POLÍTICA DE SEGURIDAD DIGITAL

EDUR
Empresa de Desarrollo
Territorial Urbano y Rural de Risaralda

DEPARTAMENTO DE
RISARALDA

Política de Seguridad Digital

Entidad	Empresa de Desarrollo Territorial Urbano y Rural de Risaralda – EDUR
Política	Política de Seguridad Digital
Dimensión MIPG	Gestión con Valores para Resultados (Gobierno Digital – Seguridad Digital)
Proceso(s) responsable(s)	Gestión de Tecnologías de la Información / Direccionamiento Estratégico
Aprobó	Comité Institucional de Gestión y Desempeño
Versión	1
Vigencia	A partir del acto administrativo de adopción, hasta su derogatoria.

1. Introducción

La transformación digital del Estado ha generado nuevas oportunidades para mejorar la gestión pública, optimizar los procesos institucionales y fortalecer la relación entre las entidades y los ciudadanos; sin embargo, este avance también implica nuevos riesgos asociados al manejo de la información y al uso de las tecnologías.

La EDUR reconoce la importancia de proteger adecuadamente la información institucional, los sistemas tecnológicos y los datos que administra en el desarrollo de sus funciones. La seguridad digital se convierte en un elemento fundamental para garantizar la confianza, la transparencia y la continuidad de los servicios que presta la entidad.

La presente política establece los lineamientos generales que orientan la protección de los activos de información, el uso seguro de las tecnologías, la prevención de riesgos y la adopción de buenas prácticas que contribuyan al fortalecimiento de la gestión institucional.

2. Objetivos

2.1. Objetivo general

Establecer los lineamientos institucionales que orienten la gestión de la seguridad digital en la EDUR, con el propósito de proteger la información institucional, los sistemas tecnológicos y los servicios digitales que soportan el desarrollo de las funciones administrativas, técnicas y misionales, promoviendo buenas prácticas en el uso de las tecnologías y la gestión de riesgos asociados.

2.2. Objetivos específicos

- Fortalecer la protección de la información institucional frente a accesos, modificaciones o divulgaciones no autorizadas.
- Prevenir y gestionar oportunamente los riesgos asociados al uso de tecnologías de la información.

- Promover una cultura institucional de seguridad digital mediante sensibilización y capacitación.
- Fortalecer la capacidad de respuesta ante incidentes de seguridad digital.
- Garantizar la disponibilidad y continuidad de los servicios tecnológicos mediante respaldo y recuperación de la información.
- Promover el cumplimiento de la normatividad vigente en materia de seguridad digital y protección de datos.
- Incorporar prácticas de seguridad digital en los procesos administrativos, técnicos y misionales de la entidad.

3. Alcance

Aplica a todos los servidores públicos, contratistas, practicantes, proveedores y terceros que, en el desarrollo de sus funciones o actividades contractuales, tengan acceso a la información institucional, a los sistemas de información o a la infraestructura tecnológica de la entidad.

Comprende todos los activos de información y recursos tecnológicos —equipos de cómputo, servidores, redes, sistemas de información, bases de datos, plataformas digitales, aplicaciones, servicios en la nube y correo institucional— y la información en cualquier forma o formato, en todas las etapas de su ciclo de vida: creación, almacenamiento, procesamiento, uso, intercambio, conservación y disposición final.

4. Marco normativo

NORMA	DESCRIPCIÓN
Constitución Política de Colombia (1991)	Reconoce el derecho a la intimidad, el habeas data y la protección de la información personal.
Ley 527 de 1999	Regula el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales.
Ley 1273 de 2009	Tipifica los delitos informáticos y protege la información, los datos y los sistemas que usan tecnologías de la información.
Ley 1581 de 2012	Define los principios, derechos y procedimientos para la protección de los datos personales.
Ley 1712 de 2014	Regula el derecho de acceso a la información pública y la transparencia en la gestión del Estado.
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector TIC; incluye la política de Gobierno Digital y la seguridad de la información.
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital; lineamientos de gestión de riesgos y ciberseguridad.
Resolución 500 de 2021 (MinTIC)	Adopta lineamientos de seguridad digital y el Modelo de Seguridad y Privacidad de la Información (MSPI).

NORMA	DESCRIPCIÓN
Decreto 767 de 2022	Actualiza la Política de Gobierno Digital en Colombia.
Modelo de Seguridad y Privacidad de la Información (MSPI)	Orienta la implementación de controles, procedimientos y buenas prácticas para proteger la información y gestionar los riesgos digitales.

5. Definiciones

Activo de información: todo recurso (datos, documentos, sistemas, equipos o servicios) que contiene o procesa información institucional y que tiene valor para la entidad.

Confidencialidad: garantía de que la información solo sea consultada o utilizada por las personas debidamente autorizadas.

Integridad: condición que asegura que la información se mantenga completa, veraz y confiable, sin alteraciones no autorizadas.

Disponibilidad: garantía de que la información y los sistemas estén accesibles cuando los usuarios autorizados los requieran.

Incidente de seguridad digital: evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información o los sistemas.

MSPI: Modelo de Seguridad y Privacidad de la Información del MinTIC, habilitador de la Política de Gobierno Digital.

6. Declaración de política y lineamientos

6.1. Principios

La gestión de la seguridad digital se orienta por los principios de confidencialidad, integridad y disponibilidad de la información, así como por la responsabilidad en el uso de los recursos, la prevención de riesgos, la mejora continua y el fomento de una cultura institucional de seguridad digital.

6.2. Gestión de activos y control de acceso

- Identificación, registro y clasificación de los activos de información de los procesos institucionales.
- Acceso a sistemas y recursos otorgado únicamente a usuarios autorizados, con mecanismos de autenticación y control.

6.3. Uso adecuado de recursos y protección frente a amenazas

- Uso responsable y exclusivamente institucional de equipos, redes, aplicaciones y correo electrónico.
- Mecanismos para prevenir, detectar y mitigar virus, software malicioso y accesos indebidos, con actualizaciones periódicas.

6.4. Gestión de incidentes, respaldo y continuidad

- Procedimientos para identificar, reportar, analizar y atender oportunamente los incidentes de seguridad digital.
- Respaldo periódico y recuperación de la información para asegurar la continuidad de las operaciones.

6.5. Protección de datos y sensibilización

- Tratamiento de datos personales conforme a la normativa vigente.
- Actividades de capacitación y sensibilización sobre buenas prácticas de seguridad digital.

6.6. Gestión de riesgos asociados

Tipo de riesgo	Descripción	Medidas de prevención y control
Confidencialidad	Acceso no autorizado a información institucional sensible o estratégica.	Control de acceso por roles, mecanismos de autenticación y reserva de la información.
Integridad	Alteración, modificación o eliminación no autorizada de datos.	Controles de cambios, registros de actividad y trazabilidad de la información.
Disponibilidad	Pérdida de información, fallas o caída de los sistemas y servicios.	Copias de seguridad periódicas, planes de recuperación y de contingencia.
Amenazas informáticas	Virus, software malicioso o ataques cibernéticos contra la infraestructura.	Herramientas de protección, actualización permanente y uso seguro de dispositivos y redes.
Cumplimiento / datos personales	Incumplimiento de la normativa de protección de datos y de seguridad digital.	Tratamiento de datos conforme a la ley, sensibilización y verificación de cumplimiento.

7. Roles y responsabilidades

ROL	RESPONSABILIDAD
Gerencia General	Orienta y respalda la implementación de la política y garantiza la asignación de los recursos necesarios.
Oficina de Planeación	Coordina el seguimiento y la evaluación y articula la política con el MIPG y los planes institucionales.
Área de Tecnologías de la Información / Sistemas	Administra la infraestructura, implementa las medidas técnicas, monitorea los sistemas, gestiona las copias de seguridad y atiende los incidentes.
Dependencias de la entidad	Garantizan el cumplimiento de los lineamientos en sus procesos y promueven el uso adecuado de los recursos tecnológicos.

ROL	RESPONSABILIDAD
Servidores públicos y contratistas	Hacen uso responsable de los recursos, cumplen los lineamientos y reportan oportunamente cualquier situación de riesgo.
Proveedores y terceros	Cumplen los lineamientos de seguridad y garantizan el manejo adecuado de la información a la que tengan acceso.

8. Articulación con el MIPG y con los planes institucionales

La política opera como habilitador transversal de la Política de Gobierno Digital dentro del MIPG y adopta el Modelo de Seguridad y Privacidad de la Información (MSPI). Sus actividades se integran al Plan de Acción institucional y se articulan con el Sistema de Control Interno y con los reportes del FURAG.

9. Seguimiento, indicadores y evaluación

La Oficina de Planeación, en articulación con el área de Sistemas, lidera el seguimiento a la implementación de la política mediante los siguientes indicadores:

- Nivel de implementación de los lineamientos de seguridad digital (semestral).
- Porcentaje de incidentes de seguridad digital gestionados oportunamente (semestral).
- Nivel de servidores públicos y contratistas capacitados en seguridad digital (anual).
- Cumplimiento de las copias de seguridad de la información institucional (trimestral).
- Nivel de actualización de los sistemas tecnológicos institucionales (semestral).

Los resultados se analizan para adoptar acciones correctivas, preventivas o de mejora, y se articulan con el MIPG, el control interno y los reportes del FURAG.

10. Control de cambios

Versión	Fecha	Descripción del cambio	Responsable
1	DD/MM/AAAA	Versión inicial estandarizada	Equipo MIPG

11. Aprobación y publicación

Aprobada por el Comité Institucional de Gestión y Desempeño de la EDUR y publicada en los canales oficiales de la entidad conforme a la Ley 1712 de 2014. Entrará en vigencia a partir de su adopción mediante el acto administrativo correspondiente y será revisada y actualizada periódicamente conforme a los cambios tecnológicos, normativos y a la evolución de los riesgos digitales.