LA DIRECTORA GENERAL DE LA UNIDAD ADMINISTRATIVA ESPECIAL PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS

En uso de sus facultades legales y reglamentarias, en especial las conferidas por la Ley 1448 de 2011, los Decretos No. 4800 y 4802 de 2011, y

CONSIDERANDO:

Que los datos e información que se genere, obtenga, use, almacene, custodie, distribuya, envíe, intercambie y/o modifique en la **Unidad para la Atención y Reparación Integral a las Víctimas**, en cada uno de sus procesos misionales y/o de apoyo, son altamente sensibles y deben manejarse en condiciones que garanticen su confiabilidad, oportunidad y seguridad.

Que mediante la Ley 1448 de 2011 en su artículo 166, se crea la Unidad para la Atención y Reparación Integral a las Víctimas, como una Unidad Administrativa Especial con personería jurídica y autonomía administrativa y patrimonial, y el Decreto 4157 de 2011 la adscribe al Departamento Administrativo para la Prosperidad Social.

Que para dar aplicación a la Ley 872 de 2003 y a los Decretos Reglamentarios números 4485 de 2009, *"Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública"*, y 0943 de 2014 *"Por el cual se actualiza el Modelo Estándar de Control Interno – MECI 2014"*, expedidos por el Gobierno Nacional, La Unidad para la Atención y Reparación Integral a las Víctimas, viene implementado el Sistema de Integrado de Gestión para dar cumplimiento a lo estipulado en dicha normativa.

Que el Decreto 4802 de 2011 *"Por la cual se establece la estructura de la Unidad Administrativa Especial para la Atención y Reparación Integral a las Víctimas"*, en el numeral 13 del artículo 10°, establece que la Oficina de Tecnologías de la Información tiene como función, *"Implementar las metodologías y procedimientos que adopte la Unidad para el desarrollo, instalación, administración, seguridad y uso de la infraestructura tecnológica, teniendo en cuenta los lineamientos que en la materia generan las entidades competentes."*

Que mediante la Resolución 0893 del 2 de septiembre de 2013, se adoptó el *"Sistema Integrado de Gestión en la Unidad para la Atención y Reparación Integral a las Víctimas"*, la cual involucra los requerimientos del Sistema de Gestión de Calidad bajo la norma NTCGP 1000:2009 y cualquier otro modelo de excelencia que asuma la Entidad.

Que la información generada por la Unidad para la Atención y Reparación Integral a las Víctimas, disponible para las víctimas, usuarios internos y/o externos, debe caracterizarse por la exactitud y oportunidad, permitiendo incrementar la confianza en los ciudadanos, procesos misionales, de apoyo, entidades del Sistema Nacional de Atención y Reparación Integral a las Víctimas (SNARIV) y entes de control.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones, en el programa de Gobierno en Línea, define lineamientos para la implementación del Modelo de Seguridad de la Información, donde se requiere definir la Política de Seguridad en el marco del Sistema de Gestión de Seguridad de la Información (SGSI).

Que la Unidad para la Atención y Reparación Integral a las Víctimas debe contar con elementos de control y gestión, por medio del establecimiento de políticas, lineamientos y metodologías que fomente el manejo adecuado de la información.

Que por lo expuesto,

RESUELVE:

ARTÍCULO 1°: OBJETO: Aprobar y adoptar las Políticas de Seguridad de la Información en la Unidad para la Atención y Reparación Integral a las Víctimas contenidas en el Anexo 1 "POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN", y las Políticas de Gobierno de Datos contenidas en el Anexo 2: "POLÍTICAS GOBIERNO DE DATOS", las cuales hacen parte integral de la presente resolución, y pretenden articular esfuerzos en la entidad para asegurar el flujo de la información, teniendo en cuenta personas, aplicaciones e infraestructura tecnológica, instalaciones, procesos y procedimientos, y permiten la mejora, protección, gestión y administración de los datos y la promoción del uso de la información de calidad.

Parágrafo 1: Las políticas de Seguridad de la Información son de obligatorio cumplimiento por funcionarios y contratistas, directos o indirectos, que por la naturaleza de sus funciones tengan acceso a la información generada u obtenida por la Unidad para la Atención y Reparación Integral a las Víctimas y/o la infraestructura o instalaciones que la soporta.

