IDECESAR

Instituto para el Desarrollo del Cesar

PLAN DE SEGURIDAD DE LA INFORMACION

2026 - 2027

INDICE

INTRODUCCIÓN

El presente Plan de Seguridad de la Información establece los lineamientos, controles y acciones necesarias para proteger la confidencialidad, integridad y disponibilidad de la información de IDECESAR, garantizando el cumplimiento normativo y la continuidad de los servicios institucionales.

El Instituto para el Desarrollo del Cesar – **IDECESAR** – en cumplimiento de su misión institucional y su responsabilidad como entidad pública del orden territorial, reconoce que la información constituye uno de sus activos más valiosos y estratégicos para la gestión administrativa, financiera, operativa y misional. En un entorno caracterizado por la transformación digital, la interconectividad de los sistemas y el incremento de riesgos cibernéticos, se hace indispensable establecer un marco estructurado que garantice la protección adecuada de los activos de información frente a amenazas internas y externas.

El presente **Plan de Seguridad de la Información de IDECESAR** se formula como un instrumento técnico, estratégico y normativo que orienta la implementación de controles, políticas, procedimientos y buenas prácticas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información institucional. Este plan se encuentra alineado con los lineamientos del Gobierno Digital en Colombia, el Modelo de Seguridad y Privacidad de la Información (MSPI), y las mejores prácticas internacionales en materia de gestión de seguridad de la información, tales como las establecidas en la norma ISO/IEC 27001.

En el contexto institucional de IDECESAR, la información se genera, procesa, almacena y transmite a través de múltiples plataformas tecnológicas, bases de datos, sistemas de información financieros y administrativos, equipos de cómputo, redes internas y servicios en la nube. Estos activos soportan procesos críticos como la gestión de créditos, cartera, contabilidad, contratación, talento humano, atención al ciudadano y gestión documental. La interrupción, alteración o divulgación no autorizada de dicha información podría generar impactos significativos en la operación institucional, en la confianza de los usuarios y en el cumplimiento de las obligaciones legales.

Por lo anterior, el Plan de Seguridad de la Información establece un marco integral que contempla:

- La identificación y clasificación de activos de información.
- La gestión y tratamiento de riesgos de seguridad y privacidad.
- La definición de políticas de control de acceso y gestión de identidades.
- La protección de la infraestructura tecnológica y de las redes institucionales.
- La implementación de mecanismos de respaldo y recuperación ante desastres.
- La gestión de incidentes de seguridad de la información.

- La sensibilización y capacitación permanente del talento humano.

Asimismo, este plan promueve una cultura organizacional basada en la responsabilidad, la ética y el uso adecuado de los recursos tecnológicos. La seguridad de la información no es exclusivamente una función del área TIC, sino una responsabilidad compartida por todos los servidores públicos, contratistas y terceros que tengan acceso a los activos de información de IDECESAR.

La adopción de este plan también responde a la necesidad de fortalecer los mecanismos de control interno, garantizar el cumplimiento de la normativa vigente en materia de protección de datos personales, transparencia y acceso a la información pública, y mejorar los niveles de madurez institucional en seguridad digital. De esta manera, IDECESAR avanza hacia una gestión más confiable, resiliente y preparada frente a riesgos tecnológicos y amenazas emergentes.

En consecuencia, el Plan de Seguridad de la Información se constituye en un componente fundamental del PETI institucional y de la Arquitectura Empresarial definida por la entidad, asegurando que las iniciativas tecnológicas estén respaldadas por un enfoque preventivo y estructurado de gestión de riesgos. Su implementación progresiva permitirá consolidar un entorno tecnológico seguro, robusto y alineado con los objetivos estratégicos de IDECESAR, contribuyendo al fortalecimiento institucional y a la generación de confianza en los ciudadanos y grupos de interés.

OBJETIVO GENERAL

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que permita gestionar riesgos, proteger los activos de información y fortalecer la confianza de ciudadanos, aliados y entes de control.

