INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (IDENTIFICACIÓN, ANÁLISIS, VALORACIÓN y MANEJO)

	PROCESO MEJORA E INNOVACIÓN	F1.E1.M	SI-MO003
		Versión 8	Página 1 de 3
	MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	Clasificación de la información CLASIFICADA	

1. IDENTIFICACIÓN																2. ANÁLISIS			3. VALIDACIÓN										4. MANEJO								
ID	FECHA DE IDENTIFICACIÓN (DD/MM/AAAA)	REGIONAL O SEDE DE LA DIRECCIÓN GENERAL	PROCESO (NIVEL DE ALCANCE)	OBJETIVO DEL PROCESO	CONTEXTO INTERNO	CONTEXTO EXTERNO	CONTEXTO DEL PROCESO	NOMBRE DE ACTIVO AFECTADO	TIPO DE ACTIVO AFECTADO	ACCIÓN RELACIONADA AL RIESGO	VULNERABILIDADES	AMENAZAS	RIESGO PRINCIPIO AFECTADO (C=1/I=2/A=3) ACTIVO DE ACTIVOS DE INFORMACIÓN – ACCIONES ASOCIADAS AL RIESGO + VULNERABILIDADES Y AMENAZAS QUE GENERAN EL RIESGO	TIPO DE RIESGO	CONSECUENCIAS NEGATIVAS	CONSECUENCIAS POSITIVAS	PERSONAS O PROCESOS AFECTADOS	PROBABILIDAD	IMPACTO	NIVEL ANTES DE CONTROLES	DESCRIPCIÓN DE LOS CONTROLES ACTUALES	Diseño	Ejecución	Desviación	El control ayuda a disminuir la probabilidad	El control ayuda a disminuir el impacto	PROBABILIDAD	NIVEL ANTES DE CONTROLES	NIVEL DESPUÉS (Responsable de Controles)	OPCIONES TRATAMIENTO	CONTROLES ANEXO A ISO 27001:2013	PROBADO	MATERIALIZACIÓN	OBSERVACIONES	PHVA SEDE
24-PSI-261	31/01/2024	SEDE DE ALMACÉN GENERAL	Protección	- FINANCIERO: Presupuesto de funcionamiento, recursos de inversión infraestructura, capacidad instalada. Líderar el diseño, actualización y desarrollo de - TALENTO HUMANO: Competencia del pone, programas, proyectos y modalidades personal, disponibilidad del personal, que establecen los derechos de los niños, niñas, responsable, compromiso, trabajo en equipo, adolescentes y jóvenes en situación de - PROCESOS: Capacidad, diseño, ejecución vulnerabilidad, amenaza, violencia, abuso o conflicto y procedimientos. con la ley - TECNOLOGÍA: Integridad de datos disponibilidad bases y sistemas, documentos, protección, mantenimiento de sistemas de información.	ECONÓMICOS Y FINANCIEROS: disponibilidad de capital, fuentes financiación, inversión, presupuestos. SOCIALES Y CULTURALES: Demografía, responsabilidad social, orden público. LEGALES Y REGLAMENTARIOS: normatividad externa (leyes, decretos, ordenanzas, acuerdos, reglamentos).	- DISEÑOS DE PROCESOS: Claridad en la descripción del alcance y objetivo de los procesos - INTERACCIONES ENTRE PROCESOS: Relación precisa con otros procesos en cuanto a insumos, productos, usuarios o beneficiarios. - PROCEDIMIENTOS ASOCIADOS: Pertinencia en los procedimientos que delimitan la operación. - RESPONSABILIDADES DEL PROCESO: Definición de responsabilidades frente a actividades y manejo de información. - COMUNICACIÓN INTERNA Y EXTERNA: Canales utilizados y su efectividad para dar a conocer los resultados del proceso. - ACTIVOS DE INFORMACIÓN DEL PROCESO: Identificación de los activos de información del proceso. PROCESO: Información, aplicaciones, hardware, servicios, personas, que se deben proteger para asegurar el buen manejo de la información.	BASE DE MÓDULO PARA I ADQUIRENTES CON DESCARGA EN LA ADQUIRIDA EN TIENDA Caracterización de la población con Discapacidad mental en el departamento de Huila DERECHO DE PETICIÓN, QUEJAS, RECLAMOS, SOLICITUDES Y DENUNCIAS HISTORIAS VERACIÓN Información de RIAS desarrolladas de gran cantidad de mujeres (más de Información de Niños, Niñas y Adolescentes atendidos en Instituto de establecimientos de detención. Listado de expertos técnicos colombianos Reportería de Niños, Niñas y Adolescentes en situación de Migración Internacional Respuesta de PQRS Seguimiento a Hoja de Intervención de Personas sin Solicitudes de adopción Solicitudes de adopción de Trámites Bilaterales de Origen	Activo	Humano Talento y Factor Humano	Falta de competencias en la aplicación de procedimientos para la actualización de usuarios. Ausencia en la creación y desactivación de usuarios en el SIM. Ausencia en el SIM Integración de datos personales y/o información sensible. Ausencia de un mecanismo de validación y depuración de usuarios en el SIM. Falta de competencias en el manejo de la información por parte de los profesionales de apoyo. Ausencia de un mecanismo de validación y depuración de usuarios en el SIM.	