Defensoría del Pueblo
COLOMBIA

Políticas de seguridad y privacidad de la información

Grupo TICs

2023

Control de cambios			
No	**Descripción del cambio**	**Fecha del cambio**	**Versión**
1	**Creación del documento**	**Diciembre de 2018**	**1.0**
2	**Cambio de formato y actualización acorde con los dominios de la norma NTC/ISO 27001**	**Noviembre de 2023**	**1.1**

ELABORÓ	REVISÓ	APROBÓ
Alexander Amezquita M. Profesional Universitario	Alexander Monroy Coordinador Grupo Tics Cesar Portilla Asesor del Despacho	Óscar Julián Valencia Loaiza Secretario General

1. Introducción. 8
2. Alcance. 8
3. Objetivo. 9
4. Generalidades. 9
5. Políticas de seguridad de la información. 13
Política de Alto Nivel del SGSI. 13
5.1.1. Políticas de seguridad de la información. 13
5.1.2. Revisión de las políticas para seguridad de la información. 13
6. Organización de la seguridad de la información. 13
6.1.1. Roles y responsabilidades para la seguridad de la información. 14
6.1.2. Separación de deberes. 17
6.1.3. Seguridad de la información en la gestión de proyectos. 17
6.2.1. Política para dispositivos móviles. 17
6.2.2. Política para teletrabajo. 18
7. Seguridad de los recursos humanos. 22
7.1.1. Selección. 22
7.1.2. Términos y condiciones del empleo. 22
7.2.1. Responsabilidades de la Alta dirección. 23
7.2.2. Toma de conciencia, educación y formación en la seguridad de la información. 23
7.2.3. Proceso disciplinario. 24
7.3.1. Políticas para terminación o cambio de empleo. 24
8. Gestión de activos. 24
8.1.1. Inventario de activos. 24
8.1.2. Propiedad de los activos. 25
8.1.3. Uso aceptable de los activos. 25
8.1.4. Devolución de los activos. 25
8.2.1. Clasificación de la información. 26
8.2.2. Etiquetado de la información. 26
8.3.1. Gestión de medios removibles. 26
8.3.2. Disposición de los medios. 26
8.3.3. Transferencia de medios físicos. 27
9. Control de acceso. 27

9.1.1. Política de control de acceso....28
9.1.2. Política sobre el uso de los servicios de red....29
9.2.1. Registro y cancelación del registro de usuarios....30
9.2.2. Suministro de acceso de usuarios....30
9.2.3. Gestión de derechos de acceso privilegiado....31
9.2.4. Gestión de información de autenticación secreta de usuarios....31
9.2.5. Revisión de los derechos de acceso de usuarios....32
9.2.6. Retiro o ajuste los derechos de acceso....32
9.3.1. Uso de la información de autenticación secreta....33
9.4.1. Restricción de acceso Información....33
9.4.2. Procedimiento de ingreso seguro....33
9.4.3. Sistema de gestión de contraseñas....34
9.4.4. Uso de programas utilitarios privilegiados....34
9.4.5. Control de acceso a códigos fuente de programas....34
10. Criptografía. 35
10.1.1. Política sobre el uso de controles criptográficos....35
10.1.2. Gestión de llaves....35
Así mismo, se deben considerar las siguientes medidas para la protección de los controles criptográficos: 35
11. Seguridad física y del entorno. 36
11.1.1. Perímetro de seguridad física....36
11.1.2. Controles físicos de entrada....38
11.1.3. Seguridad de oficinas, recintos e instalaciones....38
11.1.4. Protección contra amenazas externas y ambientales....39
11.1.5. Trabajo en áreas seguras....40
La Defensoria del Pueblo debe diseñar e implementar procedimientos específicos para el trabajo en áreas seguras, teniendo como base las directrices que se imparten a continuación:....40
11.1.6. Áreas de despacho y carga....40
11.2.1. Ubicación y protección de los equipos....41
11.2.2. Servicios de suministro....41

11.2.3. Seguridad del cableado. 42
11.2.4. Mantenimiento de equipos. 42
11.2.5. Retiro de equipos. 43
11.2.6. Seguridad de equipos y activos fuera de las instalaciones. 43
11.2.7. Disposición segura o reutilización de equipos. 44
11.2.8. Equipo de usuario desatendido. 44
11.2.9. Política de escritorio limpio y pantalla limpia. 44
12. Seguridad de las operaciones. 45
12.1.1. Procedimientos de operación documentados. 45
12.1.2. Gestión de cambios. 45
12.1.3. Gestión de la capacidad. 46
12.1.4. Separación de los ambientes de desarrollo, pruebas y operación. 47
12.2.1. Controles contra códigos maliciosos. 48
12.3.1. Respaldo de información. 49
12.3.2. Respaldo de información para usuarios finales. 50
12.4.1. Registro de eventos. 51
12.4.2. Protección de la información de registro. 51
12.4.3. Registro del administrador y del operador. 51
12.4.4. Sincronización de relojes. 52
12.5.1. Instalación de software en sistemas operativos. 52
12.6.1. Gestión de las vulnerabilidades técnicas. 52
12.6.2. Restricciones sobre la instalación de software. 53
12.7.1. Información controles de auditorías de sistemas. 54
13. Seguridad de las comunicaciones. 54
13.1.1. Controles de redes. 54
13.1.2. Seguridad de los servicios de red. 55
13.1.3. Separación en las redes. 56
13.2.1. Políticas y procedimientos de transferencia de información. 56
13.2.2. Acuerdos sobre transferencia de información. 58
13.2.3. Mensajería electrónica. 58

13.2.4. Acuerdos de confidencialidad o de no divulgación. 61

14. Adquisición, desarrollo y mantenimientos de sistemas. 61

14.1.1. Análisis y especificación de requisitos de seguridad de la información. 63

14.1.2. Protección de transacciones de los servicios de las aplicaciones 65

14.1.3. Protección de transacciones de los servicios de las aplicaciones 65

14.2.1. Política de desarrollo seguro. 66

Fase planificación – Sistemas de información DPC. 66

Fase Desarrollo – Sistemas de información DPC 68

Aplicación de buenas prácticas de Desarrollo de software 70

Verificación de cumplimiento de especificaciones del sistema 71

Fase Implementación - Sensibilización, Puesta en Producción y Mantenimiento de Sistemas de Información – DPC. 72

14.2.2. Procedimientos de control de cambios en sistemas. 73

14.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación. 73

14.2.4. Restricciones en los cambios a los paquetes de software. 75

14.2.5. Principios de construcción de sistemas seguros 76

14.2.6. Ambiente de desarrollo seguro. 77

14.2.7. Desarrollo contratado externamente. 78

14.2.8. Pruebas de seguridad de sistemas 79

14.2.9. Prueba de aceptación de sistemas 80

14.2.10. Gestión de vulnerabilidades. 81

14.3.1. Protección de datos de prueba. 81

15. Relación con los proveedores. 82

15.1.1. Política de seguridad de la información para las relaciones con proveedores. 82

15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores 83

15.1.3. Cadena de suministro de tecnología de información y comunicación. 84

15.2.1. Seguimiento y revisión de los servicios de los proveedores. 85

15.2.2. Gestión de cambios en los servicios de los proveedores. 87

16. Gestión de incidentes de seguridad de la información. 88

16.1.1. Responsabilidad y procedimientos. 88

16.1.2. Reporte de eventos de seguridad de la información. 89
16.1.3. Reporte de debilidades de seguridad de la información 89
16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. 89
16.1.5. Respuesta a incidentes de seguridad de la información. 89
16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información. 90
16.1.7. Recolección de evidencia. 90
17. Aspectos de seguridad de la información de la gestión de continuidad de negocio. 91
17.1.1. Planificación de la continuidad de la seguridad de la información. 91
17.1.2. Implementación de la continuidad de la seguridad de la información. 91
17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 92
17.2.1. Disponibilidad de instalaciones de procesamiento de información. 93
18. Cumplimiento. 94
18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales. 94
18.1.2. Derechos de propiedad intelectual. 94
18.1.3. Protección de registros. 95
18.1.4. Privacidad y protección de datos personales. 96
18.1.5. Reglamentación de controles criptográficos. 96
18.2.1. Revisión independiente de la seguridad de la información. 96
18.2.2. Cumplimiento con las políticas y normas de seguridad. 96
18.2.3. Revisión del cumplimiento técnico. 96

1. Introducción.

Las políticas de seguridad de la información identifican las responsabilidades de los usuarios, custodios y propietarios de la información y además establecen los objetivos para una protección apropiada y consistente de los activos de información de La Defensoría del Pueblo. Con la implementación de las políticas de seguridad de la información se pretende minimizar el riesgo de que en forma accidental o intencional se divulguen, modifiquen, destruyan o usen en forma indebida los activos de información (tal como se define en el alcance). Al mismo tiempo, las políticas ayudan a las áreas responsables de la administración de la seguridad de la información, a orientar y mejorar la administración de seguridad de los activos de información, y de esta manera brindar también las bases para el monitoreo de los servicios y activos de toda la Entidad.

La Defensoría del Pueblo busca mantener un esquema de seguridad que permita asegurar constantemente la confidencialidad, integridad y disponibilidad de su información, siendo ésta, uno de sus activos más valiosos. Para ello, la Entidad, desea que todo el personal que forma parte de La Defensoría conozca, participe y cumpla los lineamientos, políticas, procedimientos y demás directivas estipuladas en la Política de Seguridad de la Información diseñados e implementados para tal fin.

Para la elaboración de las políticas de seguridad de la Defensoría del Pueblo, se utilizaron las normas internacionales NTC/ISO 27001:2022 e NTC/ISO 27002:2013 como referentes por excelencia en el marco de la seguridad de la información.

2. Alcance.

Esta política de seguridad de la información aplica a todos los activos de información de propiedad de La Defensoría y su infraestructura tecnológica.

De la misma forma, estas políticas están orientadas a garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, etc.) y de servicios como Internet y el correo electrónico; brindando a los funcionarios pautas para la utilización apropiada de sus recursos, permitiendo así minimizar los riesgos de una eventual pérdida de los activos de información sensitivos para La Defensoría.

La política de seguridad de la información de La Defensoría aplica a todos los activos de información durante su ciclo de vida.

Las políticas están orientadas a proteger los activos de información como son el centro de procesamiento de datos, los sistemas de información, los equipos de usuarios, las copias de respaldo, y también asegurar que los activos de información que residen en lugares externos (pe. Oficinas regionales, proveedores de servicios, etc.), estén sometidos a controles equivalentes para su protección.

Estas políticas aplican a todos los funcionarios, defensores, consultores, contratistas, temporales o terceras partes que accedan a los activos de la información de La Defensoría del Pueblo, quienes están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de seguridad de información que los funcionarios de la Entidad.

Todas estas personas están obligadas a continuar protegiendo la información de La Defensoría, cumpliendo las políticas de seguridad después de terminar su relación con la Entidad, mediante los respectivos acuerdos de confidencialidad de la información que deben suscribirse con cada uno de ellos de acuerdo con lo indicado por esta política.

3. Objetivo.

Definir las políticas complementarias que encuentren alineación a la política de alto nivel del Sistema de gestión de seguridad de la información – SGSI de la Defensoría del Pueblo, con el fin de adelantar de manera metódica y organizada la gestión de los tres pilares de la seguridad de la información (confidencialidad, integridad y disponibilidad) sobre los activos de información en los términos de la norma NTC/ISO 27001:2022 y el anexo A de esta.

4. Generalidades.

Este documento de políticas complementarias de seguridad de la información hace parte integral del sistema de gestión de seguridad de la información, establecido en el documento Manual del SGSI.

4.1. Aplicación.

Las políticas complementarias de seguridad de la información contenidas en este documento han sido dirigidas contemplando involucrar todos los procesos y actores que dependen e interactúan con la Defensoría del Pueblo en lo que refiere a los términos de la seguridad de la información.

4.2. Definiciones.

Activos de información: Es todo activo que contenga información, la cual posee un valor y es necesaria para realizar los procesos misionales y de soporte de la Entidad. Se pueden clasificar de la siguiente manera:

- **Electrónicos**: Bases de datos, archivos, registros de auditoría, información de archivo, aplicaciones, herramientas de desarrollo y utilidades.
- **Físicos**: Documentos impresos, manuscritos y hardware.
- **Servicios**: Servicios computacionales y de comunicaciones.
- **Personas:** Incluyendo sus calificaciones, competencias y experiencia.
- **Intangibles:** Ideas, conocimiento, conversaciones.

Área segura: Instalaciones con medidas de control de acceso físico y lógico para reducir el riesgo de acceso no autorizado sobre los activos de información.

Batch: Archivo magnético que tiene almacenado una secuencia de comandos que al ejecutarse reemplaza la operación de digitar los comandos en secuencia cada vez que se requiere efectuar una operación. Se utiliza para almacenar operaciones repetitivas.

BCP: Business Continuity Planning. Es el conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos del negocio generando un impacto mínimo o nulo ante una contingencia.

Buscador en Internet: Son sitios web especializados en localizar información por criterios o por contenidos a través de internet. Entre los más utilizados y conocidos se encuentran Yahoo® y Google®.

Buzón: También conocido como cuenta de correo, es un receptáculo exclusivo, asignado en el servidor para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a la Defensoría del Pueblo.

Ciudadano: Es una persona natural con el cual la Entidad mantiene relaciones en cumplimiento de obligaciones legales y no contractuales.

COBIT®: Objetivos de Control para la Información y la Tecnología relacionada (Control Objectives for Information and Related Technology, por sus siglas en inglés). Es un marco de referencia para la dirección de IT, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio. Fue creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI) en 1992 y se encuentra en su quinta versión de desarrollo.

Contraseña o password: Es una clave secreta de acceso a un computador, a una cuenta de correo electrónico o a una cuenta de conexión a Internet, o a un Sistema de Información, que, en aras de maximizar los niveles de seguridad, control y privacidad, sólo debe conocer el usuario. Si se introduce una contraseña incorrecta, no se permitirá la entrada al sistema.

Correo Electrónico: Nombre genérico para toda comunicación no interactiva de texto, datos, imágenes o mensajes de voz, que tiene lugar entre un remitente y los destinatarios designados, y que se desarrolla en sistemas que utilizan enlaces de telecomunicación.

Correo electrónico Institucional: Es el servicio de correo electrónico que provee y administra directamente la Entidad a sus funcionarios, como herramienta de apoyo a las funciones y responsabilidades de estos.

Firewall: Dispositivo tecnológico que tiene como función el control de acceso lógico en la red de comunicaciones.

Fólder Público: Este recipiente almacena mensajes e información que se puede compartir por los usuarios a quienes se designe.

GB: Forma abreviada que se utiliza para escribir GigaByte, que es el espacio necesario para guardar en un computador mil millones de caracteres.

Gestión del cambio: Consiste en aprovechar los cambios del entorno empresarial para el bien de la organización, por ello, deben ser flexibles y quienes los manejan deben desarrollar una aguda percepción para anticiparse a los cambios y poder estar así siempre a la vanguardia.

Internet (International Net): Nombre de la mayor red informática del mundo. Red de telecomunicaciones nacida en 1969 en los Estados Unidos a la cual están conectadas centenares de millones de personas, organismos y empresas, en su mayoría ubicadas en los países más desarrollados, y cuyo rápido desarrollo está teniendo importantes efectos sociales, económicos y culturales, convirtiéndose de esta manera en uno de los medios más influyentes de la llamada Sociedad de la Información, siendo conocido en algunos ámbitos con el nombre de la Autopista de la Información. Fue conocida como Arpanet hasta 1974.

Intranet: Se llaman así a las redes tipo internet pero que son de uso interno.

ISO/IEC 27002:2013: Norma de mejores prácticas seguridad de información (anteriormente denominada ISO 17799) y donde se definen los criterios de respaldo para garantizar la continuidad de la información, así mismo la manera de inventariar dichos activos.

LAN: Red de área local (Local Area Network por sus siglas en inglés). Es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

Lista de Distribución: Es un recipiente de correo que agrupa otros recipientes, con el fin de facilitar el envío de información.

MB: Forma abreviada que se utiliza para escribir Mega Byte, que es el espacio necesario para guardar en un computador un millón de caracteres.

Mensaje Masivo: Es un mensaje enviado a un número mayor de cincuenta (50) buzones o cuentas de correo, acumulados en una o varias remisiones de este.

NTC/ISO 27001:2022: Norma ajustada para Colombia que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

Lugar de trabajo seguro: Espacio físico con las debidas medidas de protección para preservar la integridad física de las personas.

Mensajería Electrónica: Son los servicios tecnológicos utilizados para el intercambio de mensajes de forma electrónica como lo es el correo electrónico.

Módem: Dispositivo de comunicación que permite establecer una conexión a través de la línea telefónica o celular.

Oficial de Seguridad: Figura responsable por velar, mantener y gestionar la seguridad de los activos de información de la Entidad.

Paquete de Software. Conjunto de programas que se comercializan y tienen una función específica. Aplica la definición para el software que apoya procesos de una Entidad.

Proceso Misional: Procesos para el cumplimiento de la razón de ser de la entidad.

Propietario: El término propietario identifica al funcionario, terceras partes o dependencia que teniendo responsabilidad aprobada por el Despacho del Defensor, administra la realización de los procesos, el desarrollo, el mantenimiento, el uso o la seguridad de los activos asociados según el caso. El término propietario no significa que la persona sea dueña de los activos

Buzón de Correo: Este término cobija a los diferentes objetos que se pueden crear y administrar mediante el Servicio de Correo Electrónico, a saber: Buzones, Recipientes Personalizados, Fólderes Públicos y Listas de Distribución.

Recipiente Personalizado: Es un apuntador a una dirección de correo electrónico, externo a la Defensoría del Pueblo.

Red privada virtual – VPN: Método de conexión a través de una red pública o privada, que permite a los usuarios establecer conexiones seguras.

Redes: Son los dispositivos y medios utilizados para transferencia electrónica de datos.

Script: Es un archivo que contiene una secuencia de comandos que se utiliza para comunicarse en forma automática entre dos aplicaciones

Seguridad de la Información: Preservación de la confidencialidad, la integridad, y la disponibilidad de la información.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Spam: Mensajes que sin ser solicitados llegan al buzón de correo, provenientes de direcciones desconocidas en la mayoría de los casos, muy frecuentemente encaminados a ofrecer productos y servicios. También son conocidos como "correo basura".

Terceras partes: Son todos aquellos entes externos o personas que no son funcionarios de la Defensoría del Pueblo, que tienen acceso a los activos de la información.

TICs: Tecnologías de Información y las Comunicaciones.

Virus: Software o programa cuyo objetivo es causar daños en un sistema informático. Con tal fin se oculta o se disfraza para no ser detectado. Estos programas son de diferentes tipos y pueden causar problemas de diversa gravedad en los sistemas a los que afectan, desde borrar un tipo de archivos, hasta borrar toda la información contenida en el disco duro. Hoy en día se propagan fundamentalmente mediante el uso del correo electrónico y de medios de almacenamiento de información portátiles infectados como discos duros externos, CD, DVD, y Memorias USB. Se combaten con la instalación de antivirus que deben ser actualizados periódicamente.

WAN: Red de área amplia (Wide Area Network por sus siglas en Inglés). Es una red de computadoras que une varias redes locales (LAN) aunque sus miembros no están todos en una misma ubicación física.

4.3. Normas aplicables.

NTC/ISO 27001:2022

NTC/ISO 27005:2009

GTC/ISO 27002:2015

Modelo de Seguridad y Privacidad de la Información V.4.0 – MPSI de la Política de Gobierno Digital.

4.4. Cumplimiento.

Las políticas de seguridad de la información planteadas en este documento son de obligatorio cumplimiento para todos los actores que interaccionan con la Defensoría del Pueblo, Si llegase a existir una violación a estas políticas por parte de algún actor relacionado, (Proveedor, contratista, funcionario u Outsourcing) ya sea por negligencia o intencionalmente, La Defensoría del Pueblo esta en la facultad de tomar las medidas correspondientes, tales como acciones disciplinarias, despido, acciones legales, reclamo de compensación por daños y las demás que se consideren adecuadas en concordancia con la normatividad vigente, las leyes y la constitución política Colombiana.

5. Políticas de seguridad de la información.

Dominio/Control: Directrices de la Dirección en seguridad de la información.

Objetivo: Dictar las reglamentaciones requeridas para la implementación del SGSI.

Política de Alto Nivel del SGSI.

Buscando una correcta alineación con el plan estratégico institucional, la Defensoría del Pueblo establece la siguiente política de alto nivel del SGSI:

"La Defensoría del Pueblo reconoce a la información como uno de los activos más importantes con el fin de alcanzar el objetivo estratégico de: Ofrecer garantías de protección de los DDHH de la ciudadanía a través del mejoramiento de los servicios y el desarrollo de nuevas herramientas tecnológicas.

Por tal motivo, la Defensoría del Pueblo adquiere el compromiso de disponer la totalidad de los recursos que sean necesarios para gestionar y fortalecer los aspectos relevantes de la seguridad de la información al interior de la entidad, para lo cual se implementará un sistema de gestión de seguridad de la información articulado con el sistema integrado de gestión institucional de manera que se asegure la **integridad**, **disponibilidad**, **confidencialidad** y **privacidad** de la información realizando la **gestión** y el **tratamiento** de los **riesgos** en cumplimiento de los requisitos de la entidad, los legales o reglamentarios, y las obligaciones de seguridad contractuales; con servidores públicos, proveedores y partes interesadas, comprometidos a participar activamente en el desarrollo de la **cultura** de seguridad de la información."

5.1. Directrices establecidas para la seguridad de la información.

La Política de Seguridad especifica las directrices que deben ser cumplidas por parte de La Defensoría del Pueblo, sus funcionarios, contratistas, defensores, proveedores y terceros, con el fin de asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad en su información.

La Alta Dirección debe aprobar, publicar, comunicar a todos los empleados o partes externas pertinentes el documento de políticas de seguridad de la información.

5.1.1. Políticas de seguridad de la información.

Las políticas que se definen en este documento están estructuradas y direccionadas en base a cada dominio o control del anexo A de la norma NTC/ISO 27001:2022 y se encuentran articulados con el estándar de buenas prácticas de la NTC/ISO 27002:2015.

5.1.2. Revisión de las políticas para seguridad de la información.

La política de seguridad de la información se debe revisar de manera anual y cada vez que sea necesario por cambios significativos en procesos, infraestructura, software, aplicaciones y todo aspecto que influya considerablemente en la misión funcional, con el fin de garantizar que ella sigue siendo suficiente y eficaz.

6. Organización de la seguridad de la información.

6.1. Organización Interna.

El equipo de seguridad de la información en la Defensoría del Pueblo se encarga de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el Sistema de gestión de

seguridad de la información al interior de la entidad, así como planear las actividades necesarias para una adecuada administración y sostenibilidad de este.

6.1.1. Roles y responsabilidades para la seguridad de la información.

Con el fin de favorecer la correcta comprensión de cada una de las políticas aquí expuestas y los responsables en términos de seguridad de la información, a continuación, se diagrama la jerarquía de autoridades y roles establecidos en el manual del sistema de gestión de seguridad de la información adoptado por la Defensoría del Pueblo[1] y empleado como insumo para la definición de cada una de las directrices.

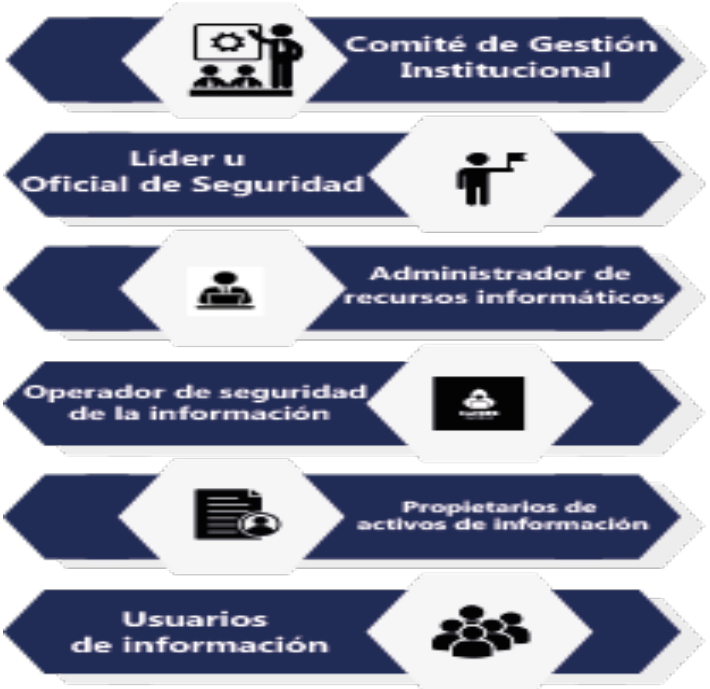

Ilustración 1 - Autoridades y Roles de seguridad de la información

Alta dirección.

Además de apoyar activamente la seguridad de la información al interior de la Defensoría del Pueblo, aprobando las directrices y lineamientos de operación del SGSI, otras funciones de la alta dirección en términos del sistema de gestión de seguridad de la información son:

- Asegurar que la mesa técnica del Sistema integrado de gestión institucional contemple todas las funciones de un Comité del SGSI.

- Incluir y mantener dentro de la planta de personal de la Defensoria del Pueblo, un funcionario que cumpla con los requisitos mínimos para el perfil de Oficial de Seguridad de la información, este será el encargado de realizar todas las gestiones necesarias frente a los temas de seguridad de la información en la entidad.

[1] Ver Manual del SGSI de la Defensoria del Pueblo

- Propender por la inclusión como integrante activo del comité de gestión institucional al Oficial de seguridad de la información de la entidad.

- Formular las directrices y políticas del SGSI, de manera que se asegure la articulación con los demás procesos de la entidad, así como el plan estratégico.

- Garantizar el cumplimiento de las políticas de seguridad de la información procurando que los controles de seguridad establecidos sean conocidos y aplicados por todos los servidores públicos, contratistas y partes interesadas.

- Especificar las responsabilidades relacionadas con la seguridad de la información a todas las dependencias de la entidad.

- Controlar que, al menos una vez al año se ejecute el plan de auditorías internas y se efectúen las mejoras requeridas por el SGSI.

- Determinar los niveles de tolerancia a los riesgos asociados a la seguridad de la información.

- Asegurar la eficacia del SGSI determinando los recursos necesarios para alcanzarla.

Comité de gestión institucional de la Defensoría del Pueblo.

A fin de realizar todas las actividades que conlleva el establecimiento, la implementación, la operación, la supervisión, la revisión, el mantenimiento y las acciones de mejora del SGSI, es imprescindible que el comité incluya dentro de sus funciones las siguientes acciones:

- Valorar y aprobar los modelos sistemáticos, estratégicos, y las políticas de seguridad de la información requeridos para la implementación al interior de la entidad.

- Especificar los principios rectores institucionales a fin de aplicar los procedimientos de protección de seguridad de la información.

- Validar y aprobar las acciones y definiciones de mejores prácticas para la implementación del SGSI.

- Generar conciencia a los diferentes procesos de la entidad a cerca de la importancia de la adopción de una correcta cultura de la seguridad de la información.

- Asegurar la adopción de decisiones que conlleven a la minimización de los riesgos de seguridad de la información.

- Valorar, aprobar y fomentar los programas de capacitación y sensibilización en todos los temas relacionados con el SGSI.

Líder u Oficial de seguridad de la información.

Alineada con las políticas de Gobierno Digital y el Modelo de Seguridad y privacidad de la información v.4.0 del MinTIC, la Defensoría del Pueblo bajo la supervisión del líder del grupo de Tecnología designará la responsabilidad que

corresponde con el rol de "Líder u Oficial de Seguridad de la información" a un servidor público con el fin de liderar y garantizar la correcta implementación, mantenimiento y mejora del SGSI, la actuación del Líder de seguridad de la información de la Defensoría del Pueblo estará supeditada por las directrices emanadas por el comité de gestión institucional sin perjuicio de los lineamientos dictados por el MinTIC en el numeral 11.2.5 del Modelo de Seguridad y privacidad de la información v.4.0.[2] los cuales definen las siguientes actividades como base:

- Definir, formular y establecer, el subproceso del SGSI en la Defensoría del Pueblo, sus directrices, reglamentaciones y controles de conformidad con las recomendaciones del Comité de gestión institucional, las buenas prácticas de normas técnicas y los requerimientos normativos vigentes.

- Planear, definir e implantar el Modelo de Seguridad y privacidad de la información acorde con la estrategia de Gobierno Digital.

- Orientar al Grupo Tecnologías de la Información acerca de las acciones necesarias para realizar la implementación de la estrategia de ciberseguridad establecida por el ministerio de Defensa Nacional.

- Coordinar todas las acciones relevantes y necesarias en términos de seguridad informática y de seguridad de la información.

- Alinear las políticas y procedimientos de seguridad de la información de acuerdo con la normatividad y reglamentos vigentes.

- Asegurar la protección de los activos de información de la Defensoría del Pueblo, incluyendo la propiedad intelectual además del cumplimiento normativo.

- Definir, verificar, mantener actualizada y presentar para la aprobación por parte del comité de gestión institucional, las diferentes políticas y responsabilidades generales en materia de Seguridad de la Información.

- Planificar las estrategias de comunicación y sensibilización para las partes interesadas en torno a la cultura de seguridad de la Información en la Defensoría del Pueblo.

- Liderar la elaboración de las políticas, directrices, procedimientos y estándares definidos en el SGSI.

- Definir los ciclos de mantenimiento necesarios para el análisis, evaluación y tratamiento de los riesgos que se ciernen sobre los activos de información de la Defensoría del Pueblo.

- Poner a prueba y dar visto bueno de conceptos técnicos de seguridad de la información, frente a las nuevas soluciones o plataformas tecnológicas.

- Elaborar la metodología acorde a los procesos de la entidad para definir el diseño de los planes de contingencia y continuidad de seguridad de la información.

- Identificar, valorar, seleccionar y orientar en la implementación de herramientas que permitan a la entidad facilitar las tareas de gestionar el SGSI.

- Establecer las directrices de control de acceso a la información de la entidad por parte de las partes interesadas en procura de mantener asegurados los pilares fundamentales de la seguridad.

[2] Modelo de seguridad y privacidad de la información V4.0 https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf

- Asegurar el correcto cumplimiento de los requerimientos de seguridad de la información en términos de la operación, desarrollo e implementación de sistemas de información, bases de datos y sistemas de comunicación informáticos

- Articular las actividades requeridas para gestionar de manera correcta los incidentes de seguridad de la información que se puedan presentar en la Defensoría del Pueblo.

- Analizar los informes referentes a la seguridad de la información y los de efectividad de los controles de la seguridad con el objetivo de determinar el estado del SGSI, además de asegurar que el sistema se encuentra en completa conformidad con los requisitos de la norma para lo cual realizando la evaluación periódica del sistema.

- Plantear y planificar los ejercicios de mejora continua para las herramientas y los controles de seguridad de la información necesarios para fortalecer la seguridad de la información en la Entidad y la correcta atención de los incidentes de seguridad de la información identificados.

6.1.2. Separación de deberes.

La Entidad definirá de forma clara y precisa, la segregación de funciones mediante el establecimiento de roles y permisos para los funcionarios de la Defensoría del Pueblo que tienen a cargo la administración técnica y funcional de los sistemas de información, aplicativos y usuarios con privilegios en los computadores. Esta división establece diferentes etapas de aprobación, autorización, ejecución y mantenimiento de registros a cargo de los funcionarios asignados en cada función. De esta manera se garantizará la transparencia, evitará los errores involuntarios y evitará posiciones de poder que faciliten actuaciones indebidas.

6.1.3. Seguridad de la información en la gestión de proyectos.

Todo proyecto que se desarrolle en la Defensoría tendrá dentro de sus consideraciones la inclusión de un capítulo relativo a la seguridad de la información que se maneje dentro del mismo, de igual forma, los procesos y procedimientos que se desarrollen como entregables de cada proyecto, deberán considerar y establecer las necesidades y mecanismos de clasificación de la información, confidencialidad y protección de la información que se administre mediante ellos.

6.2. Dispositivos móviles y teletrabajo.

El objetivo de esta política es garantizar la seguridad de la red de la Entidad cuando los usuarios utilicen dispositivos móviles en sus diferentes sedes o realicen actividades de teletrabajo. Como dispositivo móvil se incluyen: computadores portátiles, teléfonos celulares, *smartphones*, tabletas, unidades de almacenamiento USB, CD, DVD, Blu-ray o similares.

6.2.1. Política para dispositivos móviles.

Todo dispositivo móvil que requiera ser conectado a la red de la Entidad ya sea de propiedad de la Entidad o de funcionarios o terceros deberá cumplir con las siguientes políticas para su conexión y uso dentro de la red:

- Todo dispositivo móvil que se conecte a la red de la Defensoría deberá hacerlo a una red VLAN independiente de la red de usuarios y solo dispondrá de acceso a Internet. En caso de que el usuario requiera acceso a la red de la Entidad para conectarse a los sistemas de información, deberá ser autorizado por el jefe del área a la que el usuario pertenece, quien deberá hacer la autorización de permiso en los formatos establecidos para que el Grupo de TIC la pueda tramitar. En todo caso, el usuario autorizado acepta que su equipo podrá ser revisado por el responsable de dicha actividad en el Grupo de TIC, con el fin de garantizar que cumple con los mínimos de seguridad establecidos en esta política para su conexión.

- La Defensoría se reserva el derecho de implementar un sistema MDM (del inglés Mobile Device Management) que aplique de forma rigurosa las políticas establecidas para los dispositivos autorizados para ser usados dentro de su red y requerir al dueño del dispositivo el aceptar esas políticas para la conexión a la red.

Todo dispositivo que se conecte a la red deberá cumplir con lo siguiente:

- Tener todo su software debidamente licenciado.
- Disponer de un antivirus instalado y ejecutándose apropiadamente.
- Mantenerse actualizado con las últimas correcciones para el sistema operativo y antivirus.
- Los dispositivos no pueden haber sido modificados por el usuario para tener privilegios mayores en el sistema operativo, estas modificaciones se conocen como Rooted en el sistema operativo Android® de Google, o jailbroken en el sistema operativo iOS® de Apple.
- Poder ser bloqueado con una contraseña y deberá bloquearse de manera automática a más tardar a los cinco (5) minutos de inactividad.
- Si el dispositivo es de propiedad del funcionario o del tercero que requiera conectarse a la red de la Defensoría solo podrá solicitar soporte al grupo de TIC para la revisión del fallo de los aplicativos de la Entidad. Así mismo, no se podrá solicitar el servicio de soporte para la instalación de aplicativos que no son misionales ni para la revisión de fallos relacionados con el mal funcionamiento del dispositivo.
- La Entidad se reserva el derecho de desconectar equipos o suspender servicios para estos dispositivos sin previa notificación.

6.2.2. Política para teletrabajo.

En el marco de la Ley 1221 de 2008 "Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones", se establecieron las políticas para el uso de las TIC como herramientas de trabajo, documento que hace parte integral de esta política.

En situaciones estrictamente controladas, la Defensoría permitirá el acceso de terceros a sus redes internas y a los sistemas de información.

Estos accesos deberán ser explícitamente autorizados por: las directivas de la Entidad o el Responsable del Grupo de Sistemas y deberán estar avalados por el Líder u Oficial de Seguridad de la Información.

Solamente se autorizarán los accesos a la red institucional, siempre y cuando se realicen por medio del uso de una VPN (de su sigla en inglés Virtual Private Network, red privada virtual).

Todo dispositivo que se utilice para conectarse a la red mediante una VPN deberá cumplir con los siguientes requisitos:

- Tener todo su software debidamente licenciado.
- Disponer de un antivirus instalado, actualizado y ejecutándose apropiadamente.

- Poder ser bloqueado con una contraseña y deberá bloquearse de manera automática a más tardar a los cinco (5) minutos de inactividad.

- Si el dispositivo es de propiedad del funcionario o del tercero que requiera conectarse a la red de la Defensoría solo podrá solicitar soporte al grupo de Sistemas para la revisión del fallo de los aplicativos de la Entidad. Así mismo, no se podrá solicitar el servicio de soporte para la instalación de aplicativos que no son misionales ni para la revisión de fallos relacionados con el mal funcionamiento del dispositivo.

- La Entidad se reserva el derecho de desconectar equipos o suspender servicios para estos dispositivos sin previa notificación.

- Es responsabilidad absoluta del autorizado garantizar que se está cumpliendo con lo exigido, sin embargo, la Defensoría del Pueblo se reserva el derecho de verificarlo y tomar las medidas que considere pertinentes en caso de incumplimiento.

El proceso de toma de la decisión para otorgar la autorización incluye:

- Consideración de los controles en los sistemas a ser conectados
- Las normas de seguridad corporativa
- Acuerdos firmados de confidencialidad
- Resultado de una revisión del historial y experiencia del tercero.

Los privilegios de sistema para las conexiones remotas deben ser estrictamente limitados a las premisas del sistema en cuestión y a la información necesaria para lograr los objetivos del proyecto.

En caso de necesitarse una conexión de emergencia que responde a un incidente, esta solicitud se manejará a través del procedimiento de manejo de incidentes.

Toda solicitud de conexión remota deberá tener asignado un Responsable técnico, quien deberá:

- Identificar las necesidades de acceso de terceras partes y establecer los activos de información afectados.
- Realizar un análisis de riesgos del acceso solicitado.
- Basado en el análisis de riesgo autorizar o rechazar la solicitud.
- Si la solicitud es autorizada debe definir los controles requeridos para el acceso.
- Comunicación y entrega de los documentos de políticas de seguridad de la información y compromisos de confidencialidad e integridad de la información.
- Archivar los documentos de compromiso
- Autorizar el formato de novedades de usuario para creación de la cuenta de acceso.
- Verificar de forma continua el cumplimiento de los compromisos
- Notificar a los administradores y oficial de seguridad los cambios en las terceras partes.

Así mismo, será responsabilidad del Oficial de seguridad de la información las siguientes actividades:

- Evaluar los riesgos de seguridad
- Autorizar o rechazar el acceso.
- Definir los controles requeridos

Finalmente, será responsabilidad del Administrador del sistema las siguientes actividades:

- Validar la existencia de las autorizaciones requeridas.
- Creación de los accesos solicitados.

Autorización y uso de Redes inalámbricas.

La Defensoría del pueblo, en aplicación de la directriz número 16 de la directiva presidencial 02 de 2022 se reserva el derecho de implementar y poner a disposición de sus colaboradores redes inalámbricas Wi-Fi conectadas para acceso y consulta de internet, mas no para que por medio de estas se administren infraestructuras internas o se acceda a servicios misionales internos desde dispositivos no institucionales, Para su uso se reglamentan las siguientes restricciones:

- Todos los usuarios que accedan a las redes inalámbricas de la Defensoría del Pueblo aceptan de manera directa las políticas, términos y condiciones de uso descritos en este documento sin ninguna reserva, así como cualquier condición adicional que en el futuro se pudiera complementar en esta política.

- Para poder hacer uso de esas redes, los colaboradores deberán tramitar ante el Grupo de TIC la autorización respectiva.

- Los usuarios son responsables de instruirse y configurar sus dispositivos con los procedimientos básicos para el funcionamiento dentro de la red inalámbrica.

- La disponibilidad y calidad del servicio está sujeta a la interferencia de redes inalámbricas de terceros y a la cantidad de usuarios conectados a la red.

- Es responsabilidad de los usuarios contar con el software y configuración de seguridad en su equipo para minimizar el riesgo al que se puede ver expuesto a un ataque al encontrarse conectado sobre esta red, en caso de equipos de la Defensoría que no cuenten con dicho software deberá notificarse inmediatamente al Grupo de Sistemas para obtenerlo con su apoyo.

Está estrictamente prohibido:

- Revelar o ceder las credenciales de autenticación de la red inalámbrica a personal no autorizado.

- Extender el alcance de la red por medio de cualquier dispositivo físico o lógico.

- Manipular los equipos de transmisión de la red inalámbrica.

- Instalar o realizar labores de recolección o escucha de información en tránsito por la red.

- Instalar equipos o software que genere interrupción o interferencia con la emisión normal de la red inalámbrica.

-

7. Seguridad de los recursos humanos.

Esta política busca asegurar que los funcionarios, y terceras partes entiendan sus responsabilidades y sean adecuados para los roles para los que se los considera, y de esta manera reducir el riesgo de un robo, fraude o uso no adecuado de las instalaciones.

7.1. Antes de asumir el empleo.

La Subdirección de Gestión del Talento Humano tiene dentro sus funciones realizar la revisión de requisitos para proceder a la posesión como servidor público. Como parte de la función de selección se debe realizar una verificación de los antecedentes y referencias de los candidatos.

7.1.1. Selección.

Con el fin de dar cumplimiento a los requerimientos de la norma, la subdirección de gestión del talento humano, en términos de la seguridad de la información, debe cumplir las siguientes actividades para la selección de personal:

- Aplicar la normatividad vigente y aplicable del Sistema de Gestión de Seguridad de la información, así como a cualquier requerimiento de seguridad de la entidad al proceso de Gestión del Talento Humano.

- Realizar la correcta verificación de los antecedentes de todos los candidatos en concordancia con la normatividad exigible y los códigos de ética relacionados.

- Establecer en el manual de funciones los requisitos de seguridad de la información para cada cargo, los cuales deben ser proporcionales a las funciones establecidas, a la clasificación de la información a la cual va a tener acceso, y a los riesgos definidos.

- Definir mecanismos de control para asegurar el cumplimiento a lo prescrito en el Manual de Funciones de los servidores públicos y está relacionado con el Sistema de Gestión de Seguridad de la Información de la entidad.

- Conservar la documentación que funge como evidencia de la competencia de los cargos archivando y custodiando adecuadamente las historias laborales en concordancia con las tablas de retención documental.

7.1.2. Términos y condiciones del empleo.

Los términos y condiciones laborales a los cuales deben acogerse todas las personas que ingresen a la Defensoría del Pueblo en calidad de funcionarios deben estar establecidas de manera formal mediante acto administrativo, la subdirección de gestión del talento humano en términos de seguridad de la información debe contemplar las siguientes actividades en el marco de la seguridad de la información:

- Los funcionarios y las terceras partes, y los colaboradores de estos, de forma escrita se comprometen a cumplir con las políticas de seguridad de la información y del compromiso de confidencialidad, en los formatos que se establezcan para ello.

- Los supervisores o interventores de los contratos que celebre la Entidad con terceras partes, son responsables de garantizar que de forma escrita exista una aceptación por parte de estos y sus

colaboradores del conocimiento, aceptación y compromiso en cumplir con las políticas de seguridad de la información y del compromiso de confidencialidad.

- Informar acerca de la existencia del Sistema de gestión de seguridad de la información en la Defensoria del Pueblo a todos los actores involucrados (servidores públicos, contratistas y proveedores) y, en consecuencia, legalizar a través de la firma de un acta de compromiso a cerca de la seguridad de la información en la entidad, la cual hará parte de la hoja de vida.

- Definir y comprobar las habilidades especificas requeridas para los servidores públicos que hacen parte de la estructura orgánica del sistema de gestión de seguridad de la información – SGSI de la Defensoria del Pueblo.

- Asegurar que los servidores públicos vinculados a la entidad cuentan con las competencias requeridas, comprobando la documentación que certifica su educación, formación y/o experiencia y el cumplimiento de los requisitos y/o homologaciones exigidas en la normatividad aplicable.

7.2. Durante la ejecución del empleo.

Las directivas de la Defensoría del Pueblo deben exigir que todo funcionario o terceras partes que tengan acceso a los activos de información, cumplan las políticas y los procedimientos de seguridad de la información establecidos por la Entidad; esa exigencia debe hacerse en el marco del sistema de gestión de riesgos de la Defensoría del Pueblo.

7.2.1. Responsabilidades de la Alta dirección.

Dentro de las responsabilidades de la alta dirección en términos de la seguridad de la información se define la siguiente actividad:

- Asegurar el cumplimiento de las normatividades y reglamentaciones vigentes frente a la privacidad y protección de la información de datos personales aplicando los controles requeridos por el SGSI.

7.2.2. Toma de conciencia, educación y formación en la seguridad de la información.

La Defensoría adoptará un esquema de formación continua para que de forma permanente sus funcionarios y las terceras partes conozcan los riesgos de seguridad de la información y sus obligaciones para proteger los activos de información.

- Establecer procesos de evaluación a los servidores públicos frente al desempeño de la seguridad de la información, propiciar los espacios de capacitación necesarios en los cuales se adquieran y/o fortalezcan las competencias necesarias y evaluar la eficacia de las capacitaciones realizadas.

- Incluir en todos los programas de capacitación del proceso de gestión del talento humano tales como, inducción, re inducción y sensibilización capítulos que se enfoquen en favorecer la concientización de los servidores públicos a cerca de la importancia de la seguridad de la información en la entidad.

7.2.3. Proceso disciplinario.

Todo incidente de seguridad en los activos de información en los que estén involucrados funcionarios podrá ser investigado por la Oficina de Control Interno Disciplinario de la Defensoría del Pueblo de acuerdo con los procedimientos establecidos, con el fin de determinar responsabilidades e imponer las sanciones previstas en la normatividad a este respecto, para ello contará con el apoyo técnico del Líder u Oficial de Seguridad de la Información.

En los incidentes de seguridad de la información en los que estén involucrados terceras partes, que sean reportadas al Oficial de Seguridad de la Información, serán informadas por éste, de forma inmediata, al Comité de gestión institucional, el que a su vez informará a la Oficina Jurídica para el inicio de las acciones judiciales pertinentes.

7.3. Terminación o cambio de empleo.

Las políticas de este numeral buscan asegurar que los funcionarios o terceras partes terminen su vinculación laboral o contractual con la Entidad en estricto cumplimiento de lo establecido en la legislación colombiana.

7.3.1. Políticas para terminación o cambio de empleo.

- Definir las directrices para que la desvinculación o cambio de cargo de un servidor público de la Defensoria del Pueblo, se realice en cumplimiento de las políticas de seguridad de la información.

- Informar al grupo de Tecnologías de la información y las comunicaciones a cerca de las novedades que se presenten con los servidores públicos de la Defensoria del Pueblo, tales como, incapacidad, desvinculación total, licencias remuneradas y no remuneradas, suspensión, vacaciones, cambios de cargo, con el fin de que se realicen las actualizaciones en los accesos a las diferentes aplicaciones y servicios tecnológicos de la entidad.

8. Gestión de activos.

Establecer los lineamientos para identificar todos los activos de información institucionales y definir las responsabilidades de protección apropiadas.

8.1. Responsabilidad por los activos.

Este control tiene como objetivo lograr y mantener la protección adecuada de todos los activos de la información de la Entidad.

8.1.1. Inventario de activos.

El Líder u oficial de seguridad de la información o quien haga sus veces, de orientar y apoyar a la identificación de activos de información al interior de la entidad, con el objeto de garantizar que los inventarios de activos de cada una de las dependencias de la Defensoría del Pueblo se encuentren alineados tanto con las Tablas de Retención Documental como con los criterios establecidos en el procedimiento de Identificación, Valoración y Clasificación de Activos de Información, asegurando que:

- Toda la información contenida en los activos sea clasificada por su criticidad, valor y disposiciones normativas legales, atendiendo para ello lo indicado tanto por los propietarios de la información como por el la Defensoria del Pueblo

- La Matriz de identificación y clasificación de activos de información permanezca en un repositorio seguro con acceso restringido.

- La Matriz de identificación y clasificación de activos de información se actualice por lo menos una vez al año y/o cuando se presenten retiros, adquisiciones o reemplazos en los activos identificados.

Aunado a esto, la Defensoría del Pueblo debe contar un inventario de activos (hardware y software) para lograr la adecuada identificación y estado de estos activos, así como su respectiva protección contra amenazas o afectaciones por materialización de riesgos. El inventario debe incluir la información relevante al tipo de activo especificando su ubicación, características, condiciones, información de licencias y su valor económico estimado. Los activos se asignarán a un funcionario quien será responsable por su custodia y protección, según lo establecido en el Manual Integrado para el Manejo de los Bienes de Propiedad de la Defensoría del Pueblo.

8.1.2. Propiedad de los activos.

El actor relacionado con el SGSI y que adelante funciones como propietario de activos de información en la Defensoría del Pueblo, deberá:

- Garantizar que todos los activos de información que se encuentran asignados a su responsabilidad sean incluidos correctamente en el respectivo inventario.

- Validar que los activos de información a su cargo, se encuentren clasificados y protegidos en concordancia con el nivel de criticidad, valoración y las disposiciones normativas legales vigentes, Revisar periódicamente por lo menos una vez al año o cuando se incurra en un cambio significativo, las restricciones y clasificaciones de acceso a los activos de información.

- Controlar que los procedimientos de eliminación o destrucción estén acorde con la reglamentación de manera que no se permita la exposición de los activos de información a terceros.

Los activos adquiridos, así como la información que en ellos se genere, almacene o procese son de propiedad la Defensoría del Pueblo. La entidad en cualquier momento puede disponer de esos activos y asignárselo a otro funcionario o contratista para su custodia y protección.

8.1.3. Uso aceptable de los activos.

Todos los actores relacionados con el SGSI (funcionarios, contratistas, proveedores y terceras partes) que dadas sus funciones u objetos contractuales tengan bajo su propiedad o custodia activos de información de la Defensoria del Pueblo, deben dar estricto cumplimiento a lo estipulado en la *Guía de uso aceptable de los activos de información*[3]

8.1.4. Devolución de los activos.

Los activos asignados a los funcionarios o terceras partes que finalizan su relación laboral o contractual deben ser reintegrados según lo establecido en el Manual Integrado para el manejo de los bienes de propiedad de la Defensoría del Pueblo.

- El Grupo de TIC de la Defensoria del Pueblo debe garantizar que sobre todo activo de información que se encuentre bajo su custodia, o que sea devuelto o que vaya a ser reasignado o dado de baja, se apliquen los controles establecidos en el procedimiento de *Disposición segura de los medios*.

[3] Ver: la *Guía de uso aceptable de los activos de información*

8.2. Clasificación de la información.

La información de la Defensoría del Pueblo es generada tanto por dispositivos electrónicos y sistemas de información como por los funcionarios que interactúan con estos, por tanto, es obligación de la Defensoría del Pueblo garantizar la clasificación y protección de esta información.

8.2.1. Clasificación de la información.

Los niveles de clasificación de información establecidos por la Defensoría del Pueblo mediante la metodología de gestión de activos de información son: Pública, de uso interno, Reservada y Confidencial, en ese orden de ideas, el líder del proceso se obliga a clasificar y proporcionar el tratamiento adecuado a la información en concordancia con los niveles mencionados y en estricto seguimiento de los lineamientos del *Procedimiento de Valoración, identificación y clasificación de activos de información de la Defensoria del Pueblo.*

La eliminación y destrucción de la información debe realizarse acorde a su nivel de clasificación y siguiendo los lineamientos de la *Guía de clasificación y rotulado de información de la Defensoria del Pueblo.*

8.2.2. Etiquetado de la información.

Todos los activos de información de la Defensoría del Pueblo deben poseer un etiquetado en el cual se especifique el nivel de clasificación que le ha sido asignado, este (el etiquetado) debe ser empleado para la información que se encuentre tanto en medio físico como en medio electrónico.

8.3. Manejo de Activos de información.

La consideración de la clasificación anteriormente definida es obligatoria para el procesamiento, almacenamiento, manejo y comunicación de la información en la Defensoría del Pueblo.

8.3.1. Gestión de medios removibles.

El manejo de los medios removibles de almacenamiento deberá darse de acuerdo con el grado de confidencialidad de la información en él contenida, por lo tanto, el responsable de estos debe tomar mayores medidas de protección de estos, cuanto mayor sea la confidencialidad de la información contenida.

La gestión de los medios removibles comprende, la eliminación o destrucción de estos medios. Cuando ya no se requieran estos medios, su eliminación se debe hacer de forma segura y sin riesgo de que exista una posible divulgación de información confidencial. También se debe tener en cuenta que con borrar o formatear un medio determinado, es muy posible que no se elimine toda la información existente de carácter confidencial.

Los propietarios de medios deben asegurar que éstos no queden desatendidos debido a que pueden ser susceptibles de pérdida o robo de la información. El propietario es el único responsable de mantener la confidencialidad, integridad y disponibilidad de la información contenida en el medio a su cargo, por tanto, está obligado a registrar en la recepción, la entrada y salida del medio removible.

La protección a los medios debe hacerse de acuerdo con el nivel de clasificación de la información contenida en ellos.

8.3.2. Disposición de los medios.

Una vez terminado el ciclo de vida útil de un determinado medio de almacenamiento, la información allí contenida, debe ser eliminada de manera segura de acuerdo con los procedimientos formales previamente establecidos por la entidad.

8.3.3. Transferencia de medios físicos.

Cuando por razones de seguridad, del servicio o por contingencia se deba transportar afuera de la Entidad medios extraíbles de almacenamiento de información, como backups y demás información confidencial, además de las medidas razonables de seguridad a implementar, se requiere también que existan acuerdos de confidencialidad con el fin de garantizar un uso y transporte seguro de la información. Estos acuerdos son de cumplimiento obligatorio para ambas partes y deben estar vigentes por mucho más tiempo que la duración del contrato.

Para el transporte de información fuera de las instalaciones de la Defensoría en medios extraíbles, se debe considerar lo siguiente:

- Utilización de empresas que tengan acuerdos de confidencialidad firmados con todos sus empleados en lo posible de por vida.
- Empresas de más de cinco (5) años de experiencia en ese negocio.
- Empresas que cumplan con normas de calidad respaldadas por certificaciones ISO.
- Se deben firmar acuerdos de confidencialidad entre las partes.
- Los sistemas de transporte deben tener mecanismos que permitan ubicarlos durante todo su recorrido, como GPS o rastreo satelital.
- La empresa contratada debe llevar un registro en línea de los activos transportados y garantizar la existencia de seguridad física y ambiental en sus sistemas de transporte.

9. Control de acceso.

Establecer los lineamientos para evitar el acceso no autorizado a la información y a las instalaciones de procesamiento de información de la Defensoría del Pueblo.

9.1. Requisitos del negocio para control de acceso

Los siguientes son los requisitos del negocio para el control de acceso definidos para la Defensoría del Pueblo en los términos del SGSI:

- Aquellos quienes fungen como administradores de control de acceso lógico están en la obligación de definir y establecer las medidas de control pertinentes para el acceso por parte de los funcionarios, contratistas, proveedores y terceras partes, empleando mecanismos de identificación, autenticación y autorización de acceso a las redes institucionales, así como a los sistemas de información, y servicios de TI en concordancia con los perfiles y cargos establecidos en la Defensoria del Pueblo.

- Aquellos quienes fungen como administradores de control de acceso lógico están en la obligación de cumplir con la aprobación o rechazo de los permisos de conexión remota o VPN, previamente conferido por el Secretario General de la Defensoria del Pueblo o quien haga sus veces. En lo referente a la solicitud de acceso lógico que realicen los funcionarios, contratistas, proveedores o terceras partes, debe estar sustentada con los registros de vinculación a la entidad generados en el sistema administrativo y financiero – SIAF, esto con el fin de demostrar que se cuenta con una vinculación vigente.

- Aquellos quienes fungen como administradores de control de acceso lógico están en la obligación de hacer cumplir el procedimiento de autorización y controles con el fin de proteger el acceso a las redes de datos, y los diferentes recursos de red de la Defensoria del Pueblo.

- Aquellos quienes fungen como administradores de control de acceso lógico están en la obligación de realizar una verificación de los controles de acceso a los funcionarios, contratistas, proveedores y terceras partes definiendo la periodicidad en la cual se va a ejecutar, lo anterior, con el ánimo de garantizar que dichos usuarios tienen acceso únicamente a los recursos autorizados para la ejecución de sus funciones asignadas; de la misma manera, periódicamente se debe realizar la suspensión de los usuarios que contando con acceso habilitado presenten cualquier tipo de novedad que así lo merezca.

- En virtud del artículo ZZZ de la directiva presidencial número XXX del YYYY se prohíbe el uso de redes inalámbricas para uso de sistemas de información de índole misional de la Defensoria del Pueblo, sin embargo, se asegurará el acceso a internet para los usuarios externos de la entidad.

- Es responsabilidad de los funcionarios, contratistas, proveedores o terceras partes, el buen manejo y uso de los recursos, así como de las claves que le han sido asignadas.

9.1.1. Política de control de acceso.

Esta política aplica a todas las partes involucradas que por su rol definido requieran acceder a la información y a las instalaciones de procesamiento de información de la Defensoría del Pueblo.

- Registro de usuarios

- En cada aplicativo o sistema de información se debe documentar un procedimiento formal para el registro y cancelación de los usuarios del mismo y cómo se concede o revoca el acceso a la aplicación. El procedimiento debe incluir los siguientes puntos:

- La identificación única de usuario.

- Verificar que los usuarios tengan la autorización del director del área o el representante del proceso.

- Verificar que el nivel de acceso otorgado es el adecuado y acordado con el autorizado por el director del área o el representante del proceso.

- Informar formalmente por escrito a cada usuario de la declaración de sus derechos de acceso.

- Contar con el registro de aceptación del usuario de las condiciones de uso del sistema de información.

- Si la aplicación contiene información sensible o privilegiada el usuario debe aceptar formalmente el Acuerdo de Confidencialidad aplicable.

- Establecer un control para evitar que se otorgue el acceso hasta que se hayan finalizado los procedimientos de autorización.

- Retirar, bloquear inmediatamente el acceso de los usuarios que han dejado de pertenecer a la Defensoría del Pueblo, se les haya vencido o caducado sus contratos de trabajo o prestación de servicios o cambien de funciones donde no requieran el acceso al sistema de información o la red de datos de la organización.

9.1.2. Política sobre el uso de los servicios de red.

Todos los funcionarios, contratistas, proveedores o terceras partes que, con ocasión a sus funciones u objetos contractuales con la Defensoría del Pueblo, requieran acceso a los diferentes sistemas de información de la entidad, deben utilizar el nombre de usuario del Dominio **Defensoria.gov.co**, asegurando la asignación de una contraseña segura que cumpla con los requerimientos base de las políticas de seguridad de la información adoptadas por la entidad, esta contraseña, debe ser personal e intransferible.

El acceso a los sistemas de información o a la infraestructura tecnológica de la Defensoría del Pueblo, a través del uso de usuario del dominio **Defensoria.gov.co** es restringido y delimitado a las tareas, funciones, responsabilidades u objetos contractuales que lleven a cabo funcionarios, contratistas, proveedores o terceras partes en la entidad.

La asignación inicial de la contraseña de acceso a los servicios se realizará de acuerdo con el procedimiento de gestión de usuarios de dominio y es obligación del usuario realizar el cambio de esta por una contraseña segura en el momento en el que reciba su asignación de usuario.

Las contraseñas seguras están definidas de acuerdo con los siguientes criterios base:

- Definir contraseñas que no sean fáciles de descifrar evitando que contengan información relacionada con sus labores o situaciones personales como: números de identificación, números telefónicos, nombres de conyugues o hijos, direcciones postales, lugares conocidos o términos técnicos.

- Mezclar palabras (Mayúsculas o minúsculas), signos de puntuación, números y/o símbolos especiales, de manera tal que se defina una contraseña alfanumérica con símbolos.

- Transformar una palabra común utilizando un método específico.

- Definir acrónimos como contraseñas (siglas que forman una palabra)

- Crear contraseñas que contengan como mínimo 8 dígitos y cambiarla en intervalos mínimos de 60 días.

- El ingreso de una contraseña no exitosa, tendrá un número de veces definidas y establecidas por la entidad, al cumplir ese número de veces no exitosas, el usuario será bloqueado de manera inmediata, y será necesario elevar la solicitud de desbloqueo de la misma a través del gestor de incidentes de TIC a quien ejecute el rol de administración de control de acceso lógico.

Las contraseñas de acceso de un determinado sistema que sean entregadas a través de correo electrónico por el respectivo administrador, serán cambiadas de manera inmediata en el instante en que sea recibida por parte del usuario a quien ha sido asignado el acceso, teniendo como base los criterios y protocolos de seguridad de la información presentados en este documento.

Se prohíbe el almacenamiento de contraseñas en cualquier formato legible tales como documentos, post-it, agendas de trabajo, computadores carentes de sistemas de control de acceso o cualquier sitio o dispositivo en el cual personas no autorizadas puedan encontrarlas.

Si llegase a existir la sospecha por parte de algún miembro de la organización o terceras partes a cerca de la perdida de confidencialidad de alguna de las contraseñas que maneja, debe notificar de manera escrita por medio del gestor de incidentes de TI siguiendo los lineamientos del procedimiento de gestión de mesa de ayuda, o el procedimiento de gestión de incidentes de seguridad según sea el caso, con el fin de tomar las medidas necesarias y pertinentes para el aseguramiento de la información.

9.2. Gestión de acceso a usuarios.

La Defensoría del Pueblo se encuentra en el deber de asegurar, preservar y garantizar el control de acceso a todos los sistemas y aplicaciones institucionales, por lo cual, es necesario el cumplimiento de los parámetros de seguridad plasmados en los siguientes numerales.

9.2.1. Registro y cancelación del registro de usuarios.

Cada sistema de información empleado en la Defensoría del Pueblo debe contar con un procedimiento formal para el registro y cancelación de los usuarios que lo utilizan, en este se debe definir claramente cómo se realiza la concesión y revocación del acceso a la aplicación, el procedimiento debe incluir como mínimo los siguientes puntos:

- Identificación única de usuario.

- Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos, las necesidades de uso y la clasificación de la información, además de la autorización de acceso escrita o por incidente interpuesto por el líder del proceso o quien ejecute sus veces a través de la plataforma de gestión de solicitudes de tecnología de la entidad.

-

9.2.2. Suministro de acceso de usuarios.

Con el fin de proteger de accesos no autorizados los activos de información y los sistemas de información institucional, la Defensoría del Pueblo define como control la asignación de privilegios en estos activos y sistemas, haciéndolo parte integral del procedimiento de registro y cancelación de usuarios, dentro del cual se debe garantizar la implementación de las siguientes condiciones:

- Implementar recursos en los cuales se especifique las condiciones del servicio (ToS) en los cuales se explique de manera clara y precisa cuáles serán las condiciones de servicio prestado, a fin de establecer la forma en que se deben emplear los sistemas de información y las posibles consecuencias al incumplimiento de estas.

- Implementar un registro de aceptación del usuario de las condiciones de uso del sistema de información.

- En lo que respecta a la autorización inicial y continuidad en el uso de los usuarios de los aplicativos misionales de la entidad, será deber de cada una de las dependencias informar a los Administradores de las aplicaciones la novedad o novedades que surjan en cuanto a servidores públicos, contratistas, proveedores o terceras partes, con el objeto de que dichos usuarios sean autorizados y habilitados, deshabilitados o suspendidos oportunamente, según sea el caso.

9.2.3. Gestión de derechos de acceso privilegiado.

la Defensoría del Pueblo debe definir como parte del procedimiento de registro y cancelación de usuarios, la asignación de derechos de acceso privilegiado, lo anterior, a fin de mantener un control estricto teniendo en cuenta que estos accesos se perfilan como los más altos en los sistemas de información aunado a los derechos adicionales que generalmente se transmiten sobre los activos de información y los sistemas que los controlan, para lo cual es necesario tener presente las siguientes recomendaciones:

- Plena identificación de los usuarios y privilegios que le han sido concedidos para el acceso a cada módulo o componente del sistema de información.

- Asignar privilegios de conformidad con las necesidades y uso para cada módulo o parte del aplicativo.

- Contar con un registro del procedimiento de registro y cancelación de usuarios, en el cual se evidencien los accesos autorizados, así como los privilegios autorizados por el superior inmediato, lo anterior con el fin de mantener la documentación necesaria para revisiones futuras, los privilegios sobre activos de información y sistemas de información no serán otorgados hasta tanto no surtan efecto las fases de autorización del procedimiento mencionado.

- Cualquier cambio en los privilegios asignados deben ser definidos en un procedimiento de gestión de cambios, no se otorgarán o negarán privilegios si esta acción desencadena en la interferencia de alguna funcionalidad o la seguridad de la aplicación.

9.2.4. Gestión de información de autenticación secreta de usuarios.

Para todos los activos y sistemas de información de la Defensoría del Pueblo se deben definir practicas y/o técnicas de control que permitan asegurar las contraseñas de acceso a los diferentes activos y sistemas de información de la entidad reduciendo los riesgos accesos no autorizados a información y/o configuraciones, en ese sentido se deben aplicar las siguientes recomendaciones según sea el caso:

- Es obligatorio realizar la actualización de contraseñas para dispositivos de infraestructura de red tales como Routers, Switches, puntos de acceso inalámbrico entre otros, de manera que, al ponerse en servicio de la infraestructura de la entidad, no se encuentren con el acceso predeterminado por el fabricante.

- Cuando un usuario reciba una asignación o reasignación de contraseña, quien la recibe la empleará solo en el primer inicio de sesión y será obligatorio el cambio de esta, a fin de garantizar que solo el usuario la conozca.

- Cuando el software lo permita, se limitará a 5 el número de intentos fallidos, luego de lo cual la cuenta quedará deshabilitada y el usuario deberá solicitar su desbloqueo al administrador del sistema.

- EL tamaño mínimo obligado de cada contraseña es de ocho (8) caracteres, para el caso de cuentas privilegiadas (administradores de sistemas, dispositivos de infraestructura, controles de acceso físico entre otros) el tamaño mínimo será de 12 caracteres.

- Las contraseñas deben ser inusuales, es decir que no sean fácilmente reconocibles, complejas, sin sentido, compuestas de una mezcla de letras no repetidas (mezclando mayúsculas y minúsculas), números y símbolos que no contengan palabras que sean fáciles de identificar con el uso de un

diccionario de cualquier idioma o que tengan cualquier otro contexto previsible (ID del empleado, fechas etc.), o una secuencia de teclas del teclado, tales como'qwerty12345'o'asdfg09876'

- Una contraseña no puede ser usada por más de 60 días, para el caso de cuentas privilegiadas el tiempo de uso será de 45 días. Al cabo de tal periodo debe cambiarse, o cada vez que exista la sospecha de que la misma puede ser adivinada.

- Al momento de ingresar una contraseña, se debe tener en cuenta que el sistema debe "enmascarar", ocultar o de cualquier otra manera esconder el verdadero carácter ingresado en pantalla. Se recomienda observar especial cuidado al ingresar contraseñas en equipos ajenos o en presencia de otros usuarios. En caso de duda, siempre se debe cambiar la contraseña inmediatamente.

9.2.5. Revisión de los derechos de acceso de usuarios.

Quien figure como propietario de un activo o sistema de información, debe establecer un procedimiento en el cual se mantenga periódicamente el control a los privilegios de acceso a los usuarios, de manera que se garantice que cada usuario cuenta con el acceso exclusivamente a lo autorizado en concordancia con su perfil y las funciones que ejerce, adicionalmente se debe definir una verificación periódica de cuentas de usuario que se encuentren deshabilitadas por desvinculación.

El procedimiento debe considerar:

- El propietario de los activos debe revisar los privilegios de acceso de los usuarios como mínimo cada tres meses o ante cualquier cambio del perfil o de algún usuario.

- Los privilegios se deben revisar y ajustar ante cambios en el cargo o roles dentro de la Defensoría del Pueblo.

- El propietario del activo debe verificar los privilegios asignados para evitar que no se hayan asignado privilegios no autorizados.

9.2.6. Retiro o ajuste los derechos de acceso.

Una vez terminada la vinculación de funcionarios, contratistas y terceras partes con la entidad todos los propietarios de activos deben retirar los privilegios de acceso a estos, de igual manera se debe proceder con los accesos a las áreas de la entidad.

9.3. Responsabilidades de los usuarios.

En este apartado las políticas definen las directrices con el objetivo de proteger la información de la Defensoría del Pueblo de accesos no autorizados, robo, o divulgación de información clasificada por desconocimiento, descuido o desinformación de los usuarios que tienen acceso y control sobre esta.

Es deber de los funcionarios, contratistas y terceras partes conocer las responsabilidades del buen uso de todas las credenciales de acceso que le han sido asignadas tales como nombres de usuario, tarjetas de ingreso, pines de acceso entre otros a fin de evitar cualquier acceso no autorizado a activos de información, el robo o daño deliberado de información o de los servicios de procesamiento de información.

Los funcionarios, contratistas y partes interesadas a quienes se asigne una cuenta institucional están obligadas a leer y entender las políticas de seguridad, aplicables y vigentes de la organización.

9.3.1. Uso de la información de autenticación secreta.

La Defensoría del Pueblo define para todos los usuarios con acceso a los servicios de información y sistemas de información de la entidad las siguientes disposiciones a fin de proteger la información institucional, de usuarios y terceros relacionados.

- La contraseña es de carácter personal e intransferible, no debe compartirse o ser revelada a otros. El hacerlo expone al propietario a las consecuencias por las acciones que los otros hagan con esa contraseña.
- Cuando el administrador de cuentas de usuario asigne una nueva contraseña, el propietario la utilizará solo en el primer inicio de sesión. En los subsiguientes es obligatorio realizar el cambio de contraseña para garantizar que solo él la conoce.
- Los usuarios finales NO deben escribir sus contraseñas en ningún lugar físico o medio magnético. Para este efecto se recomienda utilizar métodos de creación de contraseñas fáciles de aprender y evitar la reutilización.
- La divulgación no autorizada y voluntaria de una contraseña que implique un incidente de seguridad puede dar como resultado la suspensión o negación del servicio y/o privilegios de acceso al servicio, datos o información, y las demás consecuencias en términos disciplinarios que sean aplicables.
- En los casos en los que el usuario sospeche u observe comportamientos sospechosos o anómalos a través de su cuenta, como accesos indebidos, mensajes no autorizados, debe cambiar su contraseña de forma inmediata y reportar este incidente de seguridad al grupo de sistemas de la Defensoría del Pueblo.

9.4. Control de acceso a sistemas y aplicaciones.

La Defensoría del Pueblo define los siguientes parámetros de seguridad para salvaguardar, conservar y mantener el control de acceso a los sistemas de información y activos de la entidad.

9.4.1. Restricción de acceso Información.

Con el fin de ofrecer la mayor protección a la información a continuación se presentan los criterios básicos definidos para el acceso.

- El propietario de la aplicación y de la información, deberá identificar y documentar explícitamente la sensibilidad o confidencialidad de la información contenida en los sistemas y aplicaciones de la entidad.
- Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos, las necesidades de uso y la clasificación de la información
- No está permitido para ningún servidor público, contratista, proveedor o terceras partes, acceder a la información y a las aplicaciones de un sistema de información para el cual no haya sido autorizado.

9.4.2. Procedimiento de ingreso seguro.

La Defensoría del Pueblo controlara el acceso a sistemas de información y aplicativos misionales mediante la aplicación de los siguientes criterios:

- Los propietarios de los activos de información deberán identificar y documentar de manera explícita la sensibilidad o confidencialidad de la información contenida en los sistemas y aplicaciones de la Defensoria del Pueblo.

- Los propietarios de los activos de información autorizaran el acceso a sus sistemas de información en concordancia con la perfilación de los usuarios, las necesidades de uso y la clasificación de la información.

- Está totalmente prohibido el acceso a la información y a los sistemas de información para los cuales los funcionarios, contratistas, proveedores o terceras partes no estén debidamente perfilados y autorizados.

- Los administradores de infraestructura de la Defensoria del Pueblo deben asegurar la segmentación en las redes de los diferentes grupos de servicios de información, usuarios y sistemas de información.

- Los administradores de infraestructura de la Defensoria del Pueblos deben asegurar que los usuarios empleen los perfiles definidos para los ambientes de desarrollo, pruebas y producción.

9.4.3. Sistema de gestión de contraseñas.

Con el ánimo de garantizar los accesos y la protección de la información institucional, de usuarios y terceros relacionados, La Defensoria del Pueblo deberá incluir en su infraestructura herramientas que permitan realizar el cambio de la contraseña por parte tanto de los usuarios como de los administradores.

9.4.4. Uso de programas utilitarios privilegiados.

La Defensoria del Pueblo en aras de mantener la protección de los activos de información, equipos y sistemas de información implementará herramientas mediante las cuales se controle el uso de aplicaciones utilitarias que puedan tener capacidad de anular el sistema y los controles de las aplicaciones.

En todo caso, exclusivamente se autorizará el uso de dichas herramientas a los funcionarios que fungen como administradores de los sistemas de información y activos de información (hardware) de la entidad.

9.4.5. Control de acceso a códigos fuente de programas.

La Defensoria del Pueblo, define controles de acceso a los códigos fuente de sistemas de información y aplicaciones propias de la entidad en concordancia con las siguientes disposiciones.

- El profesional encargado de la coordinación del grupo de TIC de la entidad o quien haga sus veces, deberá asignar el rol de administrador de programas fuentes, el cual tendrá bajo su custodia y protección los mencionados programas y, en virtud de esa función no podrá hacer parte de ningún equipo de desarrollo de la entidad.

- El(los) administrador(es) de programas fuentes designado(s) deben mantener una bitácora actualizada de todos los programas fuentes en uso, definiendo claramente el proyecto, desarrollador, versión, fechas de modificaciones y estado, para esto, es posible valerse del uso de herramientas de versionado que permitan un orden y clasificación de los proyectos.

-

- El(los) administrador(es) de programas fuentes designado(s) debe establecer límites de acceso a los códigos fuente de las aplicaciones de la entidad, para lo cual debe asegurarse de que los desarrolladores asignados a un proyecto sean los únicos que cuentan con el acceso autorizado.

- El(los) administrador(es) de programas fuentes designado(s) deben mantener los códigos fuente de las aplicaciones de la entidad bajo custodia en un servidor, o herramienta de versionado especializada.

- El(los) administrador(es) de programas fuentes designado(s) debe (n) mantener un registro de auditoría de todos los accesos a los repositorios o herramientas de versionado de fuentes del programa.

- El(los) administrador(es) de programas fuentes designado(s) debe(n) asegurarse de que los programas fuentes cuenten con una copia de respaldo actualizada, conforme a lo estipulado en el procedimiento de back up.

10. Criptografía.

10.1. Controles criptográficos.

La Defensoria del Pueblo define los criterios necesarios para, en caso de requerirlo, regular el uso de controles criptográficos para el aseguramiento de la información, incluyendo criterios de uso, protección y ciclo de vida de las claves criptográficas.

10.1.1. Política sobre el uso de controles criptográficos.

SI la Defensoría del Pueblo se ve avocada al uso de controles de cifrado, se definirá un administrador encargado de velar por la correcta protección al equipamiento empleado para crear, y almacenar las claves privadas considerándolo un activo crítico y de alto riesgo.

Adicionalmente, deberá garantizar que los nuevos desarrollos o actualizaciones de los sistemas de información se realice una correcta identificación de datos sensibles, y definirá los requisitos en términos de salvaguarda y mecanismos de cifrado empleados para almacenamiento, transporte, validación y control de acceso.

10.1.2. Gestión de llaves.

Las llaves o claves criptográficas deben ser protegidas contra cualquier riesgo que involucre situaciones como pérdida, modificación y destrucción no autorizadas, por lo tanto, es necesario que los administradores de estas elaboren un análisis exhaustivo de riesgos en el cual se consideren además los criterios de confidencialidad, integridad/autenticidad, no repudio, así como las tecnologías de cifrado disponibles y los costos relacionados.

Así mismo, se deben considerar las siguientes medidas para la protección de los controles criptográficos:

- Definir el protocolo para activar y recibir las claves y su distribución a los usuarios autorizados.

- Definir criterios para el almacenamiento de las claves y la forma de acceso por parte de los usuarios autorizados.

- Definir criterios para el cambio o actualización de las claves.

- Revocar las claves cuando se han puesto en peligro o cuando se retira el funcionario de la organización.

- Definir procedimiento para recuperar claves pérdidas o corruptas

- Definir criterios para archivar las claves y para destruirlas

- Mantener registros de auditoría de las actividades de gestión de claves.

- En los casos en los cuales sea necesario el uso de servicios criptográficos de terceros, se deberán incluir en los acuerdos de prestación de servicio criterios específicos de responsabilidad civil, fiabilidad y seguridad del servicio además de los tiempos de aprovisionamiento.

- Los funcionarios y contratistas a quienes les sean asignados los tokens de seguridad están obligados a salvaguardar estos dispositivos en un lugar bajo llave en el cual se evite el libre acceso a estos.

11. Seguridad física y del entorno.

Las estrategias sobre seguridad física en las áreas restringidas buscan identificar las posibles amenazas y vulnerabilidades existentes, junto con las medidas correctivas y preventivas que pudieran ser utilizadas, con el fin de proteger físicamente los recursos y la información de la organización. Estos recursos incluyen por ejemplo el personal, el sitio donde ellos laboran, los datos, los equipos y también los medios de almacenamiento; en general los activos asociados al almacenamiento, transporte y procesamiento de la información.

11.1. Áreas seguras.

La Defensoría del Pueblo define en esta política las áreas que deben ser consideradas como restringidas y por tanto susceptibles de especial protección, previniendo el acceso no autorizado que pueda desencadenar en el daño o la interferencia a la información y a las instalaciones de procesamiento de datos de la entidad.

11.1.1. Perímetro de seguridad física.

Las áreas y dependencias de la Defensoría del pueblo deben contar con esquemas de protección como barreras y controles físicos de acceso, de la misma manera, deben estar monitoreadas y supervisadas con un circuito cerrado de cámaras, se consideran como mínimo las siguientes áreas seguras y de acceso restringido:

- **Centro de procesamiento de datos:** corresponde al denominado data center, lugar en donde se albergan los dispositivos de procesamiento (servidores físicos y virtuales) que a su vez alojan los sistemas de información (aplicaciones, bases de datos), los componentes primarios de comunicaciones y los sistemas de almacenamiento.

- **Centros de cableado:** corresponde a las áreas definidas como de unión central, es decir, aquellas que se usan para conectar los dispositivos de la red del área local (LAN) de la Defensoria del Pueblo, las cuales almacenan los diferentes dispositivos de redes como: paneles de conexión, Hubs de cableado, Switches, Router, Puentes, entre otros.

- **Bodegas administradas por TI:** Son áreas definidas por el grupo de TIC para la manipulación, alistamiento, reparación y bodegaje de los equipos de infraestructura tecnológica que se administran en la entidad, usualmente empleada por los equipos de soporte técnico.

- **Cuartos de suministro:** Áreas en las cuales se encuentran localizados los dispositivos que soportan los servicios de suministro de energía como: las UPS y la planta eléctrica.
- **Archivo físico central:** Áreas en donde se administran, custodian y conservan los documentos físicos con valor administrativo, legal, permanente e histórico entre otros, para la Defensoria del Pueblo y que son transferidos por las diferentes dependencias.
- **Archivo físico de gestión:**
- Hace referencia a aquella documentación todavía en trámite que conservan las oficinas, así como a aquella que aun después de finalizado el procedimiento administrativo, está sometida a uso continuo y consulta administrativa por las mismas oficinas, aplicando para ello lo dispuesto en las tablas de retención documental.
- **Cuarto de control:** área dispuesta por la Defensoría del Pueblo para el control y monitoreo del circuito cerrado de cámaras, así como el control de vigilancia de la entidad.
- **Sala de los Derechos:** Oficina definida por la alta dirección para el manejo de situaciones especiales a nivel nacional en la cual se interrelacionan un conjunto de herramientas y organizaciones para coordinar la respuesta más rápida y eficiente a la situación presentada.
- **Oficina de tecnología:** Área en la cual convergen los diferentes profesionales que se encargan de mantener los servicios tecnológicos de la entidad en correcto estado de funcionamiento.
- **Oficina del tesorero:** Área dispuesta para la unidad organizacional encargada de administrar los recursos financieros de la Defensoría del Pueblo en concordancia con las funciones asignadas.

Para todas las dependencias de la Defensoría del Pueblo que debido a sus funciones administren información considerada reservada o sensible, deben ser consideradas como dependencias con áreas seguras, por tanto, deberán adoptarse mecanismos tendientes a salvaguardar la mencionada información, por lo anteriormente expuesto, la Defensoría del Pueblo se consideran los siguientes lineamientos a adoptar:

- Cuando las áreas cuyas ventanas estén expuestas al exterior debido a su ubicación, es necesario impedir la visibilidad hacia el interior empleando los dispositivos que sean necesarios como persianas lockout, recubrimiento a los cristales, y/o cerraduras en caso de requerirse.

- Las áreas seguras deben emplear cerraduras de seguridad.

- Implementar el uso de cerraduras de seguridad en las puertas de las áreas seguras con el objeto de que permanezcan cerradas.

- Los privilegios de acceso a las áreas seguras de la Defensoria del Pueblo deben ser definidos y otorgados por el profesional u oficina encargada del área segura, para ello debe tener en cuenta los siguientes tipos de usuario:

    - Profesionales que trabajan regularmente en las áreas seguras.

    - Profesional de soporte que requiere acceso periódico.

- Visitantes (servidores públicos, contratistas, proveedores o terceras partes) que requieren acceder muy rara vez.

11.1.2. Controles físicos de entrada.

Para el ingreso a las instalaciones de la entidad, funcionarios y contratistas deberán identificarse plenamente con el carné institucional que los acredita con vinculación a la entidad, así mismo, deberán portarlo permanentemente en un lugar visible, este requisito será exigible por el personal de seguridad de la entidad.

Todos los visitantes sin excepción deben ser anunciados y autorizados previamente por un funcionario, para su identificación como visitante se asignará una escarapela y se realizará el correspondiente registro en el sistema de control de acceso de visitantes.

Los accesos físicos a las áreas de centro de procesamiento de datos, almacenamiento de información confidencial o privada y archivo físico central permanecerán cerradas en todo momento, y el acceso será limitado exclusivamente a quienes por sus funciones se encuentren debidamente autorizados, el personal externo que requiera acceso deberá solicitarlo al jefe del área correspondiente y estará supeditado al acompañamiento permanente de un funcionario del área.

11.1.3. Seguridad de oficinas, recintos e instalaciones.

Para el aseguramiento de las oficinas y los diferentes recintos de la Defensoría del Pueblo se deberán tener presentes las siguientes directrices.

- Limpiar y eliminar todo rastro de escritura en los tableros, pizarras o Boards inteligentes de la Defensoria del Pueblo, de la misma manera, abstenerse de dejar documentos, apuntes o notas escritas en los espacios al finalizar las reuniones.

- Los visitantes que tengan acceso a las diferentes oficinas de las dependencias o a las áreas seguras de la Defensoria del Pueblo, deben estar acompañados siempre por un funcionario o contratista de la entidad.

- Cuando un visitante requiera permanecer en las oficinas de la Defensoria del Pueblo por un periodo de tiempo superior a dos (2) días deberán ser presentados a los funcionarios de la oficina en la cual permanecerán.

- La Defensoria del Pueblo implementará mecanismos de protección para los dispositivos de almacenamiento de información externos al igual que la información que se considera confidencial, sin importar el medio en el cual se encuentre, es obligación mantenerlos bajo seguridad en los horarios no hábiles o en los horarios en los cuales los funcionarios, contratistas y terceros responsables no se encuentren laborando.

- Los funcionarios encargados de las áreas del centro de procesamiento de datos o de las áreas seguras donde se ubiquen los activos de información confidencial, deben velar por que no se realicen registros fotográficos o grabaciones de video que puedan llegar a comprometer la seguridad de la información o

la imagen de la Defensoria del Pueblo, a menos que esta actividad sea debidamente autorizada por la alta dirección.

- Los funcionarios encargados del centro de procesamiento de datos deben verificar que las edificaciones donde estas sean implementadas sean discretas y no den muestra de su propósito, obviando la utilización de señales tanto internas como externas que permitan la identificación de la realización de actividades de procesamiento de información.

- Los funcionarios encargados del centro de procesamiento de datos deben velar por que exista una señalización que corresponda con las prohibiciones al interior del centro de procesamiento de datos tales como: Prohibido fumar, comer o beber, prohibido tomar fotografías o realizar grabación de video, entre otros, así mismo, propender porque las instalaciones cuenten con los mecanismos necesarios para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior.

- La Defensoria del Pueblo debe asegurar que los directorios y guías telefónicas internas que identifican los lugares de las instalaciones de los centros de procesamiento de datos mantengan un estatus de confidencial de manera que no sean accesibles a ninguna persona no autorizada.

- Los funcionarios encargados del centro de procesamiento de datos deben realizar un acompañamiento a las actividades de aseo del área, especialmente en el centro de procesamiento de datos y los centros de cableado, brindando orientación al personal de limpieza frente a las precauciones mínimas que se deben contemplar durante el proceso de mantenimiento del área, así mismo, se prohíbe completamente el ingreso de maletas, bolsos o algún objeto que no haga parte de los materiales requeridos para las labores de aseo.

11.1.4. Protección contra amenazas externas y ambientales.

La Defensoría del Pueblo en orden de proteger las áreas seguras frente a desastres naturales, ataques intencionales o accidentes define los siguientes lineamientos.

- A través de las diferentes dependencias encargadas de la infraestructura física de la entidad, se debe asegurar que las condiciones físicas y ambientales sean las adecuadas, implementando sistemas de control ambiental tanto de temperatura como de humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas cerrados de vigilancia entre otros a fin de certificar la correcta operación del sistema de gestión de seguridad de la información y los recursos de infraestructura tecnológica

- Las dependencias encargadas de la infraestructura física de la entidad deberán garantizar el buen estado la infraestructura física de los centros de cableado, cuartos de suministro de energía, centros de procesamiento datos de la Defensoria del Pueblo, y en general de las áreas seguras, elementos tales como puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, sensores, entre otros, deben recibir, mantenimiento periódico y realizar los cambios en caso de ser requeridos.

- Las dependencias encargadas de la infraestructura física de la entidad deberán velar por que los centros de procesamiento de datos, centros de cableado y cuartos de suministro de energía se encuentren

alejados de áreas que contengan líquidos inflamables o que por su ubicación se encuentren expuestas a riesgos de inundaciones o incendios.

- Los funcionarios que por sus funciones deban permanecer en las áreas seguras de tecnología definidas están obligados a mantenerlas libres de cualquier artefacto o elemento que no sea propio de la operación del centro de procesamiento de datos y centros de cableado de la Defensoria del Pueblo.

- La alta dirección de la Defensoria del Pueblo, con el respectivo acompañamiento del comité de gestión institucional, deberá Elaborar e implementar los planes de contingencia, de emergencia y de continuidad del negocio de la entidad.

11.1.5. Trabajo en áreas seguras.

La Defensoría del Pueblo debe diseñar e implementar procedimientos específicos para el trabajo en áreas seguras, teniendo como base las directrices que se imparten a continuación:

- Garantizar que las acciones de mantenimiento que se realicen a las redes eléctricas y de datos al interior del centro de procesamiento de datos, se realicen en concordancia con el procedimiento de gestión de cambios, contando con la aprobación previa del comité de cambios y ejecutado por el personal debidamente calificado para esas actividades, de la misma manera, se debe contar con una bitácora de control de la programación de los mantenimientos preventivos que se realicen.

- Asegurar que las labores de mantenimiento para los centros de cableado y cuartos de suministro eléctrico sean realizadas por personal debidamente calificado y apegados al rigor técnico que estas labores exigen; de la misma manera, el grupo de Tic de la Defensoria del Pueblo debe contar con una bitácora de control de la programación de los mantenimientos preventivos.

11.1.6. Áreas de despacho y carga.

La Defensoría del Pueblo, en aras de evitar el acceso no autorizado a las instalaciones de los centros de procesamiento de datos y demás áreas seguras buscará aislar estas e implementará controles en los puntos de acceso como áreas de despacho y carga y demás puntos críticos donde puedan acceder personas no autorizadas, para lo cual se deberán seguir los lineamientos presentados a continuación:

- Las dependencias encargadas de la infraestructura física de la entidad deberán implementar la señalización respectiva que permita identificar las áreas de despacho y carga de la Defensoria del Pueblo.

- Ejecutar acciones de control en los puntos de acceso a las áreas de despacho y carga y demás puntos críticos de acceso con el apoyo de circuitos cerrados de televisión, así como el apoyo de los colaboradores de vigilancia y seguridad.

- Permitir el acceso al área de despacho y carga desde el exterior de las instalaciones única y exclusivamente a las personas que se encuentran debidamente identificados y autorizados.

- S áreas de despacho y cargas deben ser ubicadas de modo que los materiales que se reciban o entreguen se puedan cargar y descargar sin que el personal encargado de esa labor tenga acceso a otras ubicaciones de la edificación.

- Inspeccionar y comprobar el material que ingresa a las instalaciones de la Defensoria del Pueblo a fin de identificar la existencia de materiales considerados de alto riesgo antes de que sean retirados del área de despacho y carga definida.

- Comprobar el material que entra a la Defensoria del Pueblo, a fin de identificar la evidencia de manipulación durante el recorrido, en caso de evidenciar tal manipulación, es obligatorio reportar de manera inmediata al superior encargado.

11.2. Equipos.

Con el ánimo de prevenir incidentes de seguridad tales como la perdida, el daño, o el robo de activos, y debido a esto se presente la interrupción de las operaciones de la Defensoría del Pueblo, se dictan las siguientes directrices:

11.2.1. Ubicación y protección de los equipos.

Los activos de la Defensoría del Pueblo deberán ser protegidos de manera que se reduzcan los riesgos del entorno, así como las posibilidades para el acceso no autorizado a estos, para lo cual, se aplicarán como mínimo los siguientes lineamientos:

- El grupo de TIC de la Defensoria del Pueblo debe garantizar que la infraestructura tecnológica de la entidad (Hardware, software y dispositivos de comunicaciones) cuente con medidas de protección tanto física como eléctrica, de modo que se eviten los riesgos asociados a estos activos tales como daños, accesos no autorizados, interceptación de información entre otros.

- El grupo de TIC de la entidad debe garantizar el correcto funcionamiento de toda la infraestructura tecnológica de la entidad, asegurando que todos los activos cuentan con las condiciones adecuadas mínimas para su correcto funcionamiento, en ningún caso, se removerán equipos de su ubicación asignada, sin contar con el aval del mencionado grupo.

- El grupo de TIC de la entidad deberá asegurar la protección de la infraestructura tecnológica para el procesamiento de datos de la entidad mediante la contratación de mantenimientos preventivos y correctivos.

11.2.2. Servicios de suministro.

La defensoría del Pueblo debe garantizar la protección eléctrica de todos sus activos tecnológicos evitando que se generen interrupciones en el servicio o daños en los mencionados activos, causadas por fallas en el suministro de energía, para lo cual se deben tener presentes los siguientes lineamientos mínimos:

- El grupo de infraestructura - servidores de la Defensoria del Pueblo debe mantener un estricto control de los equipos electrónicos que ingresan al centro de procesamiento de datos de la entidad.

- El grupo de infraestructura - servidores de la Defensoria del Pueblo debe garantizar la operación permanente de los servidores alojados en los centros de procesamiento de datos, así mismo planear estrategias de protección y salvaguarda de la información que se encuentra almacenada en los equipos dispuestos para este fin.

- Las dependencias encargadas de la infraestructura física de la entidad deberán implementar interruptores de emergencia ubicándolos cerca de las salidas de emergencia de las áreas seguras, a fin de facilitar un corte inmediato de la energía en caso de presentarse una situación crítica.

- Las dependencias encargadas de la infraestructura física de la entidad deberán contemplar la implementación de iluminación de emergencia que será empleada en caso de una falla en el suministro principal de energía.

- La subdirección administrativa de la Defensoria del Pueblo debe asegurar la protección de los equipos de cómputo contra cortes de energía y otras interrupciones que puedan ser provocadas por cualquier evento externo que afecte los servicios básicos.

- La subdirección administrativa de la Defensoria del Pueblo debe asegurar el correcto funcionamiento de los sistemas de alimentación ininterrumpida – (UPS por sus siglas en ingles), para lo cual se deben realizar inspecciones de manera periódica verificando que cuentan con la capacidad requerida para asegurar el funcionamiento de los dispositivos y se deben probar en concordancia con las recomendaciones de los fabricantes o proveedores.

11.2.3. Seguridad del cableado.

La entidad debe garantizar la protección frente a la interceptación, la interferencia o los daños que se puedan ocasionar al cableado de energía y de telecomunicaciones, para lo cual debe como mínimo seguir los siguientes lineamientos:

- Disponer de dispositivos de seguridad perimetral que permitan minimizar el riesgo de accesos no autorizados o de interceptación de la información que se transporta a través de las redes de datos de la entidad.

- Asegurar que el cableado eléctrico y las redes de datos se encuentran debidamente separados con el fin de evitar interferencias debido a sus diferencias funcionales.

- Garantizar que los centros de cableado y/o cuartos de suministro eléctrico cuentan con las condiciones físicas, medioambientales y de seguridad que permitan su correcto funcionamiento y protección.

11.2.4. Mantenimiento de equipos.

La entidad debe asegurar el correcto mantenimiento de los activos con los cuales se realiza el manejo de la información de modo que se asegure su continua disponibilidad e integridad, en ese sentido, se definen los siguientes lineamientos mínimos para lograr ese objetivo.

- Garantizar el correcto funcionamiento de la infraestructura tecnológica, definiendo tiempos de mantenimiento de los equipos con el grupo de TIC y su equipo de soporte técnico.

- El mantenimiento de la infraestructura tecnológica de la entidad será realizado única y exclusivamente por el personal del grupo de soporte autorizado, de igual manera aplica para el caso de reparaciones que sean requeridas.

- La Defensoria del Pueblo debe contar con un sistema de registro de todas las fallas que se presentan en la infraestructura tecnológica, esto incluye los mantenimientos preventivos y correctivos que se realizan sobre los equipos.

- En caso de requerirse un contrato de mantenimiento especializado, este deberá tener un control de supervisión en el cual se verificará el cumplimiento del objeto y las exigencias a los requerimientos planteados en el mencionado contrato.

- Establecer y supervisar que el mantenimiento se realice de acuerdo con lo definido en el contrato del operador de servicios TICs el cual contempla un mantenimiento preventivo a los servidores del centro de cómputo, por lo menos dos (2) veces al año, de acuerdo con lo definido por la OTSI.

11.2.5. Retiro de equipos.

La Defensoría del Pueblo debe garantizar que los movimientos de infraestructura tecnológica, software o información se realicen en cumplimiento de las autorizaciones otorgadas de acuerdo con las funciones que lo requieran, para esto, se definen las siguientes directrices de seguridad.

- El retiro de equipos de cómputo, del software o de la información debe contar con la autorización del jefe inmediato y con la aprobación del grupo de TIC lo anterior, con el objetivo de tener claridad en donde y que activos se encuentran fuera de la Defensoria del Pueblo y analizar los riesgos que esto conlleva.

- Todos los movimientos de equipos de cómputo o dispositivos de infraestructura tecnológica deben estar acompañados de una solicitud en el gestor de incidentes, o mesa de ayuda, esto, con el fin de contar con la trazabilidad de ubicación de estos dispositivos.

- La subdirección administrativa a través del grupo de bienes debe realizar inspecciones periódicas con el fin de identificar movimientos o retiros no autorizados de los elementos de infraestructura tecnológica.

- Todos los traslados de equipos de cómputo deben ser realizados por el personal autorizado del grupo de bienes, grupo de TIC o personal de mantenimiento, para lo cual deben estar plenamente identificados como colaboradores de la entidad con su respectivo carné institucional.

11.2.6. Seguridad de equipos y activos fuera de las instalaciones.

La Defensoría del Pueblo consciente de los riesgos asociados al trabajo en el exterior de las instalaciones de la entidad define las siguientes directrices para proteger los equipos.

- Garantizar que toda la infraestructura tecnológica de la entidad se encuentre cubierta por una póliza de seguro que incluya los riesgos asociados a la movilidad de los equipos.

- Proteger los dispositivos de infraestructura tecnológica portátiles que contengan información clasificada como **Confidencial** o **Reservada** implementando controles de seguridad que permitan garantizar la confidencialidad de la información.

- Asegurar que se informe a los funcionarios, contratistas y terceras partes interesadas a cerca de la importancia de evitar que los portátiles se encuentren a la vista al interior de los vehículos, recomendar que siempre que se viaje sean llevados como equipaje de mano asegurando su custodia.

- En caso de pérdida o robo de un equipo portátil de la Defensoria del Pueblo, se debe realizar la respectiva denuncia frente a las autoridades competentes además de informar al grupo de bienes de la subdirección administrativa con el fin de que se apliquen las disposiciones a que haya lugar.

- Cada vez que se requiera movilizar equipos portátiles, es de obligatorio cumplimiento el registro de la salida, así como el ingreso de estos en la bitácora de vigilancia.

- Emplear las políticas de grupo de los equipos para deshabilitar los puertos de transmisión y recepción de infrarrojo y bluetooth para el caso de los equipos que cuentan con estos.

11.2.7. Disposición segura o reutilización de equipos.

Los elementos de infraestructura tecnológica que contengan medios de almacenamiento y que por su tiempo de funcionamiento deban ser dispuestos para baja o que sean reasignados, deberán recibir el tratamiento apropiado de acuerdo con los siguientes lineamientos.

- Realizar un procedimiento de borrado seguro de la información y del software instalado contenida en los elementos que van a ser objeto de baja por obsolescencia tecnológica, previo respaldo de la información que en ellos este contenida, dicha información debe reposar en el archivo del grupo de TIC dando cumplimiento a las tablas de retención documental dispuestas para este fin.

- Para los equipos de cómputo reasignados se ejecutara un procedimiento de borrado seguro de la información y del software instalado de manera que no se puedan realizar procesos de recuperación no autorizada de información de estos dispositivos.

11.2.8. Equipo de usuario desatendido.

Los funcionarios, contratistas y terceras partes involucradas, deberán conocer sus responsabilidades frente a las disposiciones de seguridad de los equipos desatendidos, por tanto, la Defensoría del Pueblo define las siguientes directrices para estos casos:

- Todos los colaboradores de la Defensoria del Pueblo deben asegurarse de que cuando se ausenten de su puesto de trabajo ejecuten las disposiciones de la política de escritorio y pantalla limpios definidas.

- Todos los colaboradores de la Defensoria del Pueblo deben cerrar sus sesiones activas una vez hayan culminado con sus labores, así mismo, las pantallas deben ser bloqueadas en los momentos en los cuales deban ausentarse de sus puestos de trabajo.

11.2.9. Política de escritorio limpio y pantalla limpia.

Con el fin de proteger la información de la Defensoría del Pueblo de accesos no autorizados o de perdida por extracción o daño a la misma, la entidad define las siguientes políticas las cuales deben ser aplicadas por funcionarios, contratistas y terceras partes interesadas.

- Los funcionarios, contratistas y terceras partes interesadas que cuenten con asignación de equipos de cómputo deben conservar su escritorio libre de información de propiedad de la Defensoria del Pueblo **(documentos o unidades de almacenamiento de información externa)**, así mismo, deben conservar la pantalla del equipo libre de archivos en cualquiera de sus extensiones, de modo que no puedan ser copiados, reproducidos o accedidos por terceros no autorizados para su uso o conocimiento, dentro de las posibilidades, se deben emplear los recursos de nube (OneDrive y SharePoint) que la Defensoria del Pueblo ha dispuesto para todos los colaboradores, en ningún caso se autoriza el uso de nubes públicas con los usuarios personales de los colaboradores de la entidad.

- Cuando por algún motivo los funcionarios, contratistas y terceras partes deban ausentarse de su puesto de trabajo, estos deberán bloquear la pantalla de su equipo de cómputo asignado.

- Una vez finalizada su jornada laboral, es obligación salir de todas las aplicaciones que se estén utilizando y realizar el correcto apagado de los equipos de cómputo y demás dispositivos de infraestructura que estén ubicados en el área de trabajo.

- Cuando se realice la impresión de documentos de carácter **Confidencial**, se debe evitar la reutilización de estos, para lo cual, antes de reciclar se debe clasificar el papel que contenga información **Confidencial** para su posterior destrucción.

- En los horarios no laborales o en los momentos en los cuales los puestos de trabajo se encuentren desatendidos, la información clasificada como **Confidencial (documentos o unidades de almacenamiento de información externa)**, debe ser resguardada bajo llave.

- Al finalizar la jornada laboral se debe realizar una inspección para verificar que los elementos de infraestructura se encuentren apagados y, en caso de identificar alguno encendido, realizar los reportes.

- Definir los tiempos de inactividad de los equipos de cómputo a fin de implementar políticas de grupo en el controlador de dominio que permitan el bloqueo automático de las sesiones una vez este tiempo se haya cumplido.

- Configurar la política de grupo en los controladores de dominio de la Defensoria del Pueblo para que todos los iconos, accesos directos o documentos que se encuentren en el escritorio se oculten automáticamente.

12. Seguridad de las operaciones.

La Defensoría del Pueblo define las siguientes políticas para la seguridad en las operaciones, las cuales deben ser aplicadas por el grupo de TIC de la entidad elaborando los procedimientos documentados de todas las actividades relacionadas con las instalaciones de procesamiento de información y comunicaciones como los procedimientos de copias de respaldo, mantenimiento de equipos, encendido y apagado de dispositivos, gestión y administración de medios y gestión y seguridad del correo electrónico.

12.1. Procedimientos operacionales y responsabilidades.

Todos los procedimientos de operación que sean necesarios deberán ser debidamente documentados y puestos a disposición de todos los usuarios que en virtud de sus funciones lo requieran.

12.1.1. Procedimientos de operación documentados.

El grupo de TIC de la Defensoría del Pueblo debe realizar la documentación de todos los procedimientos necesarios para la operación, así mismo, la actualización, publicación y socialización de estos estará a cargo del mencionado grupo.

12.1.2. Gestión de cambios.

Todos los cambios que sean requeridos en la Defensoría del Pueblo en términos de los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que tengan afectación sobre la seguridad de la información deberán ser controlados, para lo cual se definen los siguientes lineamientos:

- Definir e implementar un procedimiento de gestión de cambios en el cual se identifiquen las directrices para la realización de cambios.

- Ejecutar todos los cabios que sean requeridos a la infraestructura tecnológica y/o los servicios en concordancia con las directrices internas.

- Mantener los registros actualizados a través de una bitácora de todos los cambios solicitados y gestionados en concordancia con el procedimiento definido de gestión de cambios.

- Precisar en el procedimiento de gestión de cambios los canales autorizados y formatos requeridos para la recepción de solicitudes de cambios.

- Identificar las posibles situaciones que lleven a cambios de emergencia, de manera que se asegure que los cambios se apliquen de forma rápida y controlada.

- Proyectar la ejecución de los cambios en los sistemas de información con el fin de asegurar que se contemplan todas las condiciones y restricciones requeridas para una ejecución exitosa, es necesario informar e involucrar a las partes interesadas que dadas sus funciones tengan relación directa con el sistema de información.

- Valorar los potenciales impactos que se pueden generar al realizar un cambio en un sistema de información previo a su implementación, en esta valoración se deben incluir los aspectos funcionales y de la seguridad de la información, los posibles impactos deben ser considerados en la etapa de planificación del cambio de manera que se identifiquen las acciones que permitan reducir o eliminar los impactos.

- Ejecutar las pruebas necesarias posteriores a los cambios planeados sobre los sistemas de información con el fin de garantizar que el sistema permanece operativo, se deben incluir los aspectos de seguridad de la información del sistema y verificar que el cambio realizado cumplió con el objetivo planteado.

- Definir e implementar un procedimiento formal para aprobar los cambios sobre sistemas de información existentes, tales como actualización, implementación de parches de seguridad sobre los sistemas operativos o cualquier otro cambio relacionado con los componentes de infraestructura tecnológica que soportan los sistemas de información.

- Definir dentro del plan de cambios un capítulo de roll-back en el cual se definan claramente las actividades necesarias para descartar los cambios y retornar el sistema a un estado anterior.

- Ejecutar las solicitudes de cambio sobre los sistemas de información y en los servicios de infraestructura tecnológica en concordancia con las directrices dadas en los procedimientos, a fin de garantizar la planeación de los cambios evitando generar una afectación a la disponibilidad, integridad o confidencialidad de la información.

12.1.3. Gestión de la capacidad.

El grupo de TIC debe garantizar el correcto desempeño de los sistemas de información haciendo monitoreo al uso de los recursos, realizar los ajustes requeridos y elaborar las proyecciones de ampliación de los

requerimientos sobre la capacidad de los recursos a futuro, para lo cual se deben seguir los siguientes lineamientos mínimos:

- Elaborar análisis comparativos entre la demanda y las estimaciones del incremento de los recursos de infraestructura tecnológica administrada periódicamente, con el fin de garantizar el adecuado desempeño y la correcta capacidad de la infraestructura tecnológica de la Defensoria del Pueblo.

- La consideración de estimaciones para el incremento de los recursos de infraestructura tecnológica debe incluir aspectos como el consumo de recursos de procesadores, memorias, almacenamiento, consumo de ancho de banda, conectividad, y tráfico de las redes de datos de la entidad, entre otros.

12.1.4. Separación de los ambientes de desarrollo, pruebas y operación.

Con el fin de reducir los riesgos relacionados a la implementación de sistemas de información o aplicaciones, la Defensoría del Pueblo con el apoyo del grupo de TIC debe realizar la separación de ambientes de desarrollo, pruebas y operación (producción), para lo cual se definen las siguientes directrices:

- La alta dirección de la Defensoria del Pueblo debe garantizar el aprovisionamiento de recursos amplios y suficientes para permitir la separación de ambientes de manera efectiva.

- El grupo de TIC debe proveer los recursos de infraestructura tecnológica de manera que garantice la separación de los ambientes de desarrollo, pruebas y producción definiendo dentro de las posibilidades y cuando el lenguaje de programación lo permita, los controles que se emplearan para el intercambio de información entre los ambientes de desarrollo y producción, la no existencia de compiladores, editores y códigos fuentes en los ambientes de producción así como la definición de un acceso completamente diferente en cada uno de los ambientes implementados.

- Definir un procedimiento formal para el paso de sistemas de información entre ambientes, en el cual se incluyan las condiciones que se deben cumplir para llegar a la puesta en producción de un sistema de información nuevo o para la implementación de un cambio en un sistema existente.

- Las pruebas, instalaciones o desarrollos de software se realizarán en los entornos definidos para ese fin, en ningún caso se autorizan modificaciones sobre los entornos de producción debido a que se expone el entorno a un fraude o a la inserción de código malicioso.

- La utilización de datos reales en los ambientes de desarrollo, pruebas y producción está supeditado a haber recibido un proceso de enmascaramiento de información, con el fin de proteger y limitar los riesgos por exposición o fuga de datos.

- Los diferentes ambientes deben contar con controles de autenticación y autorización independientes, de la misma manera, debe existir la definición de perfiles de acceso a los diferentes sistemas.

- Definir por cada ambiente una interfaz diferente mediante la cual se logre identificar claramente en cual instancia se está ejecutando la conexión.

- Definir plantillas graficas para la identificación clara de los ambientes a fin de evitar confusiones en el desarrollo de tareas o en la ejecución de procesos definidos para cada ambiente.

- Documentar y socializar con los procesos o dependencias propietarias de la información respecto a los cambios realizados en sistemas que se encuentran en producción y que impliquen cuestiones funcionales.

12.2. Protección contra códigos maliciosos.

La Defensoría del Pueblo con el apoyo del grupo de TIC debe proteger los activos de información de la entidad contra la ejecución de códigos maliciosos implementando controles de detección, prevención y recuperación además de la socialización para toma de conciencia adecuada de los usuarios.

12.2.1. Controles contra códigos maliciosos.

El grupo de TIC de la entidad debe garantizar la protección de la información, implementando los controles enunciados en el apartado anterior, para lo cual define los siguientes lineamientos:

- El grupo de infraestructura – servidores de la Defensoria del Pueblo debe garantizar que la infraestructura tecnológica para el procesamiento de datos cuenta con un sistema de detección y prevención de intrusos, sistemas de control de navegación y activar herramientas anti-spam en las suites de correo electrónico, con el fin de evitar la ejecución de códigos maliciosos o virus.

- Implementar políticas de grupo en los controladores de dominio de la Defensoria del Pueblo que permitan restringir la ejecución de aplicaciones, así como la actualización automática de parches de seguridad en los sistemas operativos de los equipos de cómputo instalados, de manera que se cierren las brechas de seguridad de los dispositivos y reduciendo el riesgo de contagio de software malicioso en la plataforma tecnológica de la entidad.

- Implementar herramientas de antivirus en la infraestructura tecnológica de la entidad con el objetivo de proteger a nivel de red, en contra de virus y códigos maliciosos las estaciones de trabajo de la Defensoria del Pueblo.

- Monitorear dentro de las posibilidades las diferentes comunicaciones o la información que se administre en cualquier medio de la entidad, buscando virus o códigos maliciosos, empleando las herramientas dispuestas para este fin, generando alertas a los administradores en las cuales se identifique el intento de vulneración y las actividades necesarias para mitigarlos.

- Las herramientas de seguridad implementadas en la entidad deben mantener actualizadas en sus últimas versiones funcionales, la entidad debe incluir dentro de su presupuesto lo necesario para mantener la operación continua de estas.

- Los administradores de la infraestructura tecnológica de la Defensoria del Pueblo deben generar contraseñas robustas y con un alto grado de complejidad para las bases de datos, dispositivos y servicios de red, y administración de sistemas de información.

- El grupo de TIC de la Defensoria del Pueblo debe implementar controles para la detección, análisis y restricción de software malicioso que sea descargado de sitios web con una baja calificación de reputación, así mismo, se ejecutaran controles sobre los medios de almacenamiento externo y en la suite de correo electrónico.

- Definir políticas en los dispositivos de seguridad perimetral asegurando que los equipos de cómputo solo puedan acceder a los parámetros autorizados por configuración.

- Diseñar e implementar el plan de sensibilización a funcionarios, contratistas y terceras partes interesadas de la Defensoria del Pueblo, con el objetivo de crear cultura de seguridad de la información, este plan debe considerar temas como la apropiación sobre los cuidados y las alertas que se deben tener frente a los códigos maliciosos, correos electrónicos que permiten la captura de su información personal entre otros.

Como parte integral de la protección de información de la Defensoría del Pueblo, todos los colaboradores y partes interesadas están obligados a la ejecución total o parcial de los siguientes lineamientos:

- Conocer el manejo de las herramientas de antivirus, con el fin de realizar análisis, verificación y de ser posible eliminación de virus o código malicioso que pueda afectar los equipos de trabajo, los dispositivos de almacenamiento en cualquier presentación, archivos y correos electrónicos que sean empleados para la ejecución de sus funciones.

- Emplear las herramientas de antivirus a los archivos, repositorios o dispositivos externos de almacenamiento que se considere sospechoso de contener software malicioso, en cualquier caso, siempre que se requiera, podrán buscar el apoyo de los integrantes del grupo de TIC para determinar cual es el tratamiento mas adecuado para el manejo que debe darse en caso de sospecha de malware.

- Ningún colaborador o parte interesada se encuentra autorizada para eliminar o deshabilitar las herramientas de seguridad implementadas en la Defensoria del Pueblo, en los equipos o sistemas asignados para el desempeño de sus funciones.

- Comprobar que los archivos adjuntos de los correos electrónicos descargados de internet o copiados desde cualquier medio de almacenamiento, son suministrados por una fuente de confianza, con el fin de evitar riesgos de seguridad como la instalación de software malintencionado o contagio por virus en los recursos tecnológicos de la entidad.

- Conocer el procedimiento para la gestión de incidentes de seguridad implementado en la entidad, con el fin de tener claros los lineamientos a seguir en caso de sospechar o identificar un posible incidente.

- Eliminar cualquier archivo o mensaje que haya recibido a través de cualquier medio provisto por la Defensoria del Pueblo y cuyo origen se considere desconocido o sospechoso, asi mismo, asumir la responsabilidad de las consecuencias que puede ocasionar la apertura o ejecución, para estos casos es necesario seguir los lineamientos definidos en el procedimiento para la gestión de incidentes de seguridad.

12.3. Copias de respaldo.

12.3.1. Respaldo de información.

Con el fin de salvaguardar los datos, códigos fuentes, archivos y demás documentación digital relacionada con los sistemas de información de la entidad, el grupo de TIC de la Defensoría del Pueblo deberá planificar y ejecutar procedimientos de respaldo de información en concordancia con las siguientes directrices:

- Definir y formalizar el procedimiento para la elaboración de copias de respaldo de los sistemas de información y los componentes de estos que lo requieran, especificando el alcance para cada sistema así como los estándares de nombramiento y rotulado, formatos de control, entrega y almacenamiento.

- Elaborar los instrumentos necesarios para permitir la correcta identificación de los medios de almacenamiento en los cuales se incluye la descripción de la información que es contenida por estos y su ubicación física exacta de modo que se cuente con un rápido y eficiente acceso a ellos.

- Implementar y configurar una herramienta de ejecución de copias de seguridad en la cual es obligatorio que se realice el registro de eventos tanto exitosos como de errores que se puedan presentar en la ejecución.

- Definir un esquema de nombramiento y rotulado de las copias de respaldo de modo que se cuente con la información que permita identificar cada unidad y administrarla de manera adecuada.

- Establecer un comité de análisis periódico de las necesidades de la Defensoria del pueblo en términos de respaldo de información, de manera que se determine con exactitud cuál es la información crítica y la frecuencia con la cual debe ser respaldada.

- Especificar mecanismos de verificación de la integridad de las copias realizadas y por ende de la información almacenada.

- Establecer una bitácora de uso de los medios de almacenamiento empleados para la ejecución de respaldos registrando la cantidad de veces que han sido empleados, controlando asi su tiempo de vida, a fin de evitar exceder el tiempo de uso establecido por el fabricante y la afectación a la información en ellos almacenada.

- Formular un plan de pruebas de los respaldos ejecutados en el que se incluyan ejercicios teóricos del procedimiento de restauración, elaboración de restauraciones simuladas basadas en escenarios, es decir, se ejecutan las restauraciones de acuerdo con situaciones específicas propuestas para garantizar que el resultado es completamente funcional, además de una simulación completa del entorno.

- Cada vez que se realicen cambios en las configuraciones de servicios, serán realizadas en archivos de respaldo conservando la configuración original.

- Establecer TRD (Tablas de retención documental) acordes con los requerimientos de la entidad y de la normatividad vigente para la gestión documental, en términos de copias de respaldo de sistemas de información, bases de datos, correo electrónico y demás activos de información que se administre en los centros de procesamiento de datos de la Defensoria del Pueblo.

12.3.2. Respaldo de información para usuarios finales.

Con el fin de Asegurar las operaciones correctas y seguras de las diferentes dependencias de la Defensoria del Pueblo, las siguientes directrices deben ser implementadas por todos los colaboradores con el apoyo del grupo de TIC:

- Evitar en lo posible, mantener información personal en los equipos de cómputo asignados para ejercer sus funciones labores.

- Mantener una copia de la información relevante para la ejecución de sus funciones en el espacio **OneDrive** suministrado por el grupo TIC de la entidad.

- Elaborar una copia permanente del buzón de correo electrónico empleando las herramientas de ofimática necesarias para hacerlo, en caso de requerirlo, solicitar el apoyo del grupo de TIC para recibir la instrucción necesaria para ejecutarlo.

12.4. Registro y seguimiento.

12.4.1. Registro de eventos.

El grupo de TIC de la Defensoría del Pueblo deberá habilitar y monitorear regularmente los registros de actividades de los servicios implementados, actividades de usuarios, excepciones y fallas además de los eventos de seguridad que se puedan presentar en el desarrollo de las operaciones propias del centro de procesamiento de datos de la entidad, para esto, se tendrán como mínimo las siguientes directrices:

- Implementar configuraciones de registro de eventos en la infraestructura de red, servidores, bases de datos, de manera que se registren todos los accesos de los colaboradores de la defensoría del pueblo a los diferentes sistemas, redes y aplicaciones implementadas.

- Identificar y habilitar los registros de logs requeridos para los diferentes servicios implementados en la Defensoria del Pueblo, definiendo periodos y procesos de revisión a los mismos.

- Mantener en todo caso copias de respaldo de información de eventos de auditoría, con el fin de mantener la disponibilidad de estos en caso de presentarse un incidente de seguridad de la información.

12.4.2. Protección de la información de registro.

La Defensoría del Pueblo con el apoyo del grupo de TIC implementará estrategias de protección tanto a las instalaciones como a la información de registros de manera que se eviten alteraciones y accesos no autorizados a estas, para este fin, se deben aplicar como mínimo las siguientes directrices.

- Implementar controles de acceso y de manipulación (creación, edición, eliminación) a las instalaciones e información de registro para evitar tanto accesos no autorizados, como alteración de estos.

- Procurar que los controles implementados estén centrados en la protección contra cambios no autorizados de la información que se registra en estos, entre otros, se debe contemplar el resguardo contra alteraciones a los mensajes que son registrados, a los archivos de log que son editados o eliminados además de lo que refiere al medio de almacenamiento del archivo de log evitando exceder la capacidad de espacio disponible.

12.4.3. Registro del administrador y del operador.

El grupo de TIC de la Defensoria del Pueblo deberá implementar y documentar todas las actividades que desarrolla el administrador y el operador de los sistemas, estos registros deberán ser protegidos y revisados con regularidad de acuerdo con las siguientes directrices mínimas.

- Mantener un registro actualizado de todas las actividades de operación realizadas por los administradores de la infraestructura de procesamiento de información de la Defensoria del Pueblo.

- Las actividades de administración de la infraestructura tecnológica y de procesamiento de información de la Defensoria del Pueblo se llevarán a cabo empleando una cuenta de usuario exclusiva asignada a cada administrador, esta cuenta debe ser entregada mediante un proceso formal.

12.4.4. Sincronización de relojes.

El grupo de TIC de la Defensoría del Pueblo deberá asegurar que los relojes de todos los sistemas de procesamiento de información de la entidad, incluyendo los dispositivos de red y de seguridad se encuentren sincronizados con una única fuente de referencia valida.

- Garantizar que todos los dispositivos de infraestructura tecnológica y de procesamiento de información de la Defensoria del Pueblo se encuentran sincronizados con la hora legal colombiana.

12.5. Control de software operacional.

12.5.1. Instalación de software en sistemas operativos.

El Grupo de TIC de la Defensoría del Pueblo, implementará estrategias y procedimientos para mantener control sobre las instalaciones de software en sistemas operativos acorde a las siguientes directrices.

- Definir las guías de instalación, configuración e implementación de seguridad en los servidores conectados a la red institucional.

- Asegurar que las instalaciones de servicios y servidores de la Defensoria del Pueblo sean realizadas por los administradores u operadores de servicios designados, en ningún caso, se permitirán instalaciones por parte de terceras partes o contratistas.

- Garantizar que, durante la configuración de los servidores, los permisos y programas que serán ejecutados por los usuarios, así como las restricciones de acceso a directorios se encuentren aplicados en concordancia con la normatividad vigente implementada.

- La configuración de servicios hacia internet estará configurada única y exclusivamente a través de las herramientas, servidores y/o servicios que autorice el grupo de TIC de acuerdo con la arquitectura propuesta para tal fin.

12.6. Gestión de la vulnerabilidad técnica.

12.6.1. Gestión de las vulnerabilidades técnicas.

La Defensoría del Pueblo con el apoyo del grupo de TIC, debe mantener registros de información de las posibles vulnerabilidades técnicas y de seguridad de los sistemas operativos que soportan los sistemas de información evaluando los niveles de exposición de la entidad a estas vulnerabilidades a fin de tomar las medidas necesarias para mitigar el riesgo asociado usando como base las siguientes pautas:

- Elaborar un plan anual de verificación de vulnerabilidades técnicas y de seguridad tanto a los sistemas operativos que soportan los sistemas de información como a los mismos sistemas críticos y misionales definiendo herramientas, cronogramas y actividades a seguir.

- Gestionar y corregir las vulnerabilidades encontradas aplicando los correctivos necesarios para mitigar los hallazgos, minimizar el nivel de riesgo y reducir el impacto que estos generan, asi mismo, es necesario mantener un repositorio documentado con los informes de los hallazgos y las soluciones aplicadas.

- Definir y establecer los roles y responsabilidades para la gestión de vulnerabilidades técnicas, en las cuales se debe incluir el seguimiento a las vulnerabilidades, la valoración de los riesgos asociados a estas, la aplicación de correctivos tales como parches, actualización y/o instalaciones de software requeridos para la gestión, así como las pruebas necesarias para determinar la efectiva función de las respectivas correcciones aplicadas.

12.6.2. Restricciones sobre la instalación de software.

El grupo de TIC deberá establecer estrategias para implementar y normar la instalación de software en la infraestructura tecnológica de la entidad por parte de los usuarios.

- El grupo de TIC de la Defensoría del Pueblo, a través de la mesa de ayuda es el único responsable por la gestión de activos de infraestructura tecnológica de la entidad, asi como de dar soporte a esta.

- El grupo de TIC de la Defensoría del Pueblo es la única dependencia autorizada para la administración del software, el cual debe ser custodiado de manera que se evite la copia, distribución, o usos no autorizados (comerciales o personales).

- Todo el software empleado en la Defensoría del Pueblo deberá estar debidamente licenciado, el software que no requiera licencia de uso comercial deberá ser expresamente abalado por el Grupo de TIC, luego de un análisis de pertinencia y viabilidad, evitando con esto la posible violación de los derechos de autor.

- Valorar los riesgos asociados a la instalación de actualizaciones en la infraestructura tecnológica asegurando que son eficaces y que no producen efectos adversos después de la instalación.

- Definir estrategias de restricción para la instalación de software en los equipos de cómputo de la Defensoría del Pueblo.

- Implementar herramientas de monitoreo de la infraestructura tecnológica asegurando que sea empleada para el desarrollo de las obligaciones, actividades o funciones acordadas o contratadas.

- Definir un plan de inspección periódica del software instalado sobre la infraestructura tecnológica, para desinstalar el software no autorizado.

- Todas las aplicaciones creadas por y para la Defensoría del Pueblo en el marco de su misión institucional deben ser reportadas al grupo de TIC.

- Las aplicaciones generadas por el Ministerio en desarrollo de su misión institucional deben ser reportadas a la Oficina de Tecnologías de la Información para su administración.

12.7. Consideraciones sobre auditorias de sistemas de información.

12.7.1. Información controles de auditorías de sistemas.

La Defensoría del Pueblo con el apoyo del grupo de TIC deberán trazar una cuidadosa hoja de ruta para la ejecución de auditorías que involucran la verificación de sistemas operativos minimizando las interrupciones a los procesos que afecten la misionalidad de la entidad, para esto se deben seguir como mínimo las siguientes directivas:

- Definir los requisitos de auditoria para acceso a datos y sistemas en compañía de los líderes funcionales.
- Establecer el alcance de las pruebas técnicas de la auditoria.
- Precisar el acceso exclusivamente para lectura en las pruebas de auditoría a software y datos.
- Anticipar cualquier acceso a copias aisladas de los archivos de sistema que sea diferente al de solo lectura.
- Informar acerca de la obligatoriedad de mantener archivos de auditoria en caso de ser requeridos por esta, o en su defecto proceder con el borrado seguro de estos.
- Establecer y precisar los requisitos necesarios para procesos especiales y/o adicionales.
- Las pruebas de auditoría que pudieran generar afectación en la disponibilidad del sistema deben ser realizadas fuera del horario laboral.
- Hacer monitoreo y seguimiento de todos los registros y accesos con el fin de mantener un rastro de referencia a las auditorias.

13. Seguridad de las comunicaciones.

La Defensoría del Pueblo define las siguientes políticas para la seguridad de las comunicaciones, las cuales deben ser aplicadas por el grupo de TIC de la entidad elaborando las guías, procedimientos y documentación técnica requerida a fin de fortalecer la protección de la información que es transmitida y recibida en las redes de la entidad, así como las instalaciones del centro de procesamiento de datos de la entidad, estas políticas aplican para todos los servicios de red, todas las redes y los controles implementados para proteger la información de la entidad en los procesos de transferencia.

13.1. Gestión de la seguridad de las redes.

13.1.1. Controles de redes.

La Defensoría del Pueblo, con el apoyo del grupo de TIC deberá mantener una correcta gestión de las redes internas, de manera que se ejerza el control necesario para proteger la información que los sistemas de información y las aplicaciones transmiten a través de estas, para esto, es necesario tener presente como mínimo las siguientes directivas:

- Establecer mecanismos de autenticación que funjan como controles lógicos para permitir el acceso a los diferentes recursos informáticos de la Defensoría del Pueblo, lo anterior con el ánimo de mantener los niveles de seguridad apropiados.

- Proveer a todas las dependencias, colaboradores y terceros de la entidad con los recursos tecnológicos de conectividad necesarios para que puedan ejecutar las funciones y actividades laborales asignadas.

- La seguridad perimetral debe tener mecanismos de control que incluyan: Firewall, IPS, Filtro de contenido, Antivirus y Antispam.

- Emplear mecanismos de análisis de red para ejercer el monitoreo necesario para la identificación de la correcta funcionalidad de la red institucional.

- Se prohíbe la conexión de estaciones de trabajo o a los puntos de acceso a la red institucional elementos de red (léase: Switches, enrutadores, módems, extensores de red, etc.) que no se encuentren debidamente autorizados por el grupo de TIC de la entidad.

13.1.2. Seguridad de los servicios de red.

El grupo de TIC de la Defensoría del Pueblo deberá identificar y establecer las características tanto de seguridad, como de servicios y sus respectivos acuerdos de disponibilidad de red, bien sea prestados al interior o contratados a través de un ente externo, para lo cual se deben tener en cuenta las siguientes directivas base:

- Permitir el acceso a internet exclusivamente a través de la red institucional definida para este fin, implementando un sistema de seguridad perimetral que permita el monitoreo constante de las redes institucionales.

- Implementar controles de filtrado de contenido a fin de evitar que los recursos de la Defensoría del Pueblo sean empleados en actividades diferentes a las funciones asignadas, así como evitar comprometer la seguridad de los activos de información y/o el buen nombre de la entidad.

- Establecer un portal cautivo para el uso de redes inalámbricas implementadas en la entidad, este, deberá autenticar con los usuarios de dominio de la Defensoría del Pueblo.

- Implementar dispositivos de red inalámbrica para usuarios invitados la cual permitirá únicamente el acceso a internet en las zonas de cobertura de la Defensoría del Pueblo.

- En ningún caso, las redes inalámbricas implementadas para los usuarios invitados permitirán el acceso a servicios o a los recursos de uso exclusivo de la Defensoría del Pueblo.

- Garantizar que los acuerdos de servicio tengan explicita y claramente definido:

    - Descripción del servicio.
    - Alcance del servicio.
    - Horarios de prestación.
    - Duración del servicio.
    - Exclusiones del servicio.

- Indicadores clave de desempeño KPI, que permitan medir la eficiencia del servicio prestado y cumplimiento con los ANS.

13.1.3. Separación en las redes.

Con el ánimo de preservar los principios de la seguridad de la información, la Defensoría del Pueblo a través del grupo de TIC deberá separar en las redes los grupos de servicios de información, usuarios y sistemas de información, para lo cual se tendrán como base las siguientes directivas:

- Las funciones de las operaciones de Tecnologías de la información (TI) deben estar distribuidas de forma tal que ningún funcionario o tercera parte tengan el control total de un sistema de información. A continuación, se describen las funciones que deben estar claramente definidas

  - Administrador de Red: Responsable por la administración, monitoreo, controles, seguridad y buen funcionamiento de los equipos de la red de comunicaciones de la Entidad, tanto a nivel de hardware como software.

  - Administrador de Bases de Datos: Responsable por la administración, monitoreo, controles, seguridad y buen funcionamiento de las Bases de Datos de la Defensoría.

  - Administrador de Servidores: Responsable por la administración, monitoreo, controles, seguridad y buen funcionamiento de los servidores de la Defensoría tanto a nivel de hardware como software y ejecutar los procesos batch en las aplicaciones y ejecutar las copias de respaldo.

  - Administrador de Sistemas de información: Responsable por la administración, monitoreo, controles, seguridad y buen funcionamiento de los sistemas de Información.

- Definir una arquitectura de segmentación de redes, con el ánimo de mantener el control sobre el acceso a cada segmento de red configurado de manera que se preserve la confidencialidad, integridad y disponibilidad de la información que se transporta a través de las redes de la Defensoría del Pueblo.

- Establecer los criterios técnicos para la conexión segura a los servicios a través de la red institucional.

- Definir herramientas de autenticación que permitan el acceso seguro a la red institucional.

- Clasificar las redes inalámbricas en públicas y redes internas, definiendo claramente los servicios prestados por cada una a fin de preservar los principios de la seguridad de la información.

13.2. Transferencia de información.

13.2.1. Políticas y procedimientos de transferencia de información.

EL intercambio de información busca mantener la seguridad de la información que se traslada entre la Defensoría del Pueblo y entidades externas. Es necesario que, dependiendo de la información a enviar a través de por ejemplo canales públicos, se utilicen las tecnologías existentes de cifrado cuando se trate de información considerada como confidencial.

Se requiere también que existan acuerdos que regulen el intercambio de información entre estas entidades con el fin de garantizar un uso y transporte seguro de la información. Estos acuerdos son de cumplimiento

obligatorio para ambas partes y por ninguna razón deben violar leyes estatales sobre el manejo y transporte de información.

13.2.2. Acuerdos sobre transferencia de información.

El grupo de TIC de la Defensoría del Pueblo deberá establecer las estrategias para mantener la seguridad de la información transferida tanto al interior, como hacia cualquier entidad externa, estas deberán contemplar el uso de cualquier herramienta de comunicación de información como, correo electrónico, VPN, SFTP entre otros.

- Garantizar canales seguros para la transferencia de la información entre la Defensoría del Pueblo y las partes externas, esta información debe ser claramente definida dentro de los contratos que se suscriban con los terceros.

- Todos los acuerdos de transferencia de información, de acuerdo con su origen y aplicabilidad deben incluir lo siguiente:

    - Las obligaciones de la alta dirección para ejercer el control y la notificación de las actividades de transmisión de información.
    - Las actividades necesarias para asegurar la correcta trazabilidad y no repudio.
    - La definición de los estándares técnicos mínimos para empaquetado y transmisión.
    - Los certificados de depósito de títulos en garantía.
    - La definición de los estándares de identificación de mensajería.
    - La definición de responsabilidades y obligaciones para tener claridad en el caso de incidentes de seguridad de la información, tales como pérdidas de datos.
    - La definición del sistema de etiquetado que se emplea para información sensible o crítica, de modo tal que asegure que el significado de la etiqueta es entendible de manera inmediata, y que la información está protegida de forma apropiada.
    - La normatividad vigente empleada para el registro y lectura de información y software.
    - La definición especifica de cualquier control especial que sea requerido para proteger elementos críticos.
    - El establecimiento de la cadena de custodia para la información mientras esta se encuentra en tránsito.
    - La definición de los niveles aceptables de control de acceso.

13.2.3. Mensajería electrónica.

La Defensoría del Pueblo con el apoyo del grupo de TIC deberá establecer criterios técnicos base que permitan mantener una protección adecuada de la información que será incluida en la mensajería electrónica, para lo cual es importante incluir las siguientes directrices:

- Establecer controles que permitan la protección de mensajes contra acceso no autorizado, modificación o denegación del servicio.

- Asegurar el direccionamiento y transporte correcto del mensaje empleando los protocolos y las configuraciones disponibles.

- Garantizar con los proveedores de los sistemas de correo electrónico los acuerdos de servicio para asegurar la confiabilidad y disponibilidad del servicio.

- Contemplar todas las consideraciones legales vigentes que puedan afectar la prestación del servicio, por ejemplo, los requisitos para firmas electrónicas.

En general, se asigna una única cuenta de correo electrónico por persona, para las dependencias que dadas sus funciones tengan acceso a los sistemas de información misional de la Defensoría del Pueblo se asignara una cuenta denominada cuenta general, y el responsable por las actividades que se desarrollen con esa cuenta será de la persona que funge como líder de la dependencia a la cual fue asignada.

Las siguientes consideraciones corresponden al uso correcto del correo electrónico:

- El uso del correo electrónico suministrado por la Defensoría debe ser exclusivo para propósitos laborales.

- El acceso a los buzones de correo electrónico debe estar controlado por contraseña.

- La información de clasificada como confidencial debe ser cifrada antes de ser transmitida por correo electrónico.

Los usuarios deben conocer los siguientes riesgos en el uso del correo electrónico:

- Los correos electrónicos que vengan de personas desconocidas deben ser tratados con precaución y no deben ser respondidos.

- Asegurar que, en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a las personas apropiadas.

- No se deben abrir los archivos anexos a los correos electrónicos, cuyo origen es desconocido o el mensaje no tiene una relación con las actividades de la Defensoría.

El correo electrónico es un privilegio y se debe utilizar de forma responsable; su principal propósito es servir como herramienta para agilizar las comunicaciones oficiales que apoyen la gestión institucional.

Se permite el uso personal del correo electrónico siempre y cuando sea responsable y:

- No provoque problemas legales a la entidad

- No se utilice para fines lucrativos personales

- No contravenga las políticas y directrices de la entidad

- No atente contra la imagen de la entidad.

- No interfiera con el trabajo de los funcionarios.

Todo colaborador de la entidad que tenga dudas acerca del material que puede enviar o recibir, debe consultarlo con su jefe inmediato.

Queda prohibido distribuir, acceder o guardar material ofensivo, abusivo, obsceno, racista, ilegal o no laboral utilizando los medios electrónicos de la Defensoría del Pueblo.

Así mismo, queda totalmente prohibido:

- Usar la cuenta para fines comerciales.

- Transmitir virus, programas de uso mal intencionado o introducir software malicioso en la red o en los servidores (virus, worms, ráfagas de correo electrónico no solicitado, etcétera).

- Leer correo ajeno, generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.

- Las violaciones de los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual. Entre otras actividades, se incluye la distribución o instalación de software sin la licencia de uso adecuada adquirida por la Defensoría del Pueblo (software "pirata").

- La copia no autorizada de material protegido por derechos de autor que incluye, pero no está limitado a, digitalización y distribución de imágenes o fotografías de cualquier origen (revistas, libros, páginas Web, etcétera), digitalización y distribución de música, audio o video, distribución e instalación de software de los cuales ni la Defensoría del Pueblo ni el usuario tienen la licencia debida.

- El uso del sistema con el fin de realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil.

- Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios de la Defensoría del Pueblo.

- El envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet o Intranet).

- Enviar mensajes de correo no solicitados, incluyendo junk mail (material publicitario enviado por correo) o cualquier otro tipo de anuncio comercial a personas que nunca han solicitado ese tipo de material (email spam, mensajes electrónicos masivos, no solicitados y no autorizados en el correo electrónico).

- Colocar mensajes de correo iguales o similares no relacionados con las actividades de la Defensoría del Pueblo a un gran número de grupos de noticias (newsgroup, spam, mensajes electrónicos masivos, no solicitados y no autorizados en grupos de noticias).

- Cualquier otro uso indebido.

En concordancia con los procedimientos de comunicación interna, únicamente están autorizados para el envío de mensajes electrónicos masivos, La oficina de comunicaciones e imagen institucional, la subdirección de gestión del talento humano y los administradores de correo electrónico y de red del Grupo de TIC. Los demás funcionarios deberán seguir el procedimiento definido por la Oficina de Comunicaciones e Imagen Institucional.

El Grupo de TIC es el encargado de ejercer la administración del sistema de correo electrónico, esto incluye disponer los recursos para la entrega de mensajes internos y hacia Internet, considerando además, los siguientes aspectos:

- Los Buzones de correo electrónico serán creados por el grupo de TIC de la entidad, previa verificación de la existencia de vinculación del colaborador a la Defensoría del Pueblo.

- Se Definen dos clases de buzones: Individuales y Generales. Los buzones individuales son asignados para cada colaborador de la entidad, los generales son un caso especial creado exclusivamente si se requiere acceso de una dependencia a los sistemas de información misionales.

- Los buzones son de carácter personal e intransferible. El usuario es totalmente responsable de todas las actividades realizadas con dicho buzón. Los buzones generales serán manejados por un colaborador designado y quien será responsable por las actividades realizadas con él, será el directivo de la dependencia que lo solicita.

- Las personas que administran el servicio de correo electrónico en la Defensoría del Pueblo servicio no monitorean, editan o descartan el contenido de las comunicaciones de los usuarios. Se debe tener en cuenta que los procesos de administración del Centro de procesamiento de datos podrán implicar el movimiento temporal y/o definitivo de sus correos, más no de su edición. Solo se hará monitoreo cuando exista una autorización debida.

- Las cuentas de correo electrónico son consideradas herramientas de comunicación, es decir, su uso es exclusivo para el envío y recepción de comunicaciones, en ningún caso es considerado como un sistema de información misional, por tanto, no existirá el concepto de trazabilidad para esta herramienta, se asignará un tamaño máximo de 50 GB por cuenta de correo y es responsabilidad de cada colaborador preservar un archivo local activo de manera que se mantenga un mínimo de espacio libre en las cuentas equivalente al 40% de su total asignado, de manera que no se afecte el correcto funcionamiento de estas.

13.2.4. Acuerdos de confidencialidad o de no divulgación.

La Defensoría del Pueblo con el apoyo de la oficina Jurídica, el grupo de contratación y el grupo de TIC deberá realizar actividades periódicas de identificación y documentación normativa de los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la entidad para la protección de la información.

- Definir claramente el tipo de información que se va a intercambiar entre la Defensoría del Pueblo y la entidad externa.

- Todos los contratos, convenios interadministrativos o acuerdos de la Defensoría del Pueblo con terceras partes, que conlleve el manejo de información tal como procesamiento, uso o intercambio deben contar con acuerdos de confidencialidad y/o acuerdos de protección de datos sobre el manejo de la información, los cuales harán parte integral de cada contrato.

14. Adquisición, desarrollo y mantenimientos de sistemas.

14.1. Requisitos de seguridad de los sistemas de información.

Con el apoyo del Grupo de TIC, la Defensoría del Pueblo deberá velar por que la seguridad de la información haga parte integral de todos los sistemas de información durante todo el ciclo de vida, se deben contemplar también los requisitos de seguridad para los sistemas de información que prestaran servicio en redes públicas.

14.1.1. Análisis y especificación de requisitos de seguridad de la información.

EL grupo de TIC de la Defensoría del Pueblo deberá incluir en los requerimientos técnicos mínimos para cada sistema de información nuevo o para la ejecución de mejoras en los sistemas de información existentes la definición de los requisitos que guarden relación con la seguridad de la información, para esto se deben contemplar como mínimo las siguientes directivas:

- Realizar el acompañamiento técnico a todas las dependencias de la Defensoría del Pueblo para la adquisición o actividades de mejoramiento de sistemas de información o aplicativos.

- Definir los requerimientos de seguridad de la información basados en las metodologías de desarrollo seguro de software y promover el cumplimiento de estos por los terceros relacionados a través de:

    - Las políticas de seguridad de la información y toda la normatividad vigente implementada por la Defensoría del Pueblo.

    - Determinar las posibles amenazas de seguridad de la información.

    - Realizar revisiones periódicas de incidentes de seguridad y del uso de umbrales de vulnerabilidades.

- Verificar y documentar adecuadamente todos los resultados formulados de la identificación de los requisitos de seguridad de la información por todas las partes interesadas.

- Incorporar en la fase de diseño de los sistemas de información la definición y administración de los requisitos de seguridad de la información además de la integración con los procesos asociados.
- Exigir la aplicación de mejores prácticas en el ciclo de vida de desarrollo de software (en inglés: SDLC – Systems Development Life Cycle) para los nuevos desarrollos o para las mejoras de los sistemas de información existentes en la Defensoría del Pueblo de acuerdo con cada fase asi:

- **Fase de requerimientos.**

    - Analizar y verificar los requisitos derivados de los procesos y políticas de la Defensoría del Pueblo relacionados para el desarrollo de los sistemas de información, el establecimiento de controles de autenticación y sesión tales como el manejo adecuado de sesiones, los requisitos de ingreso y seguimiento, y de no repudio entre otros, la definición de los requisitos de autenticación de usuario (Usuarios, Claves) además de la definición de los requisitos verificables para la entrega a producción de servicios tecnológicos.
    - Establecer controles de roles y responsabilidades en los sistemas de información definiendo claramente los procedimientos para conceder el acceso y autorización a los usuarios operadores de la Defensoría del Pueblo, asi como a los usuarios con privilegios especiales a través de la implementación de una matriz de roles y privilegios, socializar con los usuarios operadores y privilegiados a cerca de sus obligaciones y responsabilidades frente al manejo de los sistemas de información, Asegurar la asignación de privilegios en concordancia con los roles definidos primando siempre la asignación de menor privilegio, de manera que los usuarios tengan acceso únicamente a los sistemas de información, que dadas sus funciones sean requeridos.

- Definir los requerimientos con orientación a los riesgos, es decir, definiendo las necesidades de protección de todos los activos de información que se involucren a fin de preservar los criterios de disponibilidad, confidencialidad e integridad, manteniendo presentes los requisitos exigidos por otros controles de seguridad.
- Establecer los requisitos para la aprobación de privilegios en los diferentes sistemas en concordancia con el uso y las funciones ejercidas en la entidad.

- **Fase de análisis y diseño**
  - Definición clara de los accesos a los componentes y a la administración del sistema en concordancia con las definiciones dadas en la matriz de roles y responsabilidades
  - Definición de indicios de auditoría, es decir, generar registros en el sistema de manera que se puedan identificar las actividades que se realizan y quienes las realizan.
  - Establecer criterios para la gestión de sesiones que permita mitigar la afectación a los sistemas de información por posibles vulnerabilidades significativas.
  - Determinar los parámetros necesarios para la construcción de datos históricos que permitan mantener la trazabilidad de las acciones en los sistemas de información.
  - Seleccionar la metodología apropiada para el manejo de errores en concordancia con los estándares de desarrollo seguro.
- **Fase de implementación y codificación**:
  - Identificar e implementar metodologías para el aseguramiento de los ambientes y pruebas de desarrollo.
  - Definir estándares para la elaboración de la documentación técnica.
  - Identificar y establecer guías de buenas prácticas para la codificación segura teniendo en cuenta las siguientes directrices:
    - Definir criterios de evaluación de datos de entrada.
    - Establecer herramientas de versionado y codificación de los desarrollos.
    - Determinar el estilo de programación que se implementará en los desarrollos.
    - Especificar los campos de los registros de log de cambios y establecer mecanismos de protección de estos.
    - Aplicar metodologías de cifrado en los casos en los que sea necesario.
    - Incluir la definición de errores y logs de sistema a fin de identificar los fallos rápidamente para poder mitigar su impacto.
    - Precisar las configuraciones necesarias para la administración de archivos y almacenamiento partiendo siempre de los criterios de menor privilegio de acceso y modificación.
    - Definir procedimientos base para el manejo de recursos del sistema tales como la memoria, o el uso de procesamiento.
    - Aplicar criterios de estandarización y reutilización de funciones de seguridad.
  - Implementar criterios aplicables de seguridad en las comunicaciones.
  - Garantizar el cumplimiento de los procedimientos de seguridad para el paso a ambientes de producción.
- **Fase de pruebas**
  - Establecer puntos de verificación de calidad en relación con los controles de seguridad tanto empleando credenciales de acceso como sin emplearlas.
  - Definir y establecer herramientas para realizar pruebas de código seguro y comprobar su efectividad.
  - Establecer bases de configuración y tareas de comprobación a la gestión de configuraciones.
  - Definir estrategias de pruebas de caja blanca y caja negra según sea requerido.

- Establecer un plan de pruebas de top ten de OWASP
- Establecer un plan de pruebas de Fuzzing.

- **Fase de mantenimiento.**
  - Establecer el aseguramiento de los servicios estables basado en RIESGOS.
  - Implementar el plan de pruebas de seguridad de caja blanca y caja negra después de realizar cambios a los sistemas.
  - Elaborar un plan de respuesta a incidentes para identificar nuevas amenazas y controlarlas.

14.1.2. Protección de transacciones de los servicios de las aplicaciones.

La Defensoría del Pueblo a través del grupo de TIC deberá garantizar que toda la información que sea administrada a través de los servicios de aplicaciones que son difundidas sobre redes públicas se encuentran protegidas frente a actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas, para lo cual es necesario exigir a proveedores y terceras partes la inclusión de las siguientes consideraciones:

- Establecer mecanismos que aseguren la relación de confianza entre las partes relacionadas

- Definir en cada caso posible todos los procesos de autorización que se encuentren asociados a quién puede aprobar *(aprobar el contenido o expedir o firmar documentos transaccionales clave)*.

- Precisar los mecanismos de socialización para informar a los aliados de servicios de comunicación a cerca de sus autorizaciones para suministro o uso del servicio.

- Determinar todos los requisitos para proteger la confidencialidad, integridad, prueba de despacho y recibo de documentos clave y el no repudio de los contratos y los mecanismos para su cumplimiento.

- Especificar los requisitos de seguridad que permitan alcanzar el nivel de confianza requerido en la integridad de los documentos clave.

- Analizar y establecer todos los requisitos de protección de cualquier tipo de información, especialmente la considerada confidencial.

- Definir los mecanismos necesarios para evitar la pérdida o duplicación de información de las transacciones realizadas.

14.1.3. Protección de transacciones de los servicios de las aplicaciones.

Con el fin de evitar la transmisión incompleta, la manipulación no autorizada de mensajes incluyendo la divulgación, duplicación o reproducción y/o el enrutamiento errado, la Defensoría del Pueblo deberá implementar las estrategias de protección de la información que hace parte de las transacciones que se realizan en los sistemas de información y aplicaciones de la entidad, para lo cual es necesario contemplar las siguientes directrices de las cuales los proveedores y terceras partes deberán estar enterados y obligados:

- Proveer los recursos necesarios en términos de infraestructura y seguridad de manera que la información que hace parte de la transaccionalidad de los servicios y aplicaciones de la entidad sea protegida evitando cualquier tipo de manipulación no autorizada, la definición de los recursos, estará a cargo del grupo de TIC y sus componentes de seguridad de la información.

- Implementar en caso de ser requerido el uso de firmas electrónicas por parte de cada una de las partes involucradas en la transacción.

- Asegurar en lo posible todos los componentes directos de las transacciones tales como:
    - Validar y verificar la información de autenticación secreta de usuarios.
    - Garantizar que la privacidad asociada con las transacciones esté debidamente protegida.
    - Asegurar que las transacciones en su capa de transporte se encuentren debidamente cifrada.
    - Habilitar el uso de protocolos seguros para la comunicación de las partes interesadas.

14.2. Seguridad en los procesos de desarrollo y soporte.

La Defensoría del Pueblo deberá garantizar que dentro del ciclo de vida en las fases de planeación y desarrollo de sistemas de información se diseñen e implementen los componentes de seguridad digital requeridos para la protección de la información, para esto, deberá considerar las directivas planteadas en cada apartado siguiente:

14.2.1. Política de desarrollo seguro.

Fase planificación – Sistemas de información DPC.

El grupo de TIC de la Defensoría del pueblo es la única dependencia encargada de establecer y exigir la aplicación de reglas para el desarrollo de software y de sistemas de información, en ese sentido, este apartado permite identificar los objetivos y requisitos de seguridad que se deben contemplar e implementar para todos los desarrollos que se generan al interior de la entidad, estos se determinan de la siguiente forma:

- Establecer los componentes de arquitectura de los sistemas de información.
- Definir los componentes de infraestructura sobre los cuales se implementará el sistema de información.
- Determinar, de acuerdo con la clasificación de activos de información de la Defensoría del Pueblo en función de su nivel de confidencialidad si son datos que se almacenaran, consultaran o transferirán.
- Precisar el tipo de registros que debe generar el sistema tales como perfiles de usuario, niveles de privilegios, o el acceso a los recursos.
- Estructurar los accesos a los datos en concordancia con los perfiles de usuario definidos para lectura, escritura, modificación y eliminación.
- Seleccionar los mecanismos de autenticación para el ingreso al aplicativo idóneo y seguro.
- Identificar y valorar los posibles riegos de cada proyecto para lo cual se deben contemplar entre otros los siguientes:
    - Incorrecta planeación de los tiempos de ejecución del proyecto.
    - Definición de reuniones improductivas o insuficientes.
    - Integrantes de los grupos con habilidades o aptitudes insuficientes.
    - Errónea clasificación de la información y/o de los roles y privilegios

- Incorrecta definición y priorización de las tareas a realizar por cada integrante de los equipos.
- Deficiencia o inexistencia de las respuestas a las labores asignadas.
- Conflictos permanentes al interior del grupo de trabajo.
- Deficiente definición de los requerimientos a desarrollar.
- Documentación incompleta de los requerimientos a desarrollar.
- Inapropiada planificación la cual genera conflictos con la trazabilidad y/o priorización de los requerimientos.
- Errores o inconsistencia en la documentación de algún diagrama.
- Comunicación deficiente con los líderes del proyecto.

- Definir acciones preventivas y correctivas aplicables a los proyectos en función a los riesgos establecidos tales como:

  - Planificar los tiempos de desarrollo de componentes incluyendo holguras que permitan hacer frente a imprevistos.
  - Definir los temas de cada reunión, organizando repositorios de documentación respectiva a fin de que se cuente con el conocimiento de los temas que serán tratados en cada reunión, la mediación de en las reuniones será realizada por aquellos que figuren como responsables de cada proyecto.
  - Establecer pares responsables de modo que se supla la ausencia entre los integrantes de los grupos de trabajo a fin de que no se obstaculicen las labores proyectadas.
  - En la incorporación de nuevo personal al proyecto es recomendable adicionar en el cronograma de actividades el tiempo correspondiente a la curva de aprendizaje de la persona que recién está ingresando, esto toma importante relevancia sobre todo para las actividades que puedan ser desarrolladas directamente por el personal ingresado sin depender del resto del equipo, todo esto, teniendo en cuenta las habilidades y conocimientos con los que cuenta el personal recién integrado.
  - Quienes intervengan en los procesos deben conocer de primera mano la información que será empleada, sus características de disponibilidad y los niveles de clasificación según su importancia para el cumplimiento de los requisitos de seguridad.
  - Establecer compromisos entre usuarios que presentan requerimientos y los líderes de los proyectos, en los cuales se definan los procedimientos para escalar inconsistencias por incumplimiento de las actividades de quienes hagan parte de los mismos.

Fase Desarrollo – Sistemas de información DPC.

Para la fase de desarrollo la Defensoría del Pueblo deberá validar el cumplimiento de los requisitos mediante la aplicación de la lista de chequeo de la fase de planificación – Sistemas de información DPC y se definen los siguientes requerimientos mínimos de implementación para esta fase.

- Establecer ambientes independientes para desarrollo y producción los cuales deben mantener la mayor similitud en términos de especificaciones técnicas además de contar con las mismas configuraciones de software y controles de seguridad, de manera que se puedan prevenir comportamientos no esperados por el software desarrollado dadas las posibles diferencias técnicas entre ambientes.

- Los ambientes de desarrollo se implementan exclusivamente para ese uso, por tanto, los grupos de desarrollo deben ejecutar sus funciones estrictamente en estos y no emplear otros ambientes de manera directa.

- Debe existir una clara diferenciación en el nombramiento de los ambientes esto con el ánimo de prevenir confusiones durante las ejecuciones de desarrollo, pruebas, e implementación a producción de los sistemas desarrollados.

- Los ambientes de desarrollo y producción deben contar con sus respectivas bases de datos independientes, las cuales deben estar configuradas manteniendo el mismo motor de administración y el mismo versionado en ambos ambientes.

- Replicar absolutamente todos los componentes con los cuales el software tendrá interoperación en producción esto incluye componentes de middleware, interfaces, procesos personalizados, conexión con otras aplicaciones cliente servidor, bases de datos relacionales entre otros.

- Se debe autenticar adecuadamente a las personas con los roles y permisos definidos en la fase I para que solo tengan acceso a la información confidencial y a los sistemas informáticos.

- No se deben utilizar campos ocultos para almacenar información sensible, ya que esto podría exponer datos e información del funcionamiento interno de los aplicativos y permitir su manipulación.

- Si se requiere el uso de campos ocultos, es importante justificar por qué es la única alternativa técnica viable y asegurarse de que la información almacenada en ellos no sea confidencial o sensible. Si no es posible evitar la inclusión de información confidencial en los campos ocultos, se deben utilizar mecanismos de cifrado adecuados para proteger la integridad y confidencialidad de los datos.

- Es esencial verificar y controlar los datos que se introducen en los aplicativos para asegurarse de que estén dentro del rango de valores válidos para el tipo de dato correspondiente.

- Es necesario controlar la salida de los métodos y garantizar que el dato resultante de una operación se encuentre dentro de los parámetros definidos previamente antes de asignarlo.

- Los formatos de salida son inmodificables, esto dado que en cualquier caso un cambio no controlado puede generar errores asociados con la gestión de la memoria intermedia.

- Con el fin de que datos individuales que pueden pasar las validaciones pero que al ser combinados violan las restricciones de seguridad, se hace necesario comprobar los argumentos que se envían a un componente en otro ámbito de control de manera que se evite la introducción de argumentos alternativos y validar los datos resultantes de una combinación de datos de diferentes fuentes.

- Es importante asegurarse de que los métodos que llevan a cabo controles de seguridad sean declarados como privados o finales para restringir la extensión de los mismos. Las clases no finales pueden verse comprometidas si una subclase maliciosa reemplaza los métodos y permite con esto pasar por alto las comprobaciones.

- Es esencial garantizar la protección de la información que se muestra sobre los procesos activos en los sistemas operativos. Dado que muchos sistemas operativos permiten a un usuario visualizar información de procesos pertenecientes a otros usuarios, incluyendo argumentos de línea de comandos y configuraciones de variables de entorno, existe un riesgo potencial de que se produzcan ataques contra el software si se comparte información confidencial. Por lo tanto, es fundamental proteger adecuadamente esta información para prevenir vulnerabilidades en la seguridad del sistema.

- Antes de la implementación o modificación de un sistema, es importante evitar el uso de datos personales reales para pruebas, a menos que se garantice el nivel de seguridad adecuado para el tipo de información procesada. Esto se hace para proteger la privacidad y seguridad de la información personal de los usuarios. Si se utilizan datos personales reales para las pruebas, debe haber medidas de seguridad adecuadas en su lugar para garantizar que la información no sea expuesta o comprometida de ninguna manera.

- Para garantizar la seguridad de una aplicación, se debe evitar que el usuario tenga acceso directo a objetos del sistema, como archivos, directorios, bases de datos o claves. En su lugar, se deben utilizar mapas de referencias indirectas para referenciar objetos del servidor, empleando contraseñas que garanticen que el usuario tiene los permisos necesarios para acceder al recurso. También es importante evitar la publicación directa de recursos a través del acceso directo mediante una URL que pueda ser predecible, lo que puede comprometer la seguridad de la aplicación. En resumen, se deben utilizar métodos indirectos y contraseñas seguras para garantizar que los usuarios tengan acceso solo a los recursos para los que tienen los permisos necesarios.

- Es importante evitar generar código a partir de los valores ingresados por el usuario. Esto se debe a que los usuarios pueden ingresar valores malintencionados que podrían ser utilizados para comprometer la seguridad de la aplicación. En lugar de generar código a partir de los valores ingresados por el usuario, se deben utilizar métodos de validación y sanitización de datos para asegurarse de que los valores ingresados sean seguros y no representen una amenaza para la seguridad de la aplicación. También se deben utilizar técnicas como la separación de intereses y la validación en el servidor para garantizar la seguridad de la aplicación.

- Es recomendable utilizar procedimientos almacenados en lugar de sentencias SQL dinámicas. Los procedimientos almacenados son fragmentos de código pre compilados que se ejecutan dentro de la base de datos, lo que puede mejorar la eficiencia y la seguridad de la aplicación. Además, los procedimientos almacenados pueden limitar el acceso a la base de datos y reducir la posibilidad de inyecciones de SQL, ya que los valores de entrada son validados y escapados antes de ser procesados.

Aplicación de buenas prácticas de Desarrollo de software.

La Defensoría del Pueblo debe garantizar que los equipos realizan la implementación de buenas prácticas de desarrollo de software dentro de las cuales se deben contemplar como mínimo las siguientes:

- Establecer herramientas de control de versiones y de gestión de configuraciones, para mantener un registro de cambios en el código fuente, colaborar en un mismo código, mantener un historial de versiones, realizar seguimiento de cambios, y controlar los elementos que conforman un desarrollo.

- Implementar nombres descriptivos para la declaración de las variables, de manera que hagan alusión a su propósito o función, en lugar de su tipo de dato, esto permitirá identificar su propósito, su relación con otras variables y su contexto dentro del programa.

- Prescindir del uso de variables globales ya que pueden ser accedidas por funciones externas, tanto de manera intencional como accidental, situación que podría resultar en asignaciones no deseadas. Teniendo en cuenta que las variables globales pueden ser accedidas por múltiples funciones durante la ejecución del programa esto generaría una dificultad en la detección de errores que puedan surgir.

- Asegurarse siempre de inicializar adecuadamente las variables para prevenir errores y comportamientos inesperados.

- Es recomendable que la aplicación genere y almacene un registro de auditoría que contenga información sobre las transacciones y tablas críticas. Este registro debe permitir consultar al menos los siguientes datos: ID del usuario, fecha, hora, nombre de la máquina en la que se ejecutó la aplicación, dirección IP, MAC, tabla modificada y acción ejecutada (creación, modificación, eliminación). Si el volumen de datos y la carga transaccional de la aplicación no es muy alta, se sugiere que se registren también los valores anteriores y actuales.

- Establecer comentarios en el código de manera responsable, Los comentarios en el código deben describir la funcionalidad y en bloques de código largos es recomendable agregar un comentario al principio y separar el código con líneas en blanco. Los comentarios no deben ser excesivos y obvios.

- Evitar excederse con el número de niveles en las instrucciones anidadas porque hace que el código puede volverse confuso y difícil de seguir, lo que aumenta el riesgo de errores y hace que el proceso de depuración sea más difícil y lento.

- Mantener separados los datos del código, esto es esencial dado que permite un mejor mantenimiento del código y evita posibles errores causados por la manipulación incorrecta de los datos. Además, si en algún momento se necesitan modificar o actualizar los datos, se puede hacer sin afectar el funcionamiento del código que los utiliza.

- Evitar la utilización de métodos con un gran número de parámetros. En su lugar, se sugiere la creación de una clase que contenga las propiedades necesarias para agruparlas de manera más organizada. Esta acción puede mejorar la claridad y mantenibilidad del código reduciendo su complejidad y garantizando que cada propiedad tenga un nombre descriptivo y una función específica.

- Para evitar confusiones y aumentar la claridad en el código, se recomienda no utilizar expresiones booleanas con valores verdadero o falso de forma explícita en comparaciones. En su lugar, se puede asignar la condición a una variable y utilizar esta variable en las comparaciones. Además, es recomendable nombrar las variables de forma afirmativa, es decir, utilizar nombres que reflejen lo que la variable representa en lugar de negar lo que no representa.

- Es esencial que se valide la totalidad de los parámetros que conforman las interfaces de programación de aplicaciones (API) exportadas, para garantizar su integridad y coherencia. Este proceso debe incluir la verificación de datos que, aunque parezcan razonables, superen los límites aceptados, como, por ejemplo, tamaños de búfer excesivos. Es importante tener en cuenta que no se recomienda emplear aserciones para verificar los parámetros de las API exportadas, ya que estas no estarán disponibles en la versión final.

- Es recomendable que los desarrolladores utilicen las API criptográficas elaboradas por empresas de renombre como IBM y Microsoft, así como las desarrolladas por la academia, en vez de crear su propio software criptográfico. Al hacerlo, los desarrolladores podrán enfocarse en la creación de aplicaciones sin tener que invertir tiempo y recursos en el desarrollo de algoritmos de seguridad desde cero.

- Cuando se necesite implementar una determinada funcionalidad en varias aplicaciones, es aconsejable crear un componente, función, rutina o servicio reutilizable que pueda ser utilizado en cualquier aplicación. De esta forma, se evita tener que volver a escribir el código cada vez que se requiera la misma funcionalidad, lo que ahorra tiempo y reduce la posibilidad de errores.

Verificación de cumplimiento de especificaciones del sistema.

La Defensoría del Pueblo debe garantizar el cumplimiento los atributos de calidad y requerimientos de seguridad para lo cual se deben contemplar como mínimo las siguientes recomendaciones:

- Realizar las pruebas iniciales basándose en los requisitos y atributos de calidad previamente definidos y aprobados. El objetivo de estas pruebas es verificar que el sistema cumpla con los requisitos de seguridad de acceso al sistema, los datos y procesos definidos, así como con los diferentes recursos del sistema, además de su correcto funcionamiento y el cumplimiento de los atributos de calidad establecidos.

- Las pruebas de funcionalidad deben ser congruentes con las funcionalidades requeridas y busquen identificar y solucionar errores que puedan surgir al utilizar la aplicación o el módulo desarrollado.

- Si la solicitud de cambios proviene de un mantenimiento, es importante revisar todas las funciones del sistema que podrían ser afectadas por la integración de la nueva funcionalidad o la solución del problema que dio origen al mantenimiento.

- Es imprescindible llevar a cabo pruebas de acceso al aplicativo para garantizar que solo los usuarios autorizados puedan acceder y únicamente a los módulos definidos según su rol.

- Las pruebas de seguridad funcional deben fundamentarse en los requisitos establecidos en relación con:

- La autenticación requerida, la complejidad de las contraseñas en función de la política establecida en este documento y las limitaciones de acceso de acuerdo a los roles y permisos diseñados.

- La función de bloqueo automático de las cuentas de acceso.

- La función de captchas para verificar que el usuario que accede a ciertos datos es una persona y no un programa automatizado.

- La información consignada en los registros (logs) y su conservación.

- Los avisos de error que se deben mostrar durante las acciones confirmadas.

- Se deben efectuar pruebas de rendimiento del software, creando situaciones que sometan la aplicación a su mayor capacidad y uso de recursos para comprobar si se cumplen los criterios de calidad adecuados.

- Si se llevan a cabo pruebas en los aplicativos Misionales de la Defensoría del Pueblo, es esencial que las mismas sean realizadas por un individuo distinto al programador encargado de implementar la solicitud.

- Aunque el proyecto haya experimentado cambios en su planificación debido a la ampliación o reducción de plazos, es crucial no reducir el tiempo destinado a las pruebas. Es fundamental garantizar que el proyecto final entregado esté libre de errores, y si se reduce el tiempo dedicado a las pruebas, es más probable que se presenten errores por encima de lo normal.

- Es necesario seguir los procedimientos establecidos y obtener la aprobación correspondiente antes de publicar cualquier aplicación.

Fase Implementación - Sensibilización, Puesta en Producción y Mantenimiento de Sistemas de Información – DPC.

Para esta fase, la Defensoría del Pueblo garantizar que la puesta en marcha de los sistemas de información desarrollados tengan la debida promoción y seguimiento en sus inicios, así como el aseguramiento de los recursos para su mantenimiento, para lo cual se contemplaran los siguientes aspectos:

- La transferencia del conocimiento de las políticas de seguridad de la información.

- La sensibilización a cerca del buen uso de los sistemas de información desarrollados para la entidad.

- La toma de conciencia frente a las restricciones, roles y perfiles, administración de credenciales de acceso que serán empleadas para el uso de los aplicativos.

- Todas las aplicaciones de la Defensoría del Pueblo deben contar con características de seguridad establecidas a fin de prevenir incidentes de seguridad, manteniendo coherencia con las políticas de seguridad de la entidad, así mismo, deben permitir establecer las vulneraciones o intentos de

vulneración sobre los sistemas de información de la entidad permitiendo en caso de ser necesario, la recuperación del funcionamiento de un sistema.

- Considerar los parámetros de seguridad establecidos en este documento durante cualquier tarea de mantenimiento o incidente que surja, así como en su ejecución garantizar la confidencialidad, integridad y disponibilidad que impacten o alteren estos requisitos.

- Diseñar e implementar una lista de chequeo de cumplimiento de los requisitos de Sensibilización, Puesta en Producción y Mantenimiento de Sistemas de Información para la Defensoría del Pueblo, y ejecutar las validaciones correspondientes una vez este creada.

14.2.2. Procedimientos de control de cambios en sistemas.

La Defensoría del Pueblo a través del grupo de TIC deberá asegurar la correcta documentación y cumplimiento de los procedimientos formales de control de cambios que han sido definidos por la entidad con el fin de mantener la integridad en los diferentes sistemas de información y aplicaciones institucionales, esto debe incluir todas las etapas del ciclo de vida del sistema y debe considerar los siguientes aspectos:

- La utilización de un software de control de versiones, que posibilite la recuperación de versiones particulares en momentos necesarios.

- Examinar las repercusiones de las modificaciones y establecer los procedimientos de seguridad correspondientes.

- Una evaluación exhaustiva de los riesgos relacionados con la seguridad en el ámbito digital.

Establecer y hacer cumplir el procedimiento de gestión de cambios con el fin de asegurar la integridad con el fin de garantizar que los sistemas de información de la entidad se mantengan íntegros, es necesario implementar medidas adecuadas desde las primeras fases de diseño y continuar aplicándolas en todas las tareas de mantenimiento posteriores.

Se requiere que los nuevos sistemas y las modificaciones significativas a los sistemas ya existentes cumplan con un proceso formal que incluya la documentación, especificación, pruebas, control de calidad y gestión de la implementación.

14.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.

El Grupo de TIC de la Defensoría del Pueblo debe asegurar que, ante cualquier cambio en las plataformas de operación, se lleve a cabo una revisión exhaustiva de las aplicaciones críticas utilizadas por la Defensoría del Pueblo, y someterlas a pruebas rigurosas para garantizar que no se produzca ningún efecto negativo en la operatividad o la seguridad de la entidad, para lo cual se debe contemplar las siguientes directrices:

- Todo cambio en las plataformas de operaciones exige una revisión a los procedimientos de integridad y control en los sistemas de información, esto, debido a posibles compromisos de seguridad derivado de los cambios.

- Es importante asegurar que las notificaciones sobre los cambios en la plataforma operativa se realicen en tiempo y forma para permitir la realización de pruebas y revisiones adecuadas antes de la implementación.

- Garantizar que se realicen los cambios adecuados en los planes de continuidad del negocio para adaptarse a las nuevas condiciones y asegurar la continuidad de las operaciones.

- Es esencial garantizar que los cambios realizados en los sistemas de información se revisen mediante la exploración de vulnerabilidades y su mitigación correspondiente para asegurar la seguridad y protección de los sistemas.

14.2.4. Restricciones en los cambios a los paquetes de software.

El grupo de TIC de la Defensoría del Pueblo debe evitar en la medida de lo posible la modificación a los paquetes de software o códigos fuente, limitando esas modificaciones a cambios estrictamente necesarios y contemplando las siguientes directrices:

- Es recomendable contar con un sistema de gestión de versiones que permita la recuperación de versiones anteriores en caso de ser necesario, ya que esto brinda una forma eficaz de manejar los cambios en los sistemas de información y protegerse contra posibles errores o fallos.

- Analizar el riesgo de que los procesos de integridad y los controles incluidos se vean comprometidos, tras la modificación, esto con el fin de identificar y prevenir posibles amenazas y vulnerabilidades en el sistema. Permitiendo tomar medidas preventivas para garantizar la seguridad y protección de los sistemas de información y evitar posibles daños o interrupciones en las operaciones.

- Contar con la debida autorización del proveedor en caso de ser requerido.

- En el caso de ser un sistema de información adquirido con un tercero, obtener de este los cambios requeridos asegurando las actualizaciones necesarias.

- Es necesario evaluar el impacto que tendría para la Defensoría del Pueblo el hecho de asumir la responsabilidad del mantenimiento futuro del software como resultado de los cambios realizados en el sistema de información desarrollado por terceros. Esto implica considerar factores como los costos asociados, la disponibilidad de recursos y personal capacitado, la capacidad de respuesta a los problemas y la capacidad de adaptación a futuras necesidades y cambios en el sistema. De esta forma, se puede tomar una decisión informada y efectiva sobre la gestión y el control de los cambios del sistema de información.

- Asegurar que se instalen las actualizaciones aprobadas más recientes de todo el software y aplicaciones autorizadas estableciendo para esto un plan para la gestión de actualizaciones.

- Establecer procesos de control que permitan exigir la completa documentación y pruebas de modo que se genere un conocimiento base para poder aplicarlos nuevamente de ser necesario en la aplicación de futuras actualizaciones.

- Incluir dentro de los procesos de cambios, el escaneo de vulnerabilidades y un plan para la mitigación de estas.

14.2.5. Principios de construcción de sistemas seguros.

La Defensoría del Pueblo debe garantizar la implementación de los principios para la construcción de sistemas seguros y asegurar que se emplean para cualquier actividad de implementación de sistemas de información, para lo cual es necesario tener en cuenta los siguientes:

- Es recomendable comenzar siempre con un modelo de permisos mínimos y, a medida que sea necesario de acuerdo con los perfiles establecidos en las etapas de diseño, aumentar los privilegios de acceso.

- Es necesario validar todos los accesos realizados a los sistemas.

- En el caso de utilizar un lenguaje no compilado, es importante eliminar todo código de pruebas, comentarios y otros mecanismos que puedan permitir un acceso no autorizado antes de ponerlo en producción. Por otro lado, si se emplea un lenguaje compilado, se debe asegurar que la compilación se realice con las mejores optimizaciones disponibles y que no se incluya información para depuración.

- Es importante realizar pruebas de cobertura de código para asegurar que se pruebe todo el código.

- Todas las capas de arquitectura de los sistemas de información deben incluir los aspectos de seguridad, manteniendo un equilibrio entre la necesidad de accesibilidad y la necesidad de seguridad digital.

- Evitar las suposiciones frente a los datos que se ingresan a un sistema de información, todos los datos que se registren deben ser estrictamente validados y verificados con el fin de garantizar que la información ingresada corresponde con lo esperado evitando así ataques por inyección de código.

- Cualquier característica, campo, elemento de interfaz de usuario o elemento de menú adicional debe ser incorporado en conformidad con los requisitos de diseño establecidos. Este enfoque permitirá evitar la inclusión de fragmentos de código redundantes e innecesarios.

- Cualquier cambio que se realice en los sistemas de información y en las plataformas de operación, deben estar totalmente documentados, esto, como principio facilitador para futuros cambios.

- Dentro de las actividades del ciclo de vida del desarrollo, es fundamental adoptar practicas reconocidas de desarrollo seguro dentro de las cuales se pueden incluir OWASP, Microsoft SDL CERT Secure coding, entre otras. La articulación de los desarrollos de sistemas de información con los requerimientos de seguridad es imprescindible y debe establecer la normatividad y reglamentación necesarias para la implementación.

- Para garantizar la seguridad en el intercambio de información sensible, es necesario emplear protocolos de cifrado seguro para proteger las comunicaciones. En lo que respecta al almacenamiento de información confidencial, se recomienda el uso de algoritmos de cifrado robustos y claves de alta complejidad para reforzar la seguridad de los datos almacenados.

- Establecer el plan periódico para la revisión de los principios y métodos de construcción establecidos a fin de garantizar que están efectivamente contribuyendo a mejorar los niveles de seguridad en el proceso de desarrollo de software en la Defensoría del Pueblo.

- Antes de ser implementados en un entorno de producción específico, los sistemas de información de la Defensoría del Pueblo deben haber sido sometidos a un proceso integral de pruebas, que incluya pruebas técnicas, funcionales, de seguridad, entre otras, y haber obtenido la aprobación correspondiente.

14.2.6. Ambiente de desarrollo seguro.

Es fundamental para la Defensoría del Pueblo implementar y mantener con el apoyo del grupo de TIC, entornos de desarrollo seguros para llevar a cabo las tareas de integración y desarrollo de sistemas que abarquen todo el ciclo de vida del desarrollo de sistemas, y garantizar su protección adecuada, para lo cual, se deben tener en cuenta los siguientes controles como mínimo:

- Evitar emplear los datos guardados en el entorno de producción para llevar a cabo actividades de certificación o pruebas.

- Los datos empleados en los entornos de desarrollo, pruebas y certificación deben ser completamente diferentes a los datos utilizados en el entorno de producción.

- Permitir el funcionamiento únicamente de los módulos, servicios, protocolos y aplicaciones esenciales para garantizar el correcto funcionamiento del sistema de información, mientras que aquellos que no se empleen deben ser deshabilitados. El desarrollador tiene la responsabilidad de documentar los componentes que son estrictamente necesarios para el adecuado desempeño de la aplicación.

- Comprobar que antes de la implementación, los aplicativos cuenten con las versiones más recientes y estables tanto del software como del sistema operativo, parches de seguridad, servidor de aplicaciones, base de datos, máquina virtual de Java, en concordancia con los requerimientos del sistema de información a implementar.

- Asegurar los servidores y servicios evitando que se pueda mostrar una lista de directorios de la aplicación.

- Comprobar que en el servidor no se hayan instalado módulos, extensiones o programas por defecto que no serán utilizados por la aplicación.

- Establecer controles de acceso a los usuarios hacia los archivos de configuración o a directorios sensibles que no pueden ser borrados, restringiendo el acceso únicamente a aquellos usuarios con privilegios o autorizados para hacerlo.

- Limitar los permisos del sistema para todos los usuarios que utilicen la aplicación y el software en el servidor, incluyendo la base de datos, sftp, apache, iis, jboss, tomcat, entre otros, de manera que solo tengan acceso a los permisos necesarios.

- Garantizar que los usuarios no tengan permitido transferir archivos que contengan configuraciones del sistema.

- Establecer en los requerimientos del sistema si la aplicación requiere que los usuarios adjunten archivos, y en caso afirmativo, limitar el envío de documentos a extensiones específicas, tales como doc, docx o

pdf, y no permitir la transferencia de archivos ejecutables o extensiones referentes a lenguajes de programación.

- Definir mecanismos de verificación de la estructura de la cabecera de los archivos enviados por el usuario al servidor, ya que existe la posibilidad de que la extensión del archivo haya sido falsificada.

- Evitar que los archivos enviados por el usuario sean almacenados en el mismo entorno de trabajo de la aplicación, por lo que se recomienda guardarlos en un dispositivo aislado.

- Controlar y, en la medida de lo posible, permitir solamente la carga de archivos con extensión .pdf a los sistemas de información, evitando al máximo incluir scripts.

- Garantizar que los archivos enviados por el usuario no se almacenen en el servidor con permisos de ejecución, sino únicamente con permisos de lectura.

- El uso de rutas específicas en los parámetros o variables esta desaconsejado, en su lugar, se recomienda utilizar índices que se asocien internamente a directorios o rutas predefinidas.

- Garantizar la seguridad en la comunicación y transferencia de archivos, empleando protocolos seguros como SSH, SFTP, FTPS, VPN SSL, IP SEC, u otros similares.

- Es imprescindible que los sistemas que incorporen Web Services implementen medidas de seguridad adecuadas. Algunos aspectos que se deben considerar son:

    - Establecer la configuración para habilitar únicamente métodos HTTP seguros, como el POST, y prohibir el uso de métodos como DELETE, PUT, GET y TRACE.

    - Asegurar que los mensajes tipo SOAP sean enviados y recibidos a través del protocolo HTTPS.

    - Establecer mecanismos de cifrado y firmado de contenido en formato XML.

    - Integrar estándares de seguridad como WSSecurity, WSTrust, WS-Signature, XML Encryption, SAML, ebXML, y WS-policy.

    - Verificación y validación de datos de entrada.

    - Verificar que el XML cumpla con el esquema establecido empleando para ello la respectiva validación.

    - Crear registros de log de todas las operaciones realizadas en los Web Services.

Modificar las cabeceras HTTP para ocultar información sensible sobre las aplicaciones y versiones en el servidor.

14.2.7. Desarrollo contratado externamente.

La Defensoría del Pueblo ejecutará labores de monitoreo y seguimiento a todo lo relacionado con las actividades de desarrollo de sistemas de información única y exclusivamente a través del grupo de TIC, para lo

cual en necesario que todas las áreas de la entidad se articulen con el mencionado grupo y sigan las directrices que desde allí se impartan para todo el ciclo de vida de los sistemas de información adquiridos en la entidad.

Para lo cual la Defensoría del Pueblo deberá comprobar y hacer que el tercero cumpla con los siguientes aspectos en todo el proceso de gestión de la cadena de suministro de la Defensoría del Pueblo:

- Las cláusulas de los contratos que rigen la propiedad de los códigos, derechos de autor y licencias de uso de los contenidos externos deben tener una estricta verificación y aplicación.

- Establecer en las cláusulas de los contratos la obligación de seguir prácticas seguras de diseño, codificación y pruebas.

- Exigir al desarrollador externo el modelo de amenaza aprobado.

- Realizar pruebas de validación para evaluar la calidad y exactitud de los entregables.

- Solicitar el suministro de pruebas de cumplimiento de los umbrales de seguridad para garantizar niveles adecuados de seguridad y privacidad.

- Evidenciar la totalidad de las pruebas realizadas y que garantizaran que el sistema está protegido contra contenido malicioso, tanto intencional como no intencional, en el momento de su entrega.

- Evidenciar la totalidad de las pruebas que demuestren que el sistema ha sido sometido a pruebas exhaustivas para asegurar su protección contra vulnerabilidades conocidas.

- Contrato que establece los derechos y responsabilidades en cuanto a la implementación y seguimiento de procesos y controles de auditorías durante el desarrollo.

- Elaboración de una documentación completa sobre el entorno de desarrollo utilizado para producir los entregables.

- Establecer los compromisos oficiales para cumplir con las políticas y procedimientos establecidos en este documento.

- Ejecutar el procedimiento establecido para la transición a producción.

- Realizar un proceso de revisión de código para todos los sistemas desarrollados antes de que se publiquen, incluyendo cualquier biblioteca de terceros utilizada en el desarrollo.

- Establecer planes de prueba y definir criterios de aceptación para sistemas de información nuevos, actualizaciones y versiones posteriores.

14.2.8. Pruebas de seguridad de sistemas.

La Defensoría del Pueblo a través de su componente de seguridad de la información del grupo de TIC, debe garantizar la realización de pruebas de seguridad durante el proceso de desarrollo para evaluar su correcta funcionalidad, para esto, se deben considerar las siguientes directrices:

- La evaluación de código puede ser realizada por un tercero contratado específicamente para este propósito, o por personal interno capacitado para garantizar que la actividad sea realizada por una persona idónea.

- Se puede ejecutar empleando métodos manuales o estableciendo herramientas automatizadas pertinentes.

- Definir el grupo de personas que cuente con los conocimientos en técnicas de verificación de código y desarrollo seguro, diferentes al autor del código fuente, realicen una revisión de los cambios realizados.

- Todas las observaciones surgidas durante la revisión deben ser abordadas antes de implementar el sistema en producción.

- Los procesos de revisión deben ajustarse a las normativas y regulaciones aplicables a la Defensoria del Pueblo.

- Establecer una estrategia de evaluación de riesgos de vulnerabilidades en el código y discutir los resultados con las partes interesadas en el software desarrollado.

- Antes de implementar, es importante asegurarse de que los programas tengan las versiones más recientes y estables tanto del software como del sistema operativo, así como también los parches de seguridad, servidor de aplicaciones, base de datos y de todos los componentes necesarios para su correcto funcionamiento, entre otros aspectos.

14.2.9. Prueba de aceptación de sistemas

La Defensoría del Pueblo con el apoyo del grupo de TIC y las partes interesadas, establecerá programas de prueba para garantizar la aceptación de los sistemas de información recién desarrollados, así como de las actualizaciones y versiones posteriores, para lo cual se basará como mínimo en los siguientes elementos:

- Las necesidades del usuario.

- Especificaciones del sistema.

- Escenarios de uso.

- Procesos del negocio

- Atributos de calidad.

- Análisis de riesgo.

- Seguridad de la información.

Para todos los casos, es importante incluir en las pruebas de requisitos de seguridad de la información los siguientes aspectos:

- Realizarse en componentes y sistemas interconectados.

- Utilizar herramientas automatizadas, como programas de análisis de código o detectores de vulnerabilidades, para comprobar y asegurarse de que se han solucionado los problemas de seguridad.

14.2.10. Gestión de vulnerabilidades.

La Defensoría del Pueblo al tenor de la seguridad de la información deberá garantizar la remediación de vulnerabilidades detectadas en los sistemas de información nuevos, así como en las versiones posteriores que surjan de las actualizaciones teniendo en cuenta las siguientes consideraciones:

- Llevar a cabo una evaluación de seguridad en el entorno de producción real mediante una prueba de intrusión controlada, con el objetivo de identificar y evaluar los niveles de seguridad que rodean el ambiente final y hacer los ajustes necesarios. Es recomendable que esta revisión sea realizada por una persona distinta al desarrollador, como una revisión por pares.

- Realizar pruebas de Ethical Hacking antes de la implementación del sistema. En caso de detectar una vulnerabilidad técnica durante el proceso de desarrollo, es necesario evaluar el riesgo involucrado y establecer un plan de acción para solucionarlo.

14.3. Datos de prueba.

La Defensoría del Pueblo debe tomar las medidas adecuadas para garantizar la seguridad y privacidad de los datos que se utilizan en pruebas de desarrollo. Esto implica la implementación de políticas y prácticas de seguridad de la información, así como la utilización de tecnologías y herramientas de seguridad para prevenir cualquier posible brecha de seguridad.

14.3.1. Protección de datos de prueba.

La Defensoría del Pueblo con el apoyo del grupo de TIC debe establecer los controles adecuados para garantizar que los datos de prueba se utilicen únicamente para los fines previstos y que se evite cualquier uso no autorizado. Para lo cual se definen los siguientes lineamientos:

- Realizar una cuidadosa selección, protección y control de los datos utilizados en los desarrollos de sistemas de información. Esto implica la elección meticulosa de los datos que se utilizarán, asegurando que sean pertinentes y precisos, así como la implementación de medidas de seguridad adecuadas para garantizar su confidencialidad, integridad y disponibilidad.

- Otorgar una autorización específica para la transferencia de información operacional a un ambiente de pruebas. Esto implica la implementación de un proceso claro y controlado para asegurar que solo se transfiera la información necesaria y que se mantenga la confidencialidad y seguridad de los datos.

- Establecer un registro detallado de las acciones realizadas al copiar y utilizar información operacional, a través de un sistema de registro de actividades para proporcionar un rastro de auditoría. Esto permitirá monitorear quién accede a la información y cuándo, lo que resulta esencial para garantizar la seguridad y privacidad de los datos.

- Prevenir el empleo de registros operativos que incluyan datos privados o confidenciales para propósitos de evaluación. Si fuese necesario emplear dicha información en las pruebas, se deben implementar medidas para salvaguardar la privacidad y confidencialidad de los datos sensibles.

- Extender los procedimientos de control de acceso utilizados en los sistemas de información en funcionamiento a los sistemas de información de prueba.

- Una vez concluidas las pruebas, es imperativo eliminar de manera inmediata toda la información operacional del entorno de pruebas.

15. Relación con los proveedores.

La Defensoría del Pueblo debe establecer los términos para la entrega de servicios, deberes y medidas de supervisión que salvaguarden la información que se maneja en las interacciones con sus colaboradores externos. Estas medidas deben prevenir posibles acciones no autorizadas, como la interceptación, copia, alteración, divulgación o eliminación de la información, que podrían afectar la integridad, disponibilidad y confidencialidad de la misma.

15.1. Seguridad de la información en las relaciones con los proveedores

15.1.1. Política de seguridad de la información para las relaciones con proveedores.

La Defensoría del Pueblo debe asegurarse de tomar medidas para garantizar que los proveedores no comprometan la seguridad de los activos de información de la entidad a los que tengan acceso. Para lograrlo se deben tener en cuenta las siguientes directrices:

- Cuando se permite el acceso de proveedores a la información de la Defensoría del Pueblo, es importante que se identifiquen y se exijan los controles de seguridad necesarios y aplicables con el fin de proteger la confidencialidad, integridad y disponibilidad de los datos.

- Es importante considerar tanto los procedimientos y procesos que la Defensoria el Pueblo va a implementar, como aquellos que debe requerir a sus proveedores para su implementación. Estos incluyen:

    - Identificar y documentar los distintos proveedores a los cuales la Defensoria del Pueblo les concederá acceso a su información. Algunos ejemplos de estos proveedores pueden ser: servicios de tecnología de la información, empresas de logística, servicios financieros y proveedores de componentes de infraestructura de TI.

    - Establecer un procedimiento estandarizado y un ciclo de vida definido para administrar de manera efectiva las relaciones con los proveedores.

    - Definir los distintos niveles de acceso a la información que se otorgarán a los diferentes tipos de proveedores, así como realizar un monitoreo y control riguroso del acceso.

    - Establecer los estándares mínimos de seguridad de la información para cada tipo de acceso e información, los cuales deberán servir como base para la elaboración de acuerdos con cada uno de los proveedores, tomando en cuenta las necesidades y requerimientos del negocio de la Defensoria del Pueblo y su perfil de riesgo.

- Definir los procedimientos y procesos para monitorear el acatamiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y acceso, los cuales deben contemplar la evaluación de terceros y la validación del producto.

- Establecer los términos y condiciones bajo los cuales los requisitos y controles de seguridad de la información serán registrados en un acuerdo formal firmado por la Defensoria del Pueblo y los proveedores.

- Establecer parámetros para la administración de la gestión de incidentes y contingencias vinculados al acceso de proveedores, definiendo claramente las responsabilidades tanto de la Defensoria del Pueblo como de los proveedores.

- Proporcionar capacitación sobre conciencia y protocolos de interacción adecuados a los colaboradores de la Defensoria del Pueblo que trabajan con proveedores, en relación con las normas de comportamiento apropiadas, teniendo en cuenta la naturaleza del proveedor y su nivel de acceso a los sistemas y datos de la entidad.

- Administrar el traslado de información, equipos y cualquier otro elemento necesario, para garantizar que la seguridad de la información se mantenga intacta durante todo el proceso de transición.

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

Es responsabilidad de la Defensoría del Pueblo definir y concertar con cada proveedor que tenga la capacidad de acceder, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la entidad, todos los requerimientos de seguridad de la información relevantes. De esta manera, podemos garantizar la integridad y protección de los datos manejados por la entidad y sus proveedores, para lo cual se deben tener presentes las siguientes directrices:

- Exigir en todos los acuerdos o contratos con terceros que impliquen el intercambio, uso o procesamiento de información de la Defensoría del Pueblo, se establezcan acuerdos de confidencialidad y/o protección de datos en relación con el manejo de la información.

- Estos acuerdos de confidencialidad con los proveedores deben contemplar como mínimo los siguientes lineamientos:

    - Definición de la información que será proporcionada o a la cual se tendrá acceso, así como los procedimientos para su suministro o acceso.

    - Categorizar la información de acuerdo con el sistema de clasificación establecido en la Defensoría del Pueblo.

    - Garantizar y describir el cumplimiento de los requerimientos legales y reglamentarios, incluyendo la protección de datos, los derechos de propiedad intelectual y de autor.

    - Definir e implementar un conjunto de medidas de supervisión que comprendan restricciones de ingreso, evaluación de rendimiento, monitoreo, presentación de informes y verificación.

- Establecer las directrices para el uso apropiado de la información, incluyendo la identificación de prácticas de uso inadecuadas.

- Solicitar una relación detallada de los colaboradores del proveedor que están habilitados para acceder o recibir información de la Defensoría del Pueblo, junto con los requisitos o medidas necesarios para obtener o revocar dicha autorización de acceso o recepción por parte del personal del proveedor.

- Establecer directrices que permitan sin excepción llevar a cabo una auditoría de los procedimientos y controles de los proveedores que se vinculan con el acuerdo.

- Solicitar que los proveedores presenten regularmente un informe imparcial que evalúe la eficacia de sus medidas de restricción, y que se establezca un acuerdo sobre la corrección inmediata de los temas relevantes identificados en dicho informe.

- Supervisar el cumplimiento de las obligaciones de los proveedores respecto a los estándares de seguridad exigidos por la Defensoria del Pueblo.

15.1.3. Cadena de suministro de tecnología de información y comunicación.

La Defensoría del Pueblo está obligada a asegurar que los proveedores cumplan con los estándares necesarios para proteger la seguridad de la información de la entidad y la de los usuarios. Por lo tanto, es vital que se establezcan requisitos claros en los acuerdos con los proveedores para garantizar que se tomen medidas adecuadas para gestionar y mitigar los riesgos de seguridad de la información en la cadena de suministro, para esto, se establecen las siguientes directrices:

- Establecer los requisitos de seguridad de la información que deben aplicarse a la adquisición de productos o servicios de tecnología de la información y comunicaciones. Además de los requisitos generales de seguridad de la información que rigen las relaciones con los proveedores.

- Exigir que los proveedores de servicios de tecnología de la información y comunicaciones informen los estándares de seguridad de su organización a lo largo de la cadena de suministro si contratan a terceros para proporcionar partes de los servicios de tecnología de la información y comunicaciones suministrados a la Defensoria del Pueblo.

- Requerir que los proveedores de productos de tecnología de información y comunicaciones que incluyan componentes comprados a otros proveedores comuniquen las prácticas de seguridad adecuadas a lo largo de la cadena de suministro.

- Establecer un procedimiento de supervisión y criterios adecuados para verificar que los productos y servicios de tecnología de información y comunicación cumplan con los requerimientos de seguridad de la información.

- Definir un procedimiento para identificar los componentes de los productos o servicios que son esenciales para su funcionalidad y, por lo tanto, requieren una mayor atención y supervisión cuando son construidos fuera de la Defensoria del Pueblo. Esto es especialmente importante si el proveedor subcontrata aspectos de componentes de productos o servicios a otros proveedores.

- Determinar la normatividad para intercambiar información relacionada con la cadena de suministro, así como cualquier problema o compromiso, entre La Defensoria del Pueblo y sus proveedores.

- Definir procedimientos específicos para la gestión del ciclo de vida y la disponibilidad de componentes de tecnología de información y comunicación, así como para manejar los riesgos de seguridad asociados. Esto incluye la gestión de riesgos de componentes que ya no están disponibles debido a que los proveedores han dejado de operar o ya no ofrecen estos componentes porque se han desarrollado avances en la tecnología.

15.2. Gestión de la prestación de servicios de proveedores.

La Defensoría del Pueblo debe establecer mecanismos para supervisar la calidad de los servicios de los proveedores de manera regular. Esto implica realizar seguimientos y revisiones periódicas para asegurarse de que los servicios están siendo prestados de manera eficiente y cumpliendo con los estándares y requerimientos acordados.

15.2.1. Seguimiento y revisión de los servicios de los proveedores.

La Defensoría del Pueblo debe llevar a cabo auditorías para evaluar la calidad del trabajo del proveedor y su capacidad para cumplir con los requisitos específicos del contrato. Es importante que estas auditorías se realicen de manera objetiva y rigurosa, para garantizar que se detecten cualquier problema o deficiencia que deba ser corregida, para esto, se deben tener en cuenta las siguientes directrices:

- Garantizar el cumplimiento de los términos y condiciones de seguridad de la información establecidos en los acuerdos, y gestionar de manera adecuada los incidentes y problemas relacionados con la seguridad de la información.

- Establecer un procedimiento de comunicación para la administración del servicio entre la Defensoria del Pueblo y el proveedor con el fin de:

    - Realizar un monitoreo de los indicadores de rendimiento del servicio con el propósito de constatar el cumplimiento de los compromisos adquiridos.

    - Examinar los informes de servicio preparados por el proveedor y programar encuentros periódicos de progreso de acuerdo con lo estipulado en los acuerdos.

    - Realizar inspecciones a los proveedores, en conjunto con la evaluación de informes de auditores externos, en caso de estar disponibles, y tomar medidas sobre los problemas detectados.

    - Proporcionar datos relacionados con incidentes de seguridad de la información y examinar dicha información de acuerdo con lo estipulado en los acuerdos, así como en cualquier directriz o procedimiento de asistencia.

    - Evaluar los registros de auditoría del proveedor, así como los registros de sucesos vinculados con problemas operativos, deficiencias, rastreo de fallos e interrupciones relacionadas con el servicio proporcionado.

    - Solucionar y administrar cualquier contratiempo identificado.

- Evaluar los aspectos de seguridad de la información en las relaciones entre los proveedores y sus propios proveedores.

- Exigir que el proveedor mantenga una capacidad de servicio adecuada, junto con planes que se puedan implementar, y de esta manera garantizar el cumplimiento de los niveles acordados de continuidad del servicio en caso de fallas considerables en el servicio o en caso de desastres.

15.2.2. Gestión de cambios en los servicios de los proveedores.

La Defensoría del Pueblo tiene como responsabilidad gestionar los cambios en el suministro de servicios ofrecidos por sus proveedores, y asegurarse de que se mantengan y mejoren las políticas y controles de seguridad de la información existentes. Esto se debe hacer considerando la importancia de la información, sistemas y procesos de negocio involucrados, y también revisando regularmente los acuerdos con los proveedores para asegurar su conformidad y eficacia, para lo cual se deben considerar los siguientes aspectos:

- Administrar los cambios en la oferta de servicios proporcionados por los proveedores, lo cual incluye mantener y mejorar las políticas, procesos y controles de seguridad de la información existentes. Esto se debe hacer tomando en cuenta la importancia de la información, sistemas y procesos de la Defensoría del Pueblo afectados, así como la revisión periódica de los riesgos de seguridad de la información para su reevaluación.

- Mantener presentes los siguientes aspectos para gestionar los cambios en los servicios de los proveedores:

    - Modificaciones en los acuerdos con los proveedores.
    - Los cambios hechos por la Defensoria del Pueblo para llevar a cabo.
    - Las mejoras en los servicios actualmente proporcionados.
    - La creación de nuevas aplicaciones y sistemas.
    - Las adaptaciones o renovaciones de las políticas y procedimientos de la entidad.
    - Los controles recién implementados o ajustados para abordar incidentes de seguridad de la información y fortalecer la seguridad.

- Las modificaciones en los servicios de los proveedores:

    - Modificaciones y mejoras en las infraestructuras de red.
    - La implementación de tecnologías recientes e innovadoras.

- La adopción de nuevos productos o versiones/ediciones más recientes.

    - La implementación de herramientas y entornos de desarrollo nuevos.
    - Modificaciones en la ubicación física de las instalaciones de prestación de servicios.
    - Cambios de proveedores.
    - Vinculación de proveedores externos para servicios o suministros.

16. Gestión de incidentes de seguridad de la información.

Es responsabilidad de todos los colaboradores y terceros que trabajan con la Defensoría del Pueblo informar de manera adecuada cualquier evento o incidente relacionado con la seguridad de la información que detecten. La entidad ha establecido procedimientos específicos para el reporte de dichos eventos o incidentes y es obligatorio que todos los involucrados los sigan. Esta política se aplica a todos los niveles de la organización y a cualquier persona que tenga acceso a información confidencial de la defensoría del Pueblo.

16.1. Gestión de incidentes y mejoras en la seguridad de la información.

La Defensoría del Pueblo debe garantizar que todos los incidentes relacionados con la seguridad de la información reportada sean gestionados de manera adecuada. Para ello, se deben seguir los procedimientos establecidos para el manejo de dichos incidentes. La entidad está comprometida en tomar todas las medidas necesarias para asegurar que cualquier evento relacionado con la seguridad de la información sea manejado de forma eficiente y eficaz para proteger la integridad y confidencialidad de los datos.

16.1.1. Responsabilidad y procedimientos.

La Defensoría del Pueblo con el apoyo del grupo de TIC debe establecer claramente las responsabilidades y procedimientos para gestionar los incidentes relacionados con la seguridad de la información, con el objetivo de asegurar una respuesta rápida, eficaz y organizada. Es importante que estos procedimientos estén documentados y actualizados regularmente, para garantizar que la organización pueda responder rápidamente y de manera efectiva ante cualquier evento relacionado con la seguridad de la información, para esto, se tienen en cuenta las siguientes directrices:

- Definir los roles y responsabilidades para la gestión de incidentes de seguridad digital estableciendo claramente quiénes serán los encargados de gestionar estos incidentes y qué acciones deberán tomar. Además, se deben documentar los procedimientos de gestión y asegurarse de que sean actualizados regularmente para garantizar una respuesta eficiente y efectiva ante cualquier incidente de seguridad digital.

- Establecer el procedimiento para atender los incidentes de seguridad de la información en la Defensoria del Pueblo. La definición de este proceso debe incluir cómo se detectarán los incidentes, quiénes serán los responsables de su atención, qué acciones deberán tomarse, así como los plazos para la resolución de los mismos.

- Brindar un tratamiento apropiado a todos los incidentes de seguridad de la información reportados en la Defensoria del Pueblo. Estableciendo procesos claros para el manejo de cada incidente, desde su detección hasta su resolución, y asegurarse de que se sigan estos procesos de manera consistente.

- Todos los colaboradores involucrados en el tratamiento de incidentes deben estar capacitados y ser conscientes de sus roles y responsabilidades en el proceso.

- Crear conciencia entre todos los colaboradores y terceros acerca de los incidentes de seguridad de la información. La Defensoria del Pueblo debe establecer programas de capacitación y sensibilización para educar a su personal acerca de la importancia de la seguridad de la información y cómo prevenir y detectar incidentes. Estos programas deben ser regulares y actualizados para garantizar que los colaboradores estén al tanto de los riesgos y amenazas actuales y cómo abordarlos. Es fundamental que

todos los miembros de la entidad comprendan la importancia de proteger la información y el papel que desempeñan en ello.

16.1.2. Reporte de eventos de seguridad de la información.

Todos los colaboradores y terceras partes involucradas están en la obligación de informar sobre los eventos de seguridad de la información a través de los canales de gestión apropiados tan pronto como sea posible. Es crucial que la entidad tenga canales de comunicación eficaces para garantizar que la información se difunda de manera oportuna y precisa. Además, se debe asegurar que los colaboradores estén al tanto de estos canales y sepan cómo utilizarlos para reportar incidentes de seguridad de la información.

16.1.3. Reporte de debilidades de seguridad de la información

La Defensoría del Pueblo debe asegurarse de que todos los colaboradores y partes interesadas que utilicen los servicios y sistemas de información estén comprometidos a identificar y reportar cualquier posible fallo de seguridad en estos.

16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos.

La Defensoría del Pueblo está obligada a realizar la revisión de cada evento o incidente de seguridad de la información que se presente y utilice la escala de clasificación correspondiente para determinar su prioridad y clasificación, siguiendo lo establecido en el procedimiento definido previamente.

Así mismo, debe establecer una bitácora con los resultados de la evaluación y la decisión a fin de emplearlos en incidentes futuros como referencia y verificación. (lecciones aprendidas)

16.1.5. Respuesta a incidentes de seguridad de la información.

La Defensoría del Pueblo bajo la responsabilidad del grupo de TIC debe contar con procedimientos documentados para gestionar los incidentes de seguridad de la información que puedan ocurrir. Estos procedimientos son necesarios para garantizar que la entidad tenga una respuesta adecuada y eficiente ante cualquier incidente de seguridad, para esto, se deben contemplar las siguientes directrices:

- Recabar las pruebas necesarias tan pronto como sea posible después de que se haya producido el incidente.

- Realizar una investigación forense de seguridad de la información cuando sea necesario.

- Escalar el problema a una instancia superior, cuando sea necesario.

- Garantizar que todas las acciones de respuesta involucradas se documenten de manera apropiada para su posterior análisis.

- Informar al personal interno o externo y a las organizaciones que necesiten estar al tanto sobre la existencia de un incidente de seguridad de la información o cualquier detalle relevante al respecto.

- Abordar las deficiencias de seguridad de la información que fueron identificadas como causantes o coadyuvantes del incidente.

- Una vez que se haya abordado adecuadamente el incidente, proceder a su cierre formal y documentarlo debidamente.

- En caso de ser necesario, elevar los incidentes a instancias superiores o al control interno disciplinario.

16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información.

La Defensoría del Pueblo debe establecer mecanismos para aplicar los conocimientos adquiridos durante el análisis y resolución de incidentes de seguridad de la información con el fin de minimizar la probabilidad o el impacto de futuros incidentes, para esto deben tener presentes los siguientes lineamientos:

- Mantener un registro por escrito y debidamente documentado de todos los incidentes de seguridad de la información que sean notificados en la Defensoria del Pueblo.

- Mantener un registro de los incidentes de seguridad de la información reportados y atendidos en la Defensoria del Pueblo mediante el uso de una herramienta específica habilitada para este propósito.

16.1.7. Recolección de evidencia.

La Defensoria del Pueblo a través del grupo de TIC debe establecer y poner en práctica procedimientos que permitan identificar, recolectar, obtener y conservar información que pueda ser utilizada como evidencia en caso de ser necesario.

- Implementar y mantener procedimientos internos adecuadamente diseñados para tratar con pruebas en situaciones relacionadas con acciones legales y disciplinarias dentro de la Defensoría del Pueblo.

- Contemplar en el diseño de los protocolos para la gestión de pruebas la inclusión de diferentes actividades, tales como la identificación, recolección, adquisición y preservación de evidencia, según el tipo de medio o dispositivo y su estado, ya sea encendido o apagado. Algunos aspectos que deben ser contemplados en estos procedimientos son:

    - La cadena de custodia.
    - La protección y resguardo de la prueba obtenida.
    - La protección y bienestar de los colaboradores;
    - Los roles y responsabilidades de los colaboradores que participan en el proceso.
    - El registro detallado de la información relevante.
    - Las reuniones de información.
    - Para el traslado de evidencia, es necesario mantener la continuidad de la documentación de posesión y control (Cadena de custodia).

17. Aspectos de seguridad de la información de la gestión de continuidad de negocio.

La Defensoría del Pueblo debe establecer los controles de seguridad de la información necesarios para garantizar la continuidad de la seguridad como parte de los planes de continuidad del negocio en caso de interrupciones o desastres, En esta sección se establecen los requisitos necesarios para identificar y evaluar los riesgos asociados con la continuidad de la seguridad, así como para desarrollar y mantener planes efectivos de continuidad de negocio.

17.1. Continuidad de seguridad de la información.

El grupo de TIC de la Defensoría del Pueblo debe establecer los requisitos necesarios para identificar y evaluar los riesgos asociados con la seguridad de la información en situaciones de interrupción, así como para desarrollar y mantener planes efectivos de continuidad de seguridad de la información, además, se establecen los controles necesarios para garantizar la recuperación rápida de la seguridad de la información crítica en caso de desastres

17.1.1. Planificación de la continuidad de la seguridad de la información.

Este control ayudará a la entidad a definir los requerimientos para la planificación de la continuidad de la seguridad de la información, asegurando que la Defensoría del Pueblo cuente con los planes necesarios para garantizar la continuidad de los procesos de negocio en caso de interrupciones o situaciones adversas., para eso, se deben contemplar las siguientes directrices:

- Realizar una evaluación de los procesos de gestión de continuidad de negocio y de recuperación de desastres de la Defensoria del Pueblo para determinar si la continuación de la seguridad de la información se ha incluido adecuadamente.

- Garantizar la seguridad de la información y la continuidad operativa en escenarios indeseables, tales como catástrofes naturales o crisis, es esencial para la Defensoría del Pueblo. Por tanto, es necesario establecer los requerimientos pertinentes en estas áreas.

17.1.2. Implementación de la continuidad de la seguridad de la información.

Una vez establecidos los planes de continuidad para la seguridad de la información, el grupo de TIC de la entidad debe Definir los requerimientos para garantizar que se implementen las medidas necesarias para asegurar la continuidad de los procesos de negocio en caso de situaciones adversas. Verificación, revisión y evaluación de la continuidad de la seguridad de la información, para esto, se deben tener en cuenta los siguientes aspectos:

- Establecer, documentar, implementar y mantener:

    - Los controles de seguridad de la información en procesos de continuidad de negocio o recuperación ante desastres, junto con los sistemas y herramientas que los respaldan.

    - Las modificaciones en los procesos, procedimientos y ejecución para mantener los controles de seguridad de la información vigentes durante situaciones adversas.

- Se establecerán controles de compensación para aquellos controles de seguridad de la información que no puedan mantenerse durante situaciones adversas. Dichos controles de compensación se diseñarán y se implementarán para garantizar que se mantenga el nivel de seguridad de la información adecuado

en todo momento, incluso durante eventos imprevistos. Estos controles de compensación se revisarán periódicamente para garantizar que sigan siendo efectivos y adecuados para la situación actual.

- Definir una estructura de gestión bien definida para prepararse, mitigar y responder a cualquier evento perturbador en la Defensoría del Pueblo. Esto requiere personal capacitado y competente con la autoridad adecuada.

- Designar un equipo de respuesta a incidentes con la capacidad y autoridad adecuadas para salvaguardar la seguridad de la información en la Defensoría del Pueblo es una medida fundamental. Este equipo debe contar con las habilidades y conocimientos necesarios para manejar eficazmente cualquier incidente que pueda surgir, asegurando la continuidad de los procesos y la protección de los datos sensibles.

- Es necesario desarrollar y aprobar planes y procedimientos documentados para la respuesta y recuperación ante eventos catastróficos en la Defensoría del Pueblo. Estos planes deben especificar detalladamente cómo se gestionará un evento adverso y se mantendrá la seguridad de la información dentro de los límites establecidos previamente, de acuerdo con los objetivos de continuidad de seguridad de la información establecidos en el Manual de seguridad de la información.

17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

La Defensoría del Pueblo tiene la responsabilidad de realizar verificaciones periódicas de los controles de continuidad de la seguridad de la información establecidos e implementados, para garantizar que sean eficaces y aplicables en situaciones adversas, para esto, se tendrán en cuenta los siguientes lineamientos:

- Realizar verificaciones regulares de los controles de continuidad de la seguridad de la información establecidos e implementados en la Defensoria del Pueblo para garantizar su validez y eficacia en situaciones adversas. Se recomienda que dichas verificaciones se lleven a cabo al menos una vez al año, y se sugiere que se realicen siguiendo las siguientes actividades:

    - Efectuar ejercicios y pruebas para validar la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, asegurando que estén en línea con los objetivos de continuidad de la seguridad de la información.

    - Ejecutar ejercicios y pruebas para evaluar el conocimiento y las habilidades en la operación de los procesos, procedimientos y controles de continuidad de la seguridad de la información en la Defensoría del Pueblo, garantizando que su desempeño esté en línea con los objetivos de continuidad de la seguridad de la información.

    - Verificar regularmente la efectividad de las medidas de continuidad de la seguridad de la información, en caso de cambios en los sistemas de información, procesos, procedimientos y controles de seguridad de la información, o en los procesos y soluciones de gestión de recuperación de desastres y continuidad de negocio.

- Implementar un plan de pruebas periódico, al menos una vez al año, del plan de Contingencia de la Plataforma Tecnológica para garantizar su eficacia ante posibles situaciones adversas. Este plan de pruebas debe ser diseñado cuidadosamente para asegurar una evaluación exhaustiva del plan de contingencia y permitir la identificación y solución temprana de posibles debilidades en el mismo.

17.2. Redundancias.

Para la Defensoría del Pueblo debe ser fundamental asegurar la disponibilidad de las instalaciones de procesamiento de información. Esto implica tomar medidas para prevenir y minimizar interrupciones en la operación de los sistemas, ya sea por causas naturales o por actividades malintencionadas.

17.2.1. Disponibilidad de instalaciones de procesamiento de información.

Es importante contar con planes de contingencia y procedimientos para la recuperación ante desastres, así como mantener un monitoreo constante de los sistemas y una adecuada gestión de los riesgos, para esto se deben contemplar los siguientes lineamientos:

- Establecer un centro de datos alterno como medida de contingencia para garantizar la continuidad de los servicios críticos de la Defensoria del Pueblo en caso de interrupciones en el centro de procesamiento de datos principal. Esto debe ser implementado de acuerdo con las buenas prácticas de seguridad de la información establecidas en la normativa correspondiente.

- En la medida de lo posible, se deben probar los sistemas de información redundante de la Defensoria del Pueblo para verificar su correcto funcionamiento después de una falla de un componente a otro, asegurando la conexión automática de emergencia.

18. Cumplimiento.

La Defensoría el Pueblo con el apoyo de todos los líderes de procesos y el grupo de TIC debe identificar y documentar de manera explícita todos los requerimientos estatutarios, normativos y contractuales relevantes, así como el enfoque de la organización para mantenerlos actualizados, tanto para cada sistema de información como para la organización en su conjunto.

18.1. Cumplimiento de requisitos legales y contractuales.

Para garantizar una adecuada gestión de la seguridad de la información, es fundamental evitar el incumplimiento de cualquier obligación legal, estatutaria, regulatoria o contractual que tenga relación con la seguridad de la información, así como de cualquier requisito de seguridad aplicable.

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

Los líderes de proceso de la Defensoría del Pueblo deben apoyar con la identificación tanto de la legislación aplicable como los requisitos contractuales que sean pertinentes para el sistema de gestión de seguridad de la información, Para ello, es importante tener presente los siguientes lineamientos:

- Elaborar la documentación tanto de los controles como de las responsabilidades individuales correspondientes para garantizar el cumplimiento de los requisitos estatutarios, reglamentarios y contractuales aplicables en materia de seguridad de la información.

- Identificar toda la legislación pertinente aplicable a la Defensoria del Pueblo con el fin de cumplir con los requisitos del Ministerio de tecnologías de la información y las comunicaciones.

- Identificar y documentar de manera explícita todos los requisitos normativos legales relevantes para cada sistema de información de la Defensoría del Pueblo, así como el enfoque de la Defensoria del Pueblo para cumplir y mantener dichos requisitos actualizados.

18.1.2. Derechos de propiedad intelectual.

La Defensoría del Pueblo debe establecer protocolos adecuados para garantizar el acatamiento de las normativas relacionadas con los derechos de propiedad intelectual y la utilización de programas patentados, para esto se deben considerar las siguientes directrices:

- Elaborar una política que regule el cumplimiento de los derechos de propiedad intelectual, la cual establezca los términos legales de utilización de programas y productos informáticos.

- Asegurar que la adquisición de software se realice únicamente de fuentes confiables y reconocidas para garantizar el cumplimiento de los derechos de autor.

- Socializar y concientizar a los colaboradores de la entidad a cerca de las políticas para salvaguardar los derechos de propiedad intelectual y comunicar de forma clara la intención de aplicar medidas disciplinarias a los empleados que no las cumplan.

- Mantener un adecuado registro de los activos y distinguir aquellos que deben ser protegidos en virtud de los derechos de propiedad intelectual.

- Conservar registro y comprobantes de la titularidad de las licencias, los discos maestros y los manuales entre otros.

- Establecer medidas de gestión que prevengan el exceso de usuarios por cada licencia, a fin de garantizar el cumplimiento del límite máximo permitido.

- Realizar una inspección rigurosa para confirmar que se encuentran instalados exclusivamente software y productos autorizados con su respectiva licencia.

- Definir una normativa que asegure el mantenimiento de las condiciones adecuadas de las licencias.

- Establecer una política que regule la disposición o transferencia de software a terceras partes.

- Dar estricto cumplimiento a los términos y condiciones establecidos para el uso del software y la información obtenida a través de redes públicas.

- Solo es permitido duplicar, convertir a otro formato o extraer información de registros comerciales en conformidad con lo estipulado por las leyes de derechos de autor.

- Se prohíbe la copia total o parcial de libros, artículos, reportajes y otros documentos, excepto aquellos que estén permitidos de acuerdo con la ley de derechos de autor.

18.1.3. Protección de registros.

Para alcanzar al cumplimiento de manera correcta, la Defensoría del pueblo requiere salvaguardar los registros cumpliendo con los requerimientos legales, contractuales, de reglamentación y de negocios para prevenir su pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, para lo cual se deben contemplar los siguientes lineamientos:

- Garantizar la protección de los registros, tales como registros contables, bases de datos, logs de transacciones, auditorías y procedimientos operativos, para evitar su pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requerimientos legales, de reglamentación, contractuales y demás que implemente la Defensoria del Pueblo.

- Clasificar los registros por tipo y establecer los períodos de retención y el medio de almacenamiento adecuado para cada uno, incluyendo papel, microfichas, medios magnéticos, medios ópticos y almacenamiento en nube. Además, almacenar de manera segura cualquier llave criptográfica y programas relacionados asociados con archivos permanentes encriptados o firmas digitales para permitir la des encriptación de los registros durante el período de retención.

- Proteger los registros de la Defensoria del Pueblo implementando las siguientes acciones:

    - Desarrollar directrices claras sobre la retención, almacenamiento, manejo y disposición de registros e información.

    - Desarrollar un programa de retención que identifique los registros y los períodos de tiempo durante los cuales deben ser retenidos, de acuerdo con las tablas de retención definidas por el grupo de Gestión Documental.

    - Realizar un inventario de fuentes de información clave.

18.1.4. Privacidad y protección de datos personales.

La Defensoría del Pueblo está en la obligación de garantizar la confidencialidad y resguardar la información de datos personales de acuerdo a las normas y regulaciones aplicables.

- Crear y aplicar una política sobre los datos de la Defensoria del Pueblo que resguarde la privacidad y protección de datos personales. Garantizar que esta política sea comunicada a todas las personas involucradas en el tratamiento de información de datos personales.

18.1.5. Reglamentación de controles criptográficos.

El grupo de TIC de la Defensoría del Pueblo debe Implementar medidas criptográficas en conformidad con los acuerdos, normativas y regulaciones aplicables.

Tomar en cuenta los siguientes aspectos en relación a la adhesión a los acuerdos, leyes y regulaciones de la Defensoría del Pueblo:

- Tomar en cuenta las limitaciones de importación o exportación de hardware y software informático para la realización de funciones criptográficas.

- Considerar las restricciones de importación o exportación de hardware y software informático que ha sido creado para añadir funciones criptográficas.

- Tomar en cuenta las restricciones en el uso de la encriptación.

- Considerar los métodos obligatorios o discrecionales de acceso a información encriptada por parte de las autoridades de otros países.

18.2. Revisiones de seguridad de la información.

La Defensoría del Pueblo, apoyada en los líderes de cada proceso debe realizar evaluaciones periódicas e independientes, y en caso de cambios relevantes, analizar el enfoque de la entidad con relación a la gestión de la seguridad de la información y su implementación, incluyendo objetivos de control, políticas, procesos y procedimientos.

18.2.1. Revisión independiente de la seguridad de la información.

La Oficina de Control Interno de gestión de la Defensoría del Pueblo debe realizar una revisión independiente de la seguridad de la información, esto implica una evaluación completa, objetiva y sistemática de los controles de seguridad de la información en la entidad. Este proceso es llevado a cabo por un equipo de auditores internos o externos que son independientes del área que está siendo auditada y debe contar con una periodicidad definida.

18.2.2. Cumplimiento con las políticas y normas de seguridad.

Los líderes de los procesos de la entidad deben llevar a cabo revisiones regulares del procesamiento y los procedimientos de información en su área de responsabilidad para garantizar el cumplimiento de las políticas y normas de seguridad adecuadas, así como cualquier otro requisito de seguridad relevante.

18.2.3. Revisión del cumplimiento técnico.

El grupo de TIC de la entidad debe establecer un plan de revisión periódica de los sistemas de información para asegurar el cumplimiento de las políticas y normas de seguridad de la información. Los resultados de estas revisiones deben ser documentados y cualquier incumplimiento debe ser abordado de manera oportuna.

Además, se deben llevar a cabo revisiones adicionales cuando ocurran cambios significativos en los sistemas de información o en las políticas y normas de seguridad de la información, para esto, se deben contemplar las siguientes directrices:

- Se deberá realizar una revisión anual de los sistemas de información para garantizar el cumplimiento de las políticas y normas de seguridad de la información.

- Las pruebas de penetración o valoraciones de vulnerabilidad deben ser realizadas con precaución, ya que estas actividades pueden comprometer la seguridad de los sistemas. Es necesario planificarlas y documentarlas, además de garantizar que sean repetibles para minimizar el riesgo.

- Solo las personas competentes autorizadas pueden realizar revisiones de cumplimiento técnico o supervisar las mencionadas revisiones.