POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Grupo de Sistemas
Secretaría General
Diciembre 2018

TABLA DE CONTENIDO

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. La implementación de las políticas de seguridad busca reducir el riesgo 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 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 ISO/IEC 27001:2013 e ISO/IEC 27002:2013 como referentes por excelencia en el marco de la seguridad de la información, los cuales tienen aceptación a nivel mundial.

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 datacenter, 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, 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.

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 auditoria, información de archivo, aplicaciones, herramientas de desarrollo y utilidades.
- **Físicos**: Documentos impresos, manuscritos y hardware.
- **Servicios**: Servicios computacionales y de comunicaciones.
- **Personas: I**ncluyendo 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 los mismos.

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 MegaByte, 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 del mismo.

ISO/IEC 27001:2013: Norma 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

Recipiente 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.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias [ISO/IEC Guide 73:2002].

Script: Es una 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.

Cumplimiento

El cumplimiento de las políticas de seguridad de la información, es obligatorio para todo funcionario o tercero (contratista, proveedor, *outsourcing*). Si un individuo u organización viola las disposiciones en las políticas de seguridad por negligencia o intencionalmente, La Defensoría tomará las medidas correspondientes, tales como acciones disciplinarias, despido, acciones legales, reclamo de compensación por daños, y otras que se consideren adecuadas de acuerdo con las leyes y la Constitución Colombiana.

Dominios de la Norma

Política de seguridad: Constituye el presente documento, y es donde se estipulan las políticas con respecto a la seguridad de la información para La Defensoría.

Organización de la seguridad: Gestionar la seguridad de la información dentro de la Entidad. (Roles, compromisos, autorizaciones, acuerdos, manejo con terceros)

Seguridad del Recurso Humano: Busca asegurar que empleados, contratistas y terceros entiendan sus responsabilidades y sean adecuados para los roles a desempeñar minimizando los riesgos relacionados con personal.

Gestión de activos: Se relaciona con el mantenimiento y protección apropiados de todos los activos de información.

Control de acceso: Realiza el control físico o lógico de los accesos a los activos de la información.

Criptografía: Pretende asegurar apropiadamente y de forma efectiva el uso de criptografía para proteger la confidencialidad, autenticidad e integridad de la información**.**

Seguridad Física y ambiental: Busca prevenir accesos físicos no autorizados (perímetro), daños o interferencias a las instalaciones de la Entidad y a su información.

Seguridad en las Operaciones: Busca garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información**.**

Seguridad en las Comunicaciones: Su objetivo es asegurar la protección de la información en redes y sus instalaciones de apoyo para el procesamiento de información

Adquisición, desarrollo y mantenimiento de sistemas de información: Asegura la inclusión de todos los controles de seguridad en los sistemas de información (infraestructura, aplicaciones, servicios, etc.)

Relaciones con los proveedores: Asegura la protección de los activos de la organización que son accesibles por los proveedores.

Gestión de incidentes de seguridad: Busca que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, sean comunicados de tal manera que se tome una acción correctiva adecuada y en el momento indicado.

Aspectos de seguridad de la información dentro de la continuidad del negocio: Enfocado en reaccionar en contra de interrupciones a las actividades de la función misional y en proteger los procesos críticos contra fallas mayores en los sistemas de información o desastres, y por otro lado, asegurar que se recuperen a tiempo.

Conformidad: Busca prevenir el incumplimiento total o parcial de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

Premisas básicas de seguridad de la información

Los siguientes principios básicos fundamentan las políticas de seguridad de la información para la infraestructura tecnológica de La Defensoría.

Protección de la información

Los activos de información serán protegidos con el nivel necesario en proporción a su valor y el riesgo para la función misional. La protección debe concentrarse en los aspectos de confidencialidad, integridad y disponibilidad de los activos de información.

Protección de los recursos tecnológicos

Los recursos tecnológicos serán protegidos con el nivel necesario en proporción a su valor y el riesgo para la función misional. Dichos recursos deben ser utilizados exclusivamente para desarrollar las actividades laborales establecidas a los funcionarios, contratistas y en contratos de o*utsourcing* y así mismo su utilización se hará en forma adecuada, con el máximo de eficiencia y con ejemplar racionalidad.

Autorización de usuarios

Todos los usuarios deben ser identificados independientemente con permisos de acceso específicamente e individualmente autorizados por razones básicas de la función misional. Los métodos de acceso de usuarios deben exigir un proceso robusto de autenticación, autorización apropiada y auditoria confiable.

Responsabilidad

Los usuarios, dueños y custodios de los activos de información de La Defensoría son responsables por el uso apropiado, protección y privacidad de estos activos. Los sistemas de información de La Defensoría generarán y mantendrán unas apropiadas pistas de auditoria para identificar usuarios, y documentar los eventos relacionados con eventos de seguridad.

Disponibilidad

Los activos de información deben estar disponibles para soportar los objetivos de la función misional de La Defensoría.

Integridad

Los activos de información deben estar adecuadamente protegidos para asegurar su completitud y precisión. Las medidas de validación definidas permitirán detectar las modificaciones inapropiadas, la eliminación o la adulteración de los activos de información.

Esfuerzo de Equipo

Para que la seguridad de la información sea efectiva, se requiere el esfuerzo de equipo, donde deben participar en forma activa todos los funcionarios que tengan interacción con los activos de la información de la Entidad. Todos los funcionarios deben cumplir con las políticas de seguridad de la información y además desempeñar un papel activo para su comprensión, entendimiento y divulgación.

Revisiones de seguridad

En forma periódica La Defensoría debe efectuar las revisiones necesarias para evaluar el cumplimiento de las diferentes políticas de seguridad. Esta tarea será realizada por el Oficial de Seguridad o el responsable del Grupo de Sistemas, según el caso.

Propiedad de la información

La información soportada por la infraestructura de tecnología informática de La Defensoría pertenece a la entidad, a menos que en una relación contractual se establezca lo contrario. Sin embargo, la facultad de otorgar acceso a la información es del responsable del área que genera o es dueña de esta información, por ejemplo el director de área o en su defecto, instancias superiores.

La información propiedad de La Defensoría y sobre la cual tiene sus derechos, podrá ser suministrada a los entes de control pertinentes cuando estos lo requieran, con previa autorización expresa y aprobada por las directivas de la Entidad para estos fines.

Para efectos de control del flujo de la información de los procesos de la Entidad, se asignarán responsables de la información, quienes deben asegurar y otorgar acceso a la información que genere su área, con el fin de lograr un adecuado ambiente de control y un buen nivel de segregación de funciones.

Todas las personas vinculadas como funcionarios con contratistas de la defensoría que tengan acceso a sistemas de información, usen activos informáticos o tengan acceso a bases de datos deben leer, entender y aceptar las disposiciones de este documento. La obligación del tratamiento de información confidencial se mantendrá aun después de terminar la vinculación con la Defensoría del Pueblo por el posible daño a otros que puede ocasionar.

En caso de divulgación no autorizada de la información de propiedad de La Defensoría, se realizarán las investigaciones pertinentes para establecer sanciones, las cuales serán evaluadas con el jefe inmediato del usuario involucrado o el área encargada de adelantar procesos disciplinarios internos, para lo cual utilizarán el concepto emitido por el dueño de la información.

Políticas

Política de Seguridad

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

La dirección debe aprobar, publicar, comunicar a todos los empleados o partes externas pertinentes el documento de políticas de 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.

Organización de la seguridad de la información

Organización Interna

Define las directrices para gestionar la seguridad de la información dentro de la Entidad

Oficial o grupo de Seguridad de la Información

Las funciones del Oficial o del Grupo de Seguridad de la Información serán las siguientes:

- Liderar y coordinar la implementación de las políticas de seguridad de la información, con la participación activa de las dependencias de la Entidad.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas de información o servicios informáticos.
- Identificar las necesidades y recursos necesarios (tecnológicos, humanos, de capacitación, financieros, etc.) para el mantenimiento de la infraestructura de seguridad de la información.
- Identificar las necesidades de formación (capacitación y entrenamiento) de los encargados de la administración de los activos de la información correspondientes al Grupo de Sistemas y poner en consideración del Comité de Seguridad de la Información un plan de capacitación para formar y entrenar a los responsables.
- Actuar como un asesor en seguridad de la información para la Entidad.
- Hacer seguimiento al comportamiento de los indicadores de gestión de la seguridad de la información que adopte el Comité de Seguridad de la Información
- Liderar la creación e implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de la Entidad y adelantar su revisión, supervisión y evaluación de desempeño.
- Establecer un programa periódico (por lo menos una vez al año) de revisión de vulnerabilidades de la plataforma tecnológica de la Entidad y coordinar los respectivos aseguramientos conforme los resultados de las mencionadas pruebas.
- Reportar al Comité de Seguridad de la Información el estado de la investigación y monitoreo de los incidentes de seguridad de la información, los resultados de las auditorias periódicas, la revisión y supervisión del SGSI.
- Presentar al Comité de Seguridad de la Información iniciativas e informes periódicos del estado de seguridad de la información de la Entidad.
- Las demás que le asigne el Superior Inmediato.

Comité de Seguridad de la Información o comité de TIC (subsistema de seguridad de la información)

La Entidad establecerá el Comité de Seguridad de la Información, el cual estará conformado por miembros de alto nivel de las divisiones de la Entidad o sus delegados y liderado por Secretario General. Este Comité debe periódicamente revisar el estado general de la seguridad de la información, revisar y monitorear los incidentes de seguridad de la información, revisar y aprobar los proyectos de seguridad de la información, aprobar modificaciones o nuevas políticas de seguridad de la información y realizar otras actividades

de alto nivel relacionadas con la seguridad de la información. El Comité de Seguridad de la Información sesionará de manera ordinaria una (1) (o en el periodo que se considere necesario) vez cada mes y extraordinariamente cuando se estime pertinente por convocatoria de cualquiera de sus integrantes. A sus sesiones podrán asistir con voz, pero sin voto, los servidores de la Entidad y particulares que se convoquen, con el fin de que orienten o aclaren los temas a tratar en cada sesión.

Serán funciones del Comité de Seguridad de la Información las siguientes:

- Proponer a la Alta Direccióin, para su aprobación, los cambios en la Política de Seguridad de la Información y las responsabilidades generales en materia de seguridad de la información.
- Mantener informado a la Alta Dirección sobre el estado general de la seguridad de la información de la Entidad.
- Tener conocimiento y vigilar la investigación y el monitoreo de los incidentes de seguridad de la información por parte del Oficial o grupo de Seguridad de la Información.
- Evaluar y proponer al Defensor del Pueblo, para su aprobación, iniciativas de inversión para incrementar la seguridad de la información.
- Evaluar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Adoptar los indicadores de gestión de la seguridad de la información.
- Verificar que la seguridad sea parte del proceso de clasificación de la información.
- Verificar que la seguridad sea parte del desarrollo de sistemas de información o aplicaciones de software, desde las etapas tempranas del desarrollo.
- Promover la difusión y apoyo a la seguridad de la información dentro de la Entidad y a las campañas de sensibilización en temas de seguridad de la información.

Acuerdos de confidencialidad

La Defensoría establecerá un mecanismo de aceptación del compromiso de confidencialidad e integridad de la información institucional para ser aplicado a los funcionarios, contratistas y terceros que por cualquier razón requieran acceso a la plataforma tecnológica o a los sistemas de información de la Entidad. Dicho mecanismo deberá ser incluido en los contratos y documentos de posesión de los funcionarios, contratistas y terceros.

Segregación de funciones

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, evitar los errores involuntarios y evitar posiciones de poder que faciliten actuaciones indebidas.

Seguridad de la información en la administración 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.

Dispositivos móviles y conexiones remotas

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.

Seguridad de 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 establecidospara que el Grupo de Sistemas 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 Sistemas, 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 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.

Seguridad en conexiones remotas

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 Oficial de Seguridad de la Información.

Solamente se autorizarán los accesos a la red corporativa, 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, pero sin embargo, la Defensoría 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.

Responsabilidades para la autorización de conexión remotas

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 se reserva el derecho de implementar y poner a disposición de sus colaboradores redes inalámbricas Wi-Fi conectadas a la red de datos e Internet de la Entidad.

Para su uso se reglamentan las siguientes restricciones:

- Todos los usuarios que accedan a las redes inalámbricas de la Defensoría 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 Sistemas 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.

Seguridad del Recurso Humano

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.

Vinculación de personal

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.

Términos y condiciones laborales y contractuales

- Los términos y condiciones laborales a los cuales deben acogerse todas las personas que ingresen a la Defensoría en calidad de funcionarios deben estar establecidas de manera formal mediante acto administrativo.

- 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.

Responsabilidades de la dirección

Las directivas de la Entidad 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 administración de riesgos de la Defensoría.

Educación, formación y concienciación sobre la seguridad de los activos de 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.
- La Defensoría debe realizar evaluaciones de forma anual a sus funcionarios para establecer el grado de sensibilización y definir las estrategias de mejoramiento.
- La Defensoría en el proceso de inducción a los nuevos funcionarios, incluirá la charla de concienciación de seguridad de la información.

Procesos disciplinarios

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 Entidad 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 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 informados por éste, de forma inmediata, al Comité de Seguridad de la Información, el que a su vez informará a la Oficina Jurídica para el inicio de las acciones judiciales pertinentes.

Terminación o cambio de la vinculación laboral o contractual

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.

Responsabilidades en la terminación de la vinculación laboral o contractual

Las terminaciones de la vinculación laboral son responsabilidad del Defensor del Pueblo.

Gestión de los activos de información

Responsabilidad por los activos

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

Inventario de Activos

Se debe contar un inventario de activos para logar y mantener la protección adecuada de los activos de la Defensoría del Pueblo. 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 o contratista que 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.

Propiedad de los activos

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

Uso aceptable de los activos

El funcionario o contratista responsable por la custodia y protección de los activos se llamará designado. Se tendrá una base de datos donde se asignará a cada activo a su designado. Se debe identificar los designados para todos los activos y asignar las responsabilidades de implementación y mantenimiento de los controles adecuados.

Devolución de 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.

Clasificación de la información

Este control tiene como finalidad asegurar que la información recibe el nivel de protección adecuado.

En esta parte del documento se describe la política de seguridad para asistir en la realización del proceso de clasificación de la información. Este proceso de clasificación es fundamental para cumplir con las políticas de seguridad de la información dispuestas por la Entidad. Esta política también combina dos principios básicos del control de acceso. Para la información más sensitiva, se utiliza el principio de "necesidad de saber[1]", y para la menos sensitiva, el principio de "necesidad de retención[2]".

Debido al hecho que la información es uno de los activos o recursos más valiosos para la operación y cumplimiento de la misión funcional de la Defensoría, es necesario conocer con que activos de información se cuenta, quién es su correspondiente propietario y qué niveles de clasificación se requieren, de manera que se logre identificar claramente, cómo debe ser esta información administrada, transportada o procesada, con el fin de protegerla de acuerdo a su importancia, criticidad y nivel de confidencialidad requerido durante su utilización dentro

[1] Principio "necesidad de saber": la información será utilizada exclusivamente cuando se necesite saber y sea comprobada ésta necesidad.

[2] Principio "necesidad de retención": el acceso a la información es menos restringido y de uso más frecuente. Se puede mantener como una referencia cercana de consulta.

de la Defensoría, contra una posible divulgación no autorizada, uso indebido, modificación no autorizada y posible destrucción o borrado ya sea este intencional o accidental.

La información debe ser consistentemente protegida a lo largo de su ciclo de vida, desde su creación hasta su destrucción. Sin estas políticas la Defensoría puede estar expuesta a pérdida de credibilidad ante la opinión pública, interrupciones en la operación, costos excesivos, e inclusive demandas por parte de otras Entidades estatales o personas naturales. Esta información debe ser protegida en proporción directa a su nivel de sensibilidad, sin importar donde resida, ni su forma, sin importar que tecnología fue usada para manejarla, y sin importar el propósito para el que ella existe y debe ser revisado este nivel de clasificación al menos una vez al año.