Falta de integridad, confidencialidad y disponibilidad de los activos tipo información suministrados de procesos de información que se gestionan en SIM, por modificación y divulgación de la información no autorizada, debido a la ausencia de un mecanismo de validación y depuración de usuarios en el SIM, falta de competencias en el manejo de la información por parte de los profesionales de apoyo, ausencia de un mecanismo de validación y depuración de usuarios en el SIM, falta de competencias en el manejo de la información por parte de los profesionales de apoyo.	Riesgo de Seguridad de la Información	- Pérdida Financiera - Pérdida de imagen y good - Incumplimiento regulatorio - Sanción de Dirección	- Optimización de procesos	DIRECCIÓN GENERAL PROTECCIÓN	Muy Baja	Mayor	Alto (Muy Baja - Mayor)	ACUERDO: Realizar la asignación de usuarios de acuerdo con el procedimiento de asignación de usuarios RESPONSABLE: Profesional Especializado PERIODICIDAD: Cuatrimestre PROPÓSITO: Mantener la actualización y depuración de usuarios que no corresponden a personal activo para asegurar que la información sensible y personal solo sea accesible por los usuarios autorizados. OBSERVACIÓN DE EJECUCIÓN: Informe o MEGA con el listado de usuarios para ser depurados EVIDENCIA: Reporte de la actualización de usuarios de SIM - Casos registrados en MEC TIPO DE CONTROL: Detective HERRAMIENTA DE CONTROL: Sentido analítico CONTROL ASOCIADO ISO: Sí	Fuerte(2)	Fuerte(2)	Efectivo	Directamente	Moderadamente	Muy Baja	Alto (Muy Baja - Moderada)	Alto (Muy Baja - Moderada)	Mitigar el riesgo	A8.2. Responsabilidad por los activos. A8.2.1. Guía de clasificación de activos. A7.2. Durante la ejecución del empleo. A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información.	1 - De 6 a 12 meses	Actuar el procedimiento de atención a los incidentes de seguridad de la información para minimizar el riesgo y realizar la mediación del riesgo.		ZIP-SI261
24-PSI-262	31/01/2024	SEDE DE ALMACÉN GENERAL	Protección	Líderar el diseño, actualización y desarrollo de pone, programas, proyectos y modalidades, asegurando actuaciones oportunas y con calidad, que establecen los derechos de los niños, niñas, adolescentes y jóvenes en situación de vulneración y amenaza, violencia, abuso o conflicto con la ley	- TALENTO HUMANO: Competencia del personal, disponibilidad del personal, responsable, compromiso, trabajo en equipo, seguridad y salud ocupacional. - PROCESOS: Capacidad, diseño, ejecución, procedimientos.	TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno digital. LEGALES Y REGLAMENTARIOS: normatividad externa (leyes, decretos, ordenanzas, acuerdos, reglamentos).	CT - PROCEDIMIENTOS ASOCIADOS: Pertinencia en los procedimientos que delimitan la operación. - RESPONSABILIDADES DEL PROCESO: Definición de responsabilidades frente a actividades y manejo de información. - COMUNICACIÓN INTERNA Y EXTERNA: Canales utilizados y su efectividad para dar a conocer los resultados del proceso. PROCESOS: Información, aplicaciones, hardware, servicios, personas, que se deben proteger para asegurar el buen manejo de la información.	Acta del Comité Técnico Consultivo para el Restablecimiento de Derechos Actas comité de categorías Regional Actas comité Técnico Consultivo Nacional de Adolescentes Administrativas Actas del Comité Interinstitucional Consultivo para la Prevención de la Violencia Sexual y Atención Integral de los Niños, Niñas y Adolescentes Víctimas de Abuso Sexual Solicitudes de cambio de información de usuarios registrados en SIM Documentación Estudio de Verificación de Derechos para Niños de Protección Integral SIM Postgraduados Documentación Estudio de Niños y Niñas Víctimas de Reclutamiento Forzado Documentación Estudio de Verificación Integral Gestión Informe Anónimo Técnico Informe de seguimiento para cada adopción Instrumento de Seguimiento de Derechos de niños en Instituciones ANAR Listado RIA Mediadas que Son Pena y Medidas para Niños Niñas y Adolescentes Mecanismo de Alivio Proceso de Adopciones Publicaciones en el espacio "Mi Carpeta" Reporte de Delitos en Vías de Hecho Reporte Estratégico de Juzgamiento Revisión de procesos Migración Colombia Valoraciones Psicosociales Restricciones Red Diseños Técnicos Instrumento de seguimiento para el verificación de cumplimiento de obligaciones y controles de protección en la movilidad de entrenado, Hogar Sustituto Ordinal, Hogar Sustituto Ordinal, Instrumento de Apoyo - Apoyo Psicosocial y Apoyo Psicosocial Especializado	Activo - Físico (Información Física) - Electrónico (Información Digital) - Físico - Escritorio	Modificación en una actividad de la información o contratación	Personal Talento y Factor Humano	Falta de competencias en la aplicación de procedimientos para la actualización de usuarios. Ausencia en la creación y desactivación de usuarios en el SIM. Ausencia en el SIM Integración de datos personales y/o información sensible. Ausencia de un mecanismo de validación y depuración de usuarios en el SIM. Falta de competencias en el manejo de la información por parte de los profesionales de apoyo. Ausencia de un mecanismo de validación y depuración de usuarios en el SIM.	Falta de integridad, confidencialidad y disponibilidad de los activos tipo información suministrados de procesos de información que se gestionan en SIM, por modificación y divulgación de la información no autorizada, debido a la ausencia de un mecanismo de validación y depuración de usuarios en el SIM, falta de competencias en el manejo de la información por parte de los profesionales de apoyo, ausencia de un mecanismo de validación y depuración de usuarios en el SIM.	Riesgo de Seguridad de la Información	- Pérdida Financiera - Pérdida de imagen y good - Incumplimiento regulatorio - Sanción de Dirección Reprocesos Sanciones	- Optimización de procesos	DIRECCIÓN GENERAL PROTECCIÓN	Media	Moderado	Moderada (Media - Moderada)	RIESGO: Realizar la Asistencia Técnica RESPONSABLE: Profesional Especializado PERIODICIDAD: Trimestral PROPÓSITO: Brindar asesoría y acompañamiento que tiene como fin fortalecer el conocimiento, las competencias y habilidades de los entes territoriales. OBSERVACIÓN DE EJECUCIÓN: Brindar asesoría y acompañamiento que tiene como fin fortalecer el conocimiento, las competencias y habilidades de los entes territoriales. Tener como documentación en el Procedimiento Asistencia Técnica. EVIDENCIA: Actividades de Asistencia. TIPO DE CONTROL: Preventivo HERRAMIENTA DE CONTROL: Manual CONTROL ASOCIADO ISO: Sí ACUERDO: Responder a las solicitudes de información de las partes interesadas. RESPONSABLE: Profesional Especializado PERIODICIDAD: Cuatrimestre (programación de evidencias de cumplimiento cuatrimestral PDSEE) PROPÓSITO: Asegurar privilegios de acceso a los usuarios mediante procedimientos establecidos para eliminación de los derechos de acceso. OBSERVACIÓN DE EJECUCIÓN: Revisión de los permisos de acceso colaboradores que hacen parte del proceso. EVIDENCIA: Correos electrónicos TIPO DE CONTROL: Preventivo HERRAMIENTA DE CONTROL: Manual CONTROL ASOCIADO ISO: Sí	Fuerte(2)	Fuerte(2)	Efectivo	Directamente	Moderadamente	Media	Moderada (Media - Moderada)	Moderada (Media - Moderada)	Mitigar el riesgo	A8.1. Responsabilidad de Registro para Control de Acceso. A8.1.1. Política de Control de Acceso. A8.1. Gestión de Acceso de Usuarios. A.8.1.3. Revisión de los derechos de acceso de usuarios.	2 - De 6 a 12 meses	Actuar el procedimiento de atención a los incidentes de seguridad de la información para minimizar el riesgo y realizar la mediación del riesgo.	La solución de SIM integra con Portal Web en 2023	ZIP-SI262
24-PSI-263	31/01/2024	SEDE DE ALMACÉN GENERAL	Protección	Líderar el diseño, actualización y desarrollo de pone, programas, proyectos y modalidades, asegurando actuaciones oportunas y con calidad, que establecen los derechos de los niños, niñas, adolescentes y jóvenes en situación de vulneración y amenaza, violencia, abuso o conflicto con la ley	- TALENTO HUMANO: Competencia del personal, disponibilidad del personal, responsable, compromiso, trabajo en equipo, seguridad y salud ocupacional. - PROCESOS: Capacidad, diseño, ejecución, procedimientos.	POLÍTICOS: Cambios de gobierno, legislación, políticas públicas, regulación. TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno digital. LEGALES Y REGLAMENTARIOS: normatividad externa (leyes, decretos, ordenanzas, acuerdos, reglamentos).	- INTERACCIONES ENTRE PROCESOS: Relación precisa con otros procesos en cuanto a insumos, productos, usuarios o beneficiarios. - PROCEDIMIENTOS ASOCIADOS: Pertinencia en los procedimientos que delimitan la operación.	Actas comité de categorías Regional Declaraciones de conformidad de una Adopción Internacional DERECHO DE PETICIÓN, QUEJAS, RECLAMOS, DENUNCIAS Y SUGERENCIAS Documentación Estudio de Niños y Niñas Víctimas de Reclutamiento Forzado HISTORIAS VERACIÓN Información de Niños, Niñas y Adolescentes atendidos en Instituto de establecimientos de detención. Informes de seguimiento para cada adopción Proceso de Adopciones Reporte de Delitos en Vías de Hecho Reporte de PQRS Solicitudes de adopción Solicitudes PQRS ICBF Valoraciones Psicosociales	Activo - Físico (Información Física) - Físico - Escritorio	Acceso de visitantes/terceros en instalaciones de la sede Nivel Park	Personal Talento y Factor Humano Legal Personal	Desconocimiento de Procedimiento de Disposición de Archivos, la falta de Publicación de la información y del procedimiento de Archivos y falta de Inventario de equipos de cómputo. Ausencia de controles de acceso físico a los espacios físicos. Falta de conciencia sobre la seguridad de la información de los colaboradores con acceso a la sede. Ausencia de controles de acceso físico a los espacios físicos. Falta de conciencia sobre la seguridad de la información de los colaboradores con acceso a la sede. Ausencia de controles de acceso físico a los espacios físicos.	Riesgo de Seguridad de la Información	- Pérdida de imagen y good - Incumplimiento regulatorio - Sanción de Dirección Reprocesos Sanciones	- Optimización de procesos	DIRECCIÓN GENERAL PROTECCIÓN	Media	Moderado	Moderada (Media - Moderada)	Falta de integridad, disponibilidad y confidencialidad de la información de los clientes de información físicos protocolos de procesos, debido al incumplimiento de los procedimientos para la gestión documental, por falta de conciencia en la seguridad de la información de los colaboradores con acceso a la sede física, la ausencia de controles de acceso físico a los espacios físicos, ausencia de mecanismos de Procedimiento de Disposición de Archivos, falta de difusión de la información y del procedimiento de archivos y falta de inventario de equipos.	Fuerte(2)	Fuerte(2)	Efectivo	Directamente	Moderadamente	Media	Moderada (Media - Moderada)	Moderada (Muy Baja - Moderada)	Mitigar el riesgo	A11.1. Áreas Seguras. A.11.1.3. Seguridad de oficinas, recintos e instalaciones. A8.1. Responsabilidad por los activos. A8.1.1. Uso Aceptable de los Activos.	2 - De 6 a 12 meses	Actuar el procedimiento de atención a los incidentes de seguridad de la información para minimizar el riesgo y realizar la mediación del riesgo.	La solución de SIM integra con Portal Web en 2023	ZIP-SI263
24-PSI-264	31/01/2024	SEDE DE ALMACÉN GENERAL	Protección	- FINANCIERO: Presupuesto de funcionamiento, recursos de inversión infraestructura, capacidad instalada. Líderar el diseño, actualización y desarrollo de - TALENTO HUMANO: Competencia del pone, programas, proyectos y modalidades personal, disponibilidad del personal, que establecen los derechos de los niños, niñas, responsable, compromiso, trabajo en equipo, adolescentes y jóvenes en situación de - PROCESOS: Capacidad, diseño, ejecución, vulnerabilidad, amenaza, violencia, abuso o conflicto y procedimientos. con la ley - TECNOLOGÍA: Integridad de datos disponibilidad bases y sistemas, documentos, protección, mantenimiento de sistemas de información. - ESTRATÉGICOS: Direccionamiento estratégico, alineación institucional,	ECONÓMICOS Y FINANCIEROS: disponibilidad de capital, fuentes financiación, inversión, presupuestos. SOCIALES Y CULTURALES: Demografía, responsabilidad social, orden público. TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno digital. LEGALES Y REGLAMENTARIOS: Decisiones jurídicas,	- DISEÑOS DE PROCESOS: Claridad en la descripción del alcance y objetivo de los procesos - INTERACCIONES ENTRE PROCESOS: Relación precisa con otros procesos en cuanto a insumos, productos, usuarios o beneficiarios. - TRANSVERSALIDAD: Procesos que intervienen el mismo recurso o generan información de interés común - PROCEDIMIENTOS ASOCIADOS: Pertinencia en los procedimientos que delimitan la operación.	Base de datos publicación activos de seguimiento de Huida - SUIN, estrategia unidades móviles	Software	Vulnerabilidades Fuentes Personal Ausencia de mecanismos para la identificación y gestión de la información de riesgos de seguridad digital para los activos de información de la sede regional, a los activos fuentes y el SUIN (Sistema de Información de Unidades Móviles).	Falta de conciencia sobre la seguridad de la información de los profesionales de apoyo referente de cada regional, a los activos fuentes y el SUIN (Sistema de Información de Unidades Móviles).	C. Negativas Riesgo de Seguridad de la Información	C. Positivas - Pérdida de imagen y good - Incumplimiento regulatorio - Sanción de Dirección Reprocesos Sanciones	Afectación - Optimización de procesos	DIRECCIÓN GENERAL PROTECCIÓN	Muy Baja	Moderado	Moderada (Muy Baja - Moderada)	Falta de integridad, confidencialidad y disponibilidad de la información de los clientes debido a falta de conciencia sobre la seguridad de la información de los profesionales de apoyo referente de cada regional a los activos fuentes y el SUIN (Sistema de Información de Unidades Móviles), debido a la ausencia de mecanismos de monitoreo estadísticos para la detección de seguridad y acceso no intencionado.	Fuerte(2)	Fuerte(2)	Efectivo	Directamente	Moderadamente	Muy Baja	Moderada (Muy Baja - Moderada)	Moderada (Muy Baja - Moderada)	Mitigar el riesgo	A.7.2. Durante la ejecución del empleo. A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información.	1 - De 6 a 12 meses	Actuar el procedimiento de atención a los incidentes de seguridad de la información para minimizar el riesgo y realizar la mediación del riesgo.	La solución de SIM integra con Portal Web en 2023	ZIP-SI264