PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

IDECESAR

Instituto para el Desarrollo del Cesar

IDECESAR
Instituto para el Desarrollo del Cesar

INDICE

INTRODUCCIÓN

En Colombia se ha venido implementando la política de Gobierno Digital, como un instrumento fundamental para mejorar la gestión pública y la relación del Estado con los ciudadanos, la cual, se ha articulado con el Modelo Integrado de Planeación y Gestión como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otras políticas esenciales para la gestión pública en Colombia.

El Manual de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones establece que esta política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones, para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Según el manual, la implementación de la política de Gobierno Digital se ha definido en dos componentes: TIC para el Estado y TIC para la sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.

Estos cinco elementos, se desarrollan a través de lineamientos y estándares, que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política. El manual en mención, precisa que el habilitador de seguridad de la información busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la información –MSPI-. No obstante, el manual está amparado en el Decreto 1008 del 2018, que en su artículo 2.2.9.1.1.3 define que la política de Gobierno Digital se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos adoptados en Colombia, en particular, al principio de Seguridad de la Información, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de IDECESAR define las acciones necesarias como parte activa de la Política de Seguridad de la Información adoptada por la entidad para reducir, mitigar, aceptar o transferir los riesgos identificados que puedan afectar la confidencialidad, integridad y disponibilidad de la información, así como la protección de los datos personales, en cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI).

El Instituto para el Desarrollo del Cesar – IDECESAR, como entidad pública de carácter territorial, reconoce que la información constituye uno de sus activos más importantes para el cumplimiento de su misión institucional. En el desarrollo de sus funciones administrativas, financieras, crediticias

y de fomento empresarial, la entidad procesa información estratégica, financiera, personal y contractual que debe ser protegida frente a amenazas internas y externas.

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece las acciones necesarias para mitigar, reducir, transferir o aceptar los riesgos identificados en la matriz de riesgos de seguridad digital institucional, garantizando la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

OBJETIVO GENERAL

Definir y documentar las estrategias, controles y acciones necesarias para tratar los riesgos identificados en la gestión de seguridad y privacidad de la información de IDECESAR, reduciendo su probabilidad e impacto a niveles aceptables para la entidad.

OBJETIVOS ESPECÍFICOS

1. Implementar controles técnicos, administrativos y físicos para mitigar riesgos críticos y altos.
2. Establecer responsables y tiempos de ejecución para cada acción de tratamiento.
3. Fortalecer la cultura organizacional en seguridad de la información.
4. Cumplir con el Modelo de Seguridad y Privacidad de la Información (MSPI).
5. Proteger los datos personales conforme a la normativa colombiana.

ALCANCE

Este plan aplica a:

- Todos los procesos misionales, estratégicos y de apoyo de IDECESAR.
- Funcionarios, contratistas y terceros.
- Infraestructura tecnológica (servidores, estaciones de trabajo, redes).
- Sistemas de información y bases de datos.
- Información en formato físico y digital.

MARCO NORMATIVO Y REFERENCIAL

- ISO 27001 – Sistema de Gestión de Seguridad de la Información.
- ISO 27005 – Gestión de Riesgos de Seguridad de la Información.
- Modelo de Seguridad y Privacidad de la Información – Ministerio de Tecnologías de la Información y las Comunicaciones.
- Política de Gobierno Digital – Presidencia de la República de Colombia.
- Ley 1581 de 2012 (Protección de Datos Personales).
- Decreto 1078 de 2015.

METODOLOGÍA DE TRATAMIENTO DEL RIESGO

La metodología aplicada comprende las siguientes etapas:

Identificación del riesgo

Se identifican amenazas, vulnerabilidades y activos afectados.

Análisis del riesgo

Se evalúa la probabilidad y el impacto (bajo, medio, alto, crítico).

Valoración del riesgo

Se determina el nivel de riesgo inherente.

Tratamiento del riesgo

Se define la estrategia:

- Mitigar
- Evitar
- Transferir
- Aceptar

Monitoreo y revisión

Seguimiento trimestral por parte del área TIC y Control Interno.

ESTRATEGIAS DE TRATAMIENTO DEL RIESGO

A continuación, se describen los principales riesgos identificados y su tratamiento:

Riesgo: Ataques de Ransomware

Descripción: Posible cifrado de información institucional.
Nivel: Crítico

Tratamiento:

- Implementación de antivirus corporativo centralizado.
- Copias de seguridad automatizadas diarias.
- Segmentación de red.
- Restricción de privilegios administrativos.
- Capacitación en phishing.

Responsable: Área TIC
Plazo: 6 meses

Riesgo: Pérdida de Información por Fallas Técnicas

Nivel: Alto

Tratamiento:

- Implementar política formal de backups.
- Almacenamiento externo cifrado.
- Pruebas semestrales de restauración.
- UPS y reguladores de energía.

Riesgo: Acceso No Autorizado a Sistemas

Nivel: Alto

Tratamiento:

- Control de acceso basado en roles.
- Doble factor de autenticación.

- Bloqueo automático por intentos fallidos.
- Registro y monitoreo de logs.

Riesgo: Instalación de Software No Licenciado

Nivel: Medio

Tratamiento:

- Bloqueo de privilegios de administrador local.
- Implementación de políticas de grupo (GPO).
- Auditorías trimestrales de software.
- Inventario automatizado de activos TI.

Riesgo: Fuga de Información Confidencial

Nivel: Alto

Tratamiento:

- Clasificación de la información.
- Firma de acuerdos de confidencialidad.
- Restricción de dispositivos USB.
- Cifrado de equipos portátiles.

Riesgo: Fallas en la Seguridad Física

Nivel: Medio

Tratamiento:

- Control de acceso a sala de servidores.
- Sistema de cámaras de vigilancia.
- Registro de visitantes.
- Política de escritorio limpio.

MATRIZ DETALLADA DE TRATAMIENTO DE RIESGOS

A continuación se presenta la **Matriz Detallada de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de IDECESAR**, alineada con ISO 27001, ISO 27005 y el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones.

La matriz contempla **35 riesgos**, clasificados por tipo, con su respectiva estrategia de tratamiento, controles y responsables.

Escala utilizada:

- **Probabilidad (P):** Baja (1), Media (2), Alta (3)
- **Impacto (I):** Bajo (1), Medio (2), Alto (3)
- **Nivel de Riesgo:** P x I
    - 1–2 Bajo
    - 3–4 Medio
    - 6–9 Alto / Crítico

	Riesgo	Tipo	P	I	Nivel	Tratamiento	Controles / Acciones	Responsable	Plazo
	Ataque de ransomware	Tecnológico	3	3	9	Mitigar	Backup diario automatizado, antivirus corporativo	TIC	3 meses
	Phishing a funcionarios	Tecnológico	3	3	9	Mitigar	Capacitación semestral, filtros antispam	TIC	Permanente
	Acceso no autorizado a sistemas	Tecnológico	3	3	9	Mitigar	MFA, control por roles	TIC	4 meses
	Incendio en instalaciones	Físico	1	3	3	Transferir	Póliza seguros, extintores	Administrativa	6 meses
	Inundación	Físico	1	3	3	Mitigar	Ubicación elevada de equipos	Administrativa	6 meses
	Instalación software no licenciado	Legal/TI	3	2	6	Mitigar	Bloqueo admin local, inventario TI	TIC	2 meses
	Fuga de	Tecnológico	3	3	9	Mitigar	Bloqueo	TIC	3 meses

	información por USB						puertos USB		
	Pérdida de portátil institucional	Operativo	2	3	6	Mitigar	Cifrado disco duro	TIC	4 meses
	Uso indebido de contraseñas	Humano	3	3	9	Mitigar	Política contraseñas robustas	TIC	2 meses
	Compartir credenciales	Humano	3	3	9	Mitigar	Campañas concientización	TIC	Permanente
	Fallo en proveedor nube	Externo	2	3	6	Transferir	SLA contractual	Dirección	6 meses
	Ataque DDoS	Tecnológico	2	3	6	Mitigar	Firewall perimetral	TIC	5 meses
	Malware interno	Tecnológico	3	2	6	Mitigar	Antivirus centralizado	TIC	3 meses
	Alteración bases de datos	Tecnológico	2	3	6	Mitigar	Logs y auditoría	TIC	4 meses
	Eliminación accidental de archivos	Humano	3	2	6	Mitigar	Versionado y respaldo automático	TIC	3 meses
	Fallas eléctricas prolongadas	Físico	2	3	6	Mitigar	Planta eléctrica	Admin	8 meses
	Acceso físico no autorizado	Físico	2	3	6	Mitigar	Control biométrico	Admin	6 meses
	Violación Ley 1581 datos personales	Legal	2	3	6	Mitigar	Política protección datos	Jurídica	4 meses
	Publicación indebida info web	Operativo	2	2	4	Mitigar	Revisión doble antes publicar	Comunicaciones	Permanente
	Ingeniería social	Humano	3	3	9	Mitigar	Simulaciones phishing	TIC	Permanente
	No actualización de software	Tecnológico	3	2	6	Mitigar	Política de parches	TIC	Permanente
	Robo de equipos	Físico	2	2	4	Mitigar	Inventario y cámaras	Admin	5 meses
	Acceso remoto inseguro	Tecnológico	2	3	6	Mitigar	VPN segura	TIC	4 meses
	Uso de WiFi insegura	Tecnológico	3	2	6	Mitigar	Red segmentada	TIC	4 meses