OBJETIVOS ESPECÍFICOS

- Identificar y clasificar los activos de información.
- Gestionar riesgos de seguridad y privacidad.
- Implementar controles técnicos, administrativos y físicos.
- Fortalecer la cultura de seguridad digital.
- Cumplir con la normatividad vigente en protección de datos y gobierno digital.

ALCANCE

El presente Plan de Seguridad de la Información de IDECESAR establece el marco integral de protección de los activos de información institucionales, definiendo el alcance organizacional, técnico, normativo y operativo bajo el cual se implementarán las políticas, controles y procedimientos orientados a garantizar la **confidencialidad, integridad, disponibilidad y autenticidad** de la información.

Alcance Organizacional

El Plan aplica a:

- Todos los procesos estratégicos, misionales, de apoyo y de evaluación de IDECESAR.
- Todas las dependencias administrativas y operativas.
- Funcionarios de planta, contratistas, pasantes, proveedores y terceros que tengan acceso a información institucional.
- Miembros de comités, aliados estratégicos y cualquier parte interesada que interactúe con los sistemas de información de la entidad.

La responsabilidad de cumplimiento es transversal a toda la entidad, bajo el liderazgo de la Alta Dirección y la coordinación del área TIC.

Alcance de la Información

El Plan cubre todos los activos de información, independientemente de su formato o medio de almacenamiento, incluyendo:

- Información financiera y contable.
- Información crediticia y de cartera.
- Información administrativa y contractual.
- Bases de datos institucionales.
- Información personal de clientes, beneficiarios y funcionarios.
- Documentación física y digital.
- Correos electrónicos institucionales.

- Copias de seguridad.
- Información almacenada en servicios en la nube.
- Sistemas de gestión documental.
- Información publicada en portales web institucionales.

Incluye tanto la información generada internamente como aquella recibida de otras entidades públicas, privadas o ciudadanos.

Alcance Tecnológico

El Plan aplica a toda la infraestructura tecnológica de IDECESAR, incluyendo:

- Servidores físicos y virtuales.
- Equipos de cómputo de escritorio y portátiles.
- Dispositivos móviles institucionales.
- Equipos de red (switches, routers, firewall).
- Impresoras en red.
- Sistemas de almacenamiento.
- Sistemas de videovigilancia asociados a red.
- Plataformas en la nube.
- Software institucional (financiero, contable, gestión documental, antivirus corporativo, sistemas misionales).
- Redes internas (LAN), redes inalámbricas (WiFi) y conexiones a internet.
- Sistemas de respaldo y recuperación ante desastres.

Incluye también los mecanismos de control de acceso lógico, autenticación, gestión de usuarios y perfiles, así como la protección perimetral y seguridad de endpoints.

Alcance Normativo

El Plan se enmarca en el cumplimiento de:

- La Política de Gobierno Digital del Estado Colombiano.

- La Ley 1581 de 2012 (Protección de Datos Personales).
- La Ley 1712 de 2014 (Transparencia y Acceso a la Información Pública).
- El Modelo de Seguridad y Privacidad de la Información – MSPI.
- Lineamientos del Ministerio TIC.
- Estándares internacionales como ISO/IEC 27001 e ISO/IEC 27002 (como marco de referencia).
- Normativa interna y manuales institucionales.

Este alcance garantiza que el plan no solo sea técnico, sino también jurídico y regulatorio.

Alcance en Gestión de Riesgos

El Plan cubre la identificación, análisis, evaluación y tratamiento de riesgos asociados a:

- Ciberataques (ransomware, malware, phishing).
- Fugas de información.
- Accesos no autorizados.
- Pérdida de información por fallas técnicas.
- Desastres naturales.
- Errores humanos.
- Uso indebido de software no licenciado.
- Fallas en proveedores tecnológicos.

Incluye la implementación de controles preventivos, detectivos y correctivos, así como planes de continuidad del negocio y recuperación ante desastres.

Alcance en Seguridad Física y Ambiental

El Plan contempla medidas de protección sobre:

- Áreas de servidores y centros de datos.
- Control de acceso físico a oficinas.
- Protección contra incendios.