Parágrafo 2: Las políticas de Gobierno de Datos son de obligatorio cumplimiento por funcionarios y contratistas, directos o indirectos, que generen u obtengan información de la Unidad para la Atención y Reparación Integral a las Víctimas y den soporte a usuarios que la requieren.

ARTÍCULO 2º: FINALIDAD: Establecer las políticas para la implementación de controles, procedimientos y estándares de Seguridad de la Información en la Unidad para la Atención y Reparación Integral a las Víctimas.

ARTÍCULO 3°: El Comité de Seguridad de la Información será el encargado de definir las actividades encaminadas a la implementación de las Políticas de Seguridad de la Información en la Unidad para la Atención y Reparación Integral a las Víctimas, y de proponer las modificaciones de las Políticas de Seguridad de la Información para aprobación de la Dirección General.

ARTÍCULO 4°: El Comité Institucional de Desarrollo Administrativo será la instancia encargada de definir las actividades encaminadas a la implementación y cumplimiento de las políticas de Gobierno de Datos en la Unidad para la Atención y Reparación Integral a las Víctimas, así como de proponer las modificaciones de las Políticas de Gobierno de Datos, para aprobación de la Dirección General.

RESOLUCIÓN No. 00740 **de** 11 NOV. 2014

Mediante la cual la Unidad para la Atención y Reparación Integral de las Víctimas, adopta las políticas de Gobierno de datos y Seguridad de la Información"

ARTÍCULO 5°: VIGENCIA. La presente Resolución rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C a los 11 NOV. 2014

PAULA GAVIRIA BETANCUR
Directora General

Elaboró: Joaquín Rojas Palomino
Asesor – Oficina de Tecnologías de la Información

Revisó: Sara Sandovnik Moreno - Secretaria General
Cesar Alberto Gómez Lozano - Jefe Oficina de Tecnologías de la Información
Luis Alberto Donoso Rincon - Jefe Oficina Asesora Jurídica

POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

Unidad para la Atención y Reparación Integral a las Víctimas

Noviembre de 2014

CONFIDENCIALIDAD DEL DOCUMENTO

Toda la información contenida en el presente documento deberá mantenerse en forma estrictamente confidencial. Por favor absténgase de realizar copias y/o reproducir parcial o totalmente este documento sin la autorización formal de **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**

REVISIONES Y CAMBIOS

Fecha	Modificado por	Versión	Referencia del cambio
Marzo 2014	Oficina de Tecnologías de la Información	2.0	Actualización a ISO27001:2013
Marzo 2014	Observaciones comité directivo	2.1	Observaciones comité directivo
Mayo 2014	Recomendaciones	3.0	Recomendaciones de Agencia de Cooperación Internacional del Japón (JICA)
Octubre 2014	Recomendaciones Oficina Asesora Jurídica	3.1	Ajuste relacionado con el delegado de la Dirección General para tales fines

TABLA DE CONTENIDO

GLOSARIO 6
INTRODUCCIÓN 6
OBJETIVO 7
ALCANCE 7
1. VIGENCIA Y ACTUALIZACIÓN DE LAS POLÍTICAS 8
2. ORGANIZACIÓN DE LA SEGURIDAD 9
2.1. ORGANIZACIÓN INTERNA 9
2.2. SEPARACIÓN DE DEBERES 9
2.3. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS 9
2.4. COMPUTACIÓN Y COMUNICACIONES MÓVILES 9
3. ASPECTOS DE SEGURIDAD RELACIONADOS CON RECURSOS HUMANOS 10
3.1. RESPONSABILIDAD DEL PERSONAL 10
3.2. PROCESOS DISCIPLINARIOS 10
3.3. TERMINACIÓN O CAMBIO DE LA CONTRATACIÓN LABORAL 10
4. GESTIÓN DE ACTIVOS DE INFORMACIÓN 11
4.1. INVENTARIO DE ACTIVOS DE INFORMACIÓN Y PROPIEDAD DE LOS ACTIVOS 11
4.2. USO ADECUADO DE LOS ACTIVOS Y RECURSOS DE INFORMACIÓN 11
4.3. DEVOLUCIÓN DE ACTIVOS 11
4.4. CLASIFICACIÓN DE LA INFORMACIÓN 11
4.5. MANEJO DE MEDIOS 12
5. CONTROL DE ACCESO 12
5.1. POLÍTICA PARA EL CONTROL DE ACCESO 12
6. SEGURIDAD FÍSICA Y AMBIENTAL 12
7. SEGURIDAD DE LAS OPERACIONES 13
7.1. COPIAS DE RESPALDO 13
8. SEGURIDAD DE LAS COMUNICACIONES 13
9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 13
10. RELACIONES CON LOS PROVEEDORES 14
10.1. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES 14
11. GESTIÓN DE INCIDENTES DE SEGURIDAD 14

11.1. RESPONSABILIDADES, PROCEDIMIENTOS, REPORTE DE EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN 14

12. ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO 15

13. CUMPLIMIENTO DE REQUERIMIENTOS 15

13.1. CUMPLIMIENTO DE LAS OBLIGACIONES LEGALES 15

13.2. DERECHOS DE PROPIEDAD INTELECTUAL 15

13.3. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN 15

GLOSARIO

a- Activo:
Todo aquello que tiene valor para la Organización.

b- Autorización:
Permisos asociados con la identidad de un usuario.

c- Confidencialidad:
Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

d- Datos:
Cualquier información, sin importar la forma, contenida o procesada por sistemas de información, redes de comunicaciones, o medios de almacenamiento.

e- Disponibilidad:
La característica de los datos, información, y sistemas de información a ser accesibles y utilizables en el momento requerido.

f- Integridad:
La característica de la información correcta, completa y coherente. Certeza que el ingreso, modificación o eliminación de la información se realiza únicamente por personal autorizado.

g- Propietario de la Información:
Identifica a un individuo o entidad que tiene la responsabilidad designada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término "propietario" no quiere decir que la persona o proceso realmente tenga algún derecho de propiedad sobre el activo.

INTRODUCCIÓN

Las políticas establecidas e incluidas en este documento son un componente fundamental para la gestión en seguridad de la información de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** y se convierten en la base para la implantación de los controles, los procedimientos y los estándares de seguridad.

Este documento es de uso Interno y de propiedad de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS.** Las actualizaciones se publicarán internamente en la

Intranet de la Entidad. Para contratistas y/o terceros se anexará al contrato el documento denominado "Anexo de Políticas de Seguridad de la Información para Terceras partes". Cuando existan cambios, el delegado de la Dirección General para tal fin, lo informará a través de los medios habilitados por la Entidad a los funcionarios, contratistas y partes interesadas.

Las políticas de seguridad de la información deberán ser conocidas y cumplidas por todos los funcionarios, contratistas y partes interesadas de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS.** El incumplimiento de las mismas se considerará un incidente de seguridad, que de acuerdo con el caso podrá dar lugar a un proceso disciplinario para los funcionarios y se convertirá en una causa válida de terminación del contrato con los contratistas, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar. Para reportar un evento sospechoso o un incidente de seguridad, por favor póngase en contacto con el delegado de la Dirección General para tal fin, en los canales de comunicación que se destine para tal fin.

OBJETIVO

Establecer y divulgar las Políticas de Seguridad de la Información a todo el personal de la Entidad, para que sea de su conocimiento y cumplimiento.

ALCANCE

Este documento define las Políticas de Seguridad de la Información que deben ser cumplidos por los directivos, funcionarios, usuarios y terceros, que:

- Accedan a información de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** o de las Víctimas.
- Usen equipos informáticos y de telecomunicaciones conectados a la infraestructura de la Entidad.
- Diseñen, construyan, prueben y/o usen herramientas tecnológicas y/o servicios informáticos de la Entidad.
- Ingresen de manera física o lógica a las instalaciones de la Entidad.

1. VIGENCIA Y ACTUALIZACIÓN DE LAS POLÍTICAS

Estas Políticas se encuentran vigentes a partir del 11 de noviembre de 2014, fecha en la que se publica la primera versión de este documento y se entiende incorporado a las obligaciones de los funcionarios y a los contratos que la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** celebre con contratistas.

La Política de Seguridad de la Información seguirá un proceso de actualización permanente, de acuerdo con los cambios organizacionales (culturales, estructurales, operativos), del entorno, tecnológicos y las normas que se expidan al respecto.

La definición, actualización y mantenimiento de esta Política, es responsabilidad del delegado de la Dirección General para tal fin, previa aprobación de la Dirección. Este documento se actualizará como mínimo una vez al año o cuando se presenten cambios importantes en la Entidad. En las revisiones se tendrán en cuenta factores como: incidentes de seguridad, nuevas vulnerabilidades detectadas, cambios dentro de la infraestructura organizacional o tecnológica, cambios en los procesos, en los objetivos de la Entidad, entre otros.

El delegado de la Dirección General para tal fin, es el responsable de gestionar, brindar apoyo y realizar seguimiento en materia de Seguridad de la Información y Continuidad de la operación. La Oficina de Tecnología de la Información es el área que gestiona y brinda apoyo técnico en materia de Seguridad Informática y de Telecomunicaciones a las dependencias de la entidad.

Cualquier excepción a lo establecido en esta política, deberá contar con la aprobación formal del Comité de Seguridad de la Información.

2. ORGANIZACIÓN DE LA SEGURIDAD

2.1. Organización Interna

LA UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS ha definido una estructura organizacional, la cual se encargará de la coordinación de las actividades relacionadas con la gestión de la seguridad de la información. Esta cuenta con un delegado de la Dirección General para tal fin, y un Comité de Seguridad de la Información.

2.2. Separación de deberes

La **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**, establece que aquellas personas que realizan tareas de operación o monitoreo sobre aplicaciones o sistemas de información críticos de la Entidad, no pueden tener a su cargo las labores de administración técnica sobre los sistemas operativos o las bases de datos.

2.3. Seguridad de la Información en la Gestión de Proyectos

La Gestión de Proyectos dentro de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**, contemplará dentro de su planificación la inclusión de los requisitos de seguridad de la información sin importar el tipo de proyecto a implementar, así como la evaluación de los riesgos que pueden llegar a impactar la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad.

2.4. Computación y comunicaciones móviles

No se permitirá a los funcionarios y contratistas almacenar o transportar información confidencial fuera de las instalaciones de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** a menos que estén autorizados por el delegado de la Dirección General para tal fin, de acuerdo a solicitud enviada por el Líder o Jefe de Área, justificando la razón por la cual se requiere trasportar la información confidencial.

3. ASPECTOS DE SEGURIDAD RELACIONADOS CON RECURSOS HUMANOS

3.1. Responsabilidad del personal

Todos los funcionarios o contratistas, así como los usuarios o terceros autorizados para acceder a la infraestructura de procesamiento de información de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**, son responsables del cumplimiento de la política, procesos, procedimientos y lineamientos de seguridad de la información definidos por la Entidad.

La información almacenada en los equipos de cómputo es de propiedad de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad.

3.2. Procesos disciplinarios

Los incidentes de seguridad de la información ocurridos en la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** serán registrados e investigados con el fin de determinar sus causas y responsables. Los procesos derivados de los reportes y del análisis de los Incidentes de Seguridad serán manejados teniendo en cuenta la gravedad y las responsabilidades identificadas.

3.3. Terminación o cambio de la contratación laboral

La responsabilidad de custodia de cualquier activo de información mantenido, usado o producido por el personal que se retira o cambia de cargo recae en el jefe de departamento/área o supervisor del contrato.

Tras la finalización o cambio en la contratación laboral se revisarán los derechos de acceso de los funcionarios y contratistas a los activos asociados con los sistemas y servicios de información, esto determinará si es necesario remover los derechos de acceso.

4. GESTIÓN DE ACTIVOS DE INFORMACIÓN

4.1. Inventario de Activos de Información y propiedad de los activos

Todas las áreas de la Entidad, con el apoyo del delegado de la Dirección General para tal fin, mantendrán un inventario actualizado de los activos de información.

4.2. Uso adecuado de los activos y recursos de información

Toda la información de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** será procesada y almacenada de acuerdo con su nivel de clasificación, de manera que se protejan las propiedades de confidencialidad, integridad y disponibilidad.

Los recursos tecnológicos (equipos de cómputo, Internet, correo electrónico, herramientas de mensajería colaborativas, entre otros) proporcionados por la Entidad, deben ser usados exclusivamente por los funcionarios, contratistas y terceros autorizados.

La **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** controlará, verificará y monitoreará el uso adecuado de los recursos tecnológicos proporcionados por la Entidad.

4.3. Devolución de Activos

Todos los funcionarios, contratistas y terceros deben devolver todos los activos de información de la Entidad en su poder (software, documentos corporativos, equipamiento, dispositivos de computación móviles, tarjetas de ingreso, etc.) tras la terminación de su empleo, contrato o acuerdo.

4.4. Clasificación de la Información

Toda información perteneciente a la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** deberá ser identificada, clasificada y documentada con base en los criterios de clasificación definidos por el Comité de Seguridad de la Información, los cuales contemplan requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Los propietarios de los activos de información serán los responsables de establecer el nivel de clasificación de cada activo y dichos activos se protegerán de acuerdo con el nivel asignado.

4.5. Manejo de Medios

En los equipos de cómputo de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**, únicamente se permitirá la conexión de dispositivos o medios de almacenamiento extraíble (USB) asignados y entregados formalmente por la Entidad.

Toda la información almacenada en medios magnéticos removibles, e impresa, debe estar controlada en cuanto a su acceso, uso, transporte, almacenamiento y eliminación, acorde con su nivel de clasificación.

5. CONTROL DE ACCESO

5.1. Política para el control de Acceso

El acceso a los activos de información de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** estará permitido únicamente a los usuarios autorizados. La autorización a otros usuarios será definida y aprobada por el propietario de la información.

Los sistemas de información de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** deben contar con mecanismos de identificación individual de los usuarios y con procedimientos para el control de acceso a los mismos.

6. SEGURIDAD FÍSICA Y AMBIENTAL

Se deben identificar, documentar y proteger las áreas que se consideren de especial protección debido a la confidencialidad, integridad y disponibilidad requerida para los activos que allí permanezcan.

La **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**, protegerá la disponibilidad e integridad de la infraestructura de procesamiento de información mediante mecanismos adecuados.

Es responsabilidad de todos los funcionarios, contratistas y terceros de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**, cumplir con los lineamientos de seguridad de equipos, dentro y fuera de las instalaciones.

7. SEGURIDAD DE LAS OPERACIONES

7.1. Copias de Respaldo

La información crítica de la Entidad contenida en servidores y sistemas de información, se debe respaldar de forma periódica y los medios se almacenarán en un lugar diseñado para tal fin.

8. SEGURIDAD DE LAS COMUNICACIONES

El intercambio de información confidencial debe darse en condiciones de seguridad que garanticen que la información no estará en riesgo de ser modificada o de ser consultada por personal no autorizado.

Todos los funcionarios, contratistas y terceros deberán firmar la cláusula y/o acuerdo de confidencialidad definida por la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** y este deberá ser parte integral de cada uno de los contratos.

9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La inclusión o desarrollo de un nuevo producto de software o aplicativo en la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**, o los cambios y/o actualizaciones a los sistemas existentes, deben estar precedidas de la inclusión de los requisitos y controles de seguridad definidos por el delegado de la Dirección General para tal fin.

Todos los procesos de compra, actualización y/o desarrollo de software deberán contar con la identificación, implementación y pruebas de requisitos de seguridad de la información.

Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

10. RELACIONES CON LOS PROVEEDORES

10.1. Seguridad de la Información en las relaciones con los proveedores

El delegado de la Dirección General para tal fin, revisará y documentará los requisitos de seguridad de la información relacionados con el acceso de proveedores a los activos de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS,** los cuales se incluirán como parte integral del contrato de acuerdo al alcance del servicio prestado por el proveedor.

El acceso a la información y a la infraestructura de procesamiento de información de **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** por parte de proveedores, deberá ser solicitado por el área respectiva y autorizado por el delegado de la Dirección General para tal fin.

11. GESTIÓN DE INCIDENTES DE SEGURIDAD

11.1. Responsabilidades, procedimientos, reporte de eventos y debilidades de Seguridad de la información

Los funcionarios y contratistas de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** deben informar inmediatamente al delegado de la Dirección General para tal fin, cualquier situación sospechosa, o incidente de seguridad que comprometa la confidencialidad, integridad y/o disponibilidad de la información.

El delegado de la Dirección General para tal fin, es el responsable de realizar el seguimiento a los eventos e incidentes de seguridad reportados, con el apoyo de otras áreas de la Entidad o de entidades externas, cuando así se requiera.

La Dirección General y ante su ausencia la Oficina Asesora de Comunicaciones son los únicos autorizados por parte de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos formales ante entidades externas o medios de comunicación.

Todos los funcionarios y contratistas deben mantener confidencialidad de la información relacionada con el manejo, investigación y seguimiento de los incidentes.

12. ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

Para la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** es un compromiso con sus usuarios mantener la continuidad de las operaciones de la Entidad. En la planeación de Continuidad del Negocio, se detallan las políticas relacionadas con la Seguridad de la Información en la Continuidad de Negocio, así como las políticas de pruebas y mantenimiento del Plan.

13. CUMPLIMIENTO DE REQUERIMIENTOS

13.1. Cumplimiento de las Obligaciones Legales

Los funcionarios, contratistas y terceros, deben cumplir con la legislación aplicable a la materia, las obligaciones contractuales contraídas y las previsiones establecidas con terceros.

13.2. Derechos de propiedad intelectual

Los funcionarios, contratistas y terceros autorizados deben cumplir con la reglamentación de propiedad intelectual. La **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** podrá ejecutar revisiones periódicas para asegurar que se estén respetando los derechos de propiedad intelectual.

13.3. Revisiones de Seguridad de la Información

El delegado de la Dirección General para tal fin, verificará el cumplimiento de las Políticas de Seguridad apoyada en el equipo de auditoría y los líderes de proceso mediante revisiones periódicas al cumplimiento de los procesos y procedimientos, dentro del marco de las políticas, normas y cualquier otro requisito de seguridad aplicable.

POLÍTICAS GOBIERNO DE DATOS

POLITICAS GENERALES

Autor del Documento:	Constanza Rodriguez
Dueño del Documento:	Unidad para la Atención y Reparación Integral a las Víctimas
Fecha de actualización:	31-07-2014
Última Actualización:	Oficina de Tecnologías de la Información – Dominio Gobierno de Datos
Proyecto:	Gobernabilidad de Datos
Compañía:	Unidad para La Atención y Reparación Integral a Las Victimas

Contenido

1. INTRODUCCIÓN 3
2. OBJETIVO 3
3. ALCANCE 3
4. RESPONSABLE 4
5. GLOSARIO DE NEGOCIO 4
6. POLITICAS GOBIERNO DE DATOS 5
6.1. POLITICA INTEGRACIÓN DE DATOS 5
6.2. POLITICA ADMINISTRACIÓN DE LA CALIDAD DE LOS DATOS 6
6.3. POLITICA SEGURIDAD DE LA INFORMACIÓN 6
6.4. POLITICA ADMINISTRACIÓN DE METADATOS 6
7. VIGENCIA Y ACTUALIZACIÓN DE LAS POLITICAS 6

1. INTRODUCCIÓN

Los datos en la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**, es un activo esencial para el **GOBIERNO DE DATOS**, las políticas definidas en este documento permiten establecer los parámetros para la mejora de la calidad de los datos, la protección de los datos, la promoción del uso compartido eficaz de la información, el suministro de datos críticos del negocio y la gestión de la información a lo largo de su ciclo de vida, teniendo en cuenta los procesos de negocio y el alcance de cada uno a través de los dominios definidos. Los propietarios de los datos, que gestionan el ciclo de vida de los datos y dan soporte a la comunidad de usuarios deben cumplir las políticas definidas para **GOBIERNO DE DATOS** sin excepción y deben ser comunicadas de manera efectiva para lograr los resultados deseados.

2. OBJETIVO

El propósito de este documento es establecer, mantener, y divulgar las políticas organizacionales para **GOBIERNO DE DATOS**, estas políticas definen las expectativas de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**, en cuanto a las prácticas y métodos que se deben seguir.

3. ALCANCE

Este documento aplica para **GOBIERNO DE DATOS** de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**, y su aplicación es requerida para administración de programas como:

- ✓ Seguridad de la Información
- ✓ Administración de Metadatos
- ✓ Administración de la Calidad de los Datos
- ✓ Integración de Datos

4. RESPONSABLE

Las actividades de establecer, mantener, y divulgar las Políticas para **GOBIERNO DE DATOS** serán realizadas por Líder de Gobierno de Datos o quien delegue el Comité Directivo, según directrices del Comité Institucional de Desarrollo Administrativo.

5. GLOSARIO DE NEGOCIO

A continuación se describen los términos de negocio de tipo estándar con el fin de garantizar una comunicación clara acerca de la integración de datos:

TERMINO / ACRÓNIMO	DEFINICIÓN
Datos	Los datos son una representación simbólica (numérica, alfabética, algoritmica, etc) de un atributo o variable cuantitativa. Los datos describen hechos empíricos, sucesos y entidades.
Información	En sentido general, la información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
Acreditación	La acreditación es un proceso de la ruta de reparación de las víctimas, mediante el cual la UNIDAD es capaz de evaluar el estado de una víctima con la finalidad de acceder a los programas de reparación implementados por el estado colombiano.
Proceso	Un proceso es un conjunto de actividades mutuamente relacionadas o que, al interactuar, transforman elementos de entrada y los convierten en resultados.
Sistemas	Un sistema es un conjunto de partes o elementos organizados y relacionados que interactúan entre sí para lograr un objetivo. Los sistemas reciben (entrada) datos y proveen (salida) información.
Base de Datos	Es una colección de información organizada de forma que un programa, pueda seleccionar rápidamente los fragmentos de datos que necesite.
Metadato	Son Datos estructurados que describen características de otros datos.
Calidad de Datos	Se refiere al mejoramiento de la calidad de los datos; es un proceso, técnicas, algoritmos y operaciones encaminados a mejorar la calidad de los datos existentes.
Diccionario de Datos	Conjunto de términos y sus definiciones, asociados a un modelo de datos; el diccionario de datos contiene la definición semántica de un campo en una estructura.
Dueño	Persona la cual tiene derecho sobre los sistemas y los datos.
Custodio	Es el ente o Profesional guardián o escolta de los sistemas y datos.
Administrador	Profesional que ejecuta, mantiene, opera y asegura el funcionamiento de un sistema informático.
Información no Estructurada	Información que no tiene estructura de datos, no cuenta con un esquema particular o una estandarización ideal y definida.

Datos Analíticos	Son datos que ayudan y posibilitan la toma de decisiones, y están orientados a un determinado ámbito dentro de la UNIDAD.
Trámite	Es la gestión o diligenciamiento que se realiza para obtener un resultado, en pos de algo, a través de los sistemas.
Modificaciones	Cambiar o transformar algún sistema o dato.
Asistencia	Servicios que se presta a una persona que se recuperan del delito infligido contra ellas.
Autorización	Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de Datos Personales.
Activos de Información	Representan los datos o información tangibles o intangibles que posee una organización.

6. POLITICAS GOBIERNO DE DATOS

Para la gestión de gobernabilidad de los datos en la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**, se han considerado los siguientes componentes:

- ✓ Un mecanismo de Control: Comité de Gobierno de Datos.
- ✓ Actores o Roles de los recursos humanos que participan en el Gobierno de Datos.
- ✓ Políticas, Lineamientos, estándares y procesos a gobernar.
- ✓ Una infraestructura física para establecer la red de datos e información.
- ✓ Fuentes de Información de los procesos a gobernar.
- ✓ Herramientas tecnológicas de apoyo.

Las políticas de **GOBIERNO DE DATOS** proporcionan la dirección estratégica y operativa de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**, ya que describen las reglas para controlar la integridad, calidad de los datos, seguridad de la información y administración de los datos así:

6.1. POLITICA INTEGRACIÓN DE DATOS

La **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** garantiza información a las víctimas y al Sistema Nacional de atención y reparación integral a las víctimas (adelante **SNARIV**) a través de consumos directos, o de la interoperabilidad de sistemas de información para soportar sus tareas en información eficiente, veraz, oportuna y precisa.

6.2. POLITICA ADMINISTRACIÓN DE LA CALIDAD DE LOS DATOS

La **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** ofrecerá información confiable a las víctimas y al **SNARIV** aplicando las mejores prácticas y tecnologías para la calidad de datos, que aseguren exactitud, completitud, conformidad y consistencia.

6.3. POLITICA SEGURIDAD DE LA INFORMACIÓN

La **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS**, garantiza el derecho de acceso y uso de los activos informáticos, manteniendo la confidencialidad, integridad y disponibilidad de la información suministrada y/o solicitada por las víctimas y/o el **SNARIV**.

6.4. POLITICA ADMINISTRACIÓN DE METADATOS

La **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** reconoce sus datos como activos de valor, por lo que su registro y gestión se realizará de forma adecuada y eficiente, recopilando, almacenando y administrando las diferentes fuentes de información en pro de facilitar su interpretación y consumo a las víctimas y/o el **SNARIV**.

7. VIGENCIA Y ACTUALIZACIÓN DE LAS POLITICAS

Este conjunto de políticas será revisada y actualizada cada año desde la fecha de aprobación o con frecuencia si es necesario, en este sentido, los miembros de la **UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS** que deseen hacer comentarios sobre las políticas pueden hacerlo enviando sus sugerencias al Comité de **GOBIERNO DE DATOS.**