La información que sea catalogada como confidencial que requiera ser transmitida por medios de comunicación públicos debe utilizar un esquema de cifrado con el fin de proteger su confidencialidad.

Directrices de clasificación

Toda información existente, generada y modificada que exista en los equipos de cómputo, sistemas de información y bases de datos de la Defensoría deberá clasificarse de acuerdo con las clasificaciones establecidas en esta política por confidencialidad, integridad y disponibilidad. Se considera información confidencial cualquier dato sensible que se puede usar para discriminar, hacer daño o permitir a otros atentar o causar cualquier tipo de acción ilegal. La información que no puede ser revelada a terceros y no es pública es información confidencial.

Clasificación por confidencialidad

Por confidencialidad, la información debe clasificarse en uno de los siguientes niveles:

CF1: Información que puede estar al alcance de todos y su conocimiento no genera ninguna pérdida de vidas ni atenta contra la integridad del ciudadano. Por ejemplo, información de promoción y divulgación de derechos humanos.

CF2: Información que no es altamente confidencial pero que no debe ser pública, es decir, aquella cuyo conocimiento puede crear cierto grado de expectativas, conllevar a pérdidas económicas bajas o atentar contra la integridad personal. Por ejemplo, información de la hoja de vida de los empleados. La mayoría de la información del día a día cae bajo esta clasificación y solo deberá estar al alcance de personal autorizado.

CF3: Información altamente confidencial; su conocimiento genera situaciones de riesgo para ciudadanos, desprestigio para la entidad o detrimento patrimonial desventajas competitivas o pérdidas económicas significativas. Por ejemplo, informes de situaciones de riesgos y alertas tempranas, información financiera del peticionario.

Clasificación por integridad

Por integridad, la información debe clasificarse en uno de los siguientes niveles:

IN1: Información de naturaleza no financiera que no tenga repercusión en decisiones administrativas y gestión defensorial, si fuera errada; la pérdida que origina es muy pequeña y su reconstrucción consiste en la repetición de un proceso sencillo.

IN2: Información relacionada con la gestión defensorial y aquélla en la cual se basan las decisiones de la operación diaria de la organización y que necesita un nivel razonable de protección contra error y fraude.

IN3: Información para la toma de decisiones estratégicas de alto nivel administrativo que conlleve a la ocurrencia de un fraude con pérdidas altamente significativas. La información deberá estar libre de error y protegida contra fraude.

Clasificación por disponibilidad

Por disponibilidad, la información debe clasificarse bajo dos conceptos: retención y recuperación.

- Por Retención:

  RTN1: No hay ningún requisito de retención; depende de las necesidades de cada usuario. Por ejemplo, archivos personales de trabajo.
  RTN2: Información defensorial o financiera sobre la cual se ha normalizado, por conveniencia, un período de retención particular.
  RTN3: Información sobre la cual existen requisitos legales o contractuales especiales que exigen formas específicas de almacenamiento o duración de retención.

- Por Recuperación:

  RCP1: El tiempo de recuperación no es inmediato, puede esperar, por lo menos, una semana sin traer consecuencia alguna.
  RCP2: El tiempo máximo para recuperar y volver a iniciar el procesamiento es menor a una semana.
  RCP3: El tiempo máximo para recuperar y volver a iniciar el procesamiento es menor a un día.

Gestión de medios removibles

Entenderemos a partir de ahora como medios removibles los siguientes:

- Memorias tipo USB

  Discos duros

- Discos de almacenamiento óptico (CD, DVD, Blu-ray)

- Cintas para realizar respaldos

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 los mismos debe tomar mayores medidas de protección de los mismos 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.

Eliminación de medios

El Grupo de Sistemas será el responsable de la ejecución de la destrucción de los medios extraíbles y guardará un registro de destrucción de los mismos. Para el efecto se deben utilizar los siguientes procedimientos:

- Discos Duros: Se deberá extraer físicamente los platos internos y destruirlos en su totalidad mediante algún elemento como martillo o pinzas, y debe ser triturado, pulverizado, incinerado o desintegrado y luego desechado. Las unidades lógicas y las cajas serán conservadas.

- Discos de almacenamiento óptico (CD, DVD, etc.): Estos serán destruidos en su totalidad mediante algún elemento como martillo o pinzas y deben ser triturados, pulverizados, incinerados o desintegrados y luego ser desechados.

- Cintas de backup: serán destruidas físicamente mediante la extracción y perforación de la cinta interior, la caja será destruida también mediante algún elemento como martillo o pinzas. Debe ser triturada, pulverizada, incinerada o desintegrada y luego ser desechada.

Transporte físico de medios

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.

Control de Acceso

En este numeral se definen las políticas que deben ser cumplidas por todos los funcionarios de la Entidad y las terceras partes, en los temas relacionados con el control de acceso a los sistemas de información, la red, y en general, a los activos de información de la Defensoría.

Requisitos del negocio para el control de acceso

Todos los funcionarios y contratistas activos de la Defensoría del Pueblo deben tener una cuenta institucional asociada a los servicios que la entidad considere debe tener de acuerdo a su perfil ejemplo: directorio activo, correo electrónico, VisionWEB, etc.

La cuenta institucional debe ser el identificador único de cada usuario mientras esté activo en la organización, en caso contrario esta cuenta debe deshabilitarse junto con los servicios que tenga asociados.

Las personas que posean una cuenta institucional estarán obligadas a leer y entender las políticas de seguridad, aplicables y vigentes de la organización.

Algunos servicios podrán tener otros métodos de acceso diferente a la cuenta institucional en cuyo caso, los administradores de estos aplicativos deberán cumplir las disposiciones de seguridad vigentes.

Todos los activos de información deben asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados.

Los administradores de los activos de información deberán establecer los procedimientos formales para controlar la asignación de derechos o cuentas de acceso. Estos procedimientos deben comprender todas las fases del ciclo de vida de la aplicación teniendo correspondencia con el ciclo de vida de acceso al usuario.

Las fases del ciclo de vida de acceso al usuario son:

1. Registro inicial
2. Uso y mantenimiento
3. Cancelación final de acceso

Dado que cada activo de información tiene requerimientos diferentes en cuanto a registro de actividades de los usuarios, es responsabilidad de los administradores de dichos activos definir y documentar el tiempo que durarán los registros de acceso almacenados de usuarios activos, se debe definir cuanto tiempo se mantendrán los registros de acceso de usuarios cuyo acceso haya sido cancelado a fin de permitir una trazabilidad.

Gestión de acceso de los usuarios

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.

Gestión de privilegios

Se debe proteger los activos de información, las aplicaciones y sistemas de información de acceso no autorizado. Esto se realiza controlando la asignación, modificación y eliminación de privilegios a través de un procedimiento formal de autorización.

Para la asignación de privilegios, la Defensoría debe aplicar el principio de menor privilegio posible, que consiste en que solo se otorgan los permisos necesarios para la ejecución de las funciones.

El procedimiento de autorización de accesos debe incluir:

- Identificación de los usuarios y privilegios de acceso a cada módulo o componente del sistema de información.

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

- Tener un registro del proceso de autorización que debe ser conservado como parte de la documentación para revisiones futuras. Los privilegios no se deben otorgar hasta que los procedimientos de autorización se hayan completado.

- Los cambios en los privilegios de autorización asignados deben cumplir con los procedimientos de autorización previamente autorizados. No se puede otorgar o negar algún privilegio que interfiera con la funcionalidad requerida o la seguridad de la aplicación.

- Se debe incluir el procedimiento para la eliminación de privilegios cuando el usuario no requiera ingresar más al aplicativo.

Gestión de contraseñas para usuarios

Para todos los activos de información se deben definir los parámetros de control de contraseñas cumpliendo con lo siguiente:

- Las contraseñas predefinidas que traen los equipos nuevos tales como Routers, Switches, etc, deben cambiarse inmediatamente al poner en servicio el equipo.

- 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.

- 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.

- La mínima longitud obligatoria es de ocho (8) caracteres.

- Toda contraseña debe tener por lo menos un (1) carácter alfabético en mayúscula, uno en minúscula y un carácter numérico. Se recomienda el uso adicional de caracteres especiales (#$&-_...)

- Una contraseña no puede ser usada por más de 45 días. Al cabo de tal periodo debe cambiarse la contraseña, o cada vez que exista la sospecha de que la misma puede ser adivinada.

- Si es absolutamente necesario escribir la contraseña, debe ser "cifrada" cambiando cada carácter con un algoritmo sencillo pero privado que no muestre la contraseña en forma textual. (Ej.: p1: Juan01admin, se escribe: kVBO01BENJO. Se desplazó cada carácter alfabético una posición en el alfabeto y se cambiaron mayúsculas por minúsculas)

- 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.

Revisión de los derechos de acceso de los usuarios

El administrador de cada activo de información debe establecer un procedimiento de revisión y control periódico de los privilegios de los usuarios que garantice que solamente tengan los permisos de acuerdo a su perfil y funciones, y de ser necesario realizar los ajustes pertinentes. Adicionalmente verificar que no existan cuentas de usuario asignadas a ex-funcionarios o personal externo que no esté laborando para la entidad.

El procedimiento debe considerar:

- El administrador 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 administrador de la aplicación debe verificar los privilegios asignados para evitar que no se hayan asignado privilegios no autorizados.

Responsabilidades de los usuarios

Esta política define las directrices para evitar el acceso de usuarios no autorizados, robo, puesta en peligro de la información y de los servicios de procesamiento de información.

Los usuarios son responsables del buen uso de sus credenciales y contraseñas para evitar el acceso no autorizado, el robo o puesta en peligro de la información y de los servicios de procesamiento de información.

Las personas que posean una cuenta institucional estarán obligadas a leer y entender las políticas de seguridad, aplicables y vigentes de la organización.

Uso de la contraseña

Las siguientes disposiciones son definidas para todos los usuarios con acceso a los servicios de información y aplicaciones de la Defensoría del Pueblo con el fin de proteger la información institucional, de sus 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, puede dar como resultado la suspensión o negación del servicio y/o privilegios de acceso al servicio, datos o información.

- 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.

Las siguientes características de las contraseñas, de la cuenta institucional y de otras cuentas para acceso a servicios y aplicaciones específicas, deberán ser leídas, entendidas y aplicadas por todos los usuarios y controladas por los diferentes servicios y aplicaciones de la organización.

- Las contraseñas deben tener mínimo una longitud de ocho (8) caracteres.

- Las contraseñas deben contar con por lo menos tres (3) de las siguientes cuatro (4) características en cualquier orden: letras mayúsculas, letras minúsculas, números y símbolos. Las contraseñas deben tener una periodicidad máxima de 10 semanas. Los sistemas y aplicaciones deberán informar sobre el vencimiento de las contraseñas con suficiente anticipación.

- Si la contraseña no es cambiada en el tiempo establecido, la cuenta asociada será bloqueada automáticamente y se restringirá el acceso a los demás servicios y aplicaciones, hasta que la cuenta sea habilitada nuevamente.

- Las contraseñas no se podrán repetir en mínimo 5 iteraciones.

- Las contraseñas son personales e intransferibles. En el caso de las cuentas compartidas, de administración o listas de correo y demás, el responsable principal deberá cambiar las contraseñas e informar por un medio seguro a cada uno de los demás usuarios, los cuales aceptan que dichas contraseñas no podrán ser divulgadas a otros usuarios, así estos estén autorizados.

Adicionalmente, la Defensoría del Pueblo recomienda a los usuarios tener en cuenta las siguientes consideraciones de seguridad con las contraseñas:

- No utilizar una misma contraseña para varios correos electrónicos y/o servicios de información, internos o externos a la entidad.

- No utilizar contraseñas que tengan relación con información personal, sobrenombres, fechas importantes, teléfonos, nombres de familiares y demás información que pueda ser obtenida por ingeniería social.

- No utilizar palabras o combinación de palabras que puedan ser fácilmente descubiertas por ataques de diccionario.

- No utilizar combinaciones secuenciales del teclado como “qwerty”, “123456”, “987654” y “1qaz” entre otras.

- Utilizar contraseñas fácilmente recordables y que se puedan digitar rápidamente y preferiblemente sin mirar el teclado.

- No escribir en papel sus contraseñas y dejar dichos papeles de acceso público o a la vista. En caso de escribir las contraseñas en papel, estos deben ser almacenados bajo estrictas condiciones de seguridad.

- No instalar scripts o programas que recuerden contraseñas en sus computadores o dispositivos móviles. Tampoco se deben guardar las contraseñas en archivos o notas electrónicas dentro de computadores o dispositivos móviles. En caso de ser necesario, cualquier archivo que contenga contraseñas debe ser cifrado.

- Utilizar únicamente los computadores o dispositivos móviles de confianza.

- No enviar las contraseñas por correo electrónico, mensajes de texto ni pronunciarlas a través de llamadas telefónicas ni en sitios públicos.

Equipo de usuario desatendido

Los usuarios deben evitar dejar sus estaciones de trabajo con la sesión abierta, cuando se retiren del puesto de trabajo deberán bloquear la sesión de Windows, en particular cuando el tiempo que permanecerá el usuario alejado del equipo es considerable, como es el caso de hora de almuerzo.

Los usuarios deberán cerrar las conexiones a los sistemas de información si no van a trabajar en el mismo en lapsos de más de 30 minutos, pues se consumen recursos que podrían ser utilizados por otros usuarios.

Política de escritorio y pantalla despejados

Los funcionarios de la Entidad deben adoptar la cultura de “escritorio despejado” que consiste en:

- En los puestos de trabajo solo deben permanecer los documentos y elementos necesarios para la realización de la labores.

- Los archivadores y escritorios deben permanecer cerrados con llave.

- No dejar documentos confidenciales a la vista de otras personas.

- No arrojar documentos confidenciales a la basura, éstos deben ser destruidos, para ello la Entidad podrá disponer de máquinas destructoras de documentos o contratar con alguna empresa especializada en la destrucción de documentos confidenciales y en caso de no contar con las mismas, el usuario deberá destruirlos rompiéndolos en pedazos que no superen los 320 mm2 en fragmentos de 0,9 mm x 30 mm o tiras de 1,9 mm de ancho y deberán ser arrojados en la basura no reciclable.

- Al finalizar las labores diarias o si el funcionario se va a ausentar de su puesto de trabajo, todos los documentos confidenciales deben ser guardados en sitio seguro.

- No pegue papeles que contengan información confidencial, especialmente contraseñas.
- Mantenga organizado y en orden el puesto de trabajo
- No ingiera alimentos ni bebidas en el puesto de trabajo.
- Las estaciones de trabajo deben ser apagadas al finalizar la jornada.

Control de acceso a las redes

El objetivo de esta política es evitar el acceso no autorizado a los servicios de red.

Política de uso de los servicios de Internet

El servicio de Internet suministrado por la Defensoría del Pueblo es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios, por lo tanto, sin perjuicio de la responsabilidad penal, administrativa o disciplinaria a que haya lugar, éstos al utilizarlo, deben observar y cumplir las directrices que a continuación se enlistan:

- El servicio de Internet institucional únicamente puede ser utilizado para el desarrollo de actividades directamente relacionadas con el cumplimiento de la misión de la Defensoría del Pueblo y las funciones de sus servidores.
- La conexión a internet no debe realizarse directamente desde dispositivos no autorizados por el Grupo de Sistemas como módems, líneas telefónicas, etc.
- Este servicio no debe ser utilizado para enviar o recibir archivos de video, audio, texto, fotos, etc., con contenidos insultantes, ofensivos, injuriosos, obscenos o violatorios de los derechos de autor;
- Dicho servicio no debe ser utilizado para escuchar música o videos conectado directamente al sitio en Internet que provee este servicio o mediante el acceso directo a un equipo de la red local institucional;
- Tampoco está permitido mediante este servicio descargar, instalar o ejecutar archivos o software de procedencia desconocida.
- No se permite acceder a sitios de pornografía, juegos o apuestas.
- La navegación en Internet debe ser razonable y utilizada con propósitos laborales.
- No se deben utilizar los recursos de la Entidad para almacenamiento de archivos que contengan música, videos, y cualquier información que no sea de carácter laboral.
- El Grupo de Sistemas está habilitado para limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines institucionales.

