce que incrementan la productividad. Los funcionarios de la Entidad son responsables de su uso en el ambiente de cómputo y deben cumplir con las políticas aquí definidas.

- Todas las comunicaciones electrónicas procesadas por el ambiente de cómputo de la Unidad Administrativa Especial de Servicios Públicos, incluyendo copias de respaldo, son consideradas de propiedad de la UAESP, y no son propiedad de los usuarios del sistema de cómputo.
- La capacidad de comunicación electrónica del ambiente de cómputo de la Unidad Administrativa Especial de Servicios Públicos debe ser únicamente

utilizado para funciones autorizadas por la entidad. El uso personal en forma incidental y responsable es permitido siempre que no sea excesivo y que no interfiera con la productividad o las actividades a cargo de la entidad.

- Todas las transmisiones o recepciones de correo electrónico están sujetas a monitoreo por servidores autorizados de la UAESP.
- Los servidores de la UAESP no deben esperar privacidad relativa al envío o recepción de comunicaciones electrónicas. Todas las transmisiones podrán ser monitoreadas y revisadas por servidores autorizados en algún momento sin notificación. Sin embargo, la UAESP no monitoreará regularmente el contenido de las comunicaciones electrónicas a menos que alguna razón legítima de negocio haga requerir tal monitoreo.
- Los servidores de la UAESP no deben transmitir vía comunicación electrónica información restringida o confidencial de la Entidad, a menos que tal información sea encriptada.
- Es prohibido enviar cadenas electrónicas de cartas.
- Es prohibido enviar mensajes ofensivos o acosadores.
- Es prohibido enviar mensajes anónimos.
- Es prohibido realizar solicitudes impropias.

Conexiones a Internet

La Unidad Administrativa Especial de Servicios Públicos provee servicios de Internet a sus funcionarios para acceder a información, comunicar, recuperar o divulgar información relacionada con la Entidad.

Las conexiones a Internet deben seguir los requerimientos que a continuación se describen:

- Todos los accesos a Internet deben ser vía un dispositivo de comunicación aprobado o administrado por el área tecnológica.
- Los Ingenieros autorizados de la Oficina de TIC son los responsables de revisar regularmente todos los logs y archivos de auditoría de la actividad en línea de los usuarios de Internet, para asegurar que los servicios están siendo utilizados para beneficio de la UAESP.
- Todos los servicios de Internet deben ser configurados para evitar que servicios no deseados estén siendo habilitados o reenrutados.
- Es responsabilidad de la Oficina de TIC en título de su comité técnico evaluar e implementar las nuevas herramientas tanto de software como de hardware para que esta conexión sea lo más eficaz y eficientemente posible.

Carga y descarga de archivos

- La transferencia de información entre dos computadores de la UAESP o entre un computador de la Entidad, y otro que no lo es, está autorizado únicamente para propósitos legítimos del portafolio de servicios.
- Está prohibido cargar o descargar información a/desde computadores externos a menos que sea específicamente autorizado como parte de las funciones propias del trabajo.

- Los usuarios deben realizar una evaluación para virus de los archivos descargados.
- Todos los archivos descargados en las estaciones de trabajo deberán ser examinados a través de los anti-virus establecidos y autorizados en la red inmediatamente a los procesos de descargue.
- Los usuarios deben cumplir los requerimientos de licencia y las restricciones de copia asociadas con cualquier archivo descargado.
- Únicamente los archivos (ejecutables) absolutamente necesarios para las funciones de la UAESP, deben ser cargados por el personal técnico de la Oficina de TIC, buscando con esto conservar el espacio de almacenamiento, el desempeño de la red y evitar posibles virus en el ejecutable.

Estándares

- Los últimos service-pack deberán ser instalados una vez se haya hecho oficial su lanzamiento con sus respectivas pruebas.
- El protocolo de comunicación interno y externo debe ser TCP/IP
- Los nombres de las comunidades SNMP en los servidores no deben ser público (public), privado (private) o sistema (system). Se deben asignar nombres que lo relacionen con la función que ese servidor desempeñe.
- La auditoría debe ser habilitada en los servidores más sensibles para la Entidad.
- Las cuentas con ID supervisor, administrator o similares deben ser eliminadas de todos los servidores, se deben crear estas mismas cuentas sin privilegios y auditar su intento de uso no autorizado.
- Se debe crear un grupo administradores donde se le atribuirán permisos de admin para las tareas de soporte en la red.
- El uso de las cuentas de administrador o admin deberán ser conocidas por dos o tres personas y su password debe ser cambiado cada 30 días.
- El username y el password deben ser diferentes y sin nada que los relacione.
- Las cuentas de usuario son de uso personal y su contraseña debe ser secreta y no compartida.
- Se deben definir los usuarios con permisos de backup y restore por la persona encargada del centro de cómputo y/o servicios de Red.
- Los permisos sobre las carpetas compartidas serán definidos según las aplicaciones o responsabilidades que el usuario maneje y/o administre.
- El password debe tener un mínimo de ocho (8) caracteres obligatorios y no repetitivos.
- Todo usuario que se retira de la Entidad deber ser borrado del sistema y deben otorgarse a su reemplazo los permisos pertinentes para el acceso a las carpetas que antes esa persona tenía.
- A los usuarios en período de vacaciones se les debe suspender su cuenta en la red, por un período equivalente a dicho tiempo.
- Se deben bloquear las cuentas con más de cuatro intentos fallidos al ingresar al sistema.
- Se debe otorgar un tiempo para que la cuenta del usuario expire y deba cambiar su contraseña.
- Los usuarios deben restringirse a una dirección IP para aquellos trabajos donde se vea comprometida la seguridad de la información.

- Cada vez que sea anunciada la actualización del antivirus, inmediatamente debe ser actualizado en los servidores y estaciones de trabajo.
- El antivirus debe estar programado para ejecutarse y actualizarse automáticamente con las opciones de “sean and cure”.
- Todo el software utilizado en la Unidad Administrativa Especial de Servicios Públicos debe tener su respectiva licencia de uso sea copyright o copyleft.
- Todo el software comprado o desarrollado debe ser contabilizado a través de un sistema de inventario.

Gestión de Elementos de Red

- Los elementos y servicios de red no deben permitir que cuentas de usuario que presenten contraseñas en blanco o nulas, obtengan acceso remoto a cualquier computador, sistema o servicio de la red interna de la UAESP.
- Todas las cuentas de usuario de los elementos y servicios de red otorgados a los funcionarios de la UAESP o terceros constituyen un activo de la institución que permite identificar de manera única e irrepetible a cada usuario. En ninguna circunstancia las cuentas de usuario deberán ser compartidas o reasignadas y su contraseña revelada.
- Los administradores de los elementos y servicios de red deben definir actividades de control que permitan detectar, analizar y notificar brechas de seguridad. En algunos casos se requiere implementar logs de registro de los incidentes presentados, para detectar oportunamente intentos de violación a los sistemas de información.
- Salvo expresa autorización, ningún usuario está autorizado para escanear, acceder o manipular directa o indirectamente los sistemas de información y de comunicaciones de la red de datos de la UAESP, e instalar nuevos sistemas de comunicaciones de redes que se conecten con la red de datos de la institución.
- Realizar pruebas periódicas de identificación de vulnerabilidades y test de penetración a través de personas técnicamente preparadas (área de Sistemas o contratistas). Los responsables de la administración y/o del manejo de los sistemas de comunicaciones correspondientes no deben realizar estas pruebas.
- Definir, preparar y probar los planes de contingencias que permitan restablecer los servicios de red y la infraestructura que los soporta en el menor tiempo posible en caso de presentarse fallas o incidentes de seguridad que interrumpan las operaciones. Antes de implementar cualquier plan de contingencia las áreas responsables de la gestión de redes deben solicitar la autorización a la Oficina de Tecnologías de la Información y las Comunicaciones-TIC de la UAESP.
- Los Switches, Routers y Firewalls que se involucren en las conexiones de redes de UAESP, deberán estar convenientemente asegurados de acuerdo con un estándar mínimo de configuración de seguridad.

9.6 CONTROL DE ACCESO

Orientado a controlar el acceso lógico a la información.

9.6.1 Generalidades

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concienciar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad de los equipos de cómputo y dispositivos activos de la infraestructura tecnológica de la UAESP.

9.6.2 Objetivo

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de la UAESP y otras redes públicas o privadas.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
- Concienciar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

9.6.3 Responsabilidad

El Responsable de Seguridad Informática estará a cargo de:

- Definir documentación para la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas y la revisión de registros de actividades.
- Definir pautas de utilización de Internet para todos los usuarios.
- Participar en la definición de documentos de seguridad a implementar en el

ambiente informático (Ejemplo: sistemas operativos, servicios de red, enrutadores o gateways, Firewalls, entre otros.) y validarlos periódicamente.
- Controlar la asignación de privilegios a usuarios.
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registro de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, registro de eventos, protección de puertos, segmentación de redes, control de conexiones a la red, control de ruteo de red, entre otros.
- Concienciar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de evaluar los riesgos a los cuales se expone la información con el objeto de;

- Determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
- Definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su interés y la periodicidad de revisión de los mismos.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.

Los responsables de cada Subdirección y Oficina, junto con el Responsable de Seguridad Informática, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información. Así mismo autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

El personal que apoya la gestión en la Oficina de Tecnologías de la Información y las Comunicaciones cumplirá las siguientes funciones:

- Implementar los documentos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Definir e implementar la configuración que debe efectuarse para cada servicio

de red, con el fin de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

9.6.4 Políticas

9.6.4.1 Requerimientos para el control de acceso

9.6.4.1.1 Política de Control de Accesos

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

a. Identificar los requerimientos de seguridad de cada una de las aplicaciones.
b. Identificar toda la información relacionada con las aplicaciones.
c. Establecer criterios coherentes entre la Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes.
d. Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
e. Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
f. Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

9.6.4.1.2 Reglas de Control de Acceso

Las reglas de control de acceso especificadas deberán:

a) Indicar expresamente si las reglas son obligatorias u optativas.
b) Establecer reglas sobre la premisa “Todo debe estar prohibido a menos que se permita expresamente” y no sobre la premisa inversa de “Todo está permitido a menos que se prohíba expresamente”.
c) Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario.
d) Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.
e) Controlar las reglas que requieren la aprobación del administrador o del Propietario de la Información de que se trate, antes de entrar en vigencia y aquellas que no requieren aprobación.

9.6.4.1.3 Creación y Eliminación de Usuarios (Internos y Externos)

a. Los funcionarios, contratistas, outsourcing o terceros, antes de solicitar acceso a los sistemas de información deben firmar un acuerdo de

confidencialidad.

b. Las cuentas de usuario de los sistemas informáticos otorgados a los funcionarios de la UAESP o terceros constituyen un activo de la compañía 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.

c. La asignación de los privilegios de acceso de todos los usuarios en los sistemas informáticos de la UAESP debe regirse de acuerdo con las actividades que el usuario vaya a realizar.

d. Las cuentas de usuario (internas/externas) creadas en los sistemas de información de la compañía deben tener un identificador único y deberán solicitarse mediante un requerimiento formal, especificando su identificación, nombres y apellidos, las funciones que va a desempeñar y autorizado por el jefe inmediato del usuario. Las cuentas de usuarios externos deben ser solicitadas y autorizadas a través del Director General de la Unidad Administrativa Especial de Servicios Públicos.

e. La creación de las cuentas de usuario en los sistemas de información de la Unidad Administrativa Especial de Servicios Públicos, están sujetas a la adopción de un estándar de identificadores de usuario establecido por la Oficina de TIC, salvo que existan impedimentos técnicos justificables que impidan la adopción de dicho estándar.

f. La creación de cuentas genéricas, deben contar con el aval de la Oficina de TIC. La persona responsable de su utilización es la encargada de notificar las novedades correspondientes de la cuenta.

g. En el momento en que un empleado se retire de la compañía, su jefe inmediato debe notificar su retiro al administrador de los sistemas de información y revisar con prontitud los archivos y documentos guardados en el computador, con el fin de reasignar las tareas y delegar específicamente la responsabilidad de estos archivos que anteriormente estaban en manos del ex-empleado.

h. Los terceros están obligados a reportar, cualquier novedad que se presente con sus funcionarios (vacaciones, licencias, incapacidades, etc.) a la Oficina de TIC, gestionar ante el administrador de los sistemas de información, la solicitud de retiro inmediato de accesos.

i. Cuando un empleado se retira de la UAESP o no requiere seguir utilizando los sistemas de información, el administrador de los sistemas de información debe asegurarse que el usuario no pueda ingresar modificando la contraseña actual, esto se requiere para guardar el log de transacciones que el usuario realizó.