- Sistemas eléctricos regulados y UPS.
- Condiciones ambientales para equipos críticos.
- Custodia de archivos físicos sensibles.

Alcance en Cultura y Concientización

Incluye programas permanentes de:

- Capacitación en seguridad digital.
- Sensibilización sobre protección de datos.
- Buenas prácticas en el uso de equipos y contraseñas.
- Prevención del phishing y fraude electrónico.
- Uso adecuado del correo institucional y navegación en internet.

La cultura de seguridad es considerada un pilar fundamental para la sostenibilidad del sistema.

Alcance en Continuidad y Recuperación

El Plan contempla:

- Estrategias de copias de seguridad periódicas.
- Pruebas de restauración.
- Plan de continuidad del negocio (BCP).
- Plan de recuperación ante desastres (DRP).
- Protocolos de respuesta ante incidentes de seguridad.
- Roles y responsabilidades frente a emergencias tecnológicas.

Alcance Temporal

El Plan tiene un alcance estratégico alineado al PETI institucional y deberá:

- Ser revisado anualmente.

- Actualizarse ante cambios tecnológicos o normativos.
- Ajustarse tras incidentes significativos.
- Medirse mediante indicadores de desempeño en seguridad.

Exclusiones del Alcance

No se consideran dentro del alcance:

- Equipos personales no autorizados que no estén conectados a la red institucional.
- Sistemas externos que no tengan relación contractual o técnica con IDECESAR.
- Información de terceros que no sea administrada por la entidad.

Aplica a:

- Todos los procesos estratégicos, misionales, de apoyo y evaluación.
- Funcionarios, contratistas y terceros.
- Sistemas de información, infraestructura tecnológica y archivos físicos.
- Información en formato físico y digital.

MARCO NORMATIVO

- Política de Gobierno Digital.
- Modelo de Seguridad y Privacidad de la Información (MSPI).
- Ley 1581 de 2012 – Protección de Datos Personales.
- Decreto 1078 de 2015.
- Lineamientos de MIPG.
- Norma ISO/IEC 27001 (como referencia técnica).

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Declaración de la Política

El Instituto para el Desarrollo del Cesar – IDECESAR, en cumplimiento de su misión institucional y del marco normativo vigente en materia de Gobierno Digital, protección de datos personales y gestión de riesgos, establece la presente Política de Seguridad de la Información como instrumento rector para la protección de sus activos de información.

Esta política tiene como propósito garantizar la **confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad** de la información institucional, mediante la implementación de controles administrativos, técnicos, físicos y legales que permitan prevenir, detectar, responder y recuperar la información ante amenazas internas y externas.

La Alta Dirección de IDECESAR asume el compromiso de liderar, respaldar y promover la cultura de seguridad de la información en toda la entidad.

Objetivo

Establecer los lineamientos generales para la gestión de la seguridad de la información en IDECESAR, asegurando:

- La protección de los activos de información.
- La continuidad de los servicios institucionales.
- El cumplimiento de la normativa legal aplicable.
- La mitigación de riesgos tecnológicos.
- La protección de los datos personales de clientes, funcionarios y terceros.

Alcance

La presente política aplica a:

- Todos los procesos estratégicos, misionales, de apoyo y de evaluación.
- Funcionarios de planta, contratistas, proveedores y terceros.
- Infraestructura tecnológica (servidores, equipos de cómputo, redes, software).

- Información en formato físico y digital.
- Sistemas internos y servicios en la nube.
- Bases de datos institucionales.
- Correo electrónico institucional y plataformas digitales.

Principios de Seguridad de la Información

La gestión de la seguridad en IDECESAR se fundamenta en los siguientes principios:

Confidencialidad

La información solo será accesible por personas autorizadas.

Integridad

La información debe mantenerse completa, exacta y protegida contra modificaciones no autorizadas.

Disponibilidad

La información y los sistemas deberán estar disponibles cuando sean requeridos para el cumplimiento de la misión institucional.

Legalidad

Toda gestión de información deberá cumplir con la normatividad vigente.

