# PRINCIPIO 6. SEGURIDAD DE LA INFORMACIÓN

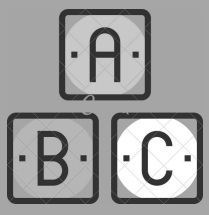
La información está protegida en sus tres principales componentes, confiabilidad, integridad y disponibilidad y de acuerdo a su clasificación se controla la divulgación y uso no autorizado.

## IMPLICACIONES

- Como estrategia para preservar la seguridad de la información, se deben establecer políticas que permitan detectar riesgos y establecer controles de seguridad, tecnologías y procedimientos para proteger y salvaguardar la información.
- Establecer un Sistema de Gestión de Seguridad de la Información, que permita minimizar y controlar los riesgos, de tal forma que se proteja los principios básicos de los datos: confidencialidad, disponibilidad e integridad.
- Tener un procedimiento para clasificación de la Información, establecer revisiones periódicas a los datos y mecanismos de acceso y control para la gestión de los datos.
- La información debe ser protegida contra accesos no autorizados que impliquen manipulación y modificación.
- Establecer mecanismos de seguimiento y control.
- La entidad deberá proporcionar los recursos humanos, técnicos y económicos para garantizar la seguridad de la información.
- Actualización periódica de las políticas y objetivos de seguridad de la información.

# PRINCIPIO: SEGURIDAD DE LA INFORMACIÓN

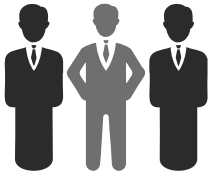
## POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN




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

El Departamento Administrativo para la Prosperidad Social estructura las responsabilidades para la gestión de la seguridad de información, claramente separadas y asignadas, incluyendo el Comité institucional de Gestión y Desempeño.

### POLÍTICA 2. SEGURIDAD DEL RECURSO HUMANO



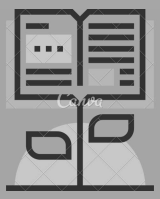
El Departamento Administrativo para la Prosperidad Social asegura que los servidores públicos, contratistas y pasantes comprendan sus responsabilidades durante la relación laboral o contractual; también garantiza el entendimiento de lo anterior, mediante la debida instrucción, socialización y suscripción de acuerdos de confidencialidad.

## POLÍTICA 3. GESTIÓN DE ACTIVOS

Los activos de información del Departamento Administrativo para la Prosperidad Social son inventariados, revisados periódicamente y asignados a un responsable; sobre estos activos se establecen niveles de protección, acceso y procedimientos para su utilización

## POLÍTICA 4. CONTROL DE ACCESO

El Departamento Administrativo para la Prosperidad Social establece las medidas de control de acceso a nivel de red, sistema operativo, base de datos, aplicaciones y acceso físico para garantizar confidencialidad de la información.

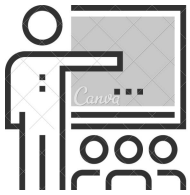


## POLÍTICA 5. CRIPTOGRAFÍA

El Departamento Administrativo para la Prosperidad Social utiliza algoritmos criptográficos fuertes para la protección de los activos de información, claves, aplicaciones, redes de telecomunicaciones, datos sensibles y demás que considere relevante.

## POLÍTICA 6. SEGURIDAD FÍSICA Y DEL ENTORNO

El Departamento Administrativo para la Prosperidad Social, establece controles para prevenir el acceso físico no autorizado y los daños por amenazas ambientales en las distintas sedes, para garantizar la disponibilidad, integridad y disponibilidad de la información. .

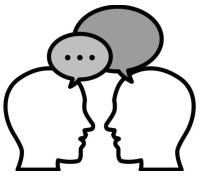


## POLÍTICA 7. SEGURIDAD DE LAS OPERACIONES

El Departamento Administrativo para la Prosperidad Social establece los procedimientos y responsabilidades de administración y seguridad pertinentes a cada ambiente tecnológico, de forma que garantice una debida gestión de cambios, gestión de la capacidad, copias de respaldo, trazabilidad de logs, gestión de vulnerabilidad, control de software operacional, separación de ambientes de desarrollo y protección contra código malicioso.

## POLÍTICA 8. SEGURIDAD EN LAS COMUNICACIONES

El Departamento Administrativo para la Prosperidad Social, asegura la protección de las redes de telecomunicaciones para evitar el acceso no autorizado a la información que se transmite en las redes y comunicaciones que utiliza la entidad.



## POLÍTICA 9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

El Departamento Administrativo para la Prosperidad Social realiza análisis e implementación de los requerimientos de seguridad en los sistemas de información desarrollados internamente y/o adquiridos, que incluyen validación de usuarios, datos de entrada y salida y el procesamiento de los mismos.

Los propietarios de los sistemas de información deben considerar los requerimientos de seguridad necesarios para mantener la integridad, confidencialidad y disponibilidad, durante todo del ciclo de vida de los mismos y la incorporación de controles relevantes.

## POLÍTICA 10. RELACIONES CON LOS PROVEEDORES

El Departamento Administrativo para la Prosperidad Social establece e implementa lineamientos y controles para que los proveedores, contratistas y terceros adopten un manejo seguro de la información acorde al Sistema de Gestión de Seguridad de la Información - SGSI de la Entidad. Estableciendo un marco de colaboración equilibrado que preserve la confidencialidad, integridad y disponibilidad de la información de la Entidad.

## POLÍTICA 11. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

El Departamento Administrativo para la Prosperidad Social promueve la debida gestión de los incidentes de Seguridad de la información, estableciendo el procedimiento, para el manejo, y atención de estos.

## POLÍTICA 12. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO.

El Departamento Administrativo para la Prosperidad Social establece los planes de contingencia tecnológica de los sistemas de información críticos para la Entidad.

## POLÍTICA 13. CUMPLIMIENTO

El Departamento Administrativo para la Prosperidad Social cumple con los requisitos legales internos y externos aplicables a la Seguridad de la Información que gestiona, incluye entre otros los derechos de propiedad intelectual, protección de datos personales, tiempos de retención de registros, privacidad de información, uso debido de los recursos de procesamiento, y recolección de evidencia y auditorías.