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

BIENESTAR FAMILIAR	PROCESO MEJORA E INNOVACIÓN	F3.G1.MI	5/04/2023
		Versión 8	Página 1 de 3
	MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	Clasificación de la Información CLASIFICADA	

1. IDENTIFICACIÓN

ID	FECHA DE IDENTIFICACIÓN DD/MM/AAAA	REGIONAL/SEDE DE LA DIRECCIÓN GENERAL	PROCESO (DUEÑO DEL RIESGO)	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-I-D) + ACTIVO O ACTIVOS DE INFORMACIÓN + ACCION RELACIONADA AL RIESGO + VULNERABILIDADES Y AMENAZAS QUE GENERAN EL RIESGO	TIPO DE RIESGO	CONSECUENCIAS NEGATIVAS	CONSECUENCIAS POSITIVAS	REGIONALES O PROCESOS AFECTADOS
24PSDG1	19/03/2024	SEDE DE LA DIRECCIÓN GENERAL	Protección	Liderar el diseño, actualización y desarrollo de planes, programas, proyectos y modalidades asegurando actuaciones oportunas y con calidad que restablezcan los derechos de los niños, niñas, adolescentes y jóvenes en situación de inobservancia, amenaza, vulneración o en conflicto con la ley	- FINANCIEROS: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada. - TALENTO HUMANO: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional. - PROCESOS: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento. - TECNOLOGÍA: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información	- ECONÓMICOS Y FINANCIEROS: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia. - SOCIALES Y CULTURALES: Demografía, responsabilidad social, orden público. - LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas, acuerdos, entre otros).	- DISEÑO DEL PROCESO: Claridad en la descripción del alcance y objetivo del proceso. - INTERACCIONES CON OTROS PROCESOS: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o beneficiarios. - PROCEDIMIENTOS ASOCIADOS: Pertinencia en los procedimientos que desarrollan los procesos. - RESPONSABLES DEL PROCESO: Grado de autoridad y responsabilidad de los funcionarios frente al proceso. - ACTIVOS DE INFORMACIÓN DEL PROCESO: Información, aplicaciones, hardware, servicios, entre otros, que se deben proteger para garantizar el funcionamiento	BASE DE NIÑOS, NIÑAS Y ADOLESCENTES CON DECLARATORIA DE ADOPTABILIDAD EN FIRME Caracterización de la población con Discapacidad en servicios de Restablecimiento de Derechos DERECHOS DE PETICIÓN, QUEJAS, RECLAMOS, DENUNCIAS Y SUGERENCIAS HISTORIA DE ATENCIÓN Información de NNA desvinculados de grupos armados al margen de la ley Información de Niños, Niñas y Adolescentes atendidos en trámites de restablecimiento de derechos. Lista de espera familias colombianas Reporte de Niños, Niñas y Adolescentes en valoración por Organismo internacional Respuesta de PQRS Seguimiento a Hijos Extramatrimoniales No Reconocidos Solicitantes de adopción Solicitud de Restitución Internacional / Régimen internacional de visitas Solicitud Prueba ADN Solicitudes de adopción Trámite Búsqueda de Orígenes	- Electrónico (Información Digital) - Físico - Electrónico	E Modificación y/o divulgación de la información sin autorización	Personal Talento y/o Factor Humano	Falta de conciencia en la aplicación del procedimiento para la activación y desactivación de usuarios. Demoras en la creación y desactivación de usuarios en el SIM. Entrega de datos personales, credenciales y hacer clic en accesos sospechosos en el marco de un ataque de ingeniería social.	Pérdida de integridad, confidencialidad y disponibilidad de los activos tipo electrónico priorizados del proceso de Protección que se gestionan en SIM, por modificación y/o divulgación de la información sin autorización, debido a la entrega de datos personales, credenciales y hacer clic en accesos sospechosos en el marco de un ataque de ingeniería social, igualmente, por demoras en la creación y desactivación de usuarios en el SIM, falta de conciencia y/o el desconocimiento del procedimiento para la asignación y desactivación de usuarios.	Riesgo de Seguridad de la información	- Pérdidas Financieras - Pérdida de reputacional - Incumplimientos legales - Llamados de Atención	- Optimización de procesos	- SEDE NACIONAL. - PROTECCIÓN
24PSDG2	19/03/2024	SEDE DE LA DIRECCIÓN GENERAL	Protección	Liderar el diseño, actualización y desarrollo de planes, programas, proyectos y modalidades asegurando actuaciones oportunas y con calidad que restablezcan los derechos de los niños, niñas, adolescentes y jóvenes en situación de inobservancia, amenaza, vulneración o en conflicto con la ley	- TALENTO HUMANO: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.	- TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno digital. - LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas, acuerdos, entre otros).	- PROCEDIMIENTOS ASOCIADOS: Pