



# REGISTRO OFICIAL<sup>®</sup>

ÓRGANO DEL GOBIERNO DEL ECUADOR

Administración del Sr. Lcdo. Lenín Moreno Garcés  
Presidente Constitucional de la República

## EDICIÓN ESPECIAL

**Año I - Nº 32**

**Quito, jueves 6 de  
julio de 2017**

**Valor: US\$ 2,50 + IVA**

**UAFE** | Unidad de Análisis  
Financiero y Económico

**ING. HUGO DEL POZO BARREZUETA**  
**DIRECTOR**

Quito: Avenida 12 de Octubre  
N23-99 y Wilson  
Segundo Piso

Oficinas centrales y ventas:  
Telf. 3941-800  
Exts.: 2301 - 2305

Sucursal Guayaquil:  
Av. 9 de Octubre Nº 1616 y Av. Del Ejército  
esquina, Edificio del Colegio de Abogados  
del Guayas, primer piso. Telf. 252-7107

Suscripción anual:  
US\$ 400 + IVA para la ciudad de Quito  
US\$ 450 + IVA para el resto del país

Impreso en Editora Nacional

64 páginas

[www.registroficial.gob.ec](http://www.registroficial.gob.ec)

**Al servicio del país  
desde el 1º de julio de 1895**

**UNIDAD DE ANÁLISIS  
FINANCIERO Y ECONÓMICO**

**RESOLUCIÓN  
UAFE-DG-VR-2017-0020**

**EXPÍDESE LA POLÍTICA  
DE SEGURIDAD DE  
INFORMACIÓN**

UAFE-DG-VR-2017-0020

**Dr. Paúl Villarreal Velásquez**  
**DIRECTOR GENERAL**  
**UNIDAD DE ANÁLISIS FINANCIERO Y**  
**ECONÓMICO (UAFE)**

**Considerando:**

Que el artículo 226 de la Constitución de la República, establece: *“Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.”;*

Que el artículo 66 número 19 de la Norma Suprema reconoce y garantiza a las personas: *“El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.”;*

Que la Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos, fue publicada en el Registro Oficial Segundo Suplemento No. 802, de 21 de julio de 2016;

Que el artículo 11 de la Ley Orgánica en referencia, dispone: *“La Unidad de Análisis Financiero y Económico (UAFE), es la entidad técnica responsable de la recopilación de información, realización de reportes, ejecución de las políticas y estrategias nacionales de prevención y erradicación del lavado de activos y financiamiento de delitos. Es una entidad con autonomía operativa, administrativa, financiera y jurisdicción coactiva adscrita al Ministerio Coordinador de Política Económica o al órgano que asuma competencias.”*

*La Unidad de Análisis Financiero y Económico (UAFE) solicitará y recibirá, bajo reserva, información sobre operaciones o transacciones económicas inusuales e injustificadas para procesarla, analizarla y de ser el caso remitir un reporte a la Fiscalía General del Estado, con carácter reservado y con los debidos soportes.*

*La Unidad de Análisis Financiero y Económico (UAFE), colaborará con la Fiscalía y los órganos jurisdiccionales competentes, cuando estos lo requieran, con toda la información necesaria para la investigación, procesamiento y juzgamiento de los delitos de lavado de activos y financiamiento de delitos.*

*En forma excepcional y para luchar contra el crimen organizado, la Unidad de Análisis Financiero y Económico (UAFE) atenderá los requerimientos de información de la Secretaría Nacional de Inteligencia o del órgano que*

*asuma sus competencias, conservando la misma reserva o sigilo que pese sobre ella.”*

Que el artículo 12 letras f) y h) de la Ley ibídem, determinan como funciones de la UAFE: *“f) Remitir a la Fiscalía General del Estado el reporte de operaciones inusuales e injustificadas con los sustentos del caso, así como las ampliaciones e información que fueren solicitadas por la Fiscalía. La Unidad de Análisis Financiero y Económico (UAFE) queda prohibida de entregar información reservada, bajo custodia, a terceros con la excepción prevista en el artículo anterior; (...) h) Crear, mantener y actualizar, con carácter reservado, una base de datos con toda la información obtenida en el ejercicio de sus competencias;”*

Que el artículo 13 de la Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos, dispone: *“La máxima autoridad de la Unidad de Análisis Financiero y Económico (UAFE) es el Director General y será designado por el Presidente de la República.”* En consecuencia, el doctor Paúl Villarreal Velásquez fue nombrado Director General de la UAFE, mediante Decreto Ejecutivo No. 1241 de 25 de noviembre de 2016, suscrito por el economista Rafael Correa Delgado, Presidente Constitucional de la República;

Que el artículo 15 de la Ley en tratamiento, ordena: *“Las funcionarias o funcionarios de la Unidad de Análisis Financiero y Económico (UAFE) están obligados a guardar secreto de las informaciones recibidas en razón de su cargo, al igual que de las tareas de análisis financiero desarrolladas, aún después de diez años de haber cesado en sus funciones.”;*

Que el artículo 17 letra b) de la Ley Orgánica de Transparencia y Acceso a la Información Pública establece: *“No procede el derecho a acceder a la información pública, exclusivamente en los siguientes casos: (...) b) Las informaciones expresamente establecidas como reservadas en las leyes vigentes.”;*

Que el artículo 18 ibídem, en su cuarto inciso dispone: *“(…) Las instituciones públicas elaborarán semestralmente por temas, un índice de los expedientes clasificados como reservados. En ningún caso el índice será considerado como información reservada. Este índice de información reservada, detallará: fecha de resolución y período de vigencia de esta clasificación.”;*

Que el artículo 6 incisos tercero y cuarto de la Ley del Sistema Nacional de Registro de Datos Públicos, dispone: *“(…) También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado.*

*La autoridad o funcionario que por la naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos.”;*

Que el artículo 2 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, establece que: “*Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento.*”;

Que el artículo 5 de la Ley ibídem, en relación a la confidencialidad y reserva, prescribe lo siguiente: “*Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia.*”;

Que el artículo 9 de la Ley en referencia, determina: “*Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.*”;

Que el artículo 9 del Reglamento a la Ley Orgánica de Transparencia y Acceso a la Información Pública, prescribe: “*De conformidad con la Constitución y la Ley, no procede el derecho de acceso a la información pública sobre documentos calificados motivadamente como reservados por el Consejo de Seguridad Nacional y aquella información clasificada como tal por las leyes vigentes (...)*”;

Que el artículo 10 del Reglamento ibídem, dispone: “*Las instituciones sujetas al ámbito de este Reglamento, llevarán un listado ordenado de todos los archivos e información considerada reservada, en el que constará la fecha de resolución de reserva, período de reserva y los motivos que fundamentan la clasificación de reserva.*”;

Que el artículo 5 de la Ley de Seguridad Pública y del Estado prescribe: “*El sistema de seguridad pública y del Estado está conformado por la Presidencia de la República, quien lo dirige, las entidades públicas, las políticas, los planes, las normas, los recursos y los procedimientos, con sus interrelaciones, definidos para cumplir con el objeto de la presente ley; y, las organizaciones de la sociedad que coadyuvan a la seguridad ciudadana y del Estado.*”;

Que el artículo 19 segundo párrafo ibídem, contempla la clasificación de la información de los organismos de seguridad del Estado, en tal virtud determina: “*(...) La información y documentación se clasificará como reservada, secreta y secretísima. El reglamento a la ley determinará los fundamentos para la clasificación, reclasificación y desclasificación y los niveles de acceso exclusivos a la información clasificada. Toda información clasificada como reservada y secreta será de libre acceso luego de transcurridos cinco y diez años, respectivamente; y si es secretísima luego de transcurridos quince años.*”

Que el artículo 6 del Reglamento a la Ley de Seguridad Pública y del Estado, define al Sistema Nacional de Inteligencia de la siguiente manera: “*Es el conjunto*

*de organismos de inteligencia independientes entre sí, funcionalmente coordinados y articulados por la Secretaría Nacional de Inteligencia, que ejecutan actividades específicas de inteligencia y contrainteligencia, para asesorar y proporcionar inteligencia estratégica a los niveles de conducción política del Estado, con el fin de garantizar la soberanía nacional, la seguridad pública y del Estado, el buen vivir y defender los intereses del Estado.*”;

Que el artículo 7 ibídem, taxativamente determina la conformación del Sistema Nacional de Inteligencia: “*Conformarán este Sistema, las siguientes instituciones: (...)* d. *La Unidad de Inteligencia Financiera;*” (actualmente Unidad de Análisis Financiero y Económico);

Que el artículo 29 del Reglamento en tratamiento, dispone: “*Los servidores públicos, ciudadanos civiles y miembros activos de las Fuerzas Armadas y de la Policía Nacional que, por el ejercicio de su cargo o profesión, vinculación o cumplimiento de sus funciones, tengan conocimiento de la información, documentación, expedientes y asuntos secretísimos, secretos y reservados que estén a cargo de la Secretaría Nacional de Inteligencia y de los organismos de seguridad; están prohibidos de divulgarlos; aún después de cesar en sus funciones. La transmisión, divulgación o reproducción de la información señalada en el inciso anterior por cualquier medio, será sancionada de conformidad con disposiciones legales pertinentes.*”;

Que la Unidad de Análisis Financiero y Económico (UAFE), mediante Resolución No. UAFE-DG-VR-2017-0003 de 27 de enero de 2017, publicada en el Registro Oficial No. 953 de 1 de marzo de 2017, expide el “Índice temático por series documentales de los expedientes clasificados como reservados y secretos de la Unidad de Análisis Financiero y Económico (UAFE)”, que contiene de forma detallada, la documentación y expedientes que se encuentran excluidos del acceso a la información pública contemplado en la Ley Orgánica de Transparencia y Acceso a la Información Pública;

Que es necesario proteger la información generada y provista por los sujetos obligados a reportar a la UAFE, con la finalidad de evitar la posible utilización dolosa de información sensible, que podría alterar el mercado económico o perjudicar la gestión de las personas naturales y/o jurídicas de derecho privado en sus negocios lícitos, y subsidiariamente la seguridad del Estado;

Que es necesario implementar una Política de Seguridad de la Información de la Unidad de Análisis y Económico (UAFE), toda vez que la información constituye un bien jurídico a proteger, razón por la que se hace imprescindible documentar en forma clara y precisa los procedimientos respecto del manejo de los sistemas y datos informáticos con los que cuenta la Unidad para realizar su labor de análisis financiero y económico, es decir, asegurar la confidencialidad e integridad de la información que deben mantener los funcionarios, servidores y terceras partes que la tengan a su cargo;

Que la información generada por la UAFE debe ser protegida en virtud del mandato legal contenido en la Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos;

En ejercicio de las facultades que le confiere la Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos; y, el artículo 10, numeral 1.1.1.1 Direccionamiento estratégico, letra h) del Estatuto Orgánico de Gestión Organizacional por Procesos de la Unidad de Análisis Financiero y Económico (UAFE);

**Resuelve:**

**Artículo 1.-** Aprobar y consecuentemente expedir la POLÍTICA DE SEGURIDAD DE INFORMACIÓN DE LA UNIDAD DE ANÁLISIS FINANCIERO Y ECONÓMICO (UAFE), documento que se encuentra anexo a la presente Resolución en cincuenta y nueve (59) fojas útiles.

**Artículo 2.-** Disponer que la Secretaría General socialice con todas las Coordinaciones y Direcciones de la Unidad de Análisis Financiero y Económico (UAFE), el contenido de la Política de Seguridad de la Información, a fin de que sea ejecutada en las labores que realizan los funcionarios, servidores y trabajadores de la Unidad, así como las terceras partes correspondientes.

**DISPOSICIÓN FINAL ÚNICA**

La presente Política de Seguridad de la Información de la Unidad de Análisis Financiero y Económico (UAFE), entrará en vigencia a partir de su suscripción, sin perjuicio a su publicación en el Registro Oficial.

Suscrito en tres (3) ejemplares originales en el despacho del señor Director General de la Unidad de Análisis Financiero y Económico (UAFE), en Quito, Distrito Metropolitano, a 30 de mayo del 2017.

f.) Dr. Paúl Villarreal Velásquez, Director General, Unidad de Análisis Financiero y Económico (UAFE).



CORTE  
CONSTITUCIONAL  
DEL ECUADOR

**UAFFE**

Unidad de Análisis  
Financiero y Económico

**DOCUMENTO DE POLÍTICA DE SEGURIDAD  
DE LA INFORMACIÓN**



## Contenido

1.	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN .....	
1.1.	<i>Normas Generales</i> .....	
1.2.	<i>Actualización</i> .....	
2.	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN .....	
2.1.	<i>Compromiso de la máxima autoridad de la Institución con la Seguridad de la Información</i> .....	
2.2.	<i>Coordinación de la Gestión de la Seguridad de la Información</i> .....	
2.3.	<i>Acuerdos sobre Confidencialidad</i> .....	
2.4.	<i>Revisión independiente de la seguridad de la información</i> .....	
2.5.	<i>Identificación de los riesgos relacionados con las partes externas</i> .....	
2.6.	<i>Aprobación</i> .....	
2.7.	<i>Responsables de la ejecución</i> .....	
2.8.	<i>Generación, revisión y actualización de esta Política</i> .....	
2.9.	<i>Base legal</i> .....	
2.10.	<i>Contenido del documento de Política de Seguridad</i> .....	
3.	GESTIÓN DE LOS ACTIVOS .....	
3.1.	<i>Inventario de activos</i> .....	
3.2.	<i>Responsable de los Activos</i> .....	
3.3.	<i>Uso aceptable de los activos</i> .....	
3.4.	<i>Clasificación de Activos de Información</i> .....	
3.5.	<i>Etiquetado y manejo de la información</i> .....	
4.	SEGURIDAD DEL TALENTO HUMANO .....	
4.1.	<i>Funciones y responsabilidades</i> .....	
4.2.	<i>Selección</i> .....	
4.3.	<i>Términos y condiciones laborales</i> .....	
4.4.	<i>Responsabilidades del OSI y del responsable de seguridad de TICS</i> .....	
4.5.	<i>Responsabilidades de la dirección a cargo del funcionario</i> .....	
4.6.	<i>Educación, formación y sensibilización en seguridad de la información</i> .....	
4.7.	<i>Proceso disciplinario</i> .....	
4.8.	<i>Responsabilidades de terminación del contrato</i> .....	
4.9.	<i>Devolución de activos</i> .....	
4.10.	<i>Retiro de los privilegios de acceso</i> .....	
5.	SEGURIDAD FÍSICA Y DEL ENTORNO.....	
5.1.	<i>Perímetro de la seguridad física</i> .....	
5.2.	<i>Controles de acceso físico</i> .....	
5.3.	<i>Seguridad de oficinas, recintos e instalaciones</i> .....	
5.4.	<i>Protección contra amenazas externas y ambientales</i> .....	
5.5.	<i>Trabajo en áreas seguras</i> .....	
5.6.	<i>Áreas de carga, despacho y acceso público</i> .....	
5.7.	<i>Ubicación y protección de los equipos</i> .....	
5.8.	<i>Servicios de suministro</i> .....	
5.9.	<i>Seguridad del cableado</i> .....	
5.10.	<i>Mantenimiento de los equipos</i> .....	
5.11.	<i>Seguridad de los equipos fuera de las instalaciones</i> .....	
5.12.	<i>Seguridad en la reutilización o eliminación de los equipos</i> .....	
5.13.	<i>Retiro de activos de la UAFE</i> .....	
6.	GESTIÓN DE COMUNICACIONES Y OPERACIONES.....	
7.	CONTROL DE ACCESO .....	
8.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN .....	
9.	GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN .....	
10.	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO .....	
11.	CUMPLIMIENTO .....	

## **1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**

### **1.1. Normas Generales**

#### **Finalidad de la Política de Seguridad**

##### Visión de la Unidad de Análisis Financiero y Económico:

Ser una Institución altamente especializada y competitiva, reconocida a nivel nacional e internacional, en permanente innovación tecnológica, basada en análisis de riesgos contra el lavado de activos y el financiamiento del terrorismo.

En concordancia con la visión, el objetivo principal de la política de seguridad de la información de la información de la Unidad de Análisis Financiero y Económico es tener un nivel adecuado de implantación de una serie de Estándares, Procesos, Procedimientos y Tecnologías que en conjunción con el pleno compromiso del personal de la Institución lleven a manejar un nivel de riesgo aceptable; garantizando así la Confidencialidad, Integridad y Disponibilidad de la Información, en los medios y tiempo que su legitimidad lo requiera.

Este documento aplica a todos los activos de Información definidos por la Unidad de Análisis Financiero y Económico.

### **1.2. Actualización**

La presente Política deberá ser revisada y actualizada anualmente, por cuando se produzcan cambios significativos a nivel operativo, legal, tecnológico, económicos, entre otros puntos.

---

## **2. Organización de la Seguridad de la Información**

### **2.1. Compromiso de la máxima autoridad de la Institución con la Seguridad de la Información.**

- a) Realizar el seguimiento de la puesta en marcha de las normas de este documento.
- b) Disponer la difusión, capacitación y sensibilización del contenido de este documento.
- c) Designar al Oficial de Seguridad de la Información (OSI).

El OSI coordinará la participación y cooperación de los cargos directivos de la institución. Se deberá llevar registros y actas de las reuniones.

### **2.2. Coordinación de la Gestión de la Seguridad de la Información**

- a) El OSI tendrá las siguientes responsabilidades:
  - Definir y mantener la política y normas institucionales particulares en materia de seguridad de la información y gestionar la aprobación y puesta en vigencia por parte de la máxima autoridad de la institución así como el cumplimiento por parte de los funcionarios de la institución.
  - Monitorear cambios significativos de 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.
- 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 la seguridad 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 institución.
- Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.
- Designar a los custodios o responsables de la información de las diferentes áreas de la entidad, que deberá ser formalizada en un documento físico o electrónico, además de consolidar la información entregada por estos.
- Gestionar la provisión permanente de recursos económicos, tecnológicos y humanos para la gestión de la seguridad de la información.
- Velar por la aplicación de la familia de normas técnicas ecuatorianas INEN ISO/IEC 27000 en la institución según el ámbito de cada norma.
- Designar formalmente al responsable de seguridad del área de Tecnologías de la Información en coordinación con el director o responsable del área de Tecnologías de la Información de la Institución.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Controlar los mecanismos de distribución y difusión de información dentro y fuera de la institución.
- Desarrollar procedimientos adecuados de concienciación de usuarios en materia de seguridad, controles de acceso a los sistemas y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucional establecidos.
- Coordinar la gestión de eventos de seguridad de la información con otras entidades gubernamentales.

b) El responsable de Seguridad del Área de Tecnologías de la Información tendrá las siguientes responsabilidades:

- Definir procedimientos para el control de cambios a los procesos operativos, los sistemas e instalaciones, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
- Establecer criterios de seguridad para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas antes de su aprobación definitiva.
- Definir y documentar controles para la detección y prevención del acceso lógico no autorizado, la protección contra software malicioso,

garantizar la seguridad de los datos y los servicios conectados a las redes de la institución.

- Controlar la existencia de documentación física o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas.
- Evaluar el posible impacto operativo a nivel de seguridad 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 para soportar potenciales amenazas a la seguridad de la información que procesan.
- Controlar la obtención de copias de resguardo de información, así como la prueba periódica de su restauración.
- Asegurar el registro de las actividades realizadas por el personal operativo de seguridad de la información, para su posterior revisión.
- Desarrollar y verificar el cumplimiento de procedimientos 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 (ej., evitar software malicioso, accesos no autorizados, etc.).
- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento (ej., cintas, discos, etc.) e informes impresos, y verificar la eliminación o destrucción segura de los mismos, cuando proceda.
- Gestionar los incidentes de seguridad de la información de acuerdo a los procedimientos establecidos.
- Otras que por naturaleza de las actividades de gestión de la seguridad de la información deban ser realizadas.

### **2.3. Acuerdos sobre Confidencialidad**

- Elaborar y aprobar los acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, la Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos, su Reglamento General; y, la normativa secundaria que para efectos de protección de la información emita la UAFE.
- Controlar que los acuerdos de confidencialidad de la información, documento físico o electrónico, sean firmados por todo el personal de la institución sin excepción.
- Gestionar la custodia de los acuerdos firmados, en los expedientes, físicos o electrónicos, de cada funcionario, por parte del área de gestión de talento humano.
- Controlar que la firma de los acuerdos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios a la institución, sin excepción.
- Gestionar la aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros (ej.,

contratistas, proveedores, pasantes, entre otros) que deban realizar labores dentro de la institución sea por medios lógicos o físicos y que involucren el manejo de información.

#### **2.4. Revisión independiente de la seguridad de la información**

- Ejecutar revisiones independientes de la gestión de la seguridad a intervalos planificados o cuando ocurran cambios significativos en la implementación
- Identificar oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control a partir de las revisiones independientes. La revisión deberá contemplar las actuaciones de la alta dirección y del OSI en materia de gestión de la seguridad.
- Registrar y documentar todas las revisiones independientes de la gestión de la seguridad de la información que la institución realice.

#### **2.5. Identificación de los riesgos relacionados con las partes externas**

- Identificar y evaluar los riesgos para la información y los servicios de procesamiento de información de la entidad en los procesos que involucran terceras partes e implementar los controles apropiados antes de autorizar el acceso.
- Bloquear el acceso de la tercera parte a la información de la organización hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y las condiciones del caso así como acuerdos de confidencialidad respecto de la información a la que tendrán acceso.
- Garantizar que la tercera parte es consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información y los servicios de procesamiento de información de la organización.
- Registrar y mantener las terceras partes vinculadas a la entidad considerando los siguientes tipos:
  - Proveedores de servicios (ej., Internet, proveedores de red, servicios telefónicos, servicios de mantenimiento, energía eléctrica, agua, entre otros);
  - Servicios de seguridad;
  - Contratación externa de proveedores de servicios y/u operaciones;
  - Asesores y auditores externos;
  - Limpieza, alimentación y otros servicios de soporte contratados externamente;
  - Personal temporal (estudiantes, pasantes, funcionarios públicos externos);
  - Ciudadanos/clientes;
  - Otros
- Identificar requisitos de seguridad antes de facilitar servicios a ciudadanos o clientes de entidades gubernamentales que utilicen o procesen información de los mismos o de la entidad.

## 2.6. Aprobación

El documento de Política de Seguridad de la Información de la Unidad de Análisis Financiero y Económico ha sido revisado por el Director de la UAFE y fue liberada para su publicación e implantación.

La Dirección General de la Unidad de Análisis Financiero y Económico ha aprobado esta Política de Seguridad de la Información para los diferentes niveles organizacionales, cualquier cambio a esta política requerirá de la aprobación de dicho Director.

## 2.7. Responsables de la ejecución

El cumplimiento de la política definida a continuación, es obligatorio para Autoridades, Funcionarios, Servidores y Personal de Servicios Complementarios de la Unidad de Análisis Financiero y Económico. La inobservancia será sancionada de acuerdo a la Ley Orgánica del Servicio Público y su Reglamento General.

Ejecutan: Personal de la Unidad de Análisis Financiero y Económico.

Control: OSI.

## 2.8. Generación, revisión y actualización de esta Política

Generación y Actualización: OSI, Direcciones de la UAFE.

Revisión: Director de la UAFE.

Aprobación: Dirección General.

Vigencia: A partir de la fecha de su aprobación.

## 2.9. Base legal

- Constitución de la República.
- Ley Orgánica de Transparencia y Acceso a la Información Pública; y, su Reglamento General.
- Ley Orgánica del Servicio Público y su Reglamento General.
- Código Orgánico Monetario y Financiero
- Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos; y, su Reglamento General.
- Ley de Seguridad Pública y del Estado; y, su Reglamento.
- Ley del Sistema Nacional de Registro de Datos Públicos.
- Acuerdo Ministerial 166, de 19 de septiembre de 2013, que contiene el "Esquema Gubernamental de Seguridad de la Información EGSI", publicado en el Registro Oficial Suplemento No. 88 de 25 de septiembre de 2013; y, todas sus reformas;
- Código Orgánico Integral Penal.

## 2.10. Contenido del documento de Política de Seguridad

Esta política contempla:

- Gestión de los Activos

- Seguridad del Talento Humano
- Seguridad Física y del Entorno
- Gestión de Comunicaciones y Operaciones
- Control de Acceso
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- Gestión de los Incidentes de la Seguridad de la Información
- Gestión de la Continuidad del Negocio
- Cumplimiento

---

### 3. Gestión de los Activos

Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y se gestionan en forma consistente en relación a los objetivos y la estrategia de riesgo de la Institución; para esto se utilizan medidas de seguridad y procedimientos de gestión para proteger el flujo de información, plataformas de software y hardware, dispositivos físicos y sistemas que se encuentran inventariados.

#### 3.1. Inventario de activos

La Dirección Administrativa y el OSI, conjuntamente con el responsable de los activos de información de cada área, identificará los activos importantes, asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información. La Dirección Administrativa será la encargada de elaborar el inventario de activos físicos de toda la institución.

Dichos inventarios serán revisados y actualizados anualmente, así como también ante cualquier modificación de la información registrada.

Los encargados de elaborar el inventario de información y mantenerlo actualizado, serán funcionarios de la UAFE que hayan sido designados como responsables de los activos de información, en su unidad de trabajo; y, la responsabilidad de consolidar los inventarios de información de cada área, será del OSI.

#### 3.2. Responsable de los Activos

- a) El Responsable del Activo tendrá las siguientes funciones:
- Elaborar el inventario de los activos a su cargo y mantenerlo actualizado.
  - Administrar la información dentro de los procesos de la institución a los cuales ha sido asignado.
  - Elaborar las reglas para el uso aceptable del mismo e implantarlas previa autorización de la autoridad correspondiente.
  - Clasificar, documentar y mantener actualizada la información y los activos.
  - Consolidar los inventarios de los activos a cargo del Responsable del Activo, por área o unidad organizativa.

### **3.3. Uso aceptable de los activos**

El OSI y el responsable del área tecnológica deben identificar, documentar e implementar las reglas sobre el uso aceptable de los activos asociados con los servicios de procesamiento de información.

- a) Para la elaboración de las reglas, el responsable del activo deberá tomar en cuenta las actividades definidas en los controles correspondientes a los ámbitos de intercambio de información y control de accesos, donde sea aplicable.
- b) El OSI es el encargado de asegurar que los lineamientos para la utilización de los recursos de las Tecnologías de la Información contemplen los requerimientos de seguridad establecidos, según la criticidad de la información que procesan.
- c) La información y documentos generados en la institución y enviados por cualquier medio o herramienta electrónica son propiedad de la misma institución.

### **3.4. Clasificación de Activos de Información**

Los responsables de activos de información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y definir los perfiles que deberán tener permisos de acceso a la información.

### **3.5. Etiquetado y manejo de la información**

El OSI coordinará los procedimientos para el etiquetado y manejo de la información, de acuerdo al esquema de clasificación definido para los activos de información. Los mismos contemplarán las acciones o gestiones que se efectuaren sobre los recursos de información tanto en formatos físicos como electrónicos.

---

## **4. Seguridad del Talento Humano**

Considerando que el talento humano llega a ser el eslabón más débil de la cadena de valor de una Institución, es imperativo la implementación de controles específicos orientados a garantizar la confidencialidad, disponibilidad e integridad de la información institucional.

### **4.1. Funciones y responsabilidades**

- a) El OSI conjuntamente con el área de Talento Humano, deberán verificar a los candidatos, previa su contratación, revisar la información entregada en su hoja de vida.
- b) El OSI deberá realizar y aplicar el procedimiento de revisión de candidatos, referente al perfil de seguridad de la información, declaración de historial personal e historial financiero del candidato.
- c) Entregar formalmente a los funcionarios sus funciones y responsabilidades.
- d) Notificar al OSI los permisos necesarios para activación y acceso a los activos de información.

- e) Informar al OSI sobre los eventos potenciales, intentos de intrusión u otros riesgos que pueden afectar la seguridad de la información de la institución.

#### **4.2. Selección**

El OSI con el delegado del área de talento humano:

- a) Verificarán los antecedentes de candidatos, verificará a los contratistas, y asignará la información a la cual se va a tener acceso y los riesgos percibidos. No debe entenderse este control como discriminatorio en ningún aspecto.
- b) Definirán los criterios y las limitaciones para las revisiones de verificación de personal actual (por motivos de designación o promoción), potenciales empleados y de terceras partes.
- c) Informarán del procedimiento de revisión y solicitar el consentimiento al personal actual (por motivos de designación o promoción), potenciales empleados y de terceras partes.

#### **4.3. Términos y condiciones laborales**

- a) Se debe verificar la firma de un acuerdo de confidencialidad o no-divulgación, antes de que el personal de la Unidad; y, contratistas tengan acceso a la información. Dicho acuerdo debe establecer los parámetros tanto de vigencia del acuerdo, información confidencial referida, formas de acceso, responsabilidades y funciones.
- b) Socializar los derechos y responsabilidades legales de los empleados, los contratistas y cualquier otro usuario sobre la protección de datos; dejando constancia de lo actuado a través de hojas de registro, informes o similares, que evidencie la realización de la misma.
- c) Responsabilizar al personal sobre el manejo, creación y almacenamiento de la información resultante durante el contrato laboral con la institución.

#### **4.4. Responsabilidades del OSI y del responsable de seguridad de TICS.**

- a) Explicar y definir las funciones y las responsabilidades respecto a la seguridad de la información, antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles.
- b) Lograr la concienciación sobre la seguridad de la información correspondiente a sus funciones y responsabilidades dentro de la institución.
- c) Verificar el cumplimiento de las funciones y responsabilidades respecto a la seguridad de la información mediante la utilización de reportes e informes.

#### **4.5. Responsabilidades de la dirección a cargo del funcionario**

- a) Acordar los términos y las condiciones laborales, las cuales incluyen la política de la seguridad de la información de la institución y los métodos apropiados de trabajo.

#### **4.6. Educación, formación y sensibilización en seguridad de la información**

- a) El OSI será el encargado de socializar y capacitar de forma periódica y oportuna sobre las normas y los procedimientos para la seguridad, las responsabilidades legales y los controles de la institución, así como en la capacitación del uso correcto de los servicios de información al personal, contratistas y usuarios de terceras partes.

#### **4.7. Proceso disciplinario**

- a) El área de Talento Humano deberá definir un procedimiento para garantizar el tratamiento imparcial y correcto para los empleados que han cometido violaciones comprobadas a la seguridad de la información.
- b) Dicho procedimiento deberá considerar sanciones graduales, dependiendo de factores tales como la naturaleza, cantidad y la gravedad de la violación, así como su impacto en la misión institucional.

#### **4.8. Responsabilidades de terminación del contrato**

- a) El Área de Talento Humano deberá comunicar oficialmente al personal las responsabilidades para la terminación de su relación laboral, lo cual debe incluir los requisitos permanentes para la seguridad de la información y las responsabilidades legales o contenidas en cualquier acuerdo de confidencialidad.
- b) Los cambios en la responsabilidad o en el contrato laboral deberán ser gestionados por parte del área de Talento Humano.
- c) Previa la terminación de un contrato se deberá realizar la transferencia de la documentación e información de la que fue responsable al nuevo funcionario a cargo, en caso de ausencia, al OSI.

#### **4.9. Devolución de activos**

- a) El área de Talento Humano será el responsable de:
  - o Definir el procedimiento de transferencia de conocimientos por parte del empleado, contratistas o terceras partes, luego de la terminación de su contrato laboral, para la continuación de las operaciones importantes dentro de la institución.
  - o Formalizar el proceso de terminación del contrato laboral, para incluir la devolución de software, documentos corporativos y los equipos. También es necesaria la devolución de otros activos de la institución tales como los dispositivos de cómputo móviles, tarjetas de acceso, tokens USB con certificados electrónicos, certificados electrónicos en archivo, memorias flash, teléfonos celulares, cámaras, manuales, bitácora de la información almacenada en medios electrónicos y otros estipulados en las políticas internas de cada entidad.
- b) Aplicar los debidos procesos para garantizar que toda la información generada por el empleado, contratista o usuario de terceras partes dentro de la institución, sea transferida, archivada o eliminada con seguridad.

#### **4.10. Retiro de los privilegios de acceso**

- a) El responsable del Área de TICS, dispondrá el retiro de los privilegios de acceso a los activos de información y a los servicios de procesamiento de información tales como: correo electrónico, accesos físicos, aplicaciones informáticas, entre otros, además de la ejecución del procedimiento de respaldo, eliminación o destrucción de información sensible, inmediatamente después de que este haya sido informado formalmente por parte del área de talento humano de la terminación o cambio de la relación laboral. El responsable del área de TICS reportará al OSI de estos retiros cada vez que le sean solicitados.

---

### **5. Seguridad Física y del Entorno**

Al establecer que la seguridad física y del entorno, debe involucrar los mecanismos de prevención y detección, destinados a proteger físicamente los recursos institucionales, a través de la implementación de contramedidas que mitiguen posibles riesgos y/o vulnerabilidades a los que estarían expuestos dichos recursos.

Los recursos que se pueden utilizar para tratar la información sensible de la institución, deben ubicarse en las zonas seguras dentro de un perímetro de seguridad que esté perfectamente definido, con barreras de seguridad y controles de entrada. Se debe proporcionar protección física contra los accesos que no estén autorizados. La protección tiene que ser proporcional a los riesgos identificados.

#### **5.1. Perímetro de la seguridad física**

Los perímetros de seguridad se deben utilizar para proteger las áreas que contengan la información y los recursos de procesamiento de información. Todas las pautas tienen que estar consideradas e implementadas en el lugar que sea necesario, estableciendo ciertos perímetros de seguridad físicos.

- a) El responsable del área Administrativa y el OSI deberán verificar:
- El perímetro de seguridad tiene que quedar perfectamente definido, en lugar y fuerza, dependiendo de los requisitos de seguridad del activo de información entre el perímetro y los resultados de la evaluación de riesgos del Sistema de Gestión de Seguridad de la Información.
  - El perímetro de un edificio debe contener todos los recursos necesarios para tratar la información ofreciéndole cierta solidez física. Todos los muros externos de la zona deben ser sólidos y todas las puertas exteriores deben ser protegidas contra accesos que no estén autorizados por la institución.
  - Se tiene que realizar la instalación de un área de recepción manual y otros medios de control de acceso físico a las instalaciones. El acceso se puede restringir sólo al personal que esté autorizado.
  - Las barreras físicas se pueden extender, si fuera necesario, desde el suelo real al techo real evitando que se realicen entradas no autorizadas.

- Las salidas de emergencia que se encuentran en el perímetro de seguridad deben contar con alarma, ser monitoreadas y probadas con respecto a la resistencia de la pared para que tengan un nivel parecido de resistencia en concordancia con los estándares regionales, nacionales e internacionales.
- Disponer de un sistema de vigilancia mediante el uso de circuito cerrado de televisión.
- Aislar los ambientes de procesamiento de información de los ambientes proporcionados por terceros.

## 5.2. Controles de acceso físico

La norma establece que se deben proteger las diferentes áreas mediante controles de entrada adecuados que aseguren que el permiso de acceso solo se ofrece al personal autorizado.

Se tiene que considerar lo siguiente:

- a) Supervisar la permanencia de los visitantes en las áreas restringidas y registrar la hora y fecha de su ingreso y salida.
  - b) Las visitas de las áreas seguras se deben supervisar. Las visitas solo tienen acceso para propósitos muy específicos y deben cumplir con los requisitos de seguridad del área y los procedimientos ante emergencias.
  - c) Controlar y limitar el acceso, exclusivamente a personal autorizado, a la información sensible y a las instalaciones de procesamiento de información. Se debe utilizar controles de autenticación como tarjetas de control de acceso más el número de identificación personal.
  - d) Se pueden exigir a todo el personal de la institución que porte la identificación de forma visible y deben saber que puede ser solicitada a las personas extrañas que no estén acompañadas y a cualquiera que no lleve la identificación visible.
  - e) Implementar que los visitantes, deben ser escoltados por una persona autorizada para el tránsito en las áreas restringidas.
  - f) Se tiene que garantizar el acceso restringido de terceras personas hacia las áreas de seguridad o los recursos de los procesos de información sensible. El acceso debe ser autorizado y monitorizado por la persona responsable.
  - g) Se debe revisar y actualizar de forma regular los derechos de acceso a las áreas de seguridad.
  - h) Los Centros de Cómputo deben contar con mecanismos de control de acceso tales como puertas de seguridad, cerradura, sistemas de control con tarjetas inteligentes, sistema de alarmas o controles biométricos.
- Nota: El OSI debe llevar un registro actualizado de las Áreas Seguras, donde se indique la identificación del Edificio y Área, principales Activos de información a proteger y medidas de protección física.

### **5.3. Seguridad de oficinas, recintos e instalaciones**

La seguridad física para oficinas, despachos y recursos tiene que ser asignada y aplicada por el OSI:

- a) Proteger las instalaciones claves de tal manera que se evite el acceso al público.
- b) Ubicar las impresoras, copiadoras, etc., en un área protegida.
- c) Disponer que las puertas y ventanas permanezcan cerradas, especialmente cuando no haya vigilancia.
- d) Los escritorios o puestos de trabajo de los servidores públicos deben mantenerse limpios y sin documentos fuera del horario de trabajo o en ausencia prolongada del sitio, esto para evitar el acceso no autorizado a la información.
- e) Los Servidores Públicos deben colocar las pantallas de sus computadores en una posición en la que se evite que personal no autorizado pueda ver la información que se encuentre desplegada en ellas.
- f) Las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a las oficinas sólo deben ser utilizados por los funcionarios autorizados y, salvo situaciones de Emergencia, estos no deben ser transferidos a otros funcionarios de la Entidad, Contratista o Terceros con su debida autorización.
- g) Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
- h) No dejar abandonada en las impresoras información confidencial y secreta, una vez se haya impreso.

### **5.4. Protección contra amenazas externas y ambientales.**

- a) Las Oficinas e instalaciones donde se procesa y/o almacena la información confidencial o secreta debe contar con sistemas de alarmas y cámaras de seguridad, sistema de detección y extinción automáticas de incendios.
- b) Se debe mantener buena ubicación de los equipos, aislado de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros y se debe almacenar los materiales combustibles o peligrosos a una distancia prudente de las áreas protegidas.
- c) Los equipos del Centro de Cómputo deben tener control de los niveles de temperatura y humedad, estos deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo allí instalada.
- d) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipo que registre información, a menos que

hayan sido formalmente autorizadas por el responsable del proceso involucrado y el OSI.

- e) No se permite comer, beber y fumar dentro de las instalaciones de la institución.

#### **5.5. Trabajo en áreas seguras**

- a) Dar a conocer al personal, la existencia de un área segura.
- b) Evitar el trabajo no supervisado para evitar actividades maliciosas.
- c) Revisar periódicamente y disponer de un bloqueo físico de las áreas seguras vacías.

#### **5.6. Áreas de carga, despacho y acceso público**

- a) Permitir el acceso al área de despacho y carga, únicamente a personal identificado y autorizado.
- b) Descargar y despachar los suministros, únicamente en el área de descarga y despacho.
- c) Asegurar las puertas externas e internas de despacho y carga.
- d) Inspeccionar el material que llega para determinar posibles amenazas.
- e) Registrar el material que llega, de acuerdo a los procedimientos de gestión de activos.

#### **5.7. Ubicación y protección de los equipos**

- a) Ubicar los equipos de modo que se elimine el acceso innecesario a las áreas de trabajo restringidas.
- b) Aislar los servicios de procesamiento de información con datos sensibles y elementos que requieran protección especial, para reducir el riesgo de visualización de la información de personas no autorizadas.
- c) Establecer directrices para no comer, beber y fumar en las cercanías de las áreas de procesamiento de información.
- d) Monitorear las condiciones ambientales de temperatura y humedad.
- e) Tener protección contra descargas eléctricas en todas las edificaciones de la institución y disponer de filtros protectores en el suministro de energía y en las líneas de comunicación.
- f) Disponer de métodos especiales de protección para equipos en ambientes industriales.

#### **5.8. Servicios de suministro**

- a) Implementar y documentar los servicios de electricidad, agua, calefacción, ventilación y aire acondicionado, suministrados a la institución.
- b) Inspeccionar regularmente todos los sistemas de suministro.
- c) Contar con un Sistema de Energía Interrumpible UPS y plantas eléctricas, para asegurar el apagado regulado y sistemático de los equipos de cómputo de la UAFE y asegurar la continuidad de las operaciones, mientras se restablecen las fallas en el suministro de energía eléctrica.
- d) Se debe contar con interruptores de emergencias que deben estar ubicados cerca de las salidas de emergencia de las instalaciones donde se encuentren los equipos de cómputo, con el fin de facilitar un corte rápido de la energía en caso tal se presente una situación crítica.

- e) Disponer de múltiples enchufes o líneas de suministro de energía eléctrica regulada.
- f) Disponer con iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.
- g) Disponer con protección contra descargas eléctricas en el edificio.

#### **5.9. Seguridad del cableado**

- a) Disponer de líneas de fuerza (energía) y de telecomunicaciones subterráneas protegidas, en cuanto sea posible.
- b) Proteger el cableado de red contra interceptación no autorizada, el cableado debe contar con conductos como canaletas para su adecuada protección.
- c) El cableado eléctrico debe estar separado del cableado de red para evitar posibles interferencias.
- d) Identificar y rotular los cables de acuerdo a normas locales o internacionales para evitar errores en el manejo.
- e) Disponer de documentación, diseños/planos y la distribución de conexiones de: datos alámbricas/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc.
- f) Controlar el acceso a los módulos de cableado de conexión (patch panel) y cuartos de cableado.

#### **5.10. Mantenimiento de los equipos**

- a) Se debe dar cumplimiento al programa de mantenimiento a los equipos de la entidad, de acuerdo a las especificaciones y recomendaciones del proveedor.
- b) Realizar el mantenimiento de los equipos únicamente con personal calificado y autorizado. Se deben realizar mantenimientos preventivos y pruebas funcionales al Sistema de UPS y/o plantas eléctricas, sistemas de detección y extinción de incendios, sistemas de aire acondicionado, servidores, equipos de comunicaciones, equipos de seguridad que conforman la plataforma tecnológica.
- c) Conservar los registros de los mantenimientos preventivos, correctivos y fallas relevantes o sospechosas.
- d) Establecer controles apropiados para realizar mantenimientos programados y emergentes.
- e) Gestionar mantenimientos planificados con hora de inicio, fin, impacto y responsables y poner previamente en conocimiento de administradores y usuarios finales.

#### **5.11. Seguridad de los equipos fuera de las instalaciones**

- a) El uso de equipos de cómputo, portátiles, discos removibles destinado al procesamiento de información, fuera de las instalaciones de la institución, será autorizado por el responsable del proceso al que pertenezca el servidor público.
- b) Custodiar los equipos y medios que se encuentren fuera de las instalaciones de la institución. Tomar en cuenta las instrucciones del fabricante para la protección de los equipos que se encuentran fuera de estas instalaciones.

- c) Disponer de controles para el trabajo que se realiza en equipos fuera de las instalaciones, mediante una evaluación de riesgos.
- d) Establecer una cobertura adecuada del seguro, para proteger los equipos que se encuentran fuera de las instalaciones.
- e) El Usuario que está autorizado a retirar un equipo de cómputo o portátil debe tener el mismo nivel de protección de la información como si estuviese en las instalaciones de la entidad.
- f) Periódicamente se debe monitorear la eficacia del control de registros de los equipos, para detectar el retiro no autorizado de activos de información de la Unidad, control que será llevado a cabo por el OSI.

#### **5.12. Seguridad en la reutilización o eliminación de los equipos**

- a) Destruir, borrar o sobrescribir los dispositivos que contienen información sensible utilizando técnicas que permitan la no recuperación de la información original.
- b) Evaluar los dispositivos deteriorados que contengan información sensible antes de enviar a reparación, borrar la información o determinar si se debería eliminar físicamente el dispositivo.

#### **5.13. Retiro de activos de la UAFE**

- a) Tener autorización previa para el retiro de cualquier equipo, información o software.
- b) Identificar a los empleados, contratistas y usuarios de terceras partes, que tienen la autorización para el retiro de activos de la institución.
- c) Establecer límites de tiempo para el retiro de equipos y verificar el cumplimiento en el momento de la devolución.
- d) Registrar cuando el equipo o activo sea retirado y cuando sea devuelto.

---

### **6. Gestión de Comunicaciones y Operaciones**

Las políticas de gestión de comunicaciones y operación van encaminadas a garantizar el funcionamiento seguro de las plataformas tecnológicas y los medios de procesamiento de la información, así como también la asignación de roles y responsabilidades para una adecuada gestión y operación de los activos de Información.

#### **6.1. Documentación de los procedimientos de Operación**

- a) Documentar el procesamiento y manejo de la información.
- b) Documentar el proceso de respaldo y restauración de la información.
- c) Documentar todos los procesos de los servicios de procesamiento de datos, incluyendo la interrelación con otros sistemas.
- d) Documentar las instrucciones para el manejo de errores y otras condiciones excepcionales que pueden surgir durante la ejecución de las tareas.
- e) Documentar los contactos de soporte, necesarios en caso de incidentes.

- f) Documentar las instrucciones para el manejo de medios e informes especiales, incluyendo procedimientos para la eliminación segura de informes de tareas fallidas.
- g) Documentar los procedimientos para reinicio y recuperación del sistema en caso de fallas.
- h) Documentar los registros de auditoría y de la información de registro del sistema.

## **6.2. Gestión del Cambio**

- a) Identificar y registrar los cambios significativos.
- b) Evaluar el impacto de dichos cambios.
- c) Aprobar de manera formal los cambios propuestos.
- d) Planificar el proceso de cambio.
- e) Realizar pruebas del cambio.
- f) Comunicar el detalle de cambios a todas las personas involucradas.
- g) Identificar responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.
- h) Establecer responsables y procedimientos formales del control de cambios en los equipos y software. Los cambios deben efectuarse únicamente cuando haya razón válida para la misión de la institución, como: cambio de versión, corrección de vulnerabilidades, costos, licenciamiento, nuevo hardware.

## **6.3. Distribución de funciones**

- a) Distribuir las funciones y las áreas de responsabilidad, para reducir oportunidades de modificaciones no autorizadas, no intencionales, o el uso inadecuado de los activos de la institución.
- b) Limitar el acceso a modificar o utilizar los activos sin su respectiva autorización.
- c) Establecer controles de monitoreo de actividades, registros de auditoría y supervisión por parte de la dirección.

## **6.4. Separación de las instancias de Desarrollo, Pruebas, capacitación y Producción**

- a) Definir y documentar diferentes entornos para desarrollo, pruebas, capacitación y producción. Para el caso que no se pueda definir diferentes entornos con recursos físicos independientes, se debe mantener diferentes directorios con su respectiva versión y delegación de acceso.
- b) Aislar los ambientes de desarrollo, pruebas, capacitación y producción.
- c) Controlar la instalación y uso de herramientas de desarrollo de software y/o acceso a bases de datos y redes en los equipos informáticos, salvo que sean parte de las herramientas de uso

- estándar o su instalación sea autorizada de acuerdo a un procedimiento expresamente definido.
- d) Implantar ambientes de prueba, iguales en capacidad, a los ambientes de producción.
  - e) Utilizar sistemas de autenticación y autorización independientes para las diversas instancias o ambientes.
  - f) Definir perfiles de usuario para las diferentes instancias o ambientes.
  - g) Aislar los datos sensibles de los ambientes de desarrollo, pruebas y capacitación
  - h) Permitir al personal de desarrollo de software el acceso al entorno de producción, únicamente en caso de extrema necesidad, con la autorización explícita correspondiente.

#### **6.5. Presentación del Servicio**

- a) Establecer controles sobre definiciones del servicio y niveles de prestación del servicio, para que sean implementados, mantenidos y operados por terceros.
- b) Establecer controles de cumplimiento de terceros, que garanticen la capacidad de servicio, planes ejecutables y diseños para la continuidad de los servicios, en caso de desastres.

#### **6.6. Monitoreo y revisión de los servicios, por terceros**

- a) Identificar los sistemas sensibles o críticos que convenga tener dentro o fuera de la institución.
- b) Monitorear los niveles de desempeño de los servicios para verificar el cumplimiento de los acuerdos.
- c) Analizar los reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos.
- d) Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionados con el servicio prestado.

#### **6.7. Gestión de los cambios en los servicios ofrecidos por terceros**

- a) Establecer un proceso de gestión de cambios en los servicios ofrecidos por terceros, en el desarrollo de aplicaciones, provisión de servicios de hardware, software, redes, otros.
- b) Coordinar el proceso de cambio cuando se necesita realizar cambios o mejoras a las redes y uso de nuevas tecnologías en los servicios ofrecidos por terceros.
- c) Coordinar el proceso de cambio cuando se realice cambio de proveedores, cambio de ubicación física en los servicios ofrecidos por terceros.

**6.8. Gestión de la capacidad**

- a) Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos.
- b) Monitorear los recursos asignados para garantizar la capacidad y rendimiento de los servicios y sistemas informáticos.
- c) Utilizar la información del monitoreo para la adquisición, asignación de recursos y evitar cuellos de botella.

**6.9. Aceptación del Sistema**

- a) Verificar el desempeño y los requerimientos de cómputo necesarios para los nuevos sistemas.
- b) Considerar procedimientos de recuperación y planes de contingencia.
- c) Poner a prueba procedimientos operativos de rutina según normas definidas para el sistema.
- d) Garantizar la implementación de un conjunto de controles de seguridad acordados.
- e) Asegurar que la instalación del nuevo sistema no afecte negativamente los sistemas existentes, especialmente en períodos pico de procesamiento.
- f) Considerar el efecto que tiene el nuevo sistema en la seguridad global de la institución.
- g) Capacitar sobre el funcionamiento y utilización del nuevo sistema.
- h) Para nuevos desarrollos, se debe involucrar a los usuarios y a todas las áreas relacionadas, en todas las fases del proceso, para garantizar la eficacia operativa del sistema propuesto.

**6.10. Controles contra código malicioso**

- a) Prohibir el uso de software no autorizado por la institución. Elaborar un listado del software autorizado.
- b) Establecer procedimientos para evitar riesgos en la obtención/descarga de archivos y software desde o a través de redes externas o por cualquier otro medio.
- c) Instalar y actualizar periódicamente software de antivirus y contra código malicioso.
- d) Mantener los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles.
- e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la institución.
- f) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos o en archivos recibidos a través de redes no confiables.

- g) Redactar procedimientos para verificar toda la información relativa a software malicioso.
- h) Emitir boletines informativos de alerta con información precisa.
- i) Concienciar al personal acerca del problema de los virus y cómo proceder frente a los mismos.
- j) Contratar con el proveedor de Internet o del canal de datos los servicios de filtrado de: virus, spam, programas maliciosos (malware), en el perímetro externo.

#### **6.11. Controles contra códigos móviles**

- a) Aislar de forma lógica los dispositivos móviles en forma similar a lo que ocurre con las VLANs.
- b) Bloquear códigos móviles no autorizados.
- c) Gestionar el código móvil mediante procedimientos de auditoría y medidas técnicas disponibles.
- d) Establecer controles criptográficos para autenticar de forma única el código móvil.

#### **6.12. Respaldo de la información**

- a) Los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información, determinarán los procedimientos para el resguardo y contención de la información.
- b) Definir el procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención.
- c) Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución.
- d) Establecer procedimientos de los medios de respaldo, una vez concluida su vida útil recomendada por el proveedor y la destrucción de estos medios.
- e) Guardar los respaldos en un sitio lejano, a una distancia suficiente para evitar cualquier daño debido a desastres en la sede principal de la institución.
- f) Proporcionar un grado apropiado de protección física y ambiental.
- g) Establecer procedimientos regulares de verificación y restauración de los medios de respaldo para garantizar sean confiables para uso de emergencia.
- h) Proteger la información confidencial por medio de encriptación.
- i) Considerar los respaldos a discos y en el mismo sitio si se tiene suficientes recursos, ya que en caso de mantenimientos de los sistemas de información, es más rápida su recuperación.

#### **6.13. Controles de las redes**

- a) Separar el área de redes del área de operaciones, cuando la capacidad y recursos lo permitan.

- b) Designar procedimientos y responsabilidades para la gestión de equipos remotos como el caso de re-direccionamiento de puertos y accesos por VPNs, incluyendo el área de operaciones y de usuarios finales.
- c) Establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por las redes públicas, redes locales e inalámbricas; así como la disponibilidad de las redes.
- d) Garantizar la aplicación de los controles mediante actividades de supervisión.
- e) Disponer de un esquema de red de los enlaces de datos, Internet y redes locales, así como la documentación respectiva.

#### **6.14. Seguridad de los servicios de la red**

- a) Incorporar tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red
- b) Implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus.
- c) Definir procedimientos para la utilización de los servicios de red para restringir el acceso a los servicios de red cuando sea necesario.

#### **6.15. Gestión de los medios removibles**

- a) Establecer un procedimiento para la gestión de todos los medios removibles.
- b) Tener autorización para la conexión de los medios removibles y registrar la conexión y retiro, para pruebas de auditoría.
- c) Almacenar los medios removibles en un ambiente seguro, según las especificaciones de los fabricantes.
- d) Evitar la pérdida de información por deterioro de los medios.

#### **6.16. Eliminación de los medios**

- a) Identificar los medios que requieran eliminación segura.
- b) Almacenar y eliminar de forma segura los medios que contienen información sensible, como la incineración, trituración o borrado de los datos.
- c) Establecer procedimientos para selección del contratista que ofrece servicios de recolección y eliminación del papel, equipos y medios.
- d) Registrar la eliminación de los medios para mantener pruebas de auditoría.

#### **6.17. Procedimientos para el manejo de la información**

- a) Establecer procedimientos para el manejo y etiquetado de todos los medios de acuerdo a su nivel de clasificación.
- b) Establecer controles de acceso para evitar el acceso de personal no autorizado.
- c) Tener un registro actualizado de los receptores de los medios.
- d) Establecer controles de protección según el nivel de sensibilidad de los datos que reside en la memoria temporal.
- e) Almacenar los medios según especificaciones del fabricante.

#### **6.18. Seguridad de la documentación del sistema**

- a) Guardar con seguridad toda la documentación de los sistemas informáticos.
- b) Mantener una lista de acceso mínima a la documentación del sistema y con su debida autorización.
- c) Mantener una protección adecuada de la documentación del sistema expuesta en la red pública.

#### **6.19. Políticas y procedimientos para el intercambio de información.**

- a) Establecer procedimientos para proteger la información intercambiada contra la interpretación, copiado, modificación, enrutamiento y destrucción.
- b) Definir procedimientos para detección y protección contra programas maliciosos, cuando se utilizan comunicaciones electrónicas.
- c) Proteger la información sensible que se encuentra en forma de adjunto.
- d) Establecer directrices para el uso de los servicios de comunicación electrónica.
- e) Definir procedimientos para el uso de las redes inalámbricas en base a los riesgos involucrados.
- f) Establecer responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la institución con un mal uso de la información.
- g) Establecer controles por medio de técnicas criptográficas.
- h) Definir directrices de retención y eliminación de la correspondencia incluyendo mensajes, según la normativa legal local.
- i) No dejar información sensible en copiadoras, impresoras, fax, contestadores
- j) No revelar información sensible al momento de tener una conversación telefónica o mantener conversaciones sin tomar los controles necesarios.
- k) No dejar datos demográficos al alcance de cualquier persona, como los correos electrónicos, ya que se puede hacer uso de ingeniería social para obtener más información

#### **6.20. Acuerdos para el intercambio**

- a) Definir procedimientos y responsabilidades para el control y notificación de transmisiones, envíos y recepciones.
- b) Establecer procedimientos para garantizar la trazabilidad y el no repudio.
- c) Definir normas técnicas para el empaquetado y transmisión.
- d) Definir pautas para la identificación del prestador de servicio de correo.
- e) Establecer responsabilidades y obligaciones en caso de pérdida de datos.
- f) Utilizar un sistema para rotulado de la información clasificada.
- g) Conocer los términos y condiciones de las licencias de software privativo o suscripciones de software de código abierto bajo las cuales se utiliza el software.
- h) Conocer sobre la propiedad de la información y las condiciones de uso.
- i) Definir procedimientos técnicos para la grabación y lectura de la información y del software en el intercambio de información.

#### **6.21. Medios físicos en tránsito**

- a) Utilizar transporte confiable o servicios de mensajería.
- b) Establecer una lista de mensajería aprobada por la dirección
- c) Definir procedimientos para identificar los servicios de mensajería.
- d) Embalar de forma segura medios o información enviada a través de servicios de mensajería, siguiendo las especificaciones del proveedor o del fabricante.
- e) Adoptar controles especiales cuando sea necesario proteger información sensible, su divulgación y modificación.

#### **6.22. Mensajería electrónica**

- a) Establecer lineamientos para proteger los mensajes contra los accesos no autorizados, modificación o denegación de los servicios.
- b) Supervisar que la dirección y el transporte de mensajes sean correctos.
- c) Tomar en cuenta consideraciones legales como la de firmas electrónicas.
- d) Encriptar los contenidos y/o información sensibles que puedan enviarse por mensajería electrónica; utilizando firmas electrónicas reconocidas por el Estado Ecuatoriano u otras tecnologías evaluadas y aprobadas por la entidad o el Gobierno Nacional.
- e) Monitorear los mensajes de acuerdo al procedimiento que establezca la institución.

#### **6.23. Sistemas de información del negocio**

- a) Proteger o tener en cuenta las vulnerabilidades conocidas en los sistemas administrativos, financieros, y demás sistemas informáticos donde la información es compartida.
- b) Proteger y tener en cuenta las vulnerabilidades en los sistemas de comunicación del negocio como la grabación de las llamadas telefónicas.
- c) Establecer políticas y controles adecuados para gestionar la forma en que se comparte la información.
- d) Categorizar la información sensible y documentos clasificados.
- e) Implementar controles de acceso a la información como acceso a proyectos confidenciales.
- f) Categorizar al personal, contratistas y usuarios que tengan acceso a los sistemas informáticos y los sitios desde cuales pueden acceder.
- g) Identificar el estado de las cuentas de usuario.
- h) Verificar la retención y copias de respaldo de la información contenida en los sistemas informáticos.
- i) Establecer requisitos y disposiciones para los recursos de emergencia.

#### **6.24. Transacciones en línea**

- a) Definir procedimientos para el uso de certificados de firmas electrónicas por las partes implicadas en la transacción.
- b) Establecer procedimientos para garantizar todos los aspectos en la transacción como credenciales de usuario, confidencialidad de la transacción y privacidad de las partes.
- c) Cifrar o encriptar el canal de comunicaciones entre las partes involucradas (por ejemplo, utilizando SSL/TLS).
- d) Establecer protocolos seguros en la comunicación de las partes involucradas por ejemplo, utilizando SSL/TLS).
- e) Establecer procedimientos para que las transacciones se encuentren fuera del entorno de acceso público.
- f) Utilizar los servicios de una entidad certificadora confiable.

#### **6.25. Información disponible al público**

- a) Establecer controles para que la información disponible al público se encuentre conforme a la normativa vigente.
- b) Definir controles para que la información de entrada sea procesada completamente y de forma oportuna.
- c) Establecer procedimientos para que la información sensible sea protegida durante la recolección, procesamiento y almacenamiento.

#### **6.26. Registros de auditorías**

- a) Identificar el nombre de usuario.

- b) Registrar la fecha, hora y detalles de los eventos clave, como registro de inicio y registro de cierre.
- c) Registrar la terminal si es posible.
- d) Registrar los intentos aceptados y rechazados de acceso al sistema.
- e) Registrar los cambios de la configuración.
- f) Registrar el uso de privilegios.
- g) Registrar el uso de las aplicaciones y sistemas.
- h) Registrar los accesos y tipos de acceso.
- i) Registrar las direcciones y protocolos de red.
- j) Definir alarmas originadas por el sistema de control de acceso.
- k) Activación y desactivación de los sistemas de protección como antivirus y los sistemas de detección de intrusos (IDS).

#### **6.27. Monitoreo de uso del sistema**

- a) Registrar los accesos autorizados, incluyendo:
  - Identificación del ID de usuario;
  - Fecha y hora de eventos clave;
  - Tipos de evento;
  - Archivos a los que se han tenido acceso;
  - Programas y utilitarios utilizados;
- b) Monitorear las operaciones privilegiadas, como
  - Uso de cuentas privilegiadas;
  - Encendido y detección del sistema;
  - Acople y desacople de dispositivos de entrada;
- c) Monitorear intentos de acceso no autorizados, como:
  - Acciones de usuario fallidas o rechazadas;
  - Violación de la política de acceso y notificaciones de firewalls y gateways;
  - Alertas de los sistemas de detección de intrusos;
- d) Revisar alertas o fallas del sistema, como:
  - Alertas y/o mensajes de consola;
  - Excepciones de registro del sistema;
  - Alarmas de gestión de red;
  - Alarmas del sistema de control de acceso;
- e) Revisar cambios o intentos de cambio en la configuración y los controles de la seguridad del sistema.

#### **6.28. Protección del registro de la información**

- a) Proteger de alteraciones en todos los tipos de mensaje que se registren.
- b) Proteger archivos de registro que se editen o se eliminen.

- c) Precautelar la capacidad de almacenamiento que excede el archivo de registro.
- d) Realizar respaldos periódicos del registro del servicio.

#### **6.29. Registros del administrador y del operador**

- a) Incluir al registro, la hora en la que ocurrió el evento.
- b) Incluir al registro, información sobre el evento.
- c) Incluir al registro, la cuenta de administrador y operador que estuvo involucrado.
- d) Añadir al registro, los procesos que estuvieron implicados.

#### **6.30. Registro de fallas**

- a) Revisar los registros de fallas o errores del sistema.
- b) Revisar las medidas correctivas para garantizar que no se hayan vulnerado los controles.
- c) Asegurar que el registro de fallas esté habilitado.

#### **6.31 Sincronización de relojes**

- a) Sincronizar los relojes de los sistemas de procesamiento de información pertinentes con una fuente de tiempo exacta (ejemplo el tiempo coordinado universal o el tiempo estándar local). En lo posible, se deberá sincronizar los relojes en base a un protocolo o servicio de tiempo de red para mantener todos los equipos sincronizados.
- b) Verificar y corregir cualquier variación significativa de los relojes sobretodo en sistemas de procesamiento donde el tiempo es un factor clave.
- c) Garantizar que la marca de tiempo refleja la fecha/hora real considerando especificaciones locales (por ejemplo, el horario de Galápagos o de países en donde existen representación diplomáticas del país, turistas extranjeros, entre otros).
- d) Garantizar la configuración correcta de los relojes para la exactitud de los registros de auditoría o control de transacciones y evitar repudio de las mismas debido a aspectos del tiempo.

---

### **7. Control de Acceso**

#### **7.1. Política de control de acceso**

- a) Gestionar los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.
- b) Definir responsabilidades para identificar, gestionar y mantener perfiles de los custodios de información.

- c) Definir claramente los autorizadores de los permisos de acceso a la información.

## 7.2. Registro de usuarios

- a) Establecer un procedimiento formal, documentado y difundido, en el cual se evidencie detalladamente los pasos y responsables para:
- Definir el administrador de accesos que debe controlar los perfiles y roles;
  - Gestionar el documento de requerimiento de accesos de los usuarios tanto internos como externos, que contemple: el solicitante del requerimiento o iniciador del proceso, validación del requerimiento, autorizador del requerimiento, ejecutor del requerimiento, forma y medio de entrega del acceso al usuario (manteniendo confidencialidad);
  - Crear los accesos para los usuarios, para lo cual la institución debe generar convenios de confidencialidad y responsabilidad con el usuario solicitante; además, validar que el usuario tenga los documentos de ingreso con Recursos Humanos (o quien haga estas funciones) en orden y completos.
  - Modificar los accesos de los usuarios;
  - Eliminar los accesos de los usuarios;
  - Suspender temporalmente los accesos de los usuarios en caso de vacaciones, comisiones, licencias, es decir, permisos temporales;
  - Proporcionar accesos temporales a usuarios externos o terceros de acuerdo al tiempo de su permanencia y limitados según las actividades para las que fueron contratados y firmar un convenio de confidencialidad;
  - Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso; al igual que de cada usuario, disponer de los permisos de acceso que han sido asignados.

## 7.3. Gestión de privilegios

- a) Controlar la asignación de privilegios a través de un proceso formal de autorización.
- b) Mantener un cuadro de identificación de los usuarios y sus privilegios asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones.
- c) Evidenciar documentadamente que cada activo de información tecnológico tenga definido los niveles de acceso basados en perfiles y permisos, a fin de determinar que privilegios se deben asignar según las actividades de los usuarios y la necesidad de la institución y su función.

**7.4. Gestión de contraseñas para usuarios**

- a) Establecer un proceso formal para la asignación y cambio de contraseñas.

**7.5. Revisión de los derechos de acceso de los usuarios**

- a) Realizar las depuraciones respectivas de los accesos de los usuarios, determinando un período máximo de 30 días; en casos de presentar cambios estructurales, esta gestión deberá hacerse inmediatamente que se ejecute el cambio organizacional.
- b) Evidenciar los cambios sobre los derechos de acceso en archivos de log o registro de los sistemas, los cuales deben estar disponibles en caso que se requieran.

**7.6. Uso de contraseñas**

- a) Documentar, en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignada.
- b) Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta.
- c) Evitar contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables.
- d) Controlar el cambio periódico de contraseñas de los usuarios.
- e) Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información.

**7.7. Equipo de usuario desatendido**

- a) Implementar medidas para que, en un determinado tiempo (ej., no mayor a 10 minutos), si el usuario no está realizando ningún trabajo en el equipo, este se bloquee, y se desbloquee únicamente si el usuario ingresa nuevamente su clave.

**7.8. Política de puesto de trabajo despejado y pantalla limpia**

- a) El Oficial de Seguridad de la Información deberá gestionar actividades periódicas (una vez cada mes como mínimo) para la revisión al contenido de las pantallas de los equipos, con el fin de que no se encuentren iconos y accesos innecesarios, y carpetas y archivos que deben ubicarse en la carpeta de documentos del usuario.

- b) Mantener bajo llave la información sensible (cajas fuertes o gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina.
- c) Desconectar de la red, servicio o sistema, las computadoras personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren desatendidas. Por ejemplo, haciendo uso de protectores de pantalla con clave.
- d) Proteger los puntos de recepción de correo y fax cuando se encuentren desatendidas.
- e) Bloquear las copiatoras y disponer de un control de acceso especial para horario fuera de oficinas.
- f) Retirar información sensible una vez que ha sido impresa.
- g) Retirar información sensible, como las claves, de sus escritorios y pantallas.
- h) Retirar los dispositivos removibles una vez que se hayan dejado de utilizar.
- i) Cifrar los discos duros de los computadores personales (escritorio, portátiles, etc.) y otros dispositivos que se considere necesarios, de las máximas autoridades de la institución.

#### **7.9. Política de uso de los servicios de red**

- a) Levantar un registro de los servicios de red la institución.
- b) Identificar por cada servicio los grupos de usuarios que deben acceder.
- c) Definir los perfiles y roles para cada grupo de usuarios que tenga acceso a la red y sus servicios.
- d) Definir mecanismos de bloqueos para que sea restringido el acceso de equipos a la red.

#### **7.10. Autenticación de usuarios para conexiones externas**

- a) Generar mecanismos para asegurar la información transmitida por los canales de conexión remota, utilizando técnicas como encriptación de datos, implementación de redes privadas virtuales (VPN) y Servicio de Acceso Remoto (SAR).
- b) Realizar un mecanismo diferenciado para la autenticación de los usuarios que requieren conexiones remotas, que permita llevar control de registros (logs) y que tenga limitaciones de accesos en los segmentos de red.

#### **7.11. Identificación de los equipos en las redes**

- a) Identificar y documentar los equipos que se encuentran en las redes.
- b) Controlar que la comunicación solo sea permitida desde un equipo o lugar específico.
- c) Tener documentada la identificación de los equipos que están permitidos, según la red que le corresponda.

- d) Utilizar métodos para que la identificación del equipo esté en relación a la autenticación del usuario.

#### **7.12. Protección de los puertos de configuración y diagnóstico remoto**

- a) Establecer un procedimiento de soporte, en el cual se garantice que los puertos de diagnóstico y configuración sean sólo accesibles mediante un acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware/ software que requiere el acceso.
- b) Los puertos, servicios (ej., tftp) que no se requieren por necesidades de la institución, deberán ser eliminados o deshabilitados.

#### **7.13. Separación en las redes**

- a) Realizar una evaluación de riesgos para identificar los segmentos de red donde se encuentren los activos críticos para la institución
- b) Dividir las redes en dominios lógicos de red, dominios de red interna, dominios de red externa e inalámbrica.
- c) Documentar la segregación de red, identificando las direcciones IP que se encuentran en cada segmento de red.
- d) Configurar la puerta de enlace (gateway) para filtrar el tráfico entre dominios y bloquear el acceso no autorizado.
- e) Controlar los flujos de datos de red usando las capacidades de enrutamiento/conmutación (ej., listas de control de acceso).
- f) La separación de las redes debe ejecutarse en base a la clasificación de la información almacenada o procesada en la red, considerando que el objetivo es dar mayor protección a los activos de información críticos en función del riesgo que éstos podrían presentar.
- g) Separar redes inalámbricas procedentes de redes internas y privadas, para evitar el acceso a terceros y de usuarios externos a las redes privadas internas.

#### **7.14. Control de conexión a las redes**

- a) Restringir la capacidad de conexión de los usuarios, a través de puertas de enlace de red (gateway) que filtren el tráfico por medio de tablas o reglas predefinidas, conforme a los requerimientos de la institución.
- b) Aplicar restricciones considerando:
  - Mensajería
  - Transferencia de archivos
  - Acceso interactivo
  - Acceso a las aplicaciones
  - Horas del día y fechas de mayor carga

- c) Incorporar controles para restringir la capacidad de conexión de los usuarios a redes compartidas especialmente de los usuarios externos a la institución.

#### **7.15. Control del enrutamiento en la red**

- a) Configurar políticas de control de acceso para el enrutamiento en la red, basándose en los requerimientos de la institución.

Las puertas de enlace de la seguridad (gateway) se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes internas y externas, si se emplean tecnologías proxy y/o de traducción de direcciones de red.

Las instituciones que utilizan proxys y quienes definen las listas de control de acceso (LCA), deben estar conscientes de los riesgos en los mecanismos empleados, a fin de que no existan usuarios o grupos de usuarios con salida libre y sin control, en base a las políticas de la institución.

#### **7.16. Procedimiento de registro de inicio seguro**

- a) Autenticar usuarios autorizados, de acuerdo a la política de control de acceso de la institución, que deberá estar documentada, definida y socializada.
- b) Llevar un registro de definición para el uso de privilegios especiales del sistema.
- c) Llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema.
- d) Utilizar mecanismos como: uso de dominios de autenticación, servidores de control de acceso y directorios.
- e) Restringir el tiempo de conexión de los usuarios, considerando las necesidades de la institución.
- f) Controlar que no se muestren identificadores de aplicación ni de sistema, hasta que el proceso de registro de inicio se haya completado exitosamente.
- g) Evitar que se desplieguen mensajes de ayuda durante el procedimiento de registro de inicio de sesión.
- h) Validar la información de registro de inicio únicamente al terminar todos los datos de entrada, y en el caso que se presentara un error o se generara sentencias de error, el sistema no indique qué parte de los datos es correcta o incorrecta o emita mensajes propios de las características del sistema.
- i) Limitar la cantidad de intentos permitidos de registro de inicio de sesión; por ejemplo, tres intentos.
- j) Limitar el tiempo de dilación antes de permitir o rechazar más intentos adicionales del registro de inicio sin autorización específica

**7.17. Identificación y autenticación de usuarios**

- a) Rastrear utilizando los identificadores de usuario y evidenciar las actividades de las personas responsables de administraciones críticas de la institución.
- b) Usar como excepción, y solo por temas de necesidad de la institución, identificadores de usuarios para un grupo de usuarios o de trabajo específico, el cual debe estar definido y documentado.
- c) Las actividades de usuarios regulares no deben ser realizadas desde cuentas privilegiadas.
- d) Evitar el uso de usuarios genéricos.
- e) Utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas inteligentes, tokens o medios biométricos de autenticación.
- f) La identificación de usuario es única e intransferible, por lo que, debe estar registrado y evidenciado en la política de accesos que no se permite el uso de una identificación de usuario de otra persona, y el responsable de toda actividad realizada con este identificador responderá a cualquier acción realizada con éste.

**7.18. Sistema de gestión de contraseñas**

- a) Evidenciar en la política de accesos, la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible.
- b) Controlar el cambio de contraseña de los usuarios y del personal de tecnología y de los administradores de tecnología, en rangos de tiempo y complejidad.
- c) Forzar el cambio de contraseña en el primer registro de acceso o inicio de sesión.
- d) Generar un procedimiento formal para la administración y custodia de las contraseñas de acceso de administración e información crítica de la institución.
- e) Documentar el control de acceso para los usuarios temporales.
- f) Almacenar y transmitir las contraseñas en formatos protegidos (encriptados o codificados).

**7.19. Uso de las utilidades del sistema**

- a) Restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles de un sistema en base a las siguientes directrices:
  - uso de procedimientos de identificación, autenticación y autorización para programas utilitarios;
  - separación de los programas utilitarios del software de aplicaciones,
  - limitación del uso de programas utilitarios a la cantidad mínima viable de usuarios de confianza autorizados;
  - autorización del uso de programas utilitarios no estándares de la entidad;

- limitación del tiempo de uso de programa utilitarios;
- registro de todo uso de programas utilitarios;
- retiro o inhabilitación de todas los programas utilitarios innecesarios.

#### **7.20. Tiempo de inactividad de la sesión**

- a) Suspender las sesiones inactivas después de un periodo definido de inactividad sin consideración de lugar dispositivo de acceso.
- b) Parametrizar el tiempo de inactividad en los sistemas de procesamiento de información para suspender y cerrar sesiones.

#### **7.21. Limitación del tiempo de conexión**

- a) Utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.

#### **7.22. Control de acceso a las aplicaciones y a la información**

- a) Controlar el acceso de usuarios a la información y a las funciones del sistema de aplicación, de acuerdo con una política definida de control de acceso;
- b) Suministrar protección contra acceso no autorizado por un programa utilitario, software del sistema operativo, software malicioso o cualquier otro software que pueda anular o desviar los controles de seguridad del sistema;
- c) Evitar poner en riesgo otros sistemas con los que se comparten los recursos de información.

#### **7.23. Restricción de acceso a la información**

- a) Controlar el acceso a las funciones de los sistemas y aplicaciones.
- b) Definir mecanismos de control para los derechos de acceso de los usuarios, para lectura, escritura, eliminación y ejecución de información.
- c) Definir y documentar mecanismos de control para los derechos de acceso de otras aplicaciones.
- d) Generar mecanismos a fin de garantizar que los datos de salida de los sistemas de aplicación que manejan información sensible sólo contengan la información pertinente y que se envíe únicamente a terminales o sitios autorizados.
- e) Generar revisiones periódicas de las salidas de los sistemas de aplicación para garantizar el retiro de la información redundante.

#### **7.24. Aislamiento de sistemas sensibles**

- a) Identificar y documentar los sistemas sensibles y al responsable de la aplicación.
- b) Identificar y registrar los riesgos, cuando una aplicación se ejecuta en un entorno compartido.
- c) Identificar y registrar aplicaciones sensibles que se encuentra compartiendo recursos.
- d) Las aplicaciones sensibles, por su criticidad para la institución, deberán ejecutarse en un computador dedicado, únicamente compartir recursos con sistemas de aplicación confiables, o utilizar métodos físicos o lógicos de aislamiento.

#### **7.25. Computación y comunicaciones móviles**

- a) Evitar exposición de equipos portátiles en sitios inseguros, públicos y de alto riesgo.
- b) La información sensible, de alta criticidad o confidencial, debe estar en una partición específica del disco del equipo portátil, y resguardada bajo métodos de cifrado.
- c) En la política para uso de equipos portátiles y comunicaciones móviles de la institución, deberá definir rangos de tiempo máximo que el equipo puede permanecer sin conexión a la red de la institución, a fin de que este actualice el antivirus y las políticas aplicadas por la institución.
- d) En el proceso de respaldos de la institución, debe estar considerado específicamente los documentos definidos como críticos, sensibles o confidenciales de las diferentes áreas; además, en el proceso de respaldo del equipo portátil deberá definirse el responsable y procedimiento de acceso a esta información.
- e) Dentro de la institución el equipo portátil deberá estar asegurado con medios físicos, mediante el uso de candados.
- f) El personal que utiliza computadores portátiles y equipos móviles, deberá estar alerta de los riesgos adicionales que se originan y los controles que se deberán implementar.

#### **7.26. Trabajo remoto**

- a) La UAFE podrá autorizar la modalidad de trabajo remoto en circunstancias específicas, siempre que en la institución se apliquen las disposiciones de seguridad y los controles establecidos, cumpliendo con la política de seguridad de la información.
- b) El funcionario deberá observar la seguridad física de la edificación y del entorno local existente en el sitio de trabajo remoto.
- c) Deberá evitarse la conexión a redes inalámbricas que no presten la seguridad de acceso y autenticación adecuados.
- d) No se permite el uso de equipo de propiedad privada que no esté bajo el control y monitoreo de la institución.

- e) Deberá definirse el trabajo que se permite realizar, las horas laborables, la confidencialidad de la información que se conserva y los sistemas y servicios internos para los cuales el trabajador tiene acceso autorizado.
- f) Deberá considerarse la protección de antivirus y reglas del Firewall
- g) Deberán estar documentadas las reglas y directrices sobre el acceso de familiares y visitantes al equipo y a la información.
- h) La institución deberá observar la disposición de una póliza de seguros para esos equipos.
- i) Determinar procesos de monitoreo y auditoría de la seguridad del trabajo remoto que se realice.
- j) Permitir al personal realizar trabajo remoto empleando tecnologías de comunicaciones cuando requiere hacerlo desde un lugar fijo fuera de su institución

---

## **8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información**

### **8.1. Análisis y especificaciones de los requerimientos de seguridad**

- a) Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones, etc.
- b) Definir los controles apropiados, tanto automatizados como manuales. En esta definición deben participar personal del requerimiento funcional y personal técnico que trabajarán en el sistema.  
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 por falla o falta de seguridad.
- c) Si se adquieren productos, los contratos con el proveedor deben contemplar los requisitos de la seguridad identificados.
- d) Cuando se proporciona funcionalidad adicional y ello causa un riesgo de la seguridad, tal funcionalidad se debe inhabilitar o cambiar.

### **8.2. Validación de datos de entrada**

- a) Especificar y utilizar controles que aseguren la validez de los datos ingresados, en el punto de entrada de los mismos, controlando también parámetros de los sistemas. (ej: dirección IP del servidor).
- b) Verificar los datos de entrada con controles que permitan la negación de ingreso de datos: duales, valores fuera de rango, caracteres no válidos, datos incompletos o ausentes, datos de controles inconsistentes o no autorizados, la secuencia de los datos, formatos incorrectos, inyección de código, etc.
- c) Definir el estándar de respuesta ante errores de validación.

- d) Definir convalidaciones para probar la credibilidad de los datos de entrada.
- e) Crear un registro de las actividades implicadas en el proceso de entrada de datos.

### **8.3. Control de procesamiento interno**

- a) Incorporar controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.
- b) Utilizar controles de sesión en los sistemas.
- c) Utilizar funciones de agregar, modificar y borrar para implementar los cambios en los datos. El borrado a través de los sistemas será siempre un borrado lógico de los datos.
- d) Crear registros de auditoría, al insertar y actualizar datos; y, si se requiere según el sistema, se mantendrá el registro (logs) de consultas de datos.
- e) Incorporar en los sistemas, validaciones necesarias para prevenir la ejecución de programas fuera de secuencia, en orden erróneo o de ejecución después de una falla.
- f) Crear el procedimiento y/o herramientas para la revisión periódica de los registros de auditoría para detectar cualquier anomalía en la ejecución de las transacciones.
- g) Identificar, crear y utilizar programas para la recuperación de datos después de fallas, con el fin de garantizar el procesamiento correcto de los datos.
- h) Utilizar controles para mantener integridad de registros y archivos.
- i) Utilizar controles para protección contra ataques por desbordamiento/exceso en el buffer.
- j) Definir y ejecutar periódicamente, procedimientos de recuperación de sistemas, que verifiquen la ejecución de los sistemas en caso de una falla o desastre, esto estará a cargo del administrador técnico de la aplicación o sistema.
- k) Definir los procedimientos que aseguren el orden correcto de ejecución de los sistemas, la finalización programada en caso de falla y la detención de las actividades de procesamiento, hasta que el problema sea resuelto.

### **8.4. Integridad del mensaje**

- a) Cuando una aplicación tenga previsto el envío de mensajes que contengan información reservada o confidencial, se implementarán los controles criptográficos determinados en el punto "8.6 Política sobre uso de controles criptográficos".

### **8.5. Validación de datos de salidas**

- a) Incorporar el control de conciliación de datos, para asegurar el procesamiento de todos los datos.

- b) Suministrar información para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.
- c) Desarrollar procedimientos para responder a las pruebas de validación de salidas.
- d) Crear un registro de las actividades del proceso de validación de la salida de datos.
- e) Generar protocolos de pruebas y los casos de pruebas para la validación de los datos de salida.

### **8.6. Política sobre el uso de controles criptográficos**

- a) Identificar el nivel requerido de protección de datos que se almacenará en el sistema, considerando: el tipo, fortaleza y calidad del algoritmo de cifrado (encriptación) requerido.
- b) Utilizar controles criptográficos para la protección de claves de acceso a: sistemas, datos y servicios. Las claves deberán ser almacenadas de manera codificada, cifrada (encriptada) en la base de datos y/o en archivos de parámetros.
- c) Desarrollar procedimientos de administración de claves, de recuperación de información cifrada en caso de pérdida, de compromiso o daño de las claves y de reemplazo de claves de cifrado.
- d) Utilizar controles de cifrado (criptográficos) para la transmisión de información clasificada, fuera del ámbito de la institución.
- e) Utilizar controles de cifrado (criptográficos) para la protección de la información sensible transportada por medios móviles o removibles, por dispositivos especiales, o a través de los medios de comunicación.
- f) Definir las normas de controles de cifrado (criptográficos) que se adoptarán, para la implementación eficaz en toda la institución; establecer la solución a usar para cada proceso del negocio.
- g) Los responsables del área de Tecnologías de la Información propondrán la siguiente asignación de funciones:
  - Implementación de la Política de Controles
  - Administración de claves: gestión de claves, incluyendo su generación
- h) Se debe garantizar:
  - Confidencialidad: uso de cifrado (encriptación) de la información para proteger información sensible o crítica, bien sea almacenada o transmitida
  - Integridad / autenticidad: uso de firmas electrónicas o códigos de autenticación de mensajes para proteger la autenticidad e integridad de información sensible o crítica transmitida o almacenada
  - No-repudio: uso de técnicas de cifrado (criptográficas) para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción.
- i) Definir los algoritmos de cifrado (encriptación) que se utilizarán en toda la institución, dependiendo del tipo de control a aplicar, el

propósito y el proceso del negocio. Esta definición debe ser periódicamente revisada y actualizada.

- j) Uso de firma electrónica:
  - Utilizar certificados electrónicos de Entidad de Certificación de Información reconocidas por el Estado Ecuatoriano para la firma de cualquier tipo de documento, mensaje de dato, transacción que se procese electrónicamente o para comunicaciones entre sistemas, aplicaciones y medios físicos.
  - Utilizar los certificados electrónicos emitidos bajo estándares por las Entidades de Certificación de Información, las cuales deben ser instituciones u organizaciones reconocidas, con controles y procedimientos idóneos establecidos para proporcionar el grado requerido de confianza.
  - Uso de los certificados electrónicos según el ámbito para la cual fue generado.

### 8.7. Gestión de claves

- a) Protección de claves cifradas (criptográficas):
  - Implementar un sistema de administración de claves cifradas (criptográficas) para respaldar la utilización por parte de la institución, de los dos tipos de técnicas criptográficas: técnicas de clave secreta (criptografía simétrica) y técnicas de clave pública (criptografía asimétrica).
  - Proteger todas las claves contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.
  - Proporcionar una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.
  - Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
  - Habilitar en los sistemas, la generación de claves en la creación de usuarios. Se generará la primera clave la cual deberá obligatoriamente cambiar el propio usuario la primera vez que ingresa al sistema.
  - Generar y obtener certificados de claves públicas.
  - Distribuir la primera clave a los usuarios, incluyendo la forma de activar y confirmar la recepción de la clave. Luego, a través de un correo electrónico recibirá un acceso al sistema, el cual validará la entrega de la clave y la obligatoriedad de cambiar dicha clave.
  - Almacenar las claves cifradas (encriptadas).
  - Incorporar funcionalidad para cambiar o actualizar las claves, incluyendo reglas sobre cuándo cambiarlas, cómo hacerlo y la forma en que los usuarios autorizados tendrán acceso a ellas.
  - Incorporar funcionalidad para tratar las claves perdidas. Bajo pedido del usuario que pierde una clave se generará una nueva, la entrega será a través del procedimiento definido para la entrega de la primera clave.

- Permitir revocar las claves, incluyendo la forma de retirarlas o desactivarlas cuando las claves se han puesto en peligro o cuando un usuario se retira de la institución.
  - Incorporar funcionalidad para recuperar claves perdidas o corruptas como parte de la gestión de continuidad de los servicios informáticos.
  - Permitir archivar claves para información archivada o con copia de respaldo.
  - Permitir la destrucción de claves que se dejen de utilizar.
  - Registrar y auditar las actividades relacionadas con la gestión de claves.
- b) Normas, Procedimientos y Métodos:
- Redactar las normas y procedimientos necesarios para generar claves para diferentes sistemas criptográficos y diferentes aplicaciones, incluyendo fechas de inicio y caducidad de vigencia de las claves.
  - Redactar las normas y procedimientos necesarios para generar y obtener certificados de clave pública de manera segura.
  - Redactar las normas y procedimientos para distribuir las claves de forma segura a los usuarios, incluyendo información sobre cómo deben activarse cuándo se reciban las mismas.
  - Redactar las normas y procedimientos para almacenar claves, incluyendo la forma de acceso a las mismas, por parte de los usuarios autorizados.
  - Redactar las normas y procedimientos para cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
  - Redactar las normas y procedimientos para revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas.
  - Redactar las normas y procedimientos para archivar claves; por ejemplo, para la información archivada o resguardada.
  - Redactar las normas y procedimientos para destruir claves.
  - Redactar las normas y procedimientos para registrar y auditar las actividades relativas a la administración de claves.

### **8.8. Control del software operativo**

- a) Definir y aplicar procesos de control de cambios para la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.
- b) Definir el proceso de paso a producción para cada sistema.
- c) Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
- d) Asignar un responsable de la implantación de cambios por sistema (no podrá ser personal que pertenezca al área de desarrollo o mantenimiento), quien tendrá como funciones principales:
  - Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.

- Asegurar que los aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
- Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del área encargada del testeo y del usuario final.
- Rechazar la implementación en caso de encontrar defectos
- e) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones para el paso a producción, el informe de pruebas previas y el informe de paso a producción.
- f) Disponer del informe de paso a producción, el cual contendrá información de todos los cambios a realizar y el plan de contingencia.
- g) Guardar o instalar únicamente los ejecutables y cualquier elemento necesario para la ejecución de un software en el ambiente de producción.
- h) Implementar el ensayo en el ambiente de pruebas. Este ambiente debe ser similar al ambiente de producción. El ensayo será en base al informe de paso a producción. Se ejecutarán todas las acciones definidas y se realizarán pruebas sobre capacidad de uso, seguridad, efectos en otros sistemas y facilidad para el usuario.
- i) Llevar un registro de auditoría de las actualizaciones realizadas.
- j) Retener las versiones previas del sistema, como medida de contingencia.
- k) Denegar permisos de modificación a los desarrolladores, sobre los programas fuentes bajo su custodia.
- l) Usar un sistema de control de configuración para mantener el control del software instalado, así como de la documentación del sistema.
- m) Entregar acceso físico o lógico al ambiente producción únicamente para propósitos de soporte, cuando sea necesario y con aprobación del responsable del área de Tecnologías de la Información, esto se realizará tanto para usuarios internos de la dirección como para proveedores.
- n) Monitorear las actividades de soporte realizadas sobre el ambiente de producción.

#### **8.9. Protección de los datos de prueba del sistema**

- a) Identificar por cada sistema, los datos que pueden ser copiados de un ambiente de producción a un ambiente de pruebas.
- b) Efectuar pruebas de los sistemas en el ambiente de pruebas, sobre datos extraídos del ambiente de producción.
- c) Solicitar autorización formal para realizar una copia de la base de datos de producción como base de datos de prueba.
- d) Personalizar los datos en el ambiente de pruebas, eliminando las contraseñas de producción y generando nuevas para pruebas.
- e) Identificar los datos críticos que deberán ser modificados o eliminados del ambiente de pruebas.

- f) Aplicar los mismos procedimientos de control de acceso que existen en la base de producción.
- g) Eliminar inmediatamente, una vez completadas las pruebas, la información de producción utilizada.
- h) Registrar la copia y la utilización de la información para futuras auditorías.
- i) Controlar que la modificación, actualización o eliminación de los datos operativos (de producción) serán realizados a través de los sistemas que procesan esos datos, y de acuerdo al esquema de control de accesos implementado en los mismos.
- j) Se considerarán como excepciones, los casos en que se requiera realizar modificaciones directamente sobre la base de datos. El OSI definirá los procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:
  - Se generará una solicitud formal para la realización de la modificación o actualización del dato. No se aceptará eliminación de datos bajo ninguna circunstancia.
  - El Propietario de la Información afectada y el OSI aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.
  - Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, la cuales estarán sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.
  - Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo. En el caso de que esta función no pueda ser separada del área de Desarrollo, se aplicarán controles adicionales de acuerdo a la separación de funciones.
  - Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el OSI.

#### **8.10. Control de acceso al código fuente de los programas**

- a) Asignar a un Administrador de programas fuentes, quien tendrá en custodia los programas fuentes y deberá:
  - Utilizar un manejador de versiones para los códigos fuentes, proporcionar permisos de acceso a los desarrolladores bajo autorizaciones.
  - Proveer al área de Desarrollo 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, autorizador, versión, fecha de última modificación y fecha/hora de compilación y estado (en modificación o en producción).
  - Verificar que el autorizador de 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, sin un manejador de versiones.
- b) Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
- c) Establecer que el responsable de implantación en producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.
- d) Desarrollar un procedimiento que garantice que cuando se migre a producción el módulo fuente, de preferencia se cree el código ejecutable correspondiente de forma automática de preferencia.
- e) Evitar que la función de Administrador de programas fuentes, sea ejercida por personal que pertenezca al área de desarrollo y/o mantenimiento.
- f) Prohibir la guarda de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.
- g) 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.
- h) Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos como respaldos de información.
- i) Cuando sea posible, las bibliotecas fuente de programas no se deberán mantener en los sistemas operativos.
- j) El código fuente de programas y las bibliotecas fuente de programas se deberán gestionar de acuerdo con los procedimientos establecidos.
- k) El personal de soporte no debe tener acceso al código fuente de programas.
- l) La actualización del código fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se deberá efectuar después de recibir la autorización apropiada.
- m) Conservar un registro para auditoría de todos los accesos al código fuente de programas.
- n) El mantenimiento y el copiado del código fuente de programas deberán estar sujetos a un procedimiento estricto de control de cambios.

#### **8.11. Procedimiento de control de cambios**

- a) Verificar que los cambios sean propuestos por usuarios autorizados y se respete los términos y condiciones que surjan de la licencia de uso, en caso de existir.

- b) Elaborar el informe de paso de pruebas a producción, que deberá contener el detalle de los cambios y acciones a ejecutar, tanto de software, bases de datos y hardware:
  - Archivos a modificar;
  - Script de base de datos a ejecutar en la secuencia correcta de ejecución;
  - Script de inicialización de datos;
  - Creación de directorios;
  - Script de creación de tareas periódicas, en caso de ser necesario;
  - Plan de contingencia;
  - Protocolo de pruebas de verificación el cambio;
  - Definir el punto de no retorno;
  - Definir las condiciones para determinar la restauración al estado anterior.
- c) Obtener aprobación formal por parte del responsable del área de Tecnologías de la Información para las tareas detalladas, antes de comenzar las tareas.
- d) Mantener un registro de los niveles de autorización acordados.
- e) Implementar funcionalidades para que se pueda solicitar la autorización del propietario de la información (e.g., información personal), cuando se hagan cambios a sistemas de procesamiento de la misma.
- f) Notificar a los usuarios del sistema sobre el cambio a realizar. Se enviará una notificación para informar sobre el tiempo que durará la ejecución del cambio y para informar cuando se haya terminado la ejecución del cambio.
- g) Abrir ventanas de mantenimiento con una duración definida, en la cual se contemple las acciones del cambio, pruebas y configuraciones.
- h) Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
- i) Solicitar la revisión del OSi para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
- j) Efectuar las actividades relativas al cambio en el ambiente de pruebas.
- k) Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.
- l) Actualizar la documentación para cada cambio implementado, tanto en los manuales de usuario como en la documentación operativa.
- m) Mantener un control de versiones para todas las actualizaciones de software.
- n) Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.
- o) Definir si los cambios a realizar tienen impacto sobre la continuidad del servicio. Si un cambio implica mucha funcionalidad o impacto al software base o infraestructura, se deberá realizar un procedimiento más complejo de cambio, para que se apruebe con un plan de contingencia y se identifiquen los riesgos posibles.

**8.12. Revisión técnica de las aplicaciones después de los cambios el sistema operativo**

- a) Revisar los procedimientos 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) Probar que los cambios realizados retornen la funcionalidad esperada.
- d) Realizar las pruebas inmediatamente después de realizar el cambio y durante la ventana de mantenimiento definida para el cambio.
- e) Disponer de un protocolo de pruebas a realizar.
- f) Entregar un informe de las pruebas realizadas.
- g) Identificar si existen problemas con los cambios, para aplicar el plan de contingencia o realizar el retorno al estado anterior al cambio.

**8.13. Restricción del cambio de paquetes de software**

- a) Disponer de la autorización del Responsable del área de Tecnologías de la Información que apruebe el cambio.
- b) Analizar los términos y condiciones de la licencia, si es del caso, a fin de determinar si las modificaciones se encuentran autorizadas.
- c) Determinar la conveniencia de que la modificación sea efectuada por la institución, por el proveedor o por un tercero, y evaluar el impacto.
- d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.
- e) Conservar el software original que se va a cambiar y los cambios se deberán aplicar a una copia claramente identificada.
- f) Definir un proceso de gestión de las actualizaciones del software para asegurarse de que los parches más actualizados aprobados y las actualizaciones de las aplicaciones están instalados en todo el software autorizado.
- g) Probar y documentar en su totalidad todos los cambios, de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software.

**8.14. Fuga de información**

- a) Explorar los medios y comunicaciones de salida para determinar la información oculta.
- b) Garantizar que un tercero no pueda deducir, extraer información de las comunicaciones, sistemas de modulación o de enmascaramiento, a partir de un comportamiento específico.
- c) Adquirir o desarrollar programas acreditados o productos ya evaluados.

- d) Realizar un monitoreo regular de las actividades del personal y del sistema.
- e) Realizar un monitoreo del uso de los recursos en los sistemas de computador y transmisión de datos por la red.
- f) Restringir el envío de información a correos externos no institucionales.
- g) Prevenir y restringir el acceso no autorizado a la red.
- h) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
- i) Controlar el acceso y las modificaciones al código instalado.
- j) Utilizar herramientas para la protección contra la infección del software con código malicioso.

#### **8.15. Desarrollo de software contratado externamente**

- a) Definir acuerdos de licencias, acuerdos de uso, propiedad de código y derechos conferidos.
- b) Definir los requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
- c) Definir procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
- d) Verificar el cumplimiento de las condiciones de seguridad requeridas.
- e) Definir acuerdos de custodia de los fuentes del software o convenios de fideicomiso (y cualquier otra información requerida) en caso de quiebra de la tercera parte.
- f) Realizar pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

#### **8.16. Control de las vulnerabilidades técnicas**

- a) Disponer de un inventario completo y actual de los activos de software. El inventario servirá para dar soporte a la gestión de la vulnerabilidad técnica e incluye los siguientes datos: vendedor del software, números de versión, estado actual de despliegue y las personas de la institución responsables del software.
- b) Definir e instaurar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica, incluyendo el monitoreo de la vulnerabilidad, la evaluación de riesgos de la vulnerabilidad, el uso de parches, el rastreo de activos y todas las responsabilidades de coordinación requeridas.
- c) Identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y para mantener la concienciación sobre ellas para el software y otras tecnologías, con base en la lista de inventario de activos.

- d) Actualizar los recursos de información en función de los cambios en el inventario o cuando se encuentren recursos nuevos o útiles.
- e) Definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales pertinentes.
- f) Identificar los riesgos asociados a una vulnerabilidad potencial y las acciones que se han de tomar; tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y/o la aplicación de otros controles.
- g) Definir la urgencia y las acciones a tomar para tratar la vulnerabilidad técnica identificada, se realizará conforme a los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información.
- h) Evaluar los riesgos asociados con la instalación de un parche para cubrir vulnerabilidades. Los riesgos impuestos por la vulnerabilidad se deberán comparar con los riesgos de instalar el parche.
- i) Probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables. Estas pruebas se realizarán en un ambiente similar al de producción.
- j) Apagar los servicios o capacidades relacionadas con la vulnerabilidad.
- k) Adaptar o agregar controles de acceso; por ejemplo, cortafuegos (firewalls), en las fronteras de la red.
- l) Aumentar el monitoreo para detectar o prevenir los ataques reales.
- m) Crear conciencia en los desarrolladores sobre la vulnerabilidad.
- n) Conservar un registro para auditoría de todos los procedimientos efectuados.
- o) Monitorear y evaluar a intervalos regulares las vulnerabilidades técnicas, para garantizar eficacia y eficiencia.
- p) Tratar primero los sistemas con alto riesgo.

---

## 9. Gestión de los Incidentes de la Seguridad de la Información

### 9.1. Reporte sobre los eventos de seguridad de la información

- a) Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información.
- b) Establecer un punto de contacto (OSI) para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto sea conocido en toda la institución, siempre esté disponible y puede suministrar respuesta oportuna y adecuada. Todos los empleados, contratistas y usuarios contratados por los proveedores deberán tener conciencia de su

- responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible.
- c) Cuando un incidente se produzca, el funcionario en turno responsable del equipo o sistema afectado, debe realizar las siguientes acciones en su orden:
- Identificar el incidente
  - Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente.
  - Notificar al OSI de la institución.
  - Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad.
  - Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultánea.
  - Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas.
  - Escalar el incidente en el caso que el funcionario en turno no pueda solucionarlo, el escalamiento deberá ser registrado en la bitácora de escalamiento de incidentes. El funcionario en turno debe escalar el incidente a su jefe inmediato, en el caso en el que el funcionario no tuviere un jefe al cual escalarlo, este debe solicitar soporte al proveedor del equipo o sistema afectado.
  - Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente.
  - Resolver y restaurar el servicio afectado por el incidente debido a la para de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes.
  - Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a "Resuelto". Confirmar con el funcionario en turno, responsable del equipo o del sistema de que el incidente ha sido resuelto.

## 9.2. Reporte sobre las debilidades en la seguridad

- a) Todos los empleados, contratistas y usuarios de terceras partes deberán informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberán ser fáciles, accesibles y disponibles. Se les debe informar a ellos que, en ninguna circunstancia, deberán intentar probar una debilidad sospechada.
- b) Cuando un empleado, contratista o usuario contratado por un proveedor detecte una vulnerabilidad o debilidad en un equipo, sistema o servicio deberá ejecutar las siguientes acciones:
- Notificar a su jefe inmediato y este al OSI de la debilidad o vulnerabilidad detectada.

- Registrar la fecha, hora, apellidos y nombres del funcionario que detectó la debilidad o vulnerabilidad, descripción de la debilidad, descripción de posibles incidentes de seguridad que pudieran ocurrir producto de esta debilidad. El responsable de llevar este reporte denominado "Reporte de vulnerabilidades o debilidades de la seguridad de la información" es el OSI.
- Nunca, por razón alguna, deberá intentar probar la debilidad o vulnerabilidad detectada en la seguridad. El ensayo de las vulnerabilidades se podría interpretar como un posible uso inadecuado del sistema, equipo o servicio y también podría causar daño al sistema o servicio de información y eventualmente podría recaer en una responsabilidad legal.
- El OSI deberá tomar las medidas pertinentes para prevenir o eliminar la vulnerabilidad o debilidad detectada.

### **9.3. Responsabilidades y procedimientos**

- a) Además de la bitácora de registro de incidentes y el reporte de vulnerabilidades de la seguridad de la información, el monitoreo de los sistemas, las alertas y las vulnerabilidades, se debería establecer y ejecutar un procedimiento para la gestión de incidentes.
- b) Identificar y clasificar los diferentes tipos de incidentes de seguridad de la información.
- c) Identificar y analizar las posibles causas de un incidente producido.
- d) Planificar e implementar acciones correctivas para evitar la recurrencia del incidente
- e) Notificar a todos los funcionarios afectados por el incidente de la restauración del equipo, sistema o servicio afectado, una vez esté solucionado el incidente.
- f) El OSI, emitirá un reporte a los jefes de las áreas afectadas por el incidente.
- g) Recolectar y asegurar pistas de auditoría y toda la evidencia relacionada con el incidente.

### **9.4. Aprendizaje debido a los incidentes de seguridad de la información**

- a) La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debe utilizar para identificar los incidentes recurrentes o de alto impacto.
- b) Determinar el número de incidentes por tipo, el número de incidentes graves, el tiempo medio de resolución de incidentes.
- c) Determinar el costo promedio por incidente.
- d) Determinar el número de incidentes recurrentes.
- e) Determinar la frecuencia de un incidente recurrente.

### **9.5. Recolección de evidencias**

- a) Desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la institución.
- b) Asegurar que los sistemas de información cumplan con las normas legales para la producción de evidencia, para lograr la admisibilidad, calidad y cabalidad de la misma.
- c) Para lograr el peso de la evidencia, se debe demostrar la calidad y cabalidad de los controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante un rastreo sólido de la evidencia. En general, dicho rastreo sólido se puede establecer en las siguientes condiciones:
  - Se deberán tomar duplicados o copias de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigos; y, el medio y el registro originales se deberán conservar intactos y de forma segura;
  - Se debe proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debe estar supervisado por personal de confianza y se debe registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

#### 9.6. **Recolección de evidencias**

- a) Desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la institución.
- b) Asegurar que los sistemas de información cumplan con las normas legales para la producción de evidencia, para lograr la admisibilidad, calidad y cabalidad de la misma.
- c) Para lograr el peso de la evidencia, se debe demostrar la calidad y cabalidad de los controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante un rastreo sólido de la evidencia. En general, dicho rastreo sólido se puede establecer en las siguientes condiciones:
  - Se deberán tomar duplicados o copias de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigos; y, el medio y el registro originales se deberán conservar intactos y de forma segura;
  - Se debe proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debe estar supervisado por personal de confianza y se debe registrar la información sobre

cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

---

## **10. Gestión de la Continuidad del Negocio**

### **10.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio**

- a) El Responsable del área de Tecnologías de la Información o su similar será designado como coordinador de continuidad de los servicios informáticos, que se encargará de supervisar el proceso de elaboración e implantación del plan de continuidad, así como de la seguridad del personal.
- b) Identificar los activos involucrados en los procesos críticos de los servicios informáticos, así como de las actividades que se deben realizar.
- c) Elaborar la política de continuidad de los servicios informáticos determinando los objetivos y el alcance del plan, así como las funciones y responsabilidades; un documento que establezca a alto nivel los objetivos, el alcance y las responsabilidades en la gestión de la continuidad.
- d) Garantizar la continuidad incorporando los procesos generados en la estructura de la institución.

### **10.2. Continuidad del negocio y evaluación de riesgos**

- a) Definir los procesos y actividades de los servicios y aplicaciones,
- b) Entender las complejidades e interrelaciones existentes entre equipamiento, personas, tareas, departamentos, mecanismos de comunicación y relaciones con proveedores externos, los cuales pueden prestar servicios críticos que deben ser considerados.
- c) Identificar y valorar el impacto de las interrupciones de los procesos, aplicaciones y servicios de los servicios informáticos, para cuantificar y calificar los impactos y saber sus efectos.
- d) Identificar el tiempo máximo de interrupción permitida para cada servicio o aplicación crítica; por ejemplo, 30 minutos, una hora o un día.
- e) Analizar los riesgos, identificando las amenazas sobre los activos y su probabilidad de ocurrencia.
- f) Analizar las vulnerabilidades asociadas a cada activo y el impacto que puedan provocar sobre la disponibilidad.
- g) Obtener un mapa de riesgos que permita identificar y priorizar aquellos que pueden provocar una paralización de las actividades de la institución.
- h) Crear una estrategia de gestión de control de riesgos y el plan de acción.

