PLAN DE CONTINGENCIA DE SEGURIDAD DE LA INFORMACION

CDI CONSTRUYENDO SUEÑOS SAN JACINTO DEL CAUCA

MODALIDAD INSTITUCIONAL

MUNICIPIO SAN JACINTO DEL CAUCA BOLIVAR 2026

PLAN DE CONTINGENCIA DE LA SEGURIDAD DE LA INFORMACION

Objetivo

Establecer acciones claras para prevenir, detectar, responder y recuperar ante incidentes que comprometan la seguridad de la información en los CDI, garantizando la protección de datos personales de niños, acudientes y talento humano.

Alcance

Organizar información física (carpetas, fichas de caracterización, historias de atención)
Información digital (bases de datos, archivos en computadores, plataformas), Personal administrativo, pedagógico y contratistas del CDI Construyendo Sueños San Jacinto, Tenche y Astillero
Identificación de Riesgos

Riesgos más relevantes

Acceso no autorizado a información de niño, Pérdida o robo de documentos físicos, Daño o pérdida de equipos tecnológicos, Virus informáticos o ataques cibernéticos, Desastres naturales (inundaciones, incendios) y Uso inadecuado de la información por parte del personal.
Escenarios de Contingencia, Pérdida o robo de información teniendo en cuenta las siguientes acciones: Notificar inmediatamente al coordinador del CDI, activar respaldo de información (copias de seguridad), reportar incidente según normativa de protección de datos.
Daño de equipos tecnológicos

Acciones

Uso de equipos de respaldo (si existen), recuperación de información desde backups y Solicitud de soporte técnico.
Acceso no autorizado
Acciones: Cambio inmediato de contraseñas, Bloqueo de usuarios comprometidos, Auditoría de accesos
Desastres naturales (incendio, inundación)
Acciones: Evacuación según plan de emergencias, Protección de archivos críticos en contenedores seguros, Recuperación desde copias externas o en la nube

Medidas Preventivas

Seguridad física, Archivadores bajo llave, Control de acceso a oficinas, Restricción de ingreso a áreas administrativas, Seguridad digital, Uso de contraseñas seguras, Copias de seguridad semanales, Antivirus

actualizado, No uso de USB desconocidos, Gestión documental, Clasificación de información confidencial, Eliminación segura de documentos y Digitalización progresiva

Plan de Recuperación

Tiempo objetivo de recuperación (RTO):
Información crítica: 24–48 horas
Procedimientos: Identificar información afectada, Restaurar desde copias de seguridad
Validar integridad de dato y reanudar operaciones
Roles y Responsables
Coordinador CDI: Lidera la respuesta a incidentes
Auxiliar administrativo: Custodia documental
Docentes: Manejo responsable de información de niños
Soporte técnico (si aplica): Recuperación digital
Comunicación del Incidente, Informar a dirección general así notificar a entidades regulatorias (si aplica) y Comunicar a padres/acudientes cuando haya riesgo sobre datos
Pruebas y Simulacros
Simulacros semestrales de incidentes para la verificación de copias de seguridad
Evaluación de tiempos de respuesta teniendo en cuenta las normatividades Aplicable (Colombia) como son la Ley 1581 de 2012 (Protección de datos personales), Decreto 1377 de 2013 y el Lineamientos del ICBF para CDI.
Evaluación anual del plan, actualización según nuevos riesgos y capacitación permanente al personal.

ALEXANDER BAÑOS CORREA
Representante legal
Fundación Saber Ser

PLAN DE GESTION DE RIESGO DE EMERGENCIAS Y DESASTRES

CDI CONSTRUYENDO SUEÑOS SEDE TENCHE Y ASTILLEROS

MODALIDAD INSTITUCIONAL

MUNICIPIO SAN JACINTO DEL CAUCA BOLIVAR 2026

Objetivo

Establecer acciones claras para prevenir, detectar, responder y recuperar ante incidentes que comprometan la seguridad de la información en los CDI, garantizando la protección de datos personales de niños, acudientes y talento humano.

Alcance

Organizar información física (carpetas, fichas de caracterización, historias de atención)
Información digital (bases de datos, archivos en computadores, plataformas), Personal administrativo, pedagógico y contratistas del CDI Construyendo Sueños San Jacinto, Tenche y Astillero
Identificación de Riesgos

Riesgos más relevantes

Acceso no autorizado a información de niño, Pérdida o robo de documentos físicos, Daño o pérdida de equipos tecnológicos, Virus informáticos o ataques cibernéticos, Desastres naturales (inundaciones, incendios) y Uso inadecuado de la información por parte del personal.
Escenarios de Contingencia, Pérdida o robo de información teniendo en cuenta las siguientes acciones: Notificar inmediatamente al coordinador del CDI, activar respaldo de información (copias de seguridad), reportar incidente según normativa de protección de datos.
Daño de equipos tecnológicos

Acciones

Uso de equipos de respaldo (si existen), recuperación de información desde backups y Solicitud de soporte técnico.
Acceso no autorizado
Acciones: Cambio inmediato de contraseñas, Bloqueo de usuarios comprometidos, Auditoría de accesos
Desastres naturales (incendio, inundación)
Acciones: Evacuación según plan de emergencias, Protección de archivos críticos en contenedores seguros, Recuperación desde copias externas o en la nube

Medidas Preventivas

Seguridad física, Archivadores bajo llave, Control de acceso a oficinas, Restricción de ingreso a áreas administrativas, Seguridad digital, Uso de contraseñas seguras, Copias de seguridad semanales, Antivirus

actualizado, No uso de USB desconocidos, Gestión documental, Clasificación de información confidencial, Eliminación segura de documentos y Digitalización progresiva

Plan de Recuperación

Tiempo objetivo de recuperación (RTO):
Información crítica: 24–48 horas
Procedimientos: Identificar información afectada, Restaurar desde copias de seguridad
Validar integridad de dato y reanudar operaciones Roles y Responsables
Coordinador CDI: Lidera la respuesta a incidentes
Auxiliar administrativo: Custodia documental
Docentes: Manejo responsable de información de niños
Soporte técnico (si aplica): Recuperación digital
Comunicación del Incidente, Informar a dirección general así notificar a entidades regulatorias (si aplica) y Comunicar a padres/acudientes cuando haya riesgo sobre datos
Pruebas y Simulacros
Simulacros semestrales de incidentes para la verificación de copias de seguridad
Evaluación de tiempos de respuesta teniendo en cuenta las normatividades Aplicable (Colombia) como son la Ley 1581 de 2012 (Protección de datos personales), Decreto 1377 de 2013 y el Lineamientos del ICBF para CDI.
Evaluación anual del plan, actualización según nuevos riesgos y capacitación permanente al personal.

ALEXANDER BAÑOS CORREA
Representante legal
Fundación Saber Ser