9.6.4.1.4 Aspectos Importantes para la Gestión de cuentas con Perfil de Administración

Las cuentas de usuario con privilegios de administración y que son propias de los sistemas de información y equipos de red, deben cumplir con los documentos de administración de cuentas especiales definido por el responsable de la Seguridad Informática y el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones-TIC.

Los privilegios especiales en los sistemas de información y equipos de red deben limitarse a aquellos que están encargados directamente de la administración o seguridad de los sistemas, y sólo deben otorgarse a aquellos usuarios designados explícitamente como administradores de sistema.

Todas las Cuentas con privilegios administrativos 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 y aplicación, especificando la siguiente información:

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

Todas las cuentas de usuario relacionadas con los servicios que presentan los sistemas de información y que son propias de los mismos, no se pueden deshabilitar y eliminar, salvo expresa autorización de la Oficina de TIC y/o La Dirección General de la UAESP.

9.6.4.2 Administración de accesos de usuarios

Con el objetivo de impedir el acceso no autorizado a la información, se implementará documentación formal para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

9.6.4.2.1 Registro a Usuario

El Responsable de Seguridad Informática definirá un documento de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.

b) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad de la Entidad, por ejemplo, que no compromete la separación de tareas.
d) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
e) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
f) Mantener un registro formal de todas las personas registradas para utilizar el servicio.
g) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización o se desvincularon de la UAESP.
h) Efectuar revisiones periódicas con el objeto de:
    - Cancelar cuentas de usuario redundantes.
    - Inhabilitar cuentas inactivas por más de 60 días.
    - Eliminar cuentas inactivas por más de a 120 días.

í) En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.
j) Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

9.6.4.2.2 Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

a) 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.
b) Asignar los privilegios a funcionarios sobre la base de la necesidad de uso y evento por evento, por ejemplo, el requerimiento mínimo para su rol funcional.
c) 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.
d) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los Propietarios de Información serán los encargados de aprobar la asignación de

privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad Informática.

9.6.4.2.3 Administración de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un documento de administración formal, mediante el cual deben respetarse los siguientes pasos:

a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración puede estar incluida en el Compromiso de Confidencialidad.
b) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisionales, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
c) Generar contraseñas provisionales seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.
d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.
e) Configurar los sistemas de tal manera que:
    - Las contraseñas tengan más de 8 caracteres.
    - Suspendan o bloqueen permanentemente al usuario luego de 4 intentos de entrar con una contraseña incorrecta (deberá pedir la rehabilitación ante quien corresponda).
    - Solicitar el cambio de la contraseña cada lapso no mayor a 45 días.

9.6.4.2.4 Administración de Contraseñas Criticas

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, entre otros. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Responsable de Seguridad Informática definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

a) Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.
b) Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
c) Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Responsable de Seguridad.

9.6.4.3 Responsabilidades del usuario

9.6.4.3.1 Uso de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir los siguientes lineamientos:

a) Mantener las contraseñas en secreto.
b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
c) Seleccionar contraseñas de calidad, de acuerdo con las prescripciones informadas por el responsable del Activo de Información de que se trate, que:
    - Sean fáciles de recordar.
    - No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
    - No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
e) Cambiar las contraseñas provisionales en el primer inicio de sesión.
f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
g) Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida o indicio de pérdida de confidencialidad.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas.

9.6.4.3.2 Equipos Desatendidos en Áreas de Usuarios

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Responsable de Seguridad Informática debe coordinar con la Subdirección Administrativa y Financiera o las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la

protección de equipos desatendidos, así como de sus funciones en relación con la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
b) Proteger los PC's contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

9.6.4.4 Control de acceso a la red

9.6.4.4.1 Política de Utilización de los Servicios de red

Las conexiones no seguras a los servicios de red pueden afectar a toda la UAESP, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de los mismos.

El responsable de la Oficina de Tecnologías de la Información y las Comunicaciones tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo con el pedido formal del titular de una Oficina y/o Subdirección que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo, áreas públicas o externas que están fuera de la administración y del control de seguridad de la UAESP.

Para esto, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

a) Identificar las redes y servicios de red a los cuales se permite el acceso.
b) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
c) Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

9.6.4.4.2 Camino Forzado

Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones de la UAESP, o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones será controlado.

Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los

servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma. Para esto se debe tener en cuenta:

a. Establecer la conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos.
b. Evitar la navegación ilimitada por la red.
c. Imponer el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red.
d. Controlar activamente las comunicaciones con origen y destino autorizado a través de un Gateway utilizando Firewalls.
e. Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro o fuera de la UAESP.

9.6.4.4.3 Autenticación de Usuarios para Conexiones Externas

Las conexiones externas son un potencial peligro para accesos no autorizados a la información de la UAESP. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El Responsable de Seguridad Informática, juntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

9.6.4.4.4 Protección de los Puertos de Diagnostico Remoto

Muchos computadores y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto “Autenticación de Usuarios para Conexiones Externas”. También para este caso deberá tenerse en cuenta el punto “Camino Forzado”.

9.6.4.4.5 Segmentación de Redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados y VLANs. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de “gateways” con funcionalidades de “firewall” o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado de acuerdo con la Política de Control de Accesos.

La segmentación en dominios y VLANs de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

9.6.4.4.6 Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. El Responsable de Seguridad Informática definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el Responsable de Oficinas y Subdirecciones a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

Se evaluará la conveniencia de generar un registro del acceso de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares. Para esto, el Responsable de Seguridad Informática junto con el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones -TIC, analizarán las medidas a ser implementadas para efectivizar dicho control, como la instalación de “Firewalls”, “proxies”, entre otros.

9.6.4.4.7 Control de Conexión a la Red

Sobre la base de lo definido en el punto "Requerimientos”, se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los “gateways” que separen los diferentes dominios o VLANs de la red.

Algunos de los entornos a los que deben implementarse restricciones son:

a) Correo electrónico.
b) Transferencia de archivos.
c) Acceso interactivo.
d) Acceso a la red fuera del horario laboral.
e) Redes sociales.

9.6.4.4.8 Seguridad de los Servicios de Red

El Responsable de Seguridad Informática junto con el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones definirán las pautas para garantizar la seguridad de los servicios de red de la UAESP, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración será revisada periódicamente por el Responsable de Seguridad Informática.

9.6.4.5 Control de acceso al sistema operativo

9.6.4.5.1 Identificación Automática de Terminales

El Responsable de Seguridad Informática junto con el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones realizará una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

Si del análisis realizado surgiera la necesidad de proveer un método de identificación de terminales, se redactará un procedimiento que indique:

a) El método de identificación automática de terminales utilizado.
b) El detalle de transacciones permitidas por terminal.

9.6.4.5.2 Conexión de Terminales

El acceso a los servicios de información sólo será posible a través de las actividades de conexión segura. La documentación de conexión en un sistema informático será diseñada para minimizar la oportunidad de acceso no autorizado.

Esta documentación, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.

El documento de identificación deberá:

a. Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se haya llevado a cabo exitosamente el proceso de conexión.
b. Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder al servicio o al servidor.
c. Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
d. 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.
e. Limitar el número de intentos de conexión no exitosos permitidos
f. Registrar los intentos no exitosos.
   - Impedir otros intentos de identificación, una vez superado el límite permitido.
   -Desconectar conexiones de comunicaciones de datos.
g. Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.

9.6.4.5.3 Identificación y Autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta

llegar a la persona responsable.

En circunstancias excepcionales, cuando existe un claro beneficio para la UAESP, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

9.6.4.5.4 Sistema de Administración de Contraseñas

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe:

a) Imponer el uso de contraseñas individuales para determinar responsabilidades.
b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
c) Imponer una selección de contraseñas de calidad según lo señalado en el punto “Uso de Contraseñas”.
d) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto “Uso de Contraseñas”.
e) Obligar a los usuarios a cambiar las contraseñas provisionales en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
f) Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
g) Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
h) Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
i) Modificar todas las contraseñas predeterminadas por el proveedor, una vez instalado el software y el hardware (por ejemplo, claves de impresoras, Switches, Routers, entre otros).

9.6.4.5.5 Uso de Utilitarios de Sistema

La mayoría de las infraestructuras informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

a) Utilizar procedimientos de autenticación para utilitarios del sistema.
b) Separar entre utilitarios del sistema y software de aplicaciones.

c) Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
d) Evitar que personas ajenas a la UAESP tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.
e) Establecer autorizaciones para uso gratuito (free) de utilitarios de sistema.
f) Registrar todo uso de utilitarios del sistema.
g) Definir y documentar los niveles de autorización para utilitarios del sistema.
h) Remover todo el software basado en utilitarios y software de sistema innecesarios.

9.6.4.5.6 Desconexión de Terminales por Tiempo Muerto

El Responsable de Seguridad Informática, junto con los propietarios de la Información de que se trate definirán cuáles se consideran terminales de alto riesgo o que sirven a sistemas de alto riesgo. Las mismas se desconectarán después de un periodo definido de los sistemas críticos, tiempo muerto, para evitar el acceso de personas no autorizadas.

Para las PC's, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red. Por otro lado, si un funcionario debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

9.6.4.6 Control de acceso a las aplicaciones

9.6.4.6.1 Restricción del Acceso a la Información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política de la UAESP para el acceso a la información.

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El Propietario de la Información involucrada será responsable de la adjudicación de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, las mismas serán llevadas a cabo por personal del área de sistemas, conforme a una autorización formal emitida por el Propietario de la Información.
b) 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.
c) Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.

d) Garantizar que las salidas de los sistemas de aplicación que administran información sensible contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a los PC's y ubicaciones autorizadas.
e) Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

9.6.4.6.2 Aislamiento de los Sistemas Sensibles

Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en un equipo de cómputo dedicado, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones. Son aplicables las siguientes consideraciones:

a) Identificar y documentar claramente la sensibilidad de un sistema de aplicación. Esta tarea será llevada a cabo por el administrador de la aplicación.
b) Identificar y acordar con el administrador de la aplicación sensible cuando la aplicación ha de ejecutarse en un ambiente compartido, los sistemas de aplicación con los cuales ésta compartirá los recursos.
c) Coordinar con el responsable de la Oficina de Tecnologías de la Información y las Comunicaciones, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo con los requerimientos de operación y seguridad especificados por el administrador de la aplicación.
d) Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.
e) Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación. Ejemplo; el equipamiento alternativo o las instalaciones de emergencia donde restablecer la aplicación.

9.6.4.7 Monitoreo del acceso y uso de los sistemas

9.6.4.7.1 Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.

Los registros de auditoría deberán incluir:

a) Identificación del usuario.
b) Fecha y hora de inicio y terminación.
c) Identidad de la terminal (por dirección IP)
d) Registros de intentos exitosos y fallidos de acceso al sistema.
e) Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de la Política de Retención de Registros.

9.6.4.7.2 Monitoreo del Uso de los Sistemas

Procedimientos v Áreas de Riesgo

Se desarrollarán documentos para monitorear el uso de los recursos de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente. Todos los funcionarios deben conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo.

9.6.4.8 Computación móvil y trabajo remoto

9.6.4.8.1 Computación Móvil

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información de la UAESP. Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Laptop o PDA (Asistente Personal Digital), Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, etc. y cualquier dispositivo de almacenamiento de conexión USB, cámaras digitales, etc. Así como también la red inalámbrica de la UAESP.

Esta lista no es exclusiva o única, ya que deberán incluirse todos los dispositivos que pudieran contener información confidencial de la UAESP y, por lo tanto, pueden ser suceptibles de sufrir un incidente en el que se comprometa la seguridad de la entidad.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

a) La protección física necesaria
b) El acceso seguro a los dispositivos
c) El acceso a los sistemas de información y servicios la UAESP a través de dichos dispositivos.
d) Los mecanismos de resguardo de la información contenida en los dispositivos.
e) La protección contra software malicioso.
f) Protección y seguridad en el entorno de la red inalámbrica.

Por otra parte, se desarrollarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información de la entidad.

9.6.4.8.2 Trabajo Remoto

Considerando que la Ley 1221 de 2008 establece las normas que promueven y regulan el Teletrabajo y teniendo en cuenta el Decreto 0884 de 2012 que la reglamenta, el presente manual toma en cuenta las especificaciones técnicas y de seguridad para esta forma de trabajo.

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el funcionario trabaje en forma remota desde un lugar externo a la UAESP. El trabajo remoto sólo será autorizado por Oficina TIC juntamente con el Responsable de Seguridad Informática, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios de la entidad, impedimento físico, entre otros.

Para esto, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

a) Utilización en lo posible de VPN entre el usuario y la UAESP.
b) En lo posible no utilizar o restringir el uso de programas de acceso remoto, a menos que sea expresamente autorizado su uso por parte del responsable de seguridad informática.
c) El ambiente de trabajo remoto propuesto.
d) Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la Unidad, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.
e) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.
f) Evitar la instalación / desinstalación de software no autorizada por la UAESP.

9.7 DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.

9.7.1 Generalidades

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad. Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los

procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas de información, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer y/o alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable. Asimismo, es necesaria una adecuada administración de la infraestructura de base. Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

9.7.2 Objetivo

- Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.
- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
- Definir los métodos de protección de la información crítica o sensible.

9.7.3 Responsabilidad

El Responsable de Seguridad Informática y el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, junto con el Propietario de la Información, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El Responsable de Seguridad Informática, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos si es necesario. Luego, el Responsable de Seguridad Informática definirá junto con el Jefe de la Oficina de TIC los métodos de encriptación a ser utilizados. Asimismo, el Responsable de Seguridad Informática cumplirá las siguientes funciones:

- Definir la documentación de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas, el control de código malicioso y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de “implementador” y “administrador de programas fuentes” al personal de la Oficina de TIC que considere adecuado. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas. La Oficina de Tecnologías de la Información y las

Comunicaciones propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

La Subdirección de Asuntos Legales, incorporarán aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software.

9.7.4 Políticas

9.7.4.1. Requerimientos de seguridad de los sistemas

9.7.4.1.1 Análisis y Especificaciones de los Requerimientos de Seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o desarrollados por terceros) y a las mejoras o actualizaciones que se les incorporen.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:

a) Definir un procedimiento para que, durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas y de seguridad informática, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.
b) Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.
c) Considerar que los controles introducidos en la etapa de diseño son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

9.7.4.2. Seguridad en los sistemas de aplicación

Para evitar la pérdida, modificación o uso inadecuado de los datos pertenecientes a los sistemas de información, se establecerán controles y registros de auditoría, verificando:

a) La validación de datos de entrada.
b) El procesamiento interno.

c) La autenticación de mensajes (interfaces entre sistemas)
d) La validación de datos de salida.

9.7.4.2.1 Validación de Datos de Entrada

Se definirá un documento que, durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Este documento considerará los siguientes controles:

a) Control de secuencia.
b) Control de monto límite por operación y tipo de usuario.
c) Control del rango de valores posibles y de su validez, de acuerdo con criterios predeterminados.
d) Control contra valores cargados en las tablas de datos.
e) Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones:

a) Se definirá un documento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quiénes deberán ser informados del resultado, entre otros.
b) Se definirá un documento que explicite las alternativas a seguir para responder a errores de validación en un aplicativo.
c) Se definirá un documento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

9.7.4.2.2 Controles de Procesamiento Interno

Se definirá un documento para que, durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

Para ello se implementarán:

a) Documentos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.
b) Documentos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.
c) Documentos que establezcan la revisión periódica de los registros de auditoría, con el fin de detectar cualquier anomalía en la ejecución de las transacciones.
d) Documentos que realicen la validación de los datos generados por el sistema.
e) Documentos que verifiquen la integridad de los datos.
f) Documentos que controlen la integridad de registros y archivos.
g) Documentos que verifiquen la ejecución de los aplicativos en el momento adecuado.

h) Documentos que aseguren el orden correcto de ejecución de los aplicativos, la finalización de la programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

9.7.4.2.3 Autenticación de Mensajes

Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán los controles determinados en el punto “Controles Criptográficos”.

9.7.4.2.4 Validación de Datos de Salidas

Se establecerán documentos para validar la salida de los datos de las aplicaciones, incluyendo:

a) Comprobaciones de la razonabilidad para probar si los datos de salida son óptimos.
b) Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.
c) Provisión de información suficiente, para que el receptor o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.
d) Documentos para responder a las pruebas de validación de salidas.
e) Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

9.7.4.3. Controles criptográficos

Se utilizarán sistemas y técnicas criptográficas para la protección de la información con base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad. La definición de estos controles es potestad del Responsable de la Seguridad Informática en conjunto con el Jefe de la Oficina de TIC.

9.7.4.3.1 Política de Utilización de Controles Criptográficos.

La UAESP establece la presente Política de uso de controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que:

a) Se utilizarán controles criptográficos en los siguientes casos:
   - Para la protección de claves de acceso a sistemas, datos y servicios.
   - Para la transmisión de información clasificada, fuera del ámbito de la Entidad.
   - Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad Informática.
b) Se desarrollarán procedimientos respecto de la administración de claves, de la

recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

c) El responsable de la Oficina de Tecnologías de la Información y las Comunicaciones propondrá la siguiente asignación de funciones:

Función
Implementación de la Política de controles Criptográficos
Administración de Claves

d) Se utilizarán los siguientes algoritmos de cifrado y tamaños de clave:

• Cifrado Simétrico, Cifrado Asimétrico

9.7.4.4. Cifrado

Mediante la evaluación de riesgos que llevará a cabo por el Propietario de la Información y el Responsable de Seguridad Informática, 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. Al implementar la Política de la UAESP en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica.

9.7.4.4.1 Firma Digital

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Pueden aplicarse a cualquier tipo de documento que se procese electrónicamente. Se implementan mediante el uso de una técnica criptográfica sobre la base de dos claves relacionadas de manera única, donde una clave, denominada privada, se utiliza para crear una firma y la otra, denominada pública, para verificarla.

Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública. Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular.

Al utilizar firmas y certificados digitales, se considerará la legislación vigente que describa las condiciones bajo las cuales una firma digital es legalmente válida.

9.7.4.4.2 Servicio de No Repudio

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

9.7.4.4.3 Administración de Claves

Normas. Procedimientos v Métodos

Se redactarán los documentos necesarios para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
b) Generar y obtener certificados de clave pública de manera segura.
c) Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.
d) Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.
e) Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
f) 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.
g) Recuperar 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.
h) Archivar claves, por ejemplo, para la información archivada o resguardada.
i) Destruir claves.
j) Registrar y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves tendrán fecha de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por el lapso no mayor a 12 meses.

9.7.4.5. Seguridad de los Archivos del Sistema

Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

9.7.4.5.1 Control de Software Operativo

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

- Toda aplicación, desarrollada por la UAESP o por un tercero tendrá un único responsable designado formalmente por el Responsable de la Oficina de Tecnologías de la Información y las Comunicaciones.
- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
- El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de “implementador” al personal de su área que considere adecuado, quien tendrá como funciones principales:
  a) Coordinar la implementación de modificaciones o nuevos programas en el

ambiente de Producción.

b) Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo con las normas y procedimientos vigentes.
c) Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable.
d) Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles que realizar son:

a) Guardar sólo los ejecutables en el ambiente de producción.
b) Llevar un registro de auditoría de las actualizaciones realizadas.
c) Retener las versiones previas del sistema, como medida de contingencia.
d) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc.
e) Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.
f) Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

9.7.4.5.2 Protección de los Datos de Prueba del Sistema

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

a) Prohibir el uso de bases de datos operativas o en producción. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.
b) Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.
c) Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

9.7.4.5.3 Control de Cambios a Datos Operativos

La modificación, actualización o eliminación de los datos operativos serán realizados a través de los sistemas que procesan dichos datos y de acuerdo con el esquema de control de accesos implementado en los mismos. Una modificación por fuera de los sistemas a un dato almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones. El Responsable de Seguridad Informática definirá documentación para la gestión de dichas excepciones que contemplarán lo siguiente:

a) Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.
b) El Propietario de la Información afectada y del Responsable de Seguridad Informática aprobarán la ejecución del cambio, evaluando las razones por las cuales se solicita.
c) Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.
d) Se designará un encargado de implementar los cambios, el cual no será personal del Grupo de Desarrollo (propio o de terceros).
e) Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Responsable de Seguridad Informática.

9.7.4.5.4 Control de Acceso a las Bibliotecas de Programas Fuentes

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

a) El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, propondrá para su aprobación por parte del superior jerárquico que corresponda, la función de “administrador de programas fuentes” al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes y deberá:
   - Proveer al Grupo de Desarrolladores los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente / ejecutable.
   - Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador. Analista Responsable qué autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
   - Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada.
   - Administrar las distintas versiones de una aplicación.
   - Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.

b) Denegar al “administrador de programas fuentes" permisos de modificación sobre los programas fuentes bajo su custodia.
c) Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
d) Establecer que el implementador de producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.
e) Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.

f) Evitar que la función de “administrador de programas fuentes” sea ejercida por personal que pertenezca al grupo de desarrollo y/o mantenimiento (propio o de terceros).
g) Prohibir el resguardo de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.
h) Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.
i) Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por la UAESP en los procedimientos que surgen de la presente política.

9.7.4.6. Seguridad de los procesos de desarrollo y soporte

Esta Política provee seguridad al software y a la información del sistema de aplicación, por lo tanto, se controlarán los entornos y el soporte dado a los mismos.

9.7.4.6.1 Control de Cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello se establecerá un documento que incluya las siguientes consideraciones:

a) Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
b) Mantener un registro de los niveles de autorización acordados.
c) Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
d) Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).
e) Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
f) Obtener aprobación formal por parte del Responsable de la Oficina de Tecnologías de la Información y las Comunicaciones para las tareas detalladas, antes que comiencen las tareas.
g) Solicitar la revisión del Responsable de Seguridad Informática para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
h) Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
i) Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.
j) Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
k) Mantener un control de versiones para todas las actualizaciones de software.
l) Garantizar que la implementación se llevará a cabo minimizando la

discontinuidad de las actividades y sin alterar los procesos involucrados.

m) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.
n) Garantizar que sea el implementador quien efectúe el paso de los objetos modificados
al ambiente operativo o de producción, de acuerdo con lo establecido en “Control del Software Operativo”.

9.7.4.6.2 Revisión Técnica de los Cambios en el Sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad. Para ello, se definirá un procedimiento que incluya:

a) Revisar los documentos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
b) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.
c) Asegurar la actualización del Plan de Continuidad de Operaciones de la UAESP.

9.7.4.6.3 Restricción del Cambio de Paquetes de Software

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:

a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
b) Determinar la conveniencia de que la modificación sea efectuada por la UAESP, por el proveedor o por un tercero.
c) Evaluar el impacto que se produce si la UAESP se hace cargo del mantenimiento.
d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando por si fuera necesario aplicarlo a nuevas versiones.

9.7.4.6.4 Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán la documentación que contemplen los siguientes puntos:

a) Acuerdos de licencias, propiedad de código y derechos conferidos (Derechos de Propiedad Intelectual).
b) Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
c) 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, etc.

d) Verificación del cumplimiento de las condiciones de seguridad contempladas en el punto “Requerimientos de Seguridad en Contratos de Tercerización”.
e) Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

Anexo

Toda aplicación generada en el grupo de desarrollo o adquirida a un proveedor es, en algún momento, implementada en un ambiente de producción. Los controles de esta transferencia deben ser rigurosos a fin de asegurar que no se instalen programas fraudulentos. Es conveniente implementar algún software para la administración de versiones y para la transmisión de programas entre los ambientes definidos, con un registro asociado para su control.

A continuación, se presenta un modelo ideal formado por tres ambientes que debe ser adoptado teniendo en cuenta las capacidades instaladas, los recursos y el equipamiento existente.

• Ambiente de Desarrollo

Es donde se desarrollan los programas fuentes y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas. El analista o programador (desarrollador) tiene total dominio sobre el ambiente. Puede recibir alguna fuente para modificar, quedando registrado en el sistema de control de versiones que administra el “administrador de programas fuentes”.

El desarrollador realiza las pruebas con los datos de la base de desarrollo. Cuando considera que el programa está terminado, lo pasa al ambiente de pruebas junto con la documentación requerida que le entregará al implementador de ese ambiente.

• Ambiente de Pruebas

El implementador de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote de datos para tal efecto, junto con el usuario de ser posible. El tester o probador realiza las pruebas con los datos de la base de pruebas. Si no detectan errores de ejecución, los resultados de las rutinas de seguridad son correctos de acuerdo con las especificaciones y considera que la documentación presentada es completa, entonces remite el programa fuente al implementador de producción por medio del sistema de control de versiones y le entrega las instrucciones. Caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

• Ambiente de Producción

Es donde se ejecutan los sistemas y se encuentran los datos productivos. Los programas fuentes certificados se guardan en un repositorio de fuentes de producción, almacenándolos mediante un sistema de control de versiones que maneja el “administrador de programas fuentes” y donde se dejan los datos del programador que

hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.