Autenticación de usuarios para conexiones externas.

- Los usuarios se comprometen a usar las conexiones de acceso remoto para propósitos estrictamente laborales.

- El acceso a información confidencial debe establecerse bajo los mecanismos apropiados de encripción, para VPN IPSEC deberá utilizarse cifrado Triple-DES y para VPN SSL debe utilizarse versión 3.0.

- No se permite la utilización de cuentas o contraseñas genéricas para las conexiones de acceso remoto.

- Las conexiones de acceso remoto deben ser registradas en los logs de auditoria.

Identificación de los equipos en las redes

Los dispositivos de cómputo y comunicaciones deben tener un nombre lógico, el cual deberá mantenerse como parte de los registros de activos, para permitirle al administrador de red identificar la ubicación y responsable del mismo.

Protección de los puertos de configuración y diagnostico remoto

- El acceso físico a los puertos de configuración y diagnostico debe estar restringido exclusivamente a los responsables de dichas actividades en los respectivos dispositivos.

- La conexión lógica a los puertos de configuración y diagnostico debe estar controlada con mecanismos de autenticación que únicamente permita su acceso a los responsables de dichas actividades en los respectivos dispositivos.

Separación en las redes

La red interna de la Defensoría debe contar con una segmentación lógica o física que agrupe los elementos de red con al menos los siguientes segmentos: Red LAN que contiene las estaciones de trabajo y dispositivos de oficina, red para visitantes y red de Servidores.

Control de conexión a las redes

La Defensoría debe aplicar el principio de menor privilegio posible, que consiste en que solo se otorgan los permisos necesarios para la ejecución de las funciones, de esta forma la conexión desde y hacia redes compartidas debe ser restringida a quienes requieren el acceso y solo con privilegios requeridos.

Control de enrutamiento de la red.

Las rutas definidas en la red de la Defensoría deben permitir exclusivamente las conexiones autorizadas y se debe evitar la existencia de rutas innecesarias.

Control de acceso al sistema operativo

Esta política tiene como objetivo evitar el acceso no autorizado a los sistemas operativos.

Procedimiento de ingresos seguros

Los sistemas implementados en la Defensoría deberán disponer de los siguientes mecanismos de ingreso seguro:

- No mostrar identificadores de aplicación ni del sistema hasta que el proceso de registro de inicio se haya completado.

- Mostrar una advertencia de notificación general indicando que sólo deberían tener acceso al computador los usuarios autorizados.

- No suministrar mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado.

- Validar la información de registro de inicio únicamente al terminar todos los datos de entrada. Si se presenta una condición de error, el sistema no debería indicar qué parte de los datos es correcta o incorrecta.

- Limitar la cantidad de intentos permitidos de registro de inicio, por ejemplo tres intentos.

- Limitar el tiempo máximo y mínimo permitido para el procedimiento de registro de inicio. Si se excede, el sistema debería finalizar esta operación.

- Al terminar un registro de inicio exitoso, mostrar la fecha y hora de registro de inicio exitoso previo y los detalles de intentos fallidos de registro de inicio desde el último registro exitoso.

- No mostrar la contraseña que se introduce o considerar esconder los caracteres mediante símbolos.

- No trasmitir contraseñas en texto claro en la red.

Identificación y autenticación de usuarios

Los sistemas implementados en la Defensoría deberán disponer de los siguientes mecanismos de identificación y autenticación de usuarios:

- Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.

- Las cuentas de usuario son de carácter individual e intransferible por lo cual todo funcionario que tenga que utilizar los servicios informáticos debe poseer su propia cuenta de usuario.

- Todas las cuentas de usuario deben utilizar al menos la validación de la contraseña que permita autenticarla y esta debe cumplir con las políticas establecidas en el numeral Uso de la contraseña.

Sistemas de Gestión de contraseñas.

Los sistemas implementados en la Defensoría deberán configurarse para que todas las contraseñas de acceso cumplan con las características de complejidad y longitud definidas en el numeral Uso de la contraseña.

Uso de las utilidades del sistema.

La instalación o utilización de herramientas que eludan los controles definidos dentro del sistema no está permitida.

Tiempo de inactividad de la sesión

- Los sistemas de información deben tener configurado la desconexión automática de sesión por inactividad de más de diez (10) minutos.

- En las estaciones de trabajo se debe habilitar el control automático de bloqueo con contraseña, para las sesiones que permanecen más de tres (3) minutos inactivas.

Limitación del tiempo de conexión.

Los sistemas implementados en la Defensoría deberán configurarse para limitar el acceso según los horarios durante los cuales se permite el acceso.

Control de acceso a las aplicaciones y a la información.

Esta política tiene como objetivo evitar el acceso no autorizado a la información contenida en los sistemas de información.

Restricción de acceso a la información

Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte de acuerdo con la política definida de control de acceso.

Los permisos otorgados dentro de cada sistema deben ser controlados por roles y perfiles de usuario que determinan los niveles de acceso de acuerdo a las funciones desempeñadas por cada usuario, según las políticas de Roles y perfiles.

Cada aplicativo debe tener incluida la funcionalidad de crear, modificar y eliminar perfiles. La creación o actualización de perfiles está relacionada con la autorización para insertar, actualizar, borrar, eliminar o consultar registros o tablas o ejecutar procedimientos almacenados. La creación, modificación o eliminación de perfiles así como la asignación/revocación de perfiles para cuentas de usuario está soportada con una justificación y la correspondiente autorización del Administrador funcional. La asignación del perfil a una cuenta de usuario se basa en la aplicación del principio de menor privilegio posible, es decir, otorgar los permisos necesarios para la ejecución de las funciones.

Se debe tener especial cuidado en la asignación de permisos para consulta o reporte en los aplicativos según la clasificación de la información establecida en la Entidad.

El administrador funcional de cada aplicativo mantiene un registro de control de los perfiles autorizados, así como sus funciones asociadas y los usuarios autorizados para cada perfil. El registro de control se verifica y/o actualiza cada vez que existan novedades de personal (ingreso, traslado o retiro de funcionarios) las cuales se comunicaran oportunamente a través de La Subdirección de Gestión del Talento Humano.

Cada 2 meses se revisarán los perfiles (privilegios) en cada aplicativo.

En el evento de que un funcionario no cumpla con esta política de restricción de acceso de la información y requiera un reporte, registros almacenados o estadísticas deberá solicitarlo directamente al responsable del área o dirección que administra el sistema de información.

Aislamiento de sistemas sensibles

Los sistemas que sean de carácter sensible no pueden estar operando en un entorno informático (servidor, base de datos) compartido y deben estar ubicados en un segmento de red especial para sistemas sensibles, protegido por un firewall y un sistema de detección de intrusos.

Controles criptográficos

Esta política tiene como objetivo proteger la confidencialidad e integridad de la información.

Política sobre el uso de los controles criptográficos

La información que contenga contraseñas de usuario o claves para el control de acceso a los sistemas de información no pueden ser almacenadas en texto plano. Es responsabilidad de los administradores de los sistemas, definir los algoritmos de encriptación más apropiados para ser utilizados en los sistemas de información críticos con base en un análisis de riesgos y considerando los criterios de confidencialidad, integridad/autenticidad, no repudio así como las tecnologías de encriptación disponibles y los costos relacionados.

Gestión de llaves

Las llaves o claves criptográficas se deben proteger contra pérdida, modificación y destrucción no autorizadas, por lo tanto, es necesario que los administradores de las mismas tomen en cuenta las siguientes medidas:

- 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 perdidas o corruptas
- Definir criterios para archivar las claves y para destruirlas
- Mantener registros de auditoria de las actividades de gestión de claves.

Seguridad Física y Ambiental

Esta política tiene el propósito de evitar el acceso no autorizado o el daño e interferencia a las instalaciones y activos de información de la Defensoría.
También define las áreas que deben ser consideradas como restringidas de acuerdo a las directrices tomadas por la Defensoría. Además define las características que estas áreas deben poseer para cumplir con las políticas de seguridad de la información. Ahora bien, si un área es catalogada como área restringida, se deben cumplir las normas y procedimientos establecidos en la política.

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.

Perímetro de seguridad física

Las áreas de acceso restringido deberán contar con esquemas de protección de su perímetro como paredes, puertas, chapas, candados y sistemas de control de acceso biométricos y alarmas. En los casos que el Oficial de Seguridad de la Información considere necesarios se deberán instalar sistemas de detección y extinción de incendios.

Se consideran al menos las siguientes áreas como de acceso restringido:

- Centro de cómputo
- Centro de cableado
- Cintoteca
- Bodegas administradas por TI
- Tableros de distribución eléctrica
- Strip Telefónico
- Cuarto de control
- Salas de crisis
- Oficina de tecnología
- Oficina del tesorero

Cintoteca

La Entidad debe contar con una cintoteca ubicada en las instalaciones del Grupo de Sistemas, para la custodia de la información. Se considera a la Cintoteca como parte funcional del centro de cómputo a pesar de que por seguridad se trata de un recinto contiguo pero independiente.

Centro de Cómputo

El oficial de seguridad, en conjunto con el comité de seguridad, deben establecer los mecanismos necesarios para la correcta protección del Centro de Datos y las áreas consideradas como restringidas, por el hecho de almacenar o transportar información crítica para lograr la función misional, de manera que se mantenga la confidencialidad y seguridad de la información que se procesa, almacena o transporta, así como la integridad de la información. Se debe contar además con mecanismos preventivos y detectives de posibles situaciones que puedan poner en peligro la operación y el cumplimiento de la misión funcional de La Defensoría.
Es necesario proporcionar el ambiente adecuado para la conservación de medios magnéticos, equipos de telecomunicaciones, computadores, servidores, y elementos tecnológicos en general.

Se debe cumplir con las normas de seguridad aceptadas o recomendadas en materia de seguridad del Centros de Cómputo, entre las cuales se encuentran:

- El centro de cómputo debe estar provisto de piso y techo falso elaborados con materiales no combustibles.

- Las áreas deben tener un sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la prestación del servicio, el cual es de suma importancia para la operación correcta de los sistemas de información. El equipo debe contar con instrumentos capaces de registrar las condiciones de humedad y temperatura, las cuales deben ser supervisadas diariamente por los operadores o la persona que se designe para esta función.

- El centro de Cómputo debe tener una planta de generación de energía, y UPS que proporcionen tiempos de respaldo adecuados, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea o prolongada.

- Eliminar al máximo la permanencia de papelería y materiales que representen riesgo de propagación de fuego.

- Se debe contar con alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central con constante supervisión.

- En todos los centros de procesamiento, sin excepción, deberán existir detectores de calor y humo, instalados en forma adecuada y en número suficiente como para detectar el más mínimo indicio de incendio.

- Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.

- Se debe tener extintores de incendios debidamente probados, y con capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.

- Las salas de procesamiento de la información deberán estar ubicadas en pisos a una altura superior al nivel de la calle a fin de evitar inundaciones.

- Las cañerías de desagüe de dichas salas y ubicadas en el piso, deberán poseer válvulas de retención de líquidos en flujo inverso a fin de que no sirvan como bocas de inundación ante sobre-flujos.

- El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.

- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.

Controles de acceso físico

Todos los funcionarios, para ingresar a la Defensoría, estarán identificados con su carné que los acredita como funcionarios de la misma; a partir de ese momento lo portan permanentemente y en lugar visible.

Para ingresar a las instalaciones de la Entidad, todos los visitantes deben ser autorizados previamente por un funcionario y se les asigna una escarapela para identificarlos. Del ingreso queda un registro en el sistema de control de acceso.

Las puertas de acceso a las áreas de procesamiento, administración o almacenamiento de información confidencial o privada, permanecen cerradas en todo momento, y el ingreso a las mismas está limitado sólo al personal autorizado.

Las áreas de Tecnología de Información (TI) con acceso restringido, estarán protegidas con controles apropiados para asegurar que solo se permite el ingreso a personal autorizado.

Toda persona que ingresa a algún área restringida de la Entidad, lo hace previa autorización del responsable de la misma, y su compromiso explícito, mediante la firma de la minuta correspondiente, de cumplir los procedimientos de control establecidos.

Protección contra amenazas externas y ambientales

- La Defensoría mantendrá las condiciones físicas y ambientales óptimas recomendadas para centros de cómputo así como controles automáticos para prevenir incendios y aumentos de temperatura. (Inundación, humedad, monitoreo por el CCTV)

- La Entidad proporcionará el ambiente adecuado para conservación de medios magnéticos y equipos.

- La Defensoría grabará en video mediante el uso de un CCTV[3], las actividades en áreas públicas (dentro de los confines de la organización), puertas de acceso a áreas restringidas y zonas de manipulación de información confidencial o privada, con el fin de mantener un control de seguridad.

- La Entidad mantendrá en condiciones óptimas de limpieza, seguridad, mantenimiento y funcionalidad cada uno de los elementos que forman parte del centro de cómputo y de la cintoteca, de acuerdo con las recomendaciones que sobre cada uno provea el fabricante.

- Todos los usuarios de La Defensoría que utilizan estaciones de trabajo para la realización de su labor, deberán acoger como práctica permanente el bloqueo de la pantalla al ausentarse de su puesto, así como mantener en orden sus papeles de trabajo, siempre pensando en la confidencialidad de la información.

- Las estaciones de trabajo de los usuarios finales serán desactivadas automáticamente si superan un tiempo de inactividad determinado en cada caso según el nivel de riesgo que corresponda, siendo necesario digitar nuevamente la clave de acceso en el momento que requiera continuar con la conexión.

- La Defensoría mantiene convenios con fabricantes de hardware tales para el reciclaje de elementos tales como cartuchos de impresión, impresoras y dispositivos en general.

- Cuando un medio magnético de propiedad de La Defensoría termine su ciclo de vida, deberá ser destruido de acuerdo a las exigencias del Grupo de Sistemas. Al disponer de un disco duro utilizado, ya sea para su entrega, reutilización o puesta asignación, deberá pasar por un proceso adecuado de borrado determinado también por el Grupo de Sistemas.

Control de Condiciones de Humedad y Temperatura

Se debe contar con instrumentos capaces de registrar las condiciones de humedad y temperatura, las cuales deben ser supervisadas diariamente por los operadores o la persona que se designe para esta función con el fin que los equipos puedan cumplir con su función adecuadamente.

[3] Circuito Cerrado de Televisión

Las áreas deben tener un sistema de refrigeración por aire acondicionado. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la prestación del servicio, el cual es de suma importancia para la operación correcta de los sistemas de información y de los equipos presentes en las instalaciones de La Defensoría.

Borrado de Información

Se debe eliminar toda información residente en los equipos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando tecnologías para realizar sobre-escrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad. Este proceso puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impacto, fuerzas o condiciones extremas.

Seguridad del cableado

El centro de cableado es el punto de unión central para el cableado y el equipo de redes, en él se conectan dispositivos activos y pasivos de red. Los centros de cableados se conectan por enlaces físicos con los centros de datos para formar la red de datos de la Defensoría del Pueblo.

Se debe limitar el acceso de los centros de cableado a funcionarios del área de soporte e infraestructura dentro del grupo de sistemas de la Defensoría del Pueblo. El personal externo o contratado que ingrese a los centros de cableado debe estar acompañado por un funcionario responsable del grupo de sistemas.

Al interior de los centros de cableado no debe permanecer o almacenar en forma temporal ni permanente ningún material inflamable como cartón, papel madera etc. Está prohibido fumar y el almacenamiento y consumo de alimentos y bebidas.

Todos los cables instalados deben estar protegidos en todo su recorrido mediante el uso de canaletas y escalerillas portacables tapadas por techos falsos u otros mecanismos que los oculten por estética y seguridad.