### **10.3. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información**

- a) Definir los equipos para ejecución del plan, donde se destacan las funciones claves que serán realizadas por los responsables:
  - Responsables de respuestas a incidentes: analizan el impacto del incidente;
  - Logística: responsable de reunir todos los medios para ayudar a la puesta en operación de las actividades;
  - Recuperación: puesta en servicio de la infraestructura.
- b) Desarrollar los procedimientos indicando el objetivo y el alcance, considerando las actividades y los tiempos de recuperación.
- c) Difundir y capacitar al personal responsable en los conceptos que contemplan la continuidad de los servicios informáticos.
- d) Definir las Estrategias:
  - Seleccionar los sitios alternos y de almacenamiento externo;
  - Duplicado de los registros tanto físicos como electrónicos;
  - Incorporar RAID en los discos de los servidores;
  - Duplicar el suministro eléctrico;
  - Estrategia de reinicio de las actividades;
  - Contratos de mantenimiento preventivo y correctivo;
  - Estrategia adecuada de respaldos;
  - Seguros para los activos;
  - Métodos, procedimientos y procesos para la recuperación de los servicios.

### **10.4. Estructura para la planificación de la continuidad del negocio**

- a) Mantener los documentos de los procesos actualizados, utilizando la Gestión de Cambios.
- b) Crear planes de respuesta a los incidentes.
- c) Definir los calendarios de pruebas e informes.
- d) Definir los acuerdos de niveles de servicios internos y con proveedores.
- e) Definir los contratos para servicios de recuperación, si fuera el caso.
- f) Definir las condiciones para activar los planes que describen el proceso a seguir antes de activar cada plan, así como sus responsabilidades.
- g) Describir los procedimientos de respaldo para desplazar las actividades esenciales de los servicios informáticos o los servicios de soporte a lugares temporales alternos, y para devolver la operatividad de los procesos en los plazos establecidos.
- h) Describir los procedimientos de reanudación con las acciones a realizar para que las operaciones de los equipos y servicios vuelvan a la normalidad.

- i) Definir los activos y recursos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación de los servicios.
- j) Distribuir la política, estrategias, procesos y planes generados.

#### **10.5. Pruebas, mantenimiento y revisión de los planes de continuidad del negocio**

- a) Evaluar la capacidad de respuesta ante desastres verificando los tiempos de respuesta, validez de los procedimientos y capacidad de los responsables. Los resultados obtenidos permitirá actualizar y mantener los planes establecidos.
- b) Realizar pruebas de:
  - Validez: revisar y discutir el plan;
  - Simulación: escenario que permitirá verificar el plan de continuidad;
  - Actividades críticas: pruebas en un entorno controlado sin poner en peligro la operación de los servicios informáticos;
  - Completa: interrupción real y aplicación del plan de continuidad.
- c) Realizar auditorías tanto internas como externas, identificando el tipo y alcance de la auditoría a realizar, se entregará un plan de medidas correctivas para llevar a cabo las recomendaciones acordadas.
- d) Ejecutar auto-evaluaciones del plan de continuidad, estrategias y procesos generados.

---

### **11. Cumplimiento**

#### **11.1. Identificación de la legislación aplicable**

- a) Inventariar todas las normas legales, estatutarias, reglamentarias y contractuales pertinentes para cada programa de software, servicio informático y en general todo activo de información que utiliza la institución.
- b) Organizar para cada activo de información las normas legales, estatutarias, reglamentarias y contractuales pertinentes.
- c) Considerar las normas y leyes más generales relacionadas a la gestión de los datos e información electrónica en el gobierno. A saber:
  - Constitución de la República del Ecuador
  - Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
  - Ley Orgánica de Transparencia y Acceso a la Información Pública
  - Ley del Sistema Nacional de Registro de Datos Públicos

- Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva
- Ley Orgánica y Normas de Control de la Contraloría General del Estado
- Leyes y normas de control del sistema financiero
- Leyes y normas de control de empresas públicas
- Ley del Sistema Nacional de Archivos
- Decreto Ejecutivo No. 1014 sobre el uso de Software Libre en la Administración Pública
- Decreto Ejecutivo No. 1384 sobre Interoperabilidad Gubernamental en la Administración Pública
- Otras normas cuya materia trate sobre la gestión de los activos de información en las entidades de la Administración Pública

#### **11.2. Derechos de Propiedad Intelectual**

- a) Adquirir software únicamente a proveedores reconocidos para garantizar que no se violen derechos de propiedad intelectual. Si el Software es Libre Open Source se considerará los términos de las licencias públicas generales.
- b) Implementar mecanismos para concienciar sobre las políticas para proteger derechos de propiedad intelectual y las acciones disciplinarias para el personal que las viole. Se aplica tanto al software libre como al privativo.
- c) Mantener registros apropiados de los activos de información para proteger los derechos de propiedad intelectual. Se aplica tanto al software libre como al privativo.
- d) Custodiar evidencia de la propiedad de licencias o suscripciones, contratos, discos maestros, manuales y toda la información relevante del software que se utiliza.
- e) Controlar y asegurar que no se exceda el número máximo de usuarios permitidos para un programa de software. Se aplica tanto al software libre como al privativo, donde corresponda.
- f) Verificar que se instale únicamente software autorizado y con las respectivas licencias en el caso de utilizar software privativo.

- g) Cumplir los términos y condiciones de uso para el software y la información, obtenidos de la Internet o proveedores (programas freeware, shareware, demostraciones o programas para pruebas).
- h) Controlar que no se duplique, convierta en otro formato, ni extraiga contenidos de grabaciones de audio y video, si no está expresamente permitido por su autor o la persona que tenga los derechos sobre el material.
- i) Controlar que no se copie total ni parcialmente software privativo, códigos fuente y la documentación de programas de software con derechos de propiedad intelectual. Se exceptúa los programas de software libre bajo los términos de sus licencias públicas.
- j) Definir y aplicar una licencia pública general al software desarrollado por la institución o contratado a terceros como desarrollo, para proteger la propiedad intelectual.
- k) Exigir a los funcionarios que utilicen solo software desarrollado, provisto o aprobado por la institución.

### **11.3. Protección de registros en cada entidad**

- a) Clasificar los registros electrónicos y físicos por tipos, especificando los periodos de retención y los medios de almacenamiento, como discos, cintas, entre otros.
- b) Mantener la documentación y especificaciones técnicas de los algoritmos y programas utilizados para el cifrado y descifrado de archivos y toda la información relevante relacionada con claves, archivos criptográficos o firmas electrónicas, para permitir el descifrado de los registros durante el periodo de tiempo para el cual se retienen.
- c) Establecer un procedimiento para revisar el nivel de deterioro de los medios utilizados para almacenar los registros. Los procedimientos de almacenamiento y manipulación se deberán implementar según las recomendaciones del fabricante. Para almacenamiento a largo plazo, se recomienda considerar el uso cintas y discos digitales utilizando formatos de archivos y datos abiertos.
- d) Establecer un procedimiento para garantizar el acceso a los datos e información registrada, tanto el medio como el formato, durante todo el periodo de retención.
- e) Establecer un procedimiento para cambiar o actualizar la tecnología del medio en el cuál se almacenan los activos de

información y registros de acuerdo a las innovaciones tecnológicas disponibles en el mercado.

- f) Los sistemas de almacenamiento de datos se deberán seleccionar de manera que los datos requeridos se puedan recuperar en el periodo de tiempo y en formatos legibles, dependiendo de los requisitos que se deben cumplir.
- g) Garantizar la identificación de los registros y el periodo de retención de los mismos tal como se defina en normas legales ecuatorianas. Este sistema debe permitir la destrucción adecuada de los registros después de este periodo, si la entidad no los necesita y las normas así lo especifican.
- h) Establecer y difundir en la entidad las directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información.
- i) Inventariar las fuentes de información clave.
- j) Implementar controles apropiados para proteger los registros contra pérdida, destrucción y falsificación de la información. Utilizar como referencia para la gestión de los registros de la institución la norma ISO 15489-1 o su homóloga ecuatoriana.

#### **11.4. Protección de los datos y privacidad de la información personal**

- a) El OSI deberá controlar la aplicación de la política de protección de datos y privacidad de la información personal.
- b) Implementar medidas técnicas y organizacionales apropiadas para gestionar de manera responsable la información personal de acuerdo con la legislación correspondiente.
- c) Implementar mecanismos de carácter organizacional y tecnológico para autorización al acceso, uso e intercambio de datos personales de las personas o ciudadanos en custodia de las entidades públicas. Prima el principio que los datos personales pertenecen a las personas y no a las instituciones, éstas los custodian al amparo de la normativa legal vigente.

#### **11.5. Prevención del uso inadecuado de servicios de procesamiento de información**

- a) Inventariar y aprobar el uso de los servicios de procesamiento de información por parte de la dirección de la entidad o quien esta delegue.

- b) Definir y comunicar los servicios de procesamiento de información aprobados, así como los criterios para establecer el uso de estos servicios para propósitos no relacionados con la entidad sin autorización de la dirección, o para cualquier propósito no autorizado.
- c) Implementar mecanismos para identificar el uso inadecuado de los servicios por medio de monitoreo u otros medios
- d) Definir y especificar en las normas internas de la entidad, las acciones legales o disciplinarias cuando se compruebe el uso no adecuado de los servicios de procesamiento de información. Se considerará también lo que establece la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento.
- e) Definir la política para autorización de uso de los servicios de procesamiento de información aprobados, misma que debe ser suscrita por cada funcionario en relación de trabajo permanente o temporal, así como contratistas, asesores, proveedores y representantes de terceras partes.
- f) Implementar en todos los servicios de procesamiento de información, el mensaje de advertencia que indique que el servicio al cual se está ingresando es propiedad de la entidad y que no se permite el acceso no autorizado. El usuario debe reconocer y reaccionar apropiadamente al mensaje de la pantalla para continuar con el proceso de registro de inicio. El uso de los servicios de procesamiento de información de la entidad tendrán como fin principal o exclusivo los asuntos de la institución y no los personales o de otra índole.
- g) Implementar mecanismos tecnológicos y organizacionales para detectar la intrusión y evitar el uso inadecuado de los servicios de procesamiento de información. Se recomienda advertir o informar a los usuarios sobre el monitoreo y obtener su acuerdo cuando los servicios de información están abiertos a la ciudadanía o son públicos.

#### **11.6. Reglamentación de controles criptográficos**

- a) Restringir importaciones y/o exportaciones de hardware y software de computadores para la ejecución de funciones criptográficas; o diseñados para adicionarles funciones criptográficas.

- b) Restringir el uso de encriptación, y especificar y documentar los ámbitos en dónde se aplicarán tales procesos (ej., comunicaciones, firma de documentos, transmisión de datos, entre otros).
- c) Restringir métodos obligatorios o discrecionales de acceso por parte de las autoridades del país a la información encriptada mediante hardware o software para brindar confidencialidad al contenido.
- d) Garantizar el cumplimiento con las leyes y los reglamentos nacionales antes de desplazar información encriptada o controles criptográficos a otros países.

#### **11.7. Cumplimiento con las políticas y las normas de la seguridad**

- a) Revisar en intervalos regulares reportes e informes de seguridad de los sistemas de información.
- b) Auditar las plataformas técnicas y los sistemas de información para determinar el cumplimiento de las normas aplicables sobre implementación de la seguridad y sus controles.
- c) Revisar con regularidad en su área de responsabilidad, el cumplimiento del procesamiento de información de acuerdo con la política de la seguridad, las normas y cualquier otro requisito de seguridad. Si se determina algún incumplimiento o no conformidad como resultado de la revisión, la dirección deberá:
  - Determinar la causa del incumplimiento
  - Evaluar la necesidad de acciones para garantizar que no se repitan estos incumplimientos
  - Determinar e implementar la acción correctiva apropiada
  - Revisar la acción correctiva que se ejecutó
- d) Registrar y conservar los resultados de las revisiones y las acciones correctivas llevadas a cabo por la dirección. Los directores deberán informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión independiente tiene lugar en el área de su responsabilidad.

#### **11.8. Verificación del cumplimiento técnico**

- a) Verificar el cumplimiento técnico bien sea manualmente (con soporte de las herramientas de software apropiadas, si es necesario) por un ingeniero de sistemas con experiencia, y/o con la

ayuda de herramientas automáticas que generen un informe técnico para la interpretación posterior por parte del especialista técnico.

- b) Aplicar evaluaciones de vulnerabilidad o pruebas de penetración considerando siempre el riesgo de que dichas actividades pueden poner en peligro la seguridad del sistema. Tales pruebas se deberán planificar, documentar y ser repetibles.
- c) Controlar que la verificación del cumplimiento técnico sea realizado por personas autorizadas y competentes o bajo la supervisión de dichas personas.
- d) Analizar los sistemas operativos para asegurar que los controles de hardware y software se han implementado correctamente. Este tipo de verificación del cumplimiento requiere experiencia técnica especializada.
- e) Ejecutar o contratar pruebas de penetración y evaluaciones de la vulnerabilidad, las cuales pueden ser realizadas por expertos independientes especialmente contratados para este propósito.

Ello puede ser útil para detectar vulnerabilidades en el sistema y verificar qué tan efectivos son los controles evitando el acceso no autorizado debido a estas vulnerabilidades. Las pruebas de penetración y las evaluaciones de vulnerabilidad no deben substituir las evaluaciones de riesgos.

#### **11.9. Controles de auditoría de los sistemas de información**

- a) Salvaguardar los servicios de procesamiento de información y las herramientas de auditoría durante las auditorías de los sistemas de información.
- b) Proteger la integridad y evitar el uso inadecuado de las herramientas de auditoría.
- c) Acordar los requisitos así como el alcance de las auditorías con la dirección correspondiente.
- d) Únicamente se deberá dar a los auditores acceso de lectura a la información.
- e) Identificar explícitamente y poner en disposición los recursos correspondientes, para llevar a cabo las auditorías.
- f) Identificar y acordar los requisitos para el procesamiento especial o adicional.

- g) Monitorear y registrar todo acceso para crear un rastreo para referencia. El uso de rastreos de referencia de tiempo se debe considerar para datos o sistemas críticos.
- h) Documentar todos los procedimientos, requisitos y responsabilidades de la auditoría.
- i) Asegurar que la persona que realiza la auditoría sea independiente de las actividades auditadas.

#### **11.10. Protección de las herramientas de auditoría de los sistemas de información**

- a) Instalar y administrar las herramientas de auditoría por parte del personal que las utiliza.
- b) Los programas de software o archivos de datos de auditoría se deben separar de los sistemas de información y de desarrollo de la entidad.
- c) Los archivos de seguridad y auditoría que generan los sistemas de procesamiento de información deben ser protegidos contra cualquier manipulación.
- d) Mantener un estricto control de respaldos y tiempo de retención de los archivos de seguridad y auditoría de acuerdo al tipo de información y la política que se defina.
- e) Mantener archivos de seguridad y auditoría en librerías de cinta, siempre que se les proporcione un nivel adecuado de protección adicional.
- f) Bloquear el acceso a los archivos de seguridad y auditoría a los funcionarios no autorizados y de acuerdo al procedimiento que se defina.

Nota: Documento basado en el Acuerdo Ministerial No. 166, Esquema Gubernamental de Seguridad de la Información