El “implementador” compila el programa fuente dentro del ambiente de producción, en el momento de realizar este paso, se debe asegurar que hay una correspondencia biunívoca con el ejecutable en producción y luego se elimina, dejándolo en el repositorio productivo de programas fuentes.

9.8 ADMINISTRACIÓN DE LA CONTINUIDAD DE OPERACIONES

Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

9.8.1. Generalidades

La administración de la Continuidad de Operaciones es un proceso critico que debe involucrar a todos los niveles de la UAESP. El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades de la UAESP puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades de la entidad y asegurar la reanudación oportuna de las operaciones indispensables.

9.8.2. Objetivo

- Minimizar los efectos de las posibles interrupciones de las actividades normales de la UAESP (sean éstas resultado de desastres naturales, accidentes, fallas en la infraestructura tecnológica, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

- Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
- Maximizar la efectividad de las operaciones de contingencia de la UAESP con el establecimiento de planes que incluyan al menos las siguientes etapas:

  a) Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.
  b) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
  c) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

- Asegurar la coordinación con el personal de la entidad y los contactos externos

que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

9.8.3. Responsabilidad

El Responsable de Seguridad Informática participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

Los Propietarios de la Información y el Responsable de Seguridad Informática cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la UAESP.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la UAESP.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la UAESP.

Los Responsables de Procesos que involucren tecnología, revisarán periódicamente los planes bajo su responsabilidad, así como también identificar cambios en las disposiciones relativas a las actividades de la UAESP aún no reflejadas en los planes de continuidad. Los administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

El Comité de Seguridad de la Información tendrá a cargo la coordinación del proceso de administración de la continuidad de operaciones de los sistemas de procesamiento de información de la entidad frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- Identificar y priorizar los procesos críticos de las actividades de la UAESP.
- Asegurar que todos los funcionarios de la UAESP comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en las actividades desarrolladas en la Entidad
- Elaborar y documentar una estrategia de continuidad de operaciones de la UAESP consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de operaciones de la UAESP de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de operaciones de la entidad.
- Proponer las modificaciones a los planes de contingencia.

9.8.4. Políticas

9.8.4.1. Proceso de la administración de la continuidad

El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la Continuidad de Operaciones de la UAESP. Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de operaciones de los sistemas de procesamiento de información de la UAESP y la infraestructura de tecnología en general frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

a) Identificar y priorizar los procesos críticos de las actividades de la UAESP.
b) Asegurar que todos los funcionarios de la UAESP comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad de la UAESP.
c) Elaborar y documentar una estrategia de continuidad de operaciones de la UAESP consecuente con los objetivos y prioridades acordados.
d) Proponer planes de continuidad de operaciones de la UAESP de conformidad con la estrategia de continuidad acordada.
e) Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
f) Coordinar actualizaciones periódicas de los planes y procesos implementados.
g) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de operaciones de la UAESP.
h) Proponer las modificaciones a los planes de contingencia.

9.8.4.2. Continuidad de las Actividades y Análisis de los Impactos

Con el fin de establecer un Plan de Continuidad de operaciones de la UAESP se deben contemplar los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en la infraestructura de tecnología y su equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, atentados, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, entre otros.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Responsable de Seguridad

Informática, considerando todos los procesos de las actividades de la entidad y no limitándose a las instalaciones de procesamiento de la información.

Según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las operaciones de la UAESP. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información y a la máxima autoridad de la UAESP para su aprobación.

9.8.4.3. Elaboración e Implementación de los planes de continuidad de las actividades de la unidad

Los dueños de procesos y recursos de información, con la asistencia del Responsable de Seguridad Informática, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades de la UAESP. Estos procesos deberán ser propuestos por el Comité de Seguridad de la Información. Las actividades de planificación de la continuidad de las operaciones considerarán los siguientes puntos:

a) Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
b) Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
c) Implementar documentos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos.
d) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
e) Instruir al personal involucrado en la documentación de reanudación y recuperación
   en los siguientes temas:
   - Objetivo del plan.
   - Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
   - Procedimientos de divulgación.
   - Requisitos de la seguridad.
   - Procesos específicos para el personal involucrado.
   - Responsabilidades individuales.
f) Probar y actualizar los planes.

Asimismo, las actividades de planificación deben concentrarse en los objetivos de las actividades misionales de la UAESP requeridos, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable.

9.8.4.4. Marco para la planificación de la continuidad de las actividades de la unidad

Se mantendrá un solo marco para los planes de continuidad de operaciones de la UAESP, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento. Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada

componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

El administrador de cada plan de continuidad será el encargado de coordinar las tareas definidas en el mismo. Estas modificaciones deberán ser propuestas por el Comité de Seguridad de la Información para su aprobación.

El marco para la planificación de la continuidad de operaciones de la UAESP, tendrá en cuenta los siguientes puntos:

a) Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.
b) Definir la documentación de emergencia que describa las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones de la UAESP y/o la vida humana.
c) Realizar los documentos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales de la UAESP o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.
d) Redactar los documentos de recuperación que describan las acciones a emprender para restablecer las operaciones normales de la Unidad.
e) Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.

f) Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las operaciones y garantizar que los procesos sigan siendo eficaces.

9.8.4.5. Ensayo, mantenimiento y reevaluación de los planes de continuidad de la unidad.

Debido a que los planes de continuidad de las actividades de la UAESP pueden fallar, por suposiciones incorrectas, errores o cambios en la infraestructura de tecnología, se establecen las siguientes pautas de acción:

- El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
- El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.