Responsabilidad

Todos los funcionarios son responsables de proteger la información bajo su custodia.

Gestión del Riesgo

La seguridad se gestionará bajo un enfoque preventivo basado en la identificación y tratamiento de riesgos.

Lineamientos Generales

Garantizar la aplicación efectiva de esta política, IDECESAR establece los siguientes lineamientos:

Gestión de Accesos

- Los usuarios solo tendrán acceso a la información necesaria para el desempeño de sus funciones.
- Se prohíbe compartir credenciales.
- Se implementará control de acceso mediante usuario y contraseña robusta.
- Los usuarios no deberán contar con privilegios de administrador local salvo autorización formal.

Uso Aceptable de Recursos Tecnológicos

- Los recursos tecnológicos son para uso institucional.
- Se prohíbe la instalación de software no autorizado o sin licencia.
- No se permitirá el uso de dispositivos externos sin autorización.
- El acceso a internet deberá realizarse bajo criterios de seguridad y productividad.

Protección contra Malware

- Se implementará antivirus corporativo centralizado.
- Se mantendrán actualizados los sistemas operativos y aplicaciones.
- Se aplicarán políticas de seguridad perimetral (firewall y control de tráfico).

Copias de Seguridad

- Se realizarán copias de seguridad periódicas de la información crítica.
- Las copias deberán almacenarse en ubicación segura.
- Se realizarán pruebas de restauración periódicas.

Seguridad Física

- El acceso al área de servidores estará restringido.
- Se implementarán controles ambientales y eléctricos adecuados.
- Los documentos físicos sensibles deberán estar bajo custodia.

Gestión de Incidentes

- Todo incidente de seguridad deberá ser reportado inmediatamente.
- Se contará con un procedimiento formal de atención de incidentes.
- Se realizará análisis de causa raíz y acciones correctivas.

Protección de Datos Personales

- Se garantizará el cumplimiento de la Ley 1581 de 2012.
- Se implementarán medidas de protección para datos sensibles.
- Se respetarán los derechos de los titulares de la información.

Continuidad del Negocio

- Se implementará un Plan de Continuidad del Negocio.
- Se definirá un Plan de Recuperación ante Desastres (DRP).
- Se identificarán procesos críticos y tiempos máximos de recuperación.

Roles y Responsabilidades

Alta Dirección

- Aprobar la política.
- Asignar recursos para su implementación.
- Hacer seguimiento al cumplimiento.

Área TIC

- Implementar controles técnicos.
- Administrar la infraestructura tecnológica.
- Monitorear riesgos tecnológicos.
- Gestionar incidentes de seguridad.

Funcionarios y Contratistas

- Cumplir la política.
- Proteger las credenciales.
- Reportar incidentes.
- Participar en capacitaciones.

Cumplimiento y Sanciones

El incumplimiento de esta política podrá generar:

- Llamados de atención.
- Procesos disciplinarios.
- Terminación contractual.

- Acciones legales si aplica.

Revisión y Actualización

La presente política será:

- Revisada anualmente.
- Actualizada cuando existan cambios tecnológicos o normativos.
- Ajustada posterior a incidentes relevantes.

GOBERNANZA DE SEGURIDAD

Responsables

- **Gerencia General**: Aprobación del plan.
- **Oficina TIC**: Implementación técnica.
- **Líderes de proceso**: Custodia de información.
- **Oficina Jurídica**: Cumplimiento normativo.
- **Control Interno**: Seguimiento y evaluación.

IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS

La Identificación y Clasificación de Activos de Información constituye un componente fundamental del Plan de Seguridad de la Información de IDECESAR, ya que permite reconocer los recursos que soportan la misión institucional y establecer los niveles de protección adecuados según su criticidad.

Un activo de información es cualquier elemento que tenga valor para la entidad y cuya pérdida, alteración, divulgación no autorizada o indisponibilidad pueda afectar el cumplimiento de los objetivos institucionales.

Objetivo

- Identificar los activos de información de IDECESAR.
- Clasificarlos según su nivel de criticidad.
- Asignar responsables (propietarios del activo).
- Establecer criterios para su protección.

- Servir de base para la gestión de riesgos de seguridad de la información.

Tipología de Activos

En IDECESAR los activos se clasifican en las siguientes categorías:

Activos de Información

- Bases de datos de clientes y beneficiarios.
- Información financiera y contable.
- Información crediticia y cartera.
- Contratos y documentos jurídicos.
- Información presupuestal.
- Historias crediticias.
- Informes de gestión.
- Datos personales sensibles.
- Archivos físicos institucionales.
- Copias de seguridad.

Activos de Software

- Sistema contable institucional.
- Software de cartera.
- Sistema de gestión documental.
- Antivirus corporativo.
- Sistema operativo de servidores.
- Aplicaciones en la nube.
- Correo institucional.

Activos de Hardware

- Servidores físicos y virtuales.
- Equipos de cómputo de escritorio.
- Portátiles institucionales.

- Impresoras de red.
- Equipos de almacenamiento.
- Equipos de red (router, switch, firewall).
- UPS y sistemas eléctricos regulados.

Activos de Servicios

- Servicio de internet.
- Hosting del sitio web institucional.
- Servicios en la nube.
- Soporte técnico externo.
- Servicios de respaldo externo.

Activos Humanos

- Funcionarios.
- Contratistas.
- Administradores TIC.
- Directivos.

Activos Físicos

- Centro de datos o cuarto de servidores.
- Archivos físicos.
- Oficinas administrativas.

Criterios de Clasificación de la Información

La información de IDECESAR se clasificará bajo los siguientes niveles:

Información Pública

Información que puede ser divulgada sin afectar a la entidad.

Ejemplos:

- Información publicada en la página web.
- Informes de gestión públicos.
- Información de transparencia.

Información de Uso Interno

Información destinada únicamente al uso de funcionarios y contratistas autorizados.

Ejemplos:

- Comunicaciones internas.
- Procedimientos administrativos.
- Informes preliminares.

Información Confidencial

Información cuyo acceso no autorizado puede generar afectación financiera, legal o reputacional.

Ejemplos:

- Información financiera detallada.
- Bases de datos de clientes.
- Información contractual en proceso.
- Credenciales de acceso.
- Configuración de servidores.

Información Sensible o Crítica

Información cuya divulgación o pérdida puede generar impacto grave en la operación institucional o violar derechos fundamentales.

Ejemplos:

- Datos personales sensibles.
- Información crediticia detallada.
- Copias de seguridad completas.
- Claves maestras y certificados digitales.

Criterios de Valoración del Activo

Cada activo deberá evaluarse según:

- **Impacto en la confidencialidad**
- **Impacto en la integridad**
- **Impacto en la disponibilidad**
- **Impacto legal**
- **Impacto reputacional**

- **Impacto financiero**

La valoración podrá clasificarse en:

- Alto
- Medio
- Bajo

Matriz General de Identificación de Activos (Ejemplo Base)

Activo	Tipo	Responsable	Clasificación	Criticidad
Base de datos de cartera	Información	Área Financiera	Confidencial	Alta
Servidor principal	Hardware	Área TIC	Crítica	Alta
Sistema contable	Software	Área Financiera / TIC	Confidencial	Alta
Página web institucional	Servicio	Área TIC	Pública	Media
Equipos de escritorio	Hardware	TIC	Uso Interno	Media
Copias de seguridad	Información	TIC	Sensible	Alta

Responsabilidad sobre los Activos

Cada activo deberá contar con:

- **Propietario del Activo:** Responsable funcional de la información.
- **Custodio Técnico:** Responsable de su protección técnica (Área TIC).
- **Usuarios Autorizados:** Personas con acceso permitido.

Lineamientos de Protección según Clasificación

Información Pública

- Puede divulgarse.
- Debe garantizarse integridad.

Uso Interno

- Acceso controlado.
- No se permite divulgación externa sin autorización.

Confidencial

- Control de acceso por roles.
- Cifrado cuando sea posible.

- Copias de seguridad protegidas.
- Registro de accesos.

Sensible o Crítica

- Acceso estrictamente restringido.
- Autenticación robusta.
- Cifrado obligatorio.
- Monitoreo continuo.
- Respaldo frecuente.
- Plan de recuperación definido.

Actualización del Inventario de Activos

- El inventario deberá actualizarse mínimo una vez al año.
- Debe actualizarse cuando se adquieran nuevos sistemas o equipos.
- Debe revisarse tras incidentes de seguridad.
- Debe estar alineado con el PETI institucional.

GESTIÓN DE RIESGOS

Introducción

La Gestión del Riesgo en Seguridad de la Información de IDECESAR establece el marco metodológico para identificar, analizar, evaluar, tratar y monitorear los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información institucionales.

Este proceso permite anticipar amenazas internas y externas, reducir la probabilidad de incidentes de seguridad y minimizar su impacto en la operación, la estabilidad financiera y la reputación de la entidad.

Objetivo

Implementar un proceso sistemático y continuo de gestión de riesgos que permita:

- Identificar amenazas y vulnerabilidades.
- Valorar los riesgos asociados a los activos de información.
- Definir controles adecuados.

- Reducir la probabilidad de materialización de incidentes.
- Garantizar la continuidad operativa de IDECESAR.

Marco de Referencia

La Gestión del Riesgo de IDECESAR se fundamenta en:

- El Modelo de Seguridad y Privacidad de la Información (MSPI).
- La Política de Gobierno Digital.
- Buenas prácticas internacionales como ISO/IEC 27001 e ISO/IEC 27005.
- Lineamientos del Ministerio TIC.
- Metodología de Administración del Riesgo adoptada por la entidad.

Alcance de la Gestión del Riesgo

Aplica a:

- Procesos estratégicos, misionales y de apoyo.
- Infraestructura tecnológica.
- Sistemas de información.
- Bases de datos institucionales.
- Información física y digital.
- Servicios en la nube.
- Recursos humanos con acceso a información.

Metodología de Gestión del Riesgo

La gestión del riesgo en IDECESAR se desarrolla en las siguientes fases:

Identificación del Riesgo

Consiste en identificar:

- Activos de información.
- Amenazas (internas y externas).
- Vulnerabilidades.
- Impactos potenciales.

Ejemplos de Amenazas:

- Ataques ransomware.

- Phishing.
- Acceso no autorizado.
- Falla de servidores.
- Pérdida de energía eléctrica.
- Error humano.
- Instalación de software no licenciado.
- Desastres naturales.

Análisis del Riesgo

Se determina:

- Probabilidad de ocurrencia (Alta, Media, Baja).
- Impacto (Alto, Medio, Bajo).

Se analiza el riesgo en términos de:

- Impacto financiero.
- Impacto operativo.
- Impacto legal.
- Impacto reputacional.
- Impacto en la prestación del servicio.

Evaluación del Riesgo

Se determina el nivel de riesgo mediante la siguiente fórmula:

Nivel de Riesgo = Probabilidad x Impacto

Clasificación:

- Riesgo Alto → Requiere tratamiento inmediato.
- Riesgo Medio → Requiere plan de mitigación.
- Riesgo Bajo → Aceptable con monitoreo.

Tratamiento del Riesgo

Las opciones de tratamiento incluyen:

1. **Mitigar:** Implementar controles.
2. **Aceptar:** Asumir el riesgo cuando es bajo.

3. **Transferir:** A través de seguros o contratos.
4. **Evitar:** Eliminar la actividad que genera el riesgo.

Monitoreo y Revisión

- Seguimiento periódico de riesgos.
- Revisión anual del mapa de riesgos.
- Actualización tras incidentes.
- Auditorías internas.

Matriz de Riesgos – IDECESAR

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Nivel	Tratamiento
Base de datos cartera	Ransomware	Falta de actualización	Alto	Media	Alto	Antivirus, backups, firewall
Servidor principal	Falla eléctrica	Sin planta alterna	Alto	Media	Alto	UPS y plan de contingencia
Correo institucional	Phishing	Falta de capacitación	Medio	Alta	Alto	Capacitación y filtros antispam
Equipos usuarios	Software ilegal	Permisos administrador	Medio	Media	Medio	Restricción de privilegios

Controles de Seguridad Implementados

Controles Preventivos

- Antivirus corporativo centralizado.
- Políticas de control de acceso.
- Restricción de privilegios de administrador.
- Firewall perimetral.
- Políticas de contraseñas robustas.
- Capacitación al personal.

Controles Detectivos

- Monitoreo de logs.

- Alertas de seguridad.
- Auditorías internas.
- Supervisión de tráfico de red.

Controles Correctivos

- Restauración de copias de seguridad.
- Procedimiento de gestión de incidentes.
- Acciones disciplinarias.
- Reconfiguración de sistemas vulnerados.

Roles y Responsabilidades

Alta Dirección

- Aprobar la metodología.
- Asignar recursos.
- Supervisar el mapa de riesgos.

Área TIC

- Identificar riesgos tecnológicos.
- Implementar controles.
- Monitorear amenazas.
- Gestionar incidentes.

Líderes de Proceso

- Identificar riesgos en su área.
- Reportar vulnerabilidades.
- Apoyar planes de mitigación.

Indicadores de Seguimiento

- Número de incidentes reportados.
- Tiempo promedio de respuesta.
- Porcentaje de equipos actualizados.
- Nivel de cumplimiento de controles.
- Número de respaldos exitosos.

Mejora Continua

La Gestión del Riesgo en IDECESAR será un proceso dinámico y continuo, alineado al PETI institucional y sujeto a:

- Evaluación anual.
- Auditorías internas.
- Ajustes ante cambios tecnológicos.
- Actualización normativa.
- Lecciones aprendidas de incidentes.

CONTROLES DE SEGURIDAD

Introducción

Los Controles de Seguridad de la Información de IDECESAR establecen el conjunto de medidas administrativas, técnicas, físicas y legales orientadas a proteger los activos institucionales frente a amenazas internas y externas.

Estos controles están alineados con el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Gobierno Digital y buenas prácticas basadas en ISO 27001, adaptadas a la realidad operativa de la entidad.

Controles Administrativos

Política y Gobierno de Seguridad

- Aprobación formal de la Política de Seguridad.
- Designación de responsable de Seguridad de la Información.
- Creación de Comité de Seguridad de la Información.
- Revisión anual del Plan de Seguridad.

Gestión de Activos

- Inventario actualizado de activos tecnológicos.
- Clasificación de la información (Pública, Interna, Confidencial, Sensible).
- Asignación de propietarios de activos.
- Etiquetado y registro de equipos institucionales.

Gestión del Riesgo

- Aplicación anual de la matriz de riesgos.
- Actualización tras incidentes.
- Plan de tratamiento de riesgos priorizados.

Gestión de Proveedores

- Cláusulas de confidencialidad en contratos.
- Evaluación de riesgos de terceros.
- Acuerdos de nivel de servicio (SLA).
- Supervisión de proveedores tecnológicos.

Controles de Gestión de Acceso

Control de Acceso Lógico

- Usuarios individuales e intransferibles.
- Política de contraseñas robustas.
- Cambio periódico de contraseñas.
- Bloqueo automático por intentos fallidos.
- Desactivación inmediata de usuarios retirados.

Principio de Mínimo Privilegio

- Restricción de permisos de administrador local.
- Acceso por roles.
- Separación de funciones críticas.

Autenticación Multifactor (MFA)

- Implementación progresiva en sistemas críticos.
- MFA obligatorio para accesos administrativos.

Control de Acceso Físico

- Restricción al centro de datos.
- Registro de visitantes.
- Control de llaves institucionales.

Controles Técnicos

Seguridad Perimetral

- Firewall configurado y actualizado.
- Segmentación de red.
- Monitoreo del tráfico.
- Cierre de puertos innecesarios.

Protección contra Malware

- Antivirus corporativo centralizado.
- Actualizaciones automáticas.
- Escaneo periódico de equipos.

Gestión de Vulnerabilidades

- Actualización periódica de sistemas operativos.
- Aplicación de parches de seguridad.
- Pruebas de vulnerabilidad.

Seguridad en Redes

- Configuración segura de WiFi institucional.
- Cifrado WPA3 o equivalente.
- Cambio de credenciales por defecto.
- Deshabilitar acceso remoto no autorizado.

Seguridad en Servidores

- Configuración segura.
- Registro de logs.
- Monitoreo continuo.
- Redundancia de almacenamiento (RAID).

Seguridad en Equipos de Usuario

- Restricción de instalación de software.
- Bloqueo automático de pantalla.
- Cifrado de discos en portátiles.
- Política de uso aceptable.

Controles de Protección de la Información

Clasificación y Etiquetado

- Marcado de documentos confidenciales.
- Control de distribución de información sensible.

Cifrado

- Cifrado de información sensible.
- Cifrado en tránsito (HTTPS, VPN).
- Cifrado en copias de seguridad críticas.

Gestión Documental

- Control de versiones.
- Trazabilidad de modificaciones.
- Restricción de edición según rol.

Controles de Copias de Seguridad y Continuidad

Copias de Seguridad

- Backups diarios de información crítica.
- Almacenamiento seguro externo o en la nube.
- Pruebas periódicas de restauración.

Plan de Continuidad del Negocio

- Identificación de procesos críticos.
- Definición de RTO y RPO.
- Procedimientos de contingencia documentados.

Plan de Recuperación ante Desastres (DRP)

- Procedimientos técnicos de recuperación.
- Responsables definidos.
- Simulacros anuales.

Controles de Gestión de Incidentes

- Procedimiento formal de reporte de incidentes.
- Registro de incidentes.
- Análisis de causa raíz.

- Plan de mejora posterior al incidente.
- Comunicación a la Alta Dirección.
- Notificación a autoridades cuando aplique.

Controles de Seguridad Física y Ambiental

- Sistema de detección de incendios.
- UPS y protección eléctrica.
- Control de temperatura en cuarto de servidores.
- Archivadores con llave para información sensible.
- Política de escritorio limpio.

Controles de Concientización y Capacitación

- Capacitaciones semestrales en ciberseguridad.
- Simulaciones de phishing.
- Sensibilización sobre protección de datos personales.
- Firma de acuerdos de confidencialidad.

Controles Legales y Normativos

- Cumplimiento Ley 1581 de 2012 (Protección de Datos).
- Cumplimiento Ley 1712 de 2014 (Transparencia).
- Manual interno de tratamiento de datos.
- Registro de bases de datos ante la SIC (cuando aplique).

Controles de Auditoría y Seguimiento

- Auditorías internas anuales.
- Indicadores de seguridad.
- Monitoreo de logs.
- Reporte periódico al Comité de Seguridad.
- Evaluación de cumplimiento del Plan.

Indicadores de Eficacia de los Controles

- % de equipos actualizados.
- % de respaldos exitosos.

- Número de incidentes reportados.
- Tiempo promedio de recuperación.
- Nivel de cumplimiento de políticas.

GESTIÓN DE INCIDENTES

- Registro de incidentes.
- Análisis de causa raíz.
- Plan de respuesta.
- Reporte a autoridades si aplica.
- Lecciones aprendidas.

CONTINUIDAD DEL NEGOCIO

- Identificación de procesos críticos.
- Plan de respaldo de información.
- Pruebas de restauración semestrales.
- Plan de contingencia tecnológica.

PLAN DE ACCIÓN

Actividad	**Responsable**	**Plazo**
Inventario de activos	Oficina TIC	Marzo
Análisis de riesgos	TIC + Control Interno	Abril
Implementación de controles	TIC	Junio
Capacitación institucional	Talento Humano	Agosto
Auditoría interna	Control Interno	Noviembre

MEJORA CONTINUA

El plan será revisado anualmente o cuando:

- Se presenten incidentes graves.

- Cambie la infraestructura tecnológica.
- Se modifique la normatividad.