	Desactualización antivirus	Tecnológico	2	2	4	Mitigar	Consola central actualizada	TIC	Permanente
	Falta de monitoreo logs	Tecnológico	2	3	6	Mitigar	SIEM básico	TIC	6 meses
	Fallo en copias de seguridad	Tecnológico	2	3	6	Mitigar	Pruebas restauración semestral	TIC	6 meses
	Ausencia plan continuidad	Estratégico	2	3	6	Mitigar	Implementar BCP	Dirección	8 meses
	Error en configuración firewall	Tecnológico	2	3	6	Mitigar	Auditoría configuración	TIC	5 meses
	Manipulación indebida archivos físicos	Físico	2	2	4	Mitigar	Archivo bajo llave	Admin	3 meses
	Desinformación interna	Organizacional	2	2	4	Mitigar	Política comunicaciones internas	Dirección	4 meses
	Uso de dispositivos personales	Tecnológico	3	2	6	Mitigar	Política BYOD	TIC	6 meses
	Incumplimiento contractual TI	Legal	2	3	6	Transferir	Cláusulas seguridad contratos	Jurídica	Permanente

CRONOGRAMA CAPACITACION FUNCIONARIOS DE IDECESAR

Tema	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Fundamentos de seguridad de la información									
Amenazas comunes									
Seguridad en el correo									

electrónico									
Cultura de Seguridad									

CRITERIOS DE ACEPTACIÓN DEL RIESGO

Un riesgo podrá aceptarse cuando:

- Su impacto sea bajo.
- El costo del control supere el beneficio.
- Existan controles compensatorios.

La aceptación debe ser aprobada por la Dirección General.

INDICADORES DE SEGUIMIENTO

- % de riesgos críticos mitigados.
- % de cumplimiento del plan de acción.
- Número de incidentes reportados.
- Tiempo promedio de respuesta a incidentes.

RESPONSABILIDADES

Comité de desempeño: Aprobar el plan.
Área TIC: Implementar controles técnicos.
Control Interno: Verificar cumplimiento.
Funcionarios: Cumplir políticas de seguridad.

PRESUPUESTO ESTIMADO

El tratamiento de riesgos podrá requerir inversión en:

- Licencias de antivirus corporativo.
- Sistemas de backups.

- Firewall perimetral.
- Capacitación en seguridad digital.
- Servicios de auditoría externa.

MEJORA CONTINUA

El presente plan será revisado anualmente o cuando:

- Ocurra un incidente grave.
- Se implementen nuevos sistemas.
- Cambie la normatividad aplicable.

CONCLUSIÓN

El Plan de Tratamiento de Riesgos de Seguridad de la Información de IDECESAR constituye un instrumento técnico y estratégico fundamental para fortalecer la capacidad institucional frente a amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de la información. En un entorno caracterizado por la creciente digitalización de los procesos administrativos, financieros y misionales, la gestión estructurada del riesgo deja de ser una actividad opcional para convertirse en un elemento esencial de la gobernanza institucional.

A través de la identificación, análisis, valoración y tratamiento de los riesgos, IDECESAR establece un marco organizado de actuación que permite priorizar recursos, definir responsabilidades y ejecutar controles de manera planificada. Este enfoque no solo reduce la probabilidad de incidentes como ataques informáticos, pérdida de información, accesos no autorizados o fallas técnicas, sino que también minimiza el impacto operativo, financiero y reputacional en caso de que estos eventos lleguen a materializarse.

El Plan demuestra que la seguridad de la información no depende exclusivamente de herramientas tecnológicas, sino de una combinación equilibrada entre controles técnicos, administrativos y físicos, respaldados por una cultura organizacional orientada a la protección de los activos de información. La participación activa de la Alta Dirección, el Área TIC, Control Interno y todos los funcionarios es determinante para que las acciones definidas no se limiten al ámbito documental, sino que se traduzcan en prácticas institucionales sostenibles.

Asimismo, este Plan se encuentra alineado con estándares internacionales como los promovidos por ISO y con los lineamientos del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones, lo que permite a IDECESAR

avanzar hacia un mayor nivel de madurez en su gestión de seguridad digital y en el cumplimiento de la normativa colombiana en materia de protección de datos personales.

Es importante resaltar que la gestión de riesgos es un proceso dinámico y continuo. Las amenazas evolucionan, las tecnologías cambian y los procesos institucionales se transforman. Por ello, el Plan de Tratamiento debe ser revisado periódicamente, actualizado frente a nuevos escenarios y fortalecido mediante procesos de seguimiento, medición e implementación de mejoras continuas. La adopción de indicadores claros, auditorías internas y evaluaciones periódicas garantizará que los controles definidos mantengan su eficacia en el tiempo.

En conclusión, el Plan de Tratamiento de Riesgos de Seguridad de la Información consolida el compromiso de IDECESAR con la protección de la información como activo estratégico, fortalece la resiliencia institucional ante incidentes de seguridad y contribuye directamente a la continuidad del servicio, la confianza ciudadana y la transparencia en la gestión pública. Su correcta implementación permitirá a la entidad no solo reaccionar ante los riesgos, sino anticiparse a ellos, consolidando una cultura de seguridad integral y sostenible.