Se deberán utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:

a) Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación las actividades utilizando pruebas de interrupciones).

b) Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).
c) Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).
d) Realizar ensayos completos probando que la Unidad, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Cada uno de los Responsables de Procesos es el responsable de las revisiones periódicas de cada uno de los planes de continuidad de su incumbencia, como también de la identificación de cambios en las disposiciones relativas a las actividades de la UAESP aún no reflejadas en dichos planes. Deberá prestarse especial atención a los cambios de:

a) Personal.
b) Direcciones o números telefónicos.
c) Ubicación, instalaciones y recursos.
d) Legislación.
e) Contratistas, proveedores y clientes críticos.
f) Procesos, o procesos nuevos / eliminados.
g) Tecnologías.
h) Requisitos operacionales.
i) Requisitos de seguridad.
j) Hardware, software y otros equipos (tipos, especificaciones, y cantidad).
k) Requerimientos de los sitios alternativos.
l) Registros de datos vitales.

Todas las modificaciones efectuadas serán propuestas por el Comité de Seguridad de la Información para su aprobación por el superior jerárquico que corresponda. Por otra parte, el resultado de estas actividades será dado a conocer a fin de que todo el personal involucrado tenga conocimiento de los cambios incorporados.

9.9 CUMPLIMIENTO

Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

A fin de asegurar la implementación de las medidas de seguridad comprendidas en este Manual, la UAESP identificará los recursos técnicos, administrativos y financieros necesarios.

9.9.1 Generalidades

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

Todos los procedimientos, manuales, instructivos, etc. a los que se hacen alusión en este Manual de Seguridad de Informática, harán parte de este, en la medida que se vayan aprobando y formalizado por parte de quien corresponda.

9.9.2 Objetivos

- Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la UAESP y/o al funcionario que incurra en responsabilidad civil o penal como resultado de su incumplimiento.
- Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la UAESP.
- Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.
- Optimizar la eficacia del proceso de auditoría y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.
- Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías
- Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la Unidad.

9.9.3 Responsabilidad

El Responsable de Seguridad Informática y el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones cumplirán las siguientes funciones:

- Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.
- Realizar revisiones periódicas de todas las áreas de la UAESP a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
- Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.
- Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoria.

El responsable de la Subdirección de Asuntos Legales de la UAESP, con la asistencia del Responsable de Seguridad Informática y el jefe de la Oficina de Tecnologías de la Información y las Comunicaciones cumplirán las siguientes funciones:

- Definir y documentar claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información.
- Redactar un Compromiso de Confidencialidad a ser firmado por todo el personal.

Los subdirectores velarán por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos en la presente Política, dentro de su área de responsabilidad.

Todos los funcionarios de los mandos medios y superiores conocerán, comprenderán, darán a conocer, cumplirán y harán cumplir la presente Política y la normativa vigente.

9.9.4 Políticas

9.9.4.1. Cumplimiento de requisitos legales

9.9.4.1.1 Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

9.9.4.1.2 Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual. Los funcionarios únicamente podrán utilizar material autorizado por el Jefe de la Oficina de TIC. La UAESP solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente. La infracción a estos derechos puede tener como resultado acciones legales que podrían derivaren demandas penales.

9.9.4.1.3 Derechos de Propiedad Intelectual de Software

El software es considerado una obra intelectual que goza de la protección de la Ley. La Ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción.

Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones y el Responsable de la Seguridad Informática, con la asistencia de la Subdirección de Asuntos Legales, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

a) Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.
b) Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las violen.
c) Mantener un adecuado registro de activos.

d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
e) Implementar controles para evitar el exceso del número máximo permitido de usuarios.
f) Verificar que sólo se instalen productos con licencia y software autorizado.
g) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
h) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
i) Utilizar herramientas de auditoría adecuadas.
j) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

9.9.4.1.4 Protección de Datos y Privacidad de la Información Personal

Todos los funcionarios deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones. La UAESP redactará un “Compromiso de Confidencialidad”, el cual deberá ser suscrito por todos los empleados. La copia firmada del compromiso será retenida en forma segura por la UAESP.

Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, difundir o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate. A través del “Compromiso de Confidencialidad” se deberá advertir al funcionario que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

9.9.4.1.5 Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información de La UAESP se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido. Todos los funcionarios deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

9.9.4.1.6 Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia. La UAESP garantizará que sus sistemas de información

cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida.

9.9.4.2 Revisiones de la política de seguridad y la compatibilidad técnica

9.9.4.2.1 Cumplimiento de la Política de Seguridad

Cada Responsable de Oficina y Subdirección, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Responsable de Seguridad Informática y el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, realizarán revisiones periódicas de todas las áreas de la Unidad a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.
b) Proveedores de sistemas.
c) Propietarios de información.
d) Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables

9.9.4.2.2 Verificación de la Compatibilidad Técnica

El Responsable de Seguridad Informática verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica especializada.

El resultado de la evaluación se plasmará en un informe técnico para su posterior interpretación por parte de los especialistas. Para esto, la tarea podrá ser realizada por un profesional experto (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que serán interpretados por un especialista técnico.

La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

Las verificaciones de cumplimiento sólo serán realizadas por personas competentes, formalmente autorizadas y bajo supervisión.

9.9.4.2.3 Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas estatutarias y convencionales que rigen al personal de la Administración Pública Nacional o Distrital, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Organismos pertinentes.

Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos constitucionales, la Ley de Procedimiento Administrativo y demás normativas específicas aplicables.

Además de las sanciones disciplinarias o administrativas, el servidor público que no da debido cumplimiento a sus obligaciones puede incurrir también en responsabilidad civil o patrimonial - cuando ocasiona un daño que debe ser indemnizado y/o en responsabilidad penal cuando su conducta constituye un comportamiento considerado delito por el Código Penal y leyes especiales.

Control de cambios

Versión	Fecha	Descripción de la modificación
1	10/10/2013	Creación del documento.
2	26/3/2020	Se modifica el nombre del documento pasando de Manual de Políticas de Seguridad Informática por Manual de Políticas de Seguridad de la Información, teniendo en cuenta el alcance del documento y las necesidades de la entidad. El documento fue aprobado el 5 de diciembre de 2019 en el Comité de Seguridad de la Información y Gobierno Digital.

	Nombre	Cargo	Firma
Elaboró	Gisela Arias Salazar	Profesional Universitario Oficina de la Información y las Comunicaciones	
	Adriana García Henao	Profesional Universitario Oficina de la Información y las Comunicaciones	
	Ruben Buitrago Daza	Contratista Oficina de la Información y las Comunicaciones	
Revisó	César Mauricio Beltrán López	Jefe Oficina de la Información y las Comunicaciones	
Aprobó	German Guillermo Sandoval Pinzón	Jefe Oficina Asesora de Planeación	