Mantenimiento de los equipos

Los equipos deben recibir un mantenimiento preventivo y correctivo adecuado de acuerdo a las directrices estipuladas por los diferentes fabricantes, y su periodicidad también dependerá de lo recomendado por el fabricante. Debe mantenerse los contratos de mantenimiento de manera regular para garantizar que los equipos no sufran fallas por esa razón que atenten contra la disponibilidad e integridad de la información.

Ingreso y retiro de activos de Información

El retiro e ingreso de todo activo de información de propiedad de los funcionarios de la Entidad, utilizados para fines personales, debe ser autorizado por el Jefe de la Dependencia correspondiente mediante orden escrita. El personal de vigilancia de recepción verifica y registra, respectivamente, las características de identificación del activo de información.

El retiro e ingreso de todo activo de información de los visitantes que presten servicios a la Defensoría (Consultores, periodistas, otros), debe ser autorizado por el Jefe de la Dependencia correspondiente. El personal de vigilancia de recepción verifica o registra, respectivamente, las características de identificación del activo de información.

Seguridad de los equipos fuera de las instalaciones

Se debe suministrar una seguridad adecuada para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización. Los equipos que se retiren de las instalaciones de la Entidad deben:

- Disponer de tecnologías de cifrado para la información residente en el disco duro.
- Asegurarse con guaya de seguridad para estadías en hoteles y centros de convenciones.
- Tener establecida una contraseña en la BIOS del sistema.
- Portarse en un maletín que no sea de color negro y que no parezca de los típicamente usados por los ingenieros de soporte de computación para el transporte de sus computadores.
- Estar bajo mayor cuidado en los aeropuertos, restaurantes etc. El dueño no debe por ninguna razón dejar el equipo desatendido.
- Utilizar todas las recomendaciones definidas en las políticas de seguridad sobre contraseñas y controles de acceso lógico.

Administración de operaciones

Procedimientos operacionales y responsabilidades

En este numeral se definen las políticas para garantizar la correcta y segura operación de los servicios de procesamiento de información

Documentación de los procedimientos operativos

Es responsabilidad del Grupo de Sistemas, mantener debidamente actualizada toda la documentación referente a la plataforma tecnológica de la entidad.

Gestión del Cambio

Cualquier cambio a la plataforma tecnológica de La Defensoría (a excepción de las estaciones de trabajo) deberá ser completamente documentado y controlado por el Grupo de Sistemas.

Todos los cambios en el ambiente de producción deberán ceñirse a las regulaciones establecidas para la adecuada puesta en producción, por el Grupo de Sistemas.

Todo cambio en la Infraestructura de TI, debe ser realizado a través del proceso formal de administración de cambios de TI.

Los cambios deben claramente detallar las actividades previas, las actividades durante el cambio, las actividades posteriores al cambio y las actividades en caso de regreso del cambio (Rollback).

Los Administradores de los sistemas que originan el cambio son los responsables de presentar el cambio y coordinar todas las actividades para su ejecución.

Los cambios que se lleven a cabo deben ser evaluados y probados de forma integral y se debe contar con una participación de los administradores de los diferentes componentes de la solución.

Distribución de funciones

La Defensoría del Pueblo debe asignar funciones que permitan separar las actividades que realicen los funcionarios para reducir el riesgo sobre los activos de información por colusión.

Para cada sistema de información se debe establecer el rol de propietario de la aplicación. El propietario será quien deba asegurarse que se cumplan con los estándares de desarrollo, requerimientos funcionales, análisis de los riesgos y cumplimiento de pruebas adecuadas antes de la puesta en producción.

Las funciones y responsabilidades del personal de desarrollo deben estar separadas de las funciones del personal de soporte y administración de las aplicaciones.

Todo sistema debe soportar la definición de un usuario especial (superusuario) quien es el único que pueda modificar el esquema de seguridad, creación de usuarios e instalación de software de seguridad entre otros. Adicionalmente debe controlar que los programas y los datos no sean alterados fuera de línea. El administrador debe contar con procedimientos estándares que le permitan realizar labores asociadas al aseguramiento de la información.

Dentro del personal del grupo de sistemas debe existir un cintotecario, como único responsable de la administración de la cintoteca.

Se prohíbe que los programadores y analistas de sistemas tengan acceso al centro de cómputo.

El acceso físico al centro de datos está permitido únicamente para el personal autorizado por la dirección.

Separación de ambientes

Los ambientes donde están las aplicaciones y bases de datos de desarrollo, pruebas y producción deben ser físicamente independientes y tener diferenciación de privilegios de acuerdo al ambiente:

- Ambiente de desarrollo: Es el utilizado por los analistas de desarrollo y programadores para crear y modificar los programas de aplicación. El acceso a este ambiente debe estar restringido al grupo de desarrollo.

- Ambiente de Pruebas: Es el utilizado por el grupo de pruebas para ejecutar las pruebas a los programas modificados por el grupo de desarrollo. El acceso a este ambiente es de ejecución para el grupo de pruebas y desarrollo. El paso del ambiente de desarrollo a pruebas debe ser ejecutado por el Administrador del Sistema.

- Ambiente de Producción: Es el utilizado por los usuarios del sistema para procesar la información real de la función misional de la Defensoría. El grupo de desarrollo o pruebas no debe tener acceso a este ambiente, el acceso está determinado por las necesidades de la función misional.

Protección contra código malicioso y móvil

Los sistemas de información y equipos de cómputo de escritorio y móviles son vulnerables a códigos maliciosos como virus, gusanos, caballos troyanos, adware, spyware, hoax y bombas lógicas, por ello:

- Los usuarios no pueden instalar ni utilizar software sin la debida autorización del Grupo de Sistemas.

- La Defensoría contará permanentemente con las herramientas de protección a nivel de red y de PC, con un sistema efectivo contra código malicioso que será administrado bajo la responsabilidad del Grupo de Sistemas.

- Los usuarios deberán cumplir con las recomendaciones y mejores prácticas establecidas por La Entidad con respecto al uso del Antivirus.

- Es responsabilidad de cada funcionario o tercero, revisar que todos los medios magnéticos extraíbles sean chequeados con un antivirus provisto por la entidad antes de procesarlos en los computadores personales o servidores de la entidad.

- Es responsabilidad del funcionario designado el mantener en estado óptimo de funcionamiento (configuración, actualización, licenciamiento) las herramientas y procedimientos que permitan prevenir, detectar y corregir incidentes por código malicioso.

- El antivirus debe ser configurado desde la consola para que diariamente realice escaneo de detección de código malicioso y reportar a la consola de Antivirus.

Respaldo de la información

Todos los activos de información deben ser objeto de una copia de respaldo para proteger su información. Los responsables de los activos de información deben establecer los procedimientos de rutina para implementar la estrategia de respaldo más adecuada para cada activo, hacer copias de seguridad de los datos, probar sus tiempos de restauración e integridad.

Las actividades de gestión de copias de seguridad deben ser realizadas por el grupo de sistemas y se deben seguir las siguientes directrices:

- Definir el nivel necesario para la información de respaldo.

- Se debe hacer registros exactos y completos de las copias de respaldo y generar procedimientos documentados de restauración.

- El tipo del respaldo (por ejemplo completo, diferencial o integral) y la frecuencia de los respaldos, deben reflejar los requisitos de la Defensoría del Pueblo, los requisitos de seguridad de la información involucrada, la importancia de la operación continua de la organización y los criterios de retención de la información.

- Las copias de respaldo se deben proteger física y ambientalmente. Los controles aplicados a los medios en las instalaciones de la Defensoría del Pueblo se deben extender para cubrir el sitio en donde está el respaldo.

- Es conveniente probar con regularidad los medios de respaldo para garantizar que sean confiables para uso en emergencias.

- Los procedimientos de restauración se deben verificar y probar periódicamente para garantizar su eficacia y que se pueden completar dentro del tiempo designado en los procedimientos operativos para la recuperación. Los tiempos designados y los periodos de pruebas deben estar claramente especificados en la estrategia de respaldo acordada.

- Si de acuerdo a la clasificación de los activos de información descrito previamente en este documento, la información respaldada es clasificada como confidencial, los respaldos se deben proteger por medio de cifrado.

- Ningún tipo de información que se refiera a la misión funcional de La Defensoría puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo. Para estos casos, es responsabilidad de cada usuario replicar la información en las carpetas de archivos que residen en los servidores.

- Deben existir al menos dos copias de la información, una de las cuales deberá permanecer fuera de las instalaciones de la entidad, con excepción de aquellos archivos que provienen de entidades externas, o que, en razón de cambios en la tecnología, no puedan ser duplicados.

- Es responsabilidad del dueño de la información, definir los periodos de retención y la frecuencia de los Backups que garanticen la continuidad del negocio y la consulta histórica de su información.

- Es responsabilidad del Grupo de Sistemas el mantenimiento adecuado de las versiones de las aplicaciones en el medio de almacenamiento utilizado en su momento que le permita atender requerimientos legales o internos.

- Las solicitudes para entrega de información por parte del custodio externo deben ser tramitada con la debida autorización del responsable del Grupo de Sistemas.

- Diariamente los responsables del centro de cómputo verificarán la ejecución correcta del BACKUP, suministrará las cintas requeridas para cada trabajo de copia, controlaran la vida útil de cada cinta o medio y de las acciones necesarias para el procedimiento de limpieza de la unidad de grabación.

- El administrador de las bases de datos realizará pruebas mensuales de restauración de la información mediante la rotación de los medios y en un ambiente de pruebas adaptado para tal fin, con el objetivo de garantizar que las cintas se encuentran adecuadas para una eventual restauración.

- El Grupo de Sistemas debe mantener un inventario actualizado de las copias de respaldo.

- Los medios que vayan a ser eliminados deben ser destruidos para garantizar que no quede información remanente en los mismos.

- Es responsabilidad del Grupo de Sistemas garantizar a la entidad que se están recogiendo en forma adecuada los backups de información que garanticen la continuidad de los servicios de la plataforma tecnológica.

- Es responsabilidad de cada dependencia mantener depurada la información de las carpetas compartidas, como mejor práctica para la optimización de uso de los recursos que entrega la entidad a sus funcionarios.

Registros y Monitoreo

En este numeral se definen las políticas para detectar actividades de procesamiento de la información no autorizadas.

Registro de auditorias

Los servidores, equipos de comunicaciones, sistemas de información, herramientas y computadores personales, deben tener habilitada la opción de registro de auditorías.

El registro de eventos es una de las herramientas más importantes de la administración de la seguridad. El registro de eventos debe estar permanentemente activo en todas las plataformas y sistemas de información de la Defensoría. Se debe tener un equilibrio entre los eventos a registrar y el impacto en el desempeño de las plataformas en producción.
Responsables de la definición y la administración

El Oficial de Seguridad y el dueño de la información participan en la definición de los eventos a registrar de las diferentes plataformas.

El Oficial de Seguridad, revisa los archivos de registro de eventos de manera periódica y realiza informes de los eventos registrados.

Monitoreo del sistema

Los administradores de plataforma, administradores de red**,** revisan periódicamente los archivos de registros de eventos técnicos para establecer posibles fallas, problemas de capacidad y eventos de seguridad. De acuerdo a la categoría se deben tomar las medidas respectivas como son: solicitar soporte en caso de fallas, realizar un análisis de capacidad cuando hay problemas de desempeño o reportar al oficial de seguridad de la información cuando se presenten incidentes de seguridad.

Protección de la información de los registros

Los registros de auditoria deben ser almacenados en las librerías de backup y solo se debe permitir acceso a los administradores del sistema. Cualquier información que deba investigarse en los logs se realizará sobre una copia del archivo original de forma que garantice la integridad de la fuente original.

Registros del administrador y operador

Todos los sistemas de información, computación o comunicaciones de la Defensoría deben tener un registro de las actividades del operador que muestren los tiempos de inicio y terminación de los procesos, tiempos de inicio del sistema, cambios en la configuración del sistema, errores y acciones correctivas.

Los registros de las actividades del operador de todos los computadores de los sistemas de información de La Entidad deben ser revisados cada semana por el administrador del equipo y en caso de encontrar algún evento anormal, contactar inmediatamente al oficial de seguridad. Las actividades realizadas por estos administradores también deben estar sujetas a registro.

Registros de falla

Se deben registrar todas las fallas de las plataformas de cómputo y comunicaciones con el fin de hacer un seguimiento a los problemas presentados, reducir su incidencia, prevenir su recurrencia y evitar alteraciones a la continuidad de las operaciones de la Entidad. El administrador del sistema debe revisar los reportes de fallas identificadas en los registros de cada una de las plataformas de tecnología, en caso de encontrar un evento adverso y fuera de lo normal debe reportarlo inmediatamente al oficial de seguridad.

Se recomienda la implementación de la herramienta Syslog para garantizar una adecuada protección a los registros de auditoria, que reciba toda la información de los diferentes sistemas considerados como críticos. Es indispensable que los administradores de los respectivos sistemas ya sean de cómputo o de comunicaciones no estén en capacidad de modificar o eliminar esta información sin estar autorizados por el oficial de seguridad para

ello. Se recomienda utilizar algunas herramientas que ayude a realizar un análisis o síntesis de los eventos que se encuentran almacenados en estos registros con el fin de que esta actividad sea más efectiva y eficiente.

Gestión de la vulnerabilidad técnica

Esta política tiene como objetivo reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.

Control de vulnerabilidades técnicas

Para mantener el control sobre las vulnerabilidades técnicas se debe:

- Mantener un inventario actualizado de los componentes de los sistemas de información para identificar las vulnerabilidades técnicas que se presenten
- El grupo de sistemas es responsable de establecer un mecanismo por el cual sea informado de las vulnerabilidades existentes en sus Sistemas (Sistemas operativos, software base, software aplicativo, bases de datos, herramientas de colaboración, etc.).
- Definir una línea de tiempo para reaccionar ante la notificación de las vulnerabilidades técnicas potenciales
- Identificar los riesgos asociados y las acciones a tomar, determinando prioridades para los sistemas con alto riesgo; se deben mantener los controles relacionados con la gestión de cambios en Sistemas Operativos, Bases de datos, software para aplicaciones Web.
- Una vez se presente una vulnerabilidad para la cual exista un parche de seguridad que la elimina, El Grupo de sistemas debe realizar un análisis del impacto de la vulnerabilidad y decidir si se aplica o no el parche respectivo.
- El análisis debe estar debidamente documentado, en caso de tomarse la decisión de aplicar el parche o las medidas de control sugeridas por el fabricante, se debe argumentar esta decisión y debe estar aprobada por el responsable técnico.
- Si está disponible un parche, se debe probar y evaluar antes de su instalación. Si no hay parches disponibles se deben considerar otras medidas tales como: desactivar los servicios relacionados con la vulnerabilidad; aumentar el monitoreo para detectar o prevenir ataques; crear conciencia sobre la vulnerabilidad.
- Mantener registros de todos los procedimientos realizados
- Monitorear y evaluar periódicamente el proceso para asegurar su eficacia y eficiencia.

Gestión de la seguridad de las redes

En este numeral se definen las políticas para asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

Controles de las redes

El administrador de la red es responsable por aplicar los controles necesarios que garanticen la seguridad en la red y de los datos en tránsito. Debe velar que se apliquen al menos los siguientes controles:

- Toda conexión a la red debe contar con un mecanismo de autenticación que valide que el usuario es válido.

- Los usuarios de la red deben utilizar las herramientas de protección configuradas por el Grupo de sistemas, como son antivirus y parches de seguridad.

- El acceso a Internet es realizado únicamente por los medios provistos por la Entidad.

- Toda conexión con terceras partes debe cumplir con lo estipulado en la sección Seguridad en conexiones remotas.

- Las conexiones de acceso remoto deben cumplir con lo establecido en las políticas de seguridad móvil.

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

- Las conexiones con las redes públicas deben estar protegidas por un Firewall y los mecanismos de control, que posea las reglas apropiadas para filtrar el tráfico permitido entre las redes.

- Los usuarios de la red deben hacer uso razonable y con propósitos laborales de la red de comunicaciones.

- Las conexiones de red de área extendida (WAN), deben estar protegidas por encripción.

Seguridad de los servicios de red

Los responsables por los servicios de red de la Defensoría, deben controlar que los proveedores del servicio, internos o externos, cumplan con:

- 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

- La entidad tiene implementado controles de filtrado de contenido para evitar que los recursos de la entidad sean utilizados para: visitar páginas no autorizadas que contribuyan a la disminución de la productividad de los funcionarios, comprometer la seguridad de los activos de información de la Entidad y comprometer el buen nombre de la Entidad.

- Adelantar auditorias para verificar que se esté cumpliendo con la política de seguridad de la información

- Mantener un constante monitoreo sobre la red interna, implementando las herramientas que le permitan detectar, prevenir y recuperarse contra código malicioso encontrado en su plataforma tecnológica.

- Implementar las herramientas que permitan medir la calidad del servicio y monitorear los elementos activos de la red.

- Implementación de sistemas de alertas de fallas en los equipos activos, para activar las acciones correctivas.

- Medir los niveles de servicio a través de los KPI.

- Mensualmente se debe presentar un informe sobre la calidad y oportunidad de los servicios de red que incluya al menos:
  - Estado general del servicio
  - KPI de los servicios de red.
  - Incidentes y fallas presentadas, junto con los planes de acción.
  - Análisis de capacidad de la red y utilización.

- Hacer pruebas aleatorias de la validez de la información de los KPI reportados

Segregación de usuarios en redes

Las funciones de las operaciones de 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.

Intercambio de información

En este numeral se definen las políticas para mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.

Políticas y procedimientos para el intercambio de información

EL intercambio de información busca mantener la seguridad de la información que se traslada entre la Defensoría 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[4] 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.

[4] Una de las tecnologías ampliamente utilizadas para enviar información confidencial cuando se trata de medios públicos son las redes virtuales privadas o corrientemente conocidas como VPN (Virtual Private Network), las cuales permiten autenticar, y garantizar la confidencialidad y la integridad, usando técnicas de cifrado como 3DES o AES y de integridad MD5 y SHA-1.

Para el transporte de información fuera de las instalaciones de la Defensoría, 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 este 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
- 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.

La información confidencial que sea transportada a través del sistema de correo electrónico debe utilizar un sistema de cifrado de al menos 128 bits para la clave de cifrado. Entre los algoritmos disponibles para ser usados están los sistemas de llave pública y llave privada, y en casos de mayor seguridad se puede implementar opcionalmente sistemas PKI (public key infrastructure). Se debe considerar que las comunicaciones relacionadas con el correo electrónico por defecto no estarán cifradas.

Cuando se requiera conectar la red de la Defensoría con otra entidad, o sistemas de información de la Entidad con otros sistemas de información, esta solicitud debe ser estudiada por el oficial o grupo de seguridad, incluyendo un análisis de los posibles riesgos asociados con esta interconexión y luego escalarse al comité de seguridad para su respectiva aprobación, considerando siempre que haya una necesidad que apoye la misión funcional de la Defensoría.

Acuerdos para el intercambio

Cuando se requiera, la Defensoría debe tramitar acuerdos de intercambio de información con otras entidades del Gobierno y terceros, los cuales deben considerar que el intercambio se realice de acuerdo con lo establecido en el Manual de Gobierno en Línea y deben incluirse los respectivos acuerdos de confidencialidad.

Medios físicos en tránsito

La información que físicamente debe ser movilizada, debe estar debidamente identificada, marcada y clasificada, conforme a lo establecido.

El transito físico de información debe realizarse con las medidas de protección que garanticen que no van a ser extraviadas, duplicadas o destruidas.

Correo electrónico

Se entiende por cuenta de correo electrónico la asignación por parte de la Defensoría del Pueblo de:

- Una dirección electrónica con la forma usuario@defensoria.org.co o usuario@defensoria.gov.co.

- Un buzón (espacio en disco) para almacenar los mensajes.

- La posibilidad de enviar y recibir mensajes dentro de la Defensoría del Pueblo y hacia Internet utilizando la dirección electrónica asignada.

Con el fin de garantizar que la identificación del usuario en la dirección de correo sea única, se seguirá la misma regla de construcción establecida para utilizar los otros servicios y aplicaciones de la Defensoría del Pueblo. Por tanto, la identificación de usuario se construirá con la inicial del nombre del usuario y las letras del primer apellido (sin tildes ni signos propios de algunos idiomas). En caso de presentarse coincidencias en la identificación de dos usuarios se resolverá de acuerdo con el orden de procesamiento: el primer usuario recibirá la identificación antes mencionada, el segundo será alterado recurriendo a la primera y siguientes letras del segundo nombre. Ejemplo: supongamos que hay dos usuarios, uno se llama José Eduardo Ramírez Pardo y otro se llama Jorge Enrique Ramírez Puerto, el primero recibiría la identificación de usuario jramirez@defensoría.gov.co y el segundo sería jeramirez@defensoria.gov.co. Para las personas que contaban con direcciones de correo antiguas definidas desde hace varios años, su identificador de usuario antiguo no tendrá validez y será construido uno nuevo con la regla enunciada antes. La creación de alias de una cuenta de correo electrónico podrá ser solicitada por el usuario cumplimentando un formulario.

A la hora de solicitar la cuenta de correo, el usuario debe facilitar información veraz, exacta y completa sobre su identidad, en relación con los datos que se solicitan en el formulario correspondiente, así como a mantener actualizada dicha información. Si el usuario facilitara cualquier dato falso, inexacto o incompleto, o si se tuviesen motivos suficientes para sospechar que dicha información fuera falsa, inexacta o incompleta, el servicio de correo electrónico tendrá derecho a cancelar o bloquear la cuenta de correo

El usuario recibirá los datos relativos a su cuenta y contraseña por correo, en un plazo aproximado de 5 días laborables desde la recepción de la solicitud. El Usuario podrá cambiar la contraseña de acceso en cualquier momento, por medio de un interfaz web disponible en nuestro servicio.

En general, se facilita una única cuenta de correo por persona. En el caso particular de personas responsables de alguna dependencia de la Defensoría (Directores Nacionales, Defensores Delegados, Defensores del Pueblo Regionales y Seccionales, etc.) se ofrece la posibilidad de una segunda cuenta vinculada a dicha dependencia.

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 empleado 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, se prohíbe:

- 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.

Están autorizados para el envío de mensajes electrónicos masivos, el Defensor del Pueblo, el Secretario General, los funcionarios del Nivel Directivo, y los administradores de correo electrónico y de red del Grupo de Sistemas. Los demás funcionarios deberán solicitar la autorización respectiva a la Oficina de Comunicaciones e Imagen Institucional.

Administración y seguimiento del sistema de correo electrónico.

El Grupo de Sistemas es el encargado de ejercer la administración del sistema de correo electrónico, lo cual incluye disponer los recursos para la entrega de mensajes internos y de o hacia Internet o Intranet., considerando, además, los siguientes aspectos:

- Los recipientes de correo serán creados y sobre ellos se darán permisos a los funcionarios vinculados a la Entidad, previa aprobación del Grupo de Sistemas de la solicitud enviada por el Jefe inmediato del funcionario, o por él mismo, en caso de que sea Directivo. Los permisos para crear Fólderes Públicos se asignarán siguiendo el mismo procedimiento.

- Se asignarán dos clases de buzones: Individuales y Globales. Los buzones individuales son manejados por un solo funcionario, mientras que los globales por varios funcionarios.

- Los buzones individuales son de carácter personal e intransferible. El usuario es totalmente responsable de todas las actividades realizadas con dicho buzón. Los buzones globales serán manejados por varios funcionarios quienes serán responsables mancomunadamente de las actividades realizadas con ellos.

- Es deber de los funcionarios que manejan los buzones globales colocar el nombre del remitente en los mensajes enviados.

- Las personas que administran este 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 Cómputo, podrán implicar el movimiento temporal y/o definitivo de sus correos, más no de su edición. Solo se hará monitoreo cuando haya la autorización debida.

- El tamaño máximo asignado del buzón es de 50 GB

- Se suspenderá por un mes el servicio de correo electrónico a los funcionarios que se les compruebe que están realizando uso indebido de él y definitivamente en caso de reincidir.

Sistemas de información de la misión funcional

La Defensoría define políticas y procedimientos para proteger la información de los sistemas del negocio, incluyendo las siguientes:

- Realizar revisiones de vulnerabilidades a los sistemas de apoyo que comporten información con los sistemas misionales.

- Identificar vulnerabilidades en los sistemas de comunicación del negocio tales como: grabación de llamadas telefónicas, confidencialidad de la las conversaciones telefónicas, almacenamiento de fax, distribución de correspondencia, etc.

- Identificar los funcionarios o terceras partes que pueden tener acceso a información del negocio y establecer los sitios desde donde se puede tener acceso, tanto de forma física como lógica.

Transacciones en línea

Las transacciones en línea deben considerar lo siguiente:

- Utilización de firmas digitales por parte de cada una de participante de las transacciones
- Garantizar la integridad y confidencialidad de la transacción a través de:
  - Validación de las credenciales de ambas partes.
  - La información se mantiene confidencial
  - Utilización de encripción.
  - Los detalles de la transacción son almacenados con la protección para evitar acceso público.

Adquisición, desarrollo y mantenimiento de sistemas de información.

Requisitos de seguridad de los sistemas de información

Esta política tiene como objetivo garantizar que la seguridad es parte integral de los sistemas de información.

Análisis y especificaciones de los requisitos de seguridad.

En la fase de inicio del desarrollo del sistema de información así como en el proceso de evaluación de paquetes, se especifican los requerimientos funcionales y los requerimientos de seguridad y control. Para determinar y avalar dichos requerimientos se cuenta con la participación de los propietarios de los activos de Información, el Oficial de seguridad, el Grupo de Sistemas y terceras partes cuando sea necesario.

Procesamiento correcto de las aplicaciones

Esta política tiene como objetivo evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.

Validación de los datos de entrada

Se deben incorporar los siguientes controles para asegurar la validez de los datos que se ingresan al sistema tales como:

- Validación a nivel individual: tipo de datos, datos obligatorios, longitud del campo, rangos de razonabilidad, conjuntos de valores válidos, despliegue protegido de valores.
- Validación con mayor grado de inteligencia en la captura: Validar 2 o más campos de una transacción, validar contra tablas, utilizar datos de transacciones previamente generadas,

razonabilidad de fechas contra calendario oficial, incluir datos de tipo referencial del documento fuente.

- Validación generada por las relaciones del modelo de datos: validación de llaves únicas, llaves foráneas, creación o eliminación de padres e hijos.
- Ejecución de procedimientos automáticos de respuesta ante errores de validación.
- Revisión periódica del contenido de los campos para confirmar su validez e integridad.
- Inspección de documentos de entrada impresos para determinar cambios no autorizados.
- Registrar las actividades de ingreso de datos.
- Definición de responsabilidades para todo el personal que participa en el proceso de entrada de datos.
- Las transacciones de creación, modificación y eliminación deben generar pistas de auditoria que contengan el código del usuario que lo realizó, la transacción utilizada, fecha de la transacción, tipo de transacción (creación, modificación) y campos afectados con los valores anteriores.

Control de procesamiento interno

Se deben implementar en los casos en los que apliquen, los siguientes controles para asegurar la integridad de los datos en el procesamiento tales como:

- Mecanismos automáticos que validen la ejecución lógica del procesamiento.
- Validar que los procesos implícitos en el software de aplicación se ajusten a los procedimientos aprobados.
- Protección contra ataques empleando desbordamiento
- Definición del calendario y responsables del envío o recepción de datos, para ejecutar los procesos de actualización periódicos o de corte.
- Procedimientos automatizados para realizar procesos de conciliación de los datos recibidos y procesados desde cada una de las fuentes de ingreso.
- Las transacciones de creación y modificación deben generar pistas de auditoria que contengan el código del usuario lo realizo, la transacción utilizada, fecha de la transacción, tipo de transacción (creación, modificación y eliminación) y campos afectados con los valores anteriores.
- Facilidades de manejo de errores de procesamiento (procedimientos estándar para cada módulo, mensajes en españoles claros y soportados en documentación técnica adecuada. El sistema informa al usuario la consecuencia de aquellas acciones de modificación o eliminación ya sea de archivos o registros y permite cancelar la acción hasta último momento.)
- Controles de balance para verificar los totales de inicio y cierre...
- Generación automática de reportes de inconsistencias presentadas durante el procesamiento.

- Procedimientos para reportar y reprocesar transacciones que se detectaron erradas durante la ejecución de los procesos.

Integridad del mensaje

Se debe realizar una evaluación de riesgos de seguridad para determinar si se requiere integridad del mensaje y para identificar el método más apropiado de implementación.

Validación de los datos de salida

Se deben implementar los siguientes controles, siempre que apliquen, para validar los datos de salida del sistema y asegurar el correcto procesamiento tales como:

- Facilidades para generar en forma automática o manual los reportes que genera el sistema
- Generación automática de los reportes de inconsistencias presentadas durante el procesamiento.
- Verificaciones de la veracidad para probar si los datos de salida son razonables
- Cuentas de control de conciliación para asegurar el procesamiento de todos los datos
- Procedimientos para manejar los resultados de las pruebas de validación de las salidas
- Marcación de la información para identificar los destinatarios de la misma y poder aplicar los controles respectivos a la información privada y confidencial.
- Definición de las responsabilidades de todo el personal que participa en el proceso de las salidas de datos
- Procedimientos de utilización/destino de los informes generados por el sistema en el nivel adecuado de la Entidad.
- Registro de las actividades del proceso de validación de las salidas de datos

Seguridad de los archivos del sistema

Esta política tiene como objetivo proteger la confidencialidad e integridad de la información.

Control de software operativo

Cuando se cambian los sistemas operativos, las aplicaciones críticas para la función misional se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la entidad.

Cambios en Paquetes de Software.

Los paquetes de software que adquiera la Defensoría se utilizarán según las especificaciones del proveedor. En caso de ser necesario realizar cambios ya sea en los parámetros de configuración de los paquetes o en el código fuente, es necesario tener en cuenta los siguientes aspectos:

- Verificar el cumplimiento de las condiciones acordadas en el contrato de adquisición

- Hacer un análisis y evaluación de riesgos de manera que incluya el riesgo de comprometer los controles operacionales y la seguridad incorporada en el paquete de software.

- El impacto para la Entidad si se hace responsable de mantenimientos futuros o se establece un programa estándar de actualizaciones con el proveedor.

- Conservar la versión original del software y mantener un control de versiones del software.

Implementar un procedimiento para gestión de actualizaciones del software que incluya las pruebas a las nuevas versiones antes de su instalación en ambiente productivo.

Protección de los datos de pruebas del sistema y código fuente

El objetivo de este control es gestionar la protección de datos de prueba y código fuente, que utilizan las aplicaciones.

Lo siguientes son los agentes involucrados:

- Usuarios del área funcional: Realizan las pruebas de los sistemas de información en el ambiente de pruebas bajo la coordinación del administrador funcional y administrador técnico.

- Administrador Técnico: Solicita autorización para restaurar datos utilizados para pruebas durante una vigencia determinada. Mantiene el control de versiones de los programas fuentes.

- Responsable del grupo desarrollo: Evalúa y autoriza la utilización de datos de prueba y controla la vigencia de los mismos. Mantiene custodia permanente sobre los programas fuente de los sistemas de información.

Los datos de prueba deben ser gestionados de acuerdo con lo siguiente:

Ambiente de Desarrollo (Líderes de proyecto y desarrolladores):

1. Cada vez que sea necesaria la utilización de datos para pruebas, será gestionada a través de una orden de proceso debidamente autorizada por el responsable del Grupo de Sistemas.

2. Los programas fuente deben estar protegidos en el ambiente de desarrollo de forma que solo el administrador técnico asignado tenga acceso.

3. Toda solicitud de restauración de datos para pruebas (orden de proceso), tendrá un solicitante que en todos los casos debe ser un funcionario de la Entidad. El solicitante debe establecer la vigencia de los datos y será el responsable del borrado de los mismos tan pronto expira la vigencia. Si se requiere aplazar la vigencia de los datos de prueba deberá tramitar una nueva orden de proceso con todos los requisitos establecidos.

4. El control de las vigencias de los datos de prueba se hará a través de la herramienta que posea la entidad, para lo cual se creará una categoría denominada "Datos de Prueba" que poseerá como mínimo los siguientes datos:

    - Nombre de la aplicación
    - Nombre del archivo o librería

- Fecha a la que corresponden los datos
- Vigencia de los datos
- Nombre del responsable de los datos

5. Los ambientes de desarrollo y producción se deben mantener independientes y no se permite la transferencia de datos o código fuente del ambiente de desarrollo al de producción. Por otra parte, ningún usuario de desarrollo puede tener cuentas activas en el ambiente de producción.

6. Es responsabilidad del responsable del grupo de Desarrollo, revisar los registros en la herramienta, para hacer el seguimiento requerido. El Oficial de Seguridad debe tener acceso a la categoría de Datos de Prueba para efectos de verificación de cumplimiento de los controles de seguridad.

7. Para todos los efectos, para cualquier dependencia que posea en forma definitiva o temporal un ambiente de desarrollo de software, sus usuarios se consideran desarrolladores y les aplica las medidas de control de que se ocupa esta política.

Ambiente de Prueba (Usuarios Finales):

1. Se considera que los datos almacenados en este ambiente, son propiedad del mismo usuario que realiza las pruebas, y por tanto no existen medidas de control distintas que el cumplimiento natural de la confidencialidad que le compete a todos los funcionarios de la Entidad. Dentro de éste ambiente, los Desarrolladores tendrán acceso a los datos únicamente en modo de consulta.

2. Los ambientes de prueba y producción se deben mantener independientes y no se permite la transferencia de datos del ambiente de pruebas al de producción. Por otra parte, los usuarios definidos en este ambiente no deben utilizar la misma contraseña utilizada en el ambiente de producción.

Los Programas Fuentes deben ser gestionados de acuerdo con lo siguiente:

1. Dentro del ambiente de desarrollo solo está permitido que permanezcan los códigos fuente que están siendo objeto de modificación. Es responsabilidad del Líder de Proyecto, que una vez las modificaciones han sido trasladadas al ambiente de Producción, todos los fuentes sean removidos del ambiente de desarrollo.

2. Los ambientes de desarrollo y producción se deben mantener independientes y no se permite la transferencia de código fuente del ambiente de desarrollo al de producción. Por otra parte, ningún usuario de desarrollo puede tener cuentas activas en el ambiente de producción.

3. Los programas fuente deben estar almacenados en medios magnéticos destinados para tal propósito bajo la custodia del responsable del Grupo de Sistemas (una copia) y otra en un sitio externo con los debidos controles de custodia.

4. Los programas fuente deben ser catalogados una vez se ha aprobado su paso a producción, de forma que se identifique claramente la última versión vigente. Se debe mantener una copia de las versiones anteriores debidamente identificada.

5. Los programas fuente deben tener dentro del código una descripción de los cambios que son ejecutados identificando el responsable y fecha de modificación.

6. El administrador técnico de los aplicativos es responsable de mantener el control de versiones de los programas fuentes y de que la documentación de los sistemas de información se encuentre actualizada y debidamente custodiada.

Seguridad en los procesos de desarrollo y soporte

Esta política tiene como objetivo mantener la seguridad del software y de la información del sistema de aplicaciones.

Procedimientos de control de cambios

Este control tiene por objetivo definir los criterios y ambientes bajo los cuales deben trabajar quienes crean y hacen mantenimiento del software.

Los roles que intervienen son:

- Desarrollador autorizado: Descarga los programas fuente, y efectúa los cambios solicitados.
- Grupo de Sistemas: Autoriza mediante el responsable de desarrollo, los cambios sobre los programas fuente según los requerimientos aprobados.
- Oficial de seguridad: Verifica el cumplimiento del procedimiento de control de cambios de software.

Actividades:

Cada vez que sea necesario hacer cambios en los archivos fuente por parte de los desarrolladores se deben seguir los siguientes pasos explicados a continuación:

- Una vez evaluado que el mantenimiento se va a llevar a cabo, el responsable para el manejo de la herramienta de control de versiones respectiva, crea la solicitud de cambio, si el sistema lo requiere.
- El desarrollador autorizado debe ingresar al sistema de control de versiones y descargar los programas fuente que requiere para atender el requerimiento.
- Solo un desarrollador al tiempo puede tener los archivos fuentes y la persona que lo tenga es la responsable por la confidencialidad de esa información. Si el archivo fuente esta tomado deberá coordinar con su jefe de área para definir el orden en debe ser atendido el requerimiento.
- Al terminar las modificaciones, el desarrollador libera la versión para las pruebas de usuario y congela el programa fuente.
- Si las pruebas de usuario determinan la necesidad de hacer nuevos cambios, el programa fuente será puesto a disposición del desarrollador para dichos cambios. Estos dos pasos se repetirán las veces que sea necesario hasta obtener la aprobación del cambio por parte del usuario.
- Una vez obtenido el visto bueno por parte del usuario y se genera la orden de proceso para paso a producción los fuentes son actualizado en el repositorio de fuentes y el objeto será reemplazado en el ambiente de producción.

Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

Cuando se cambian los sistemas operativos, las aplicaciones críticas para la función misional se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la entidad.

Desarrollo de aplicaciones Web.

Para construir código seguro en el desarrollo interno o contratado de aplicaciones Web considerar las siguientes prácticas:

- Utilizar personal idóneo para el desarrollo de la aplicación
- En código privilegiado utilizar variables estáticas y finales y colocar el método que alberga el código privilegiado en una clase que pertenezca a un paquete restringido. Definir además, el contexto en el cual funcionará la aplicación utilizando herramientas como policytol (java), Caspol (.net) y demás.
- Para intercambio de información, los objetos que manejan información sensible deben ser inmutables. Se debe declarar el parámetro que contiene la información sensible como private transient y utilizar los métodos propios del lenguaje encargados de realizar el proceso de serialización y deserialización.
- Para envío de XML se deben cifrar los datos contenidos en los archivos XML. Si el servicio Web es abierto a consumo masivo se debe verificar la estructura general del XML recibido por tags inválidos.
- Para proteger contra inyección LDAP se debe validar toda la información entrante y saliente y utilizar listas blancas de validación. Así mismo, purgar la información entrante de caracteres potencialmente peligrosos. Adicionalmente, se deben implementar controles de acceso sobre los datos en el directorio LDAP, configurar permisos sobre los objetos, determinar cuáles objectclass utiliza la aplicación y si el usuario tiene permiso para modificarlos, validar la longitud de la información que entra a la aplicación contra la longitud máxima para el campo. Se debe centralizar toda la validación en el servidor que aloja la aplicación.
- Para proteger contra Cross Site Scripting se debe validar toda la información entrante y saliente; utilizar listas blancas de validación, purgar la información entrante con caracteres peligrosos; utilizar el tag <pre> </pre> de html para mostrar código tal y como fue escrito, se debe capacitar al usuario de la aplicación para que solamente ingrese a la aplicación digitando manualmente su ubicación no a través de links. Utilizar mensajes/pantallas genéricas para avisar sobre errores al momento de ejecutar una acción. No retornar al cliente la información mal ingresada (feedback). Considerar las vulnerabilidades innatas de los navegadores.
- Para proteger contra inyección SQL se debe validar toda la información entrante y saliente; utilizar listas blancas de validación, purgar la información entrante de caracteres peligrosos; validar la longitud de la información de entrada, utilizar la opción de "sentencia precompilada / sentencia parametrizable" que ofrece el lenguaje utilizado; encapsular en procedimientos almacenados (Stored Procedures) al interior de la base de datos, reglas para ciertas acciones como añadir, eliminar, actualizar; eliminar los procedimientos almacenados que no se utilicen; Utilizar mensajes/pantallas genéricas para avisar sobre errores al ejecutar una acción: no retornar al cliente la información mal ingresada.
- Para proteger contra buffer overflow además de aplicar controles en entrada y salida mencionadas anteriormente, se debe evitar el uso de librerías que no provean un

mecanismo de control de ingreso de información; centralizar toda la validación en el servidor que aloja la aplicación; conocer el sistema operativo sobre el cual se ejecutará la aplicación para aumentar la seguridad de la aplicación.

Fuga de información

Para limitar el riesgo de fuga de información se deben considerar los siguientes aspectos:

- La información de salida debe contar con la marcación, clasificación de información y destinatarios definidos y solo estos pueden tener acceso a la información.
- Explorar los medios y comunicaciones de salida para determinar la información oculta.
- Verificar el comportamiento de las comunicaciones y del sistema de modulación y enmascaramiento para reducir la probabilidad de que un tercero pueda deducir información a partir de tal comportamiento.
- Utilizar sistemas y software suficientemente probados
- Monitorear periódicamente las actividades del personal clave de sistemas siempre que esté conforme a la normatividad vigente de la Defensoría.
- Monitorear periódicamente el uso de los recursos en los sistemas de información.

Desarrollo de software contratado externamente

El desarrollo del software contratado con terceros, debe ser verificado y monitoreado por el Grupo de Sistemas cuyos funcionarios siguen las siguientes medidas:

- Definir acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual.
- Incluir contractualmente las pólizas de cumplimiento y calidad del trabajo realizado.
- Incluir derechos contractuales de auditar la calidad y exactitud del trabajo realizado.
- Establecer convenios de fideicomiso en caso de fallas de la tercera parte
- Definir requisitos contractuales sobre la calidad y la funcionalidad de la seguridad del código.
- Los terceros deben cumplir con las políticas de seguridad de la información y deben aplicar el presente documento.
- Realizar pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

Planificación y aceptación del sistema

En este numeral se definen las políticas para minimizar el riesgo de fallas de los sistemas.

Gestión de la capacidad

La Defensoría debe revisar periódicamente la capacidad y el desempeño de los componentes tecnológicos.

Todos los componentes críticos deben ser revisados periódicamente, teniendo en cuenta como mínimo los siguientes factores de monitoreo:

- Utilización de procesador (es)
- Capacidad en Discos Duros
- Capacidad en Memoria RAM
- Búsqueda de errores en el System Log syslog o del Event Viewer
- Sistemas de Gestión SNMP (Opcional)
- Rendimiento o velocidad en la conectividad (Throughput)
- Desempeño de I/O

Esta información debe ser registrada, por cada uno de los encargados del componente tecnológico, en la bitácora.

Aceptación del sistema

Los cambios, actualizaciones, nuevas versiones o nuevo desarrollo de sistemas de Información deben cumplir con un proceso formal y metodológico de aceptación por parte del responsable del desarrollo, considerando como mínimo lo siguiente:

- Aceptación formal de los cambios por parte de los administradores técnico y funcional del sistema de Información o del supervisor cuando se trate de nuevo desarrollo.
- Verificación de los niveles de desempeño de los servidores.
- Documentación de los cambios o actualizaciones
- Análisis de riesgos y vulnerabilidades.
- Procedimientos para reinicio de los servicios.
- Entrenamiento en la operación del cambio
- Consideración de los cambios en el plan de contingencias

Gestión de la prestación del servicio por terceras partes

En este numeral se definen las políticas para implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes.

Prestación del servicio

La Defensoría, mediante la figura de interventoría o supervisión, exige y vigila que los controles de seguridad, las definiciones del servicio y sus niveles de prestación incluidos en los contratos o convenios suscritos con terceras partes, sean implementados, mantenidos y operados por éstas.

Los servicios prestados por terceras partes deben realizarse de una forma controlada, segura y organizada definida a través de Acuerdos de niveles de servicio ANS, que de forma clara determinen:

- 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.

Monitoreo y revisión de los servicios por terceras partes

Los supervisores o interventores de contratos como responsables de la Defensoría por la prestación de servicios por parte de terceros, deben controlar que los mismos cumplan con:

- Las terceras partes están obligadas a medir los niveles de servicio a través de los KPI y presentarlos con la periodicidad acordada en el contrato.

- Mensualmente o con la periodicidad especificada en el ANS, se debe verificar que los KPI están ajustados a los niveles de servicio.

- Mensualmente se debe verificar la validez de la información de lo KPI suministradas por el tercero.

Gestión de los cambios en los servicios por terceras partes

Los cambios en la infraestructura de TI generados por terceras partes, deben realizarse cumpliendo con lo establecido en el numeral Gestión del cambio.

Es necesario que el interventor o supervisor de contrato realice una nueva evaluación de los riesgos de acuerdo a lo establecido por la Entidad.

Gestión de los incidentes de la seguridad de la información

Reporte sobre los eventos y las debilidades de la seguridad de la información

Esta política tiene como objetivo asegurar que los eventos y las debilidades de la seguridad de la información asociados con los activos de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente y que se aplica un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información.

Responsabilidades y procedimientos.

Responsabilidades

- **Funcionario**: Reporta el evento o incidente de seguridad siguiendo el procedimiento establecido para ello.

- **Mesa de ayuda**: Recibe el reporte, en el cual se expone el evento o incidente de seguridad que ocurrió o está ocurriendo en un activo de información, diligencia el formato establecido lo identifica y clasifica e inicia el trámite de atención directa o escalamiento pertinente.

- **Nota:** Se debe promover la motivación de los funcionarios para que reporten oportunamente y sin temor los eventos o incidentes de seguridad, siguiendo el procedimiento definido para ello.

- **Responsable del Grupo de Sistemas:** Recibe de la Mesa de Ayuda el formato con el reporte del incidente de seguridad, lo valora y activa la solución pertinente e informa de manera detallada al oficial de seguridad.

- **Oficial de seguridad**: Registra el incidente de seguridad en la bitácora dispuesta para tal fin. Analiza la solución para determinar si es suficiente, colabora en la resolución de los problemas y propone la implementación de medidas preventivas y correctivas. Si se requiere, lleva al Comité de Seguridad y al Comité Institucional de Informática, recomendaciones para la toma de decisiones estratégicas.

- **Comité de seguridad**: Decide la conveniencia de las soluciones estratégicas técnicas y las propone al CII.

- **Comité Institucional de Informática**: Decide la adopción de la solución propuesta por el Comité de seguridad.

- **Administrador técnico**: Formula y mejora el procedimiento detallado e implanta la solución al incidente de seguridad.

Políticas

- El Oficial de Seguridad debe tener permisos de acceso a la herramienta de registro para el capítulo de incidentes de seguridad, con el fin de garantizar la continua supervisión y seguimiento de las categorías allí registradas.

- De manera particular, y con el fin de que los incidentes de acceso físico también sean registrados en la herramienta que la entidad posee para soporte, se debe conceder acceso a la misma al responsable de la seguridad física de la Entidad.

- Existirán casos en los cuales un evento operacional reportado a mesa de ayuda se convierta en un incidente de seguridad identificado por el funcionario que atiende ese caso. En esta circunstancia se traslada el evento reportado, a la categoría denominada Incidentes de Seguridad de la información.

- Mesa de ayuda tendrá dentro de la herramienta disponible para la atención a usuarios, una categoría denominada Incidentes de Seguridad Informática, con subcategorías como las siguientes: Incidentes por virus, incidentes de acceso lógico, incidentes de acceso físico y ataques a la red de datos y recursos tecnológicos. Bajo esta clasificación registrará los incidentes reportados por los usuarios y documentará las acciones correctivas sobre los mismos.

La Administración de incidentes de Seguridad contempla las siguientes actividades:

- Registro y clasificación de los incidentes bajo la categoría Incidentes de seguridad
- Determinar y ejecutar el plan de acción para eliminar el incidente
- En caso de que la acción no haya sido exitosa, escalar el problema
- Realizar el diagnóstico de los efectos causados por el incidente
- Documentar el caso indicando las acciones que deban ser ejecutadas en los componentes y por los usuarios afectados
- Aprender de la situación ocurrida

Los diferentes mecanismos de reporte de incidentes a mesa de ayuda que la Entidad mantiene disponibles son:

- Correo electrónico
- Atención telefónica
- Notificación Verbal
- Notificación escrita

Actividades en la administración de los incidentes de seguridad

Incidente por virus

Para el propósito de este documento, la definición de un incidente de virus corresponde a una situación en particular en la cual ha sido infectado un servidor de archivos o una estación de trabajo. Si el virus llegara a reaparecer después de ser removido, debe ser considerado como un nuevo incidente de seguridad de la información.

Por otro lado, archivos infectados adjuntos al correo electrónico entrante no son considerados como incidentes de seguridad relacionados con virus, debido a que estos no han entrado dentro del perímetro de la red de datos de la entidad. El usuario que por alguna razón reciba un correo de origen desconocido o con datos adjuntos, deberá eliminarlo inmediatamente sin abrirlo.

Todos los usuarios de la red de datos de la Defensoría tienen la responsabilidad de reportar inmediatamente los incidentes de virus a mesa de ayuda para que sean atendidos por el personal de soporte y poder así minimizar el riesgo de propagación.

A continuación procedemos a describir ejemplos de situaciones que pudieran indicar la presencia de un código malicioso o virus:

- Lentitud inusual para realizar ciertas actividades en un equipo de cómputo. En este punto se debe tratar de comparar con el tiempo de respuesta de otros funcionarios o entrar en un proceso de reporte de incidente de seguridad.
- El sistema operativo se empieza a comportar de manera diferente y extraña. Por ejemplo, el explorador de Windows no abre, los documentos de Office cambian de icono, de tamaño o de fuente en forma inexplicable, o simplemente no se pueden abrir cierto tipo de archivos.

Un incidente de virus infeccioso significativo está definido como la aparición de cinco (5) o más situaciones de virus en un periodo no mayor a un día, o la aparición repetitiva del mismo evento durante una semana, manifestada en cualquier área interna o externa de la Entidad.

El reporte de esta situación se hará con el Grupo de Sistemas y a través de mesa de ayuda y será informado en forma inmediata el Oficial de Seguridad, quien con base en los componentes amenazados, identificará en el mapa de riesgos la criticidad de la situación y procederá a determinar las acciones correctivas necesarias, que podrían inclusive llegar a la desconexión parcial o total de la red mientras se controla la situación o se activa un plan de contingencias.

La documentación de este tipo de incidentes debe contener como mínimo la siguiente información:

- El nombre del virus
- Descripción de los síntomas
- Fecha de origen y periodo en el cual se ha venido presentando el incidente.
- Acción local tomada
- Estado del incidente

Si a juicio del Oficial de Seguridad se requiere desconectar la red de datos de la Entidad, se debe reportar la situación al Comité de Seguridad, y actuar de acuerdo con su autorización.

Por su parte, el Grupo de Sistemas es responsable por generar los mecanismos de erradicación del virus a nivel de toda la Entidad y también debe mantener completamente informado al Oficial de Seguridad de la información hasta que esté solucionado el problema.

Incidentes de acceso lógico

Un incidente de acceso lógico está definido como un evento en que se hace uso de permisos, recursos, servicios, sistemas de información de manera no autorizada con un posible impacto para el correcto funcionamiento de la Defensoría.

A continuación se describen situaciones típicas que identifican de forma sencilla este tipo de eventos:

- "La contraseña ha sido bloqueada de manera imprevista y sin autorización"
- "Alguien utilizó mi estación de trabajo sin mi consentimiento"
- "Creo que alguien pudiera conocer mi contraseña"
- "Tengo evidencia de que alguien está enviando correo electrónicos a mi nombre"

Cualquiera de estas situaciones obliga al usuario final a hacer el reporte a mesa de ayuda donde será clasificado el caso como un incidente de seguridad de acceso lógico.

El Grupo de Sistemas es responsable de atender y dar respuesta a los incidentes de acceso lógico reportados por cualquier usuario de la Entidad.

Incidentes de acceso físico

Un Incidente de acceso físico está definido como todo evento que pueda afectar los activos físicos de la Defensoría, y pueda también comprometer la seguridad de la información.

Lo anterior significa que cualquier funcionario de la Entidad está en la obligación de reportar al responsable de la seguridad física de la Entidad, movimientos o actitudes extrañas de personas dentro de las instalaciones.

Si un incidente de acceso físico es detectado dentro de una de las siguientes áreas: Centro de Cómputo, Cintoteca, Strip telefónico, taller del Grupo de Sistemas, Bodega del Grupo de Sistemas, el responsable de la seguridad física de la Entidad deberá reportarlo al Grupo de Sistemas.

Incidentes contra la red de datos y recursos tecnológicos

Un incidente contra los recursos tecnológicos o la red de datos, se define como un evento adverso que pueda tener el potencial de interrumpir algunos de los siguientes elementos:

- Tráfico sobre la red
- Los sistemas operativos
- Amenace la confidencialidad, integridad o disponibilidad de cualquier componente tecnológico de la red de La Defensoría.

El reporte de esta situación se hará con el Grupo de Sistemas. El Oficial de Seguridad, con base en los componentes amenazados, identificará en el mapa de riesgos la criticidad de la situación y procederá a determinar las acciones correctivas, que en algunos casos podrían inclusive llegar a la desconexión parcial o total de la red mientras se controla y maneja la situación.

La documentación de este tipo de incidentes debe estar contenida en la categoría de incidentes por ataques a la red de datos y recursos tecnológicos, dentro de la herramienta que la Entidad utilice para mesa de ayuda y debe contener como mínimo la siguiente información:

- Descripción de los síntomas

- Fechas y hora del incidente
- Periodo en el que se ha venido presentando el incidente
- Acción local tomada
- Estado del incidente

Se debe establecer una estrategia de respuesta (dependiendo del ataque) entre mesa de ayuda y el Oficial de Seguridad Informática. El Oficial de Seguridad en un periodo no mayor a 24 horas realizará la evaluación sobre las posibles consecuencias del incidente y el tiempo estimado para su solución.

Escalamiento de casos de incidentes de seguridad

Los casos de seguridad abiertos críticos que sobrepasen las veinticuatro (24) horas deben ser escalados al oficial de seguridad y después de cuarenta y ocho (48) horas al comité de seguridad con el fin de tomar medidas correctivas.

Recolección de evidencia

- **Sistemas operativos**

Uno de los primeros pasos de cualquier investigación preliminar es obtener información suficiente para determinar una respuesta apropiada. Los pasos que se necesitan hacer para confirmar si ha ocurrido o no un incidente, varían dependiendo del tipo de incidente. Los objetivos de una respuesta inicial las podemos resumir diciendo: Primero, confirmar la existencia del incidente de seguridad y segundo, poder obtener la mayor cantidad posible de información de tipo volátil, que posiblemente desaparecerá al apagar el sistema.

- Información a recolectar:
  - Fecha y hora del sistema
  - Lista de usuarios conectados
  - Tiempos relacionados con todos los archivos del sistema
  - Lista de puertos abiertos
  - Aplicaciones abiertas y en estado de escucha(listening)
  - Lista de los sistemas conectados o que se conectaron en un lapso
  - Vaciado de la memoria RAM[5]
  - Información relevante del *Registry* o archivos de configuración
  - Listado de todos los procesos activos[6]

- Se debe almacenar la información obtenida del paso anterior, en un sistema que sea seguro, donde esta información no puede ser borrada por usuarios no autorizados para ellos. Ejemplos pudieran ser: CD-ROM, Memoria USB o una estación especialmente definida para esta funcionalidad.

- Una vez almacenada la información recolectada se debe garantizar la integridad de esta información. Para ello se necesita calcular el *checksum* o la función *hash* de este archivo con una utilidad como el caso de la función md5sum o cualquier otra.

- Organizar y documentar su investigación: Se requiere con el fin de tener un proceso adecuado de gestión de incidentes, contar con una adecuada metodología, y un sistema de documentación. Se recomienda llevar un registro de cada comando

[5] Ramdom Access Memory: memoria de acceso aleatorio, donde están los datos volátiles del sistema y se almacenan las aplicaciones en ejecución.

[6] Usar el comando ps en Unix. Para Windows existe una utilidad Pslist en www.foundstone.com.

ejecutado en la maquina investigada donde se considera la hora, el comando ejecutado, y comentarios adicionales que se consideren pertinentes. También se recomienda ser consistentes con los nombres que se dan a los archivos que almacenan información extraída. Se deben considerar los siguientes temas en la creación del formato de documentación:

- Resumen ejecutivo
- Objetivos
- Evidencia analizada
- Hechos relevantes encontrados
- Detalles que soporten los hechos encontrados
- Anexos relevantes

- **Dispositivos de red**

Para la respuesta inicial se requiere un plan para obtener la mayor cantidad de información existente en los dispositivos, sin afectar algún tipo de evidencia potencial. Debe generarse un conjunto de herramientas para la obtención de información forense en dispositivos de red. Dentro de estas herramientas se puede agregar un *sniffer*[7] que nos permita obtener y analizar el tráfico que viaja o viajó por la red, luego salvar esta información garantizando la integridad de ella.

- Información a recolectar:
  - Fecha y hora del sistema
  - Lista de puertos abiertos
  - Vaciado de la memoria RAM[8]
  - Rutas estáticas
  - Rutas dinámicas
  - Algoritmos de enrutamiento habilitados
  - Listas de acceso
  - Mecanismo de seguridad habilitados
  - Salvar la información de los registros

- Se debe almacenar la información obtenida del paso anterior, en un sistema que sea seguro, donde esta información no puede ser borrada por usuarios no autorizados para ellos. Ejemplos pudieran ser: CD-ROM, Memoria USB o una estación especialmente definida para esta funcionalidad.

- Una vez almacenada la información recolectada se debe garantizar la integridad de esta información. Para ello se necesita calcular el *checksum* o la función *hash* de este archivo con una utilidad como el caso de la función md5sum o cualquier otra que la Defensoría tenga experiencia utilizándola.

- Organizar y documentar su investigación: Se requiere con el fin de tener un proceso adecuado de gestión de incidentes, contar con una adecuada metodología, y un sistema de documentación. Se recomienda llevar un registro de cada comando ejecutado en la maquina investigada donde se considera por ejemplo la hora, el comando ejecutado, y comentarios adicionales que se consideren pertinentes. También se recomienda ser consistentes con los nombres que se dan a los archivos que almacenan la información extraída para uso posterior en la investigación.
  - Resumen ejecutivo
  - Objetivos
  - Evidencia analizada

[7] Un sniffer ampliamente conocido es el Whireshark en https://www.wireshark.org/

[8] Ramdom access memory: memoria de acceso aleatorio, donde están los datos volátiles del sistema y se almacenan las aplicaciones en ejecución.

- Hechos relevantes encontrados
- Detalles que soporten los hechos encontrados
- Anexos relevantes

Gestión de la continuidad del negocio

El Objetivo principal de esta política es velar por la disponibilidad de la plataforma tecnológica y los procesos del negocio para actuar en caso de desastres que impiden la realización normal de las operaciones de La Defensoría.

La función de Continuidad del Negocio será gestionada por el Líder de Continuidad del Negocio.

El Líder de Continuidad del Negocio es el responsable de velar por la implantación de las medidas relativas a esta. Igualmente, es responsable de desarrollar las tareas necesarias para el mantenimiento de estas medidas.

El Líder de Continuidad se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velará por la implantación y cumplimiento de las mismas.

Con base en los análisis de riesgos y los análisis de impacto el Líder de Continuidad participará en la planeación de los controles requeridos para garantizar la continuidad de la plataforma tecnológica y de los procesos del negocio.

Para realizar la función de Gestión de Continuidad del Negocio los responsables se apoyarán en herramientas tecnológicas que permitan una adecuada administración, monitoreo y control de los recursos informáticos.

Responsabilidades del Líder de Continuidad.

- Definir y actualizar normas, procedimientos y estándares relacionados con Continuidad del Negocio.
- Validar la arquitectura de contingencias de La Defensoría para los procesos críticos del negocio
- Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad del negocio
- Evaluar, seleccionar e implantar herramientas que faciliten la labor de seguridad y contingencia.
- Conducir los análisis de impacto al negocio periódicamente – por lo menos una vez al año
- Definir, conformar y mantener los equipos de continuidad del negocio: Equipo de recuperación de redes, de servidores, de manejo de crisis, de evaluación de daños, de activación del centro alterno entre otros.
- Establecer las medidas de seguridad para operar en contingencia y en los sitios alternos que se activen.
- Velar por que los planes de contingencias, de recuperación de desastres y de continuidad del negocio se mantengan actualizados.

- Coordinar con los proveedores y terceros la participación de ellos en los grupos de continuidad de La Defensoría y verificar que estas tareas formen parte de los contratos vigentes.

- Programar y realizar pruebas periódicas a los planes de continuidad de acuerdo con los escenarios de desastre que se definan en la organización.

- Reportar los resultados de los análisis de impacto y de las pruebas de los planes de continuidad.

- Coordinar la realización periódica de programas de capacitación, sensibilización y entrenamiento en temas de continuidad del negocio.

Pruebas, mantenimiento y reevaluación del plan de continuidad de La Defensoría

Al menos una vez al año, el Oficial de seguridad de la información y el Líder de Continuidad del Negocio debe efectuar una revisión del Plan de Continuidad del negocio teniendo en cuenta los puntos que se describen a continuación:

- Mejora de la efectividad del BCP

- Requerimientos de negocio

- Administración del riesgo

- Requerimientos de BCP

- Procesos de negocio que afecten a los procedimientos de negocio existentes

- Entornos legales o normativos

- Recursos requeridos

Las pruebas ejecutadas al plan de continuidad de negocio (1 al año al menos), deben ser revisadas para establecer las oportunidades de mejoramiento; se debe verificar:

- Alcance de la prueba.

- Eficiencia de la estrategia de continuidad

- Tiempos de recuperación dentro del margen tolerable.

- Funcionamiento del esquema de comunicaciones

- Entrenamiento y preparación de los responsables y usuarios finales.

- Procedimientos para el retorno a la normalidad de las operaciones.

Cumplimiento

Derechos de propiedad intelectual

La Defensoría debe adoptar medidas para garantizar que la Entidad y los colaboradores de la misma cumplan con los requisitos legales de los derechos de propiedad intelectual, para lo cual se definen las siguientes normas:

- Todo material utilizado por la Entidad que sea objeto de derechos de propiedad intelectual, debe ser adquirido cumpliendo con los requisitos legales.

- En los computadores y dispositivos móviles de propiedad de la Defensoría del Pueblo solo se puede instalar y usar software licenciado, software libre o de dominio público. Se considera software libre aquel que se puede ejecutar, copiar, distribuir, estudiar, modificar y mejorar libremente de varias formas. El software de dominio público no requiere de licencia y tiene libertad de derechos de explotación para todos.

- Cada funcionario o contratista de la Defensoría y las terceras partes son responsables de garantizar que todo material utilizado con propósito laboral cumple con la legislación de derechos de propiedad intelectual.

- Está completamente prohibido que usuarios finales instalen programas de software en los computadores personales de la Entidad, esta función es exclusiva del personal de soporte del Grupo de Sistemas.

- El Grupo de Sistemas debe tener un control de las licencias de los programas de software y velar por que no exista software sin la debida licencia de uso.

- Únicamente el Grupo de Sistemas puede tomar copias de respaldo con propósito de proteger los medios originales de los programas de software licenciados.

- La instalación por parte de funcionarios y contratistas de la Defensoría o terceras partes de programas de software en los computadores personales de la Entidad sin la debida autorización, es considerada como un incidente de seguridad.

- Las licencias de uso de los programas de software deben ser debidamente registradas ante el fabricante.

- Programas de software o información de terceras partes sujetas a derechos de autor que no contengan una autorización explícita del propietario no pueden ser instalados en los activos de la Defensoría.

- Los funcionarios de la Entidad, contratistas y terceras partes, no pueden por ningún motivo descargar o almacenar archivos de música, fotos, videos, o material sujeto a propiedad intelectual en los equipos de la Defensoría.

- Los funcionarios de la Defensoría, contratistas y terceras partes, no pueden por ningún motivo descargar, instalar, almacenar o utilizar herramientas de software o hardware que puedan ser utilizadas para evaluar o comprometer los sistemas de seguridad de la información, a no ser que exista una autorización del Oficial de Seguridad de la Información o del Defensor del Pueblo, ejemplo de estas herramientas son: crackers de software, software de descubrimiento de contraseñas, detección de vulnerabilidades o utilidades de encripción y desencripción.

- Toda información propietaria o confidencial de terceras partes que haya sido confiada a la Defensoría, debe ser protegida con los mismos controles que si fuera clasificada como confidencial.

- Está prohibido, usar, distribuir, descargar sin autorización, compartir, vender o instalar el software licenciado por la Defensoría del Pueblo en computadores y dispositivos móviles que no sean propiedad de la entidad.

- En caso de que un funcionario o contratista haga uso de su propio computador y/o dispositivo móvil para la ejecución de las actividades asignadas a su rol, debe asegurarse que el software instalado no sea propiedad de la Defensoría del Pueblo. Si tiene

instalado software de propiedad de la Defensoría del Pueblo deberá retirarlo del equipo o de los equipos donde fue instalado.

Protección de los registros de la Entidad

Los registros de información institucional de la Entidad deben ser protegidos contra eventos no autorizados: acceso, divulgación, modificación, duplicidad, destrucción; o actos de alteración, sustracción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y de la misión institucional.

- Los dueños de la información responsables de los diferentes activos de información de carácter confidencial y privada, deben velar por los controles necesarios que garanticen la integridad, confidencialidad y disponibilidad.

- Los registros de información confidencial y privada deben ser gestionados con los criterios definidos para los mismos en el ítem Gestión de los activos de información.

- Los registros de información clasificados como confidenciales y privados, no pueden ser extraídos fuera de las instalaciones de la Defensoría, a no ser que exista una autorización escrita por parte del dueño de la información.

- Siempre que un funcionario de la Entidad o tercera parte tenga acceso a información confidencial o privada, se debe anotar en una bitácora su nombre, fecha de entrega, fecha de devolución y propósito.

- La información confidencial debe permanecer en custodia por los términos estipulados por la ley.

Protección de los datos y privacidad de la información personal

La Defensoría adoptó e implementó los procedimientos necesarios para garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.

Recolección de información privada

- Toda información privada de funcionarios, terceras partes o ciudadanos que sea recolectada por la Defensoría, debe estar expresamente autorizada por el propietario.

- Se debe especificar el propósito para el cual se recolecta la información privada de los funcionarios, terceras partes o ciudadanos.

- La recolección de información privada de menores de edad debe estar expresamente autorizada por los acudientes del menor.

- Se debe informar cuando se haga uso de dispositivos electrónicos de monitoreo, como la utilización de circuito cerrado de televisión o grabación de conversaciones telefónicas.

- El Grupo de sistemas puede revisar los logs de Internet para establecer los sitios Web visitados y establecer si existe mala utilización de los recursos.

Almacenamiento de información privada

- La Defensoría debe implementar los controles necesarios para garantizar que la información privada de los funcionarios, terceras partes o ciudadanos no sea divulgada ni alterada sin el debido consentimiento del propietario.

- La información privada funcionarios, terceras partes o ciudadanos, solo puede permanecer almacenada por el tiempo necesario para cumplir con el propósito para el que fue recolectada, posteriormente debe ser eliminada.

- La información privada de funcionarios, terceras partes o ciudadanos, no puede ser utilizada con propósitos diferentes a los autorizados por el propietario.

- La información privada de funcionarios, terceras partes o ciudadanos, no puede ser suministrada a terceras partes sin la expresa autorización de su propietario, a excepción de los requerimientos por parte de las autoridades a través de los procedimientos formales.

Corrección de la información privada

- Todo funcionario, tercera parte o ciudadano tiene el derecho de exigir que la información que no sea correcta sea corregida y almacenada correctamente.

Transmisión de información privada

- La Defensoría debe garantizar que la información de funcionarios, terceras partes o ciudadanos que es transmitida por un medio público cuente con los mecanismos apropiados de cifrado que garanticen la confidencialidad e integridad.

- La movilización de información física dentro de las instalaciones de la Defensoría o fuera de ella, debe contar con los controles necesarios para garantizar la confidencialidad e integridad de la misma.

Destrucción de Información privada

- Una vez se ha cumplido con el propósito para el cual fue recolectada la información privada, la Defensoría debe proceder a su destrucción.

Prevención del uso inadecuado de los servicios de procesamiento de información

El uso inadecuado de los servicios de procesamiento de información y de los activos de información está prohibido en la Defensoría. La Entidad ha adoptado los mecanismos de difusión y disciplinarios que considera apropiados para disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.

El usuario por el solo hecho de empezar a usar las herramientas tecnológicas ofrecidas, acepta de manera previa y expresa tales condiciones y manifiesta que ha sido plenamente informado sobre este punto y que otorga su consentimiento previo, pleno e informado para tales efectos y que por lo mismo se desvirtúa y pierde cualquier expectativa de privacidad frente al uso de estos recursos y herramientas.

Se prohíbe todo lo que sea ilegal en la legislación colombiana o esté en contra de las normas internas de uso de los computadores y dispositivos móviles de la Defensoría del Pueblo. Se prohíbe utilizar computadores o dispositivos móviles para interferir o degradar el desempeño y rendimiento de los aplicativos, sistemas de información y la red. Se prohíbe los usos contrarios a lo estipulado en la presente Política de Seguridad de la información.

El uso prohibido incluye la discriminación, violación de derechos de autor marcas comerciales o licencias, obscenidad y acoso ilegal.

Los computadores, portátiles, equipos de red e impresoras de propiedad de la Defensoría del Pueblo solo pueden ser conectados a la red de la Defensoría del Pueblo por personal del Grupo de Sistemas.

Para salvaguardar la integridad y velocidad de la red ningún dispositivo como routers, hubs, multiplexores, switches, sniffers o puntos de acceso inalámbricos pueden ser colocados en la red sin la aprobación formal del Grupo de Sistemas.

Está prohibido:

- Realizar intentos de obtener acceso y/o contraseñas de aplicativos, y cuentas de funcionarios y contratistas de la Defensoría del Pueblo.
- Acceso al correo electrónico de funcionarios y contratistas sin la debida autorización.
- Interceptación de las transmisiones de comunicaciones electrónicas sin la debida autorización.
- Alteración de configuraciones de software o hardware con fines de hacer daño o sustraer información.
- Transmisión de mensajes como correo electrónico u otro aplicativo suplantando a otra persona.
- Uso de los recursos informáticos, equipos y de la red de la Defensoría del Pueblo para acosar a otros o falsificar la identidad.
- Uso de equipos, redes de la Defensoría del Pueblo para propagar virus, código malicioso, gusanos, troyanos y key loggers (registradores de pulsadores de teclas).
- Mantener credenciales de acceso a través de notas escritas, impresiones u otros visibles en el puesto de trabajo que permitan que personal no autorizado tengan acceso a ellas.

En caso de detectarse alguna de las conductas señaladas la Defensoría del Pueblo puede tomar las medidas legales y administrativas pertinentes contra las personas responsables de realizar la actividad prohibida.

En el caso particular del servicio de correo electrónico, el usuario se compromete a:

- No usar los servicios de correo electrónico de la Defensoría del Pueblo en actividades prohibidas por la Constitución, la legislación vigente, las políticas y reglamentos existentes en la organización, las buenas costumbres, el respeto por los demás, las normas de protección a menores y la infancia, las etiquetas, y demás reglas de buen comportamiento en la red. El usuario se obliga a no realizar actividades que afecten, alteren, vulneren, interrumpan, debiliten de alguna manera, el servicio de correo electrónico.
- No usar el servicio de correo electrónico en actividades diferentes a su rol dentro de la Defensoría del Pueblo, por ejemplo: uso del servicio de correo con fines comerciales, usar el servicio de correo para invadir la privacidad de otras personas, atentar contras las normas vigentes sobre protección de datos personales – data protection – Habeas Data, TICS, delitos informáticos, usar el servicio de correo para obtener o distribuir información confidencial o privilegiada de la Defensoría del Pueblo o de otros usuarios, usar el servicio de correo electrónico para enviar información abusiva, profana, tendenciosa o terrorista, usar el correo electrónico para enviar información publicitaria, comercial, política o religiosa, usar el servicio correo para acosar, amenazar, calumniar o injuriar a otras personas, usar el servicio de correo

electrónico para propagar cadenas, “SPAM” o cualquier otro tipo de material con información que no haya sido expresamente solicitada o acordada con el destinatario, usar el servicio de correo electrónico para distribuir software malicioso, virus o programas con fines ilegales.

- No alterar o manipular la información de los encabezados de correo con el fin de evitar, alterar u ocultar el origen de los correos.

- Eliminar y a informar al remitente de la misma, sobre la recepción de información que no está dirigida a él.

- Comprender que la información que se encuentre disponible por medio del servicio de correo electrónico puede ser confidencial y privilegiada o estar protegida por las normas sobre Propiedad Intelectual, Protección de Datos personales – Data Protection – Habeas Data; en consecuencia, acuerda expresamente proteger de manera activa dicha información de la revelación o publicación sin autorización.

- Aceptar que este servicio sea monitoreado y supervisado para efectos de verificar su debida utilización, mantener y garantizar su buen funcionamiento. Si el monitoreo de esta herramienta revela la violación de la ley o de los reglamentos y políticas de la Defensoría del Pueblo, esta información podrá ser entregada a los organismos judiciales que lo requieran o podrá ser usada dentro de los procesos disciplinarios a que haya lugar según sea el caso.

- Mantener su cuenta de correo dentro de los límites asignados por la Defensoría del Pueblo.

- Aceptar que el servicio de correo electrónico no permite la recuperación de buzones individuales o de correos específicos en caso de que estos sean eliminados definitivamente de la papelera de reciclaje o sean borrados sin ser enviados a la papelera de reciclaje, estos no se podrán recuperar.

Reglamentación de los controles criptográficos

La Entidad utiliza controles criptográficos bajo el estricto cumplimiento de todos los acuerdos, las leyes y los reglamentos pertinentes.

Cumplimiento con las políticas y normas de seguridad

En la Entidad todos los funcionarios son responsables del cumplimiento de la política y normas de seguridad establecidas. La Entidad designó en los Jefes de dependencia y responsables de Grupo el compromiso de controlar que los funcionarios a su cargo conozcan, acepten y cumplan las políticas de seguridad de la información y velar por que se cumplan los procedimientos definidos por la Entidad.

Verificación del cumplimiento técnico

La Entidad a través del Oficial de Seguridad verifica periódicamente el cumplimiento de las normas de implementación de seguridad, para ello, debe evaluar semestralmente el cumplimiento de las políticas de seguridad de la información, la eficiencia de los controles implementados y los niveles de riesgo presentes.

Auditoria a los activos de información

La Oficina de Control Interno planificará y realizará las actividades de auditoria a los activos de información para hacer las recomendaciones necesarias a fin de minimizar los riesgos sobre la confidencialidad, integridad y disponibilidad de los procesos de La Entidad

Las actividades de auditoria de verificación de configuraciones de los sistemas operativos, deben ser de tipo no intrusivo y su uso debe ser debidamente planificado con el dueño de la información.

El administrador del sistema debe verificar los procedimientos automáticos de verificación y garantizar que son solo de lectura y no de escritura.

Previo a la verificación se deben tomar los respaldos necesarios que garanticen la recuperación de información.

Protección de las herramientas de auditoria de los sistemas de información

Las herramientas de auditoria utilizadas por la Defensoría y los resultados de las mismas deben estar protegidas para evitar acceso, divulgación o alteración no autorizados. El acceso debe estar restringido a la Oficina de Control Interno de la Entidad.

Protección Legal

La Defensoría conserva el derecho de retirar de los sistemas de información cualquier material que pueda ser considerado ofensivo o potencialmente ilegal.

El administrador del sistema o el Oficial de Seguridad no leerá o facilitará a otra persona que lea el contenido de ningún archivo de correo electrónico del personal sin obtener el permiso del usuario, excepto en caso que exista un motivo razonable para hacerlo. Dichos motivos pueden incluir, sin limitarse a ello, mantener la integridad del sistema (tal como la eliminación de virus), cumplir obligaciones legales (tal como citaciones judiciales) y efectuar ciertas funciones de administración del sistema (tal como remitir los mensajes con direcciones erróneas).

No obstante lo anterior, La Defensoría puede obtener acceso a la información de los funcionarios y/o terceros en caso que se requiera dicha información para investigaciones o en caso de emergencia como por ejemplo: si el funcionario y/o tercero está ausente durante un período prolongado de tiempo debido a enfermedad u otro motivo, previa autorización escrita del jefe inmediato, para necesidades del servicio y de la Oficina de Control Interno para las respectivas investigaciones.

La Defensoría se reserva el derecho de interceptar o vigilar cualquier tráfico de información que pase a través del sistema de la Entidad como parte de sus actividades de vigilancia, mantenimiento, investigación, auditoria o seguridad del desempeño del sistema. Todo el personal debe estar consciente de esto cuando use los sistemas de tecnologías de información de la Entidad.

La Defensoría a través del Oficial de Seguridad de la entidad y la Oficina de Control Interno se reserva el derecho de monitorear o inspeccionar en cualquier momento todos los sistemas de información de la entidad. Esta evaluación puede tomar lugar con o sin el consentimiento, presencia o conocimiento de los funcionarios involucrados. Los sistemas de información sujetos a tal examen incluyen pero no están limitados a: sistemas de archivo de correo electrónico, archivos en discos duros de computadores personales, archivos de correo de voz, archivos en colas de impresión, y salidas de máquinas de fax.

La Entidad podrá contar con un contrato de respaldo alterno de equipos, para ser utilizado en caso de contingencia.

Es responsabilidad del dueño de la información, definir los periodos de retención y la frecuencia de los Backups que garanticen el cumplimiento legal y los propios.

Normatividad

Las políticas de seguridad de la información de La Defensoría fueron diseñadas para ajustarse o exceder, sin contravenir, las medidas de protección establecidas en las leyes y regulaciones; si algún funcionario o tercero de La Defensoría considera que alguna política de seguridad de información está en conflicto con las leyes y regulaciones existentes, lo debe reportar en forma inmediata al Oficial de Seguridad de la entidad.

- **Constitución Política de Colombia:** Por medio de la cual se promulga el marco jurídico, democrático y participativo que garantiza el orden político, económico y social justo, así como el compromiso a impulsar la integración de la comunidad latinoamericana.
- **Ley 527 de 1999:** Por la cual se define y regula el uso de los mensajes de texto, comercio electrónico y firmas digitales.
- **Ley 1341 de 2009:** Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- **Ley Estatutaria 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 025 de 2014:** Por el cual se modifica la estructura orgánica y se establece la organización y funcionamiento de la Defensoría del Pueblo.
- **Decreto 2573 de 2014:** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- **Decreto 943 de 2014:** Modelo Estándar de Control Interno (MECÍ)
- **Resolución 1014 de 2013:** Por la cual se adopta el Plan Estratégico de la Defensoría del Pueblo para la vigencia 2013-2016.
- **Resolución 1296 de 2014:** Manual de Supervisión e Interventoría de la Defensoría del Pueblo.
- **Norma NTC ISO 9001:** Sistemas de Gestión de la Calidad.
- **Norma NTCGP 1000:2009**: Norma Técnica de Calidad en la Gestión Pública – ICONTEC.
- **Norma NTC-ISO-IEC 27001:** Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.
- **Norma NTC-ISO-IEC 27002:** Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información.

ELABORÓ	REVISÓ	APROBÓ
Cargo: Profesional Especializado	Cargo: Profesional Especializado	Cargo: Secretario General
Nombre: Orlando Burgos	Nombre: Giovanni De Los Reyes	Nombre: Juan Manuel Quiñones Pinzón
Firma:	Firma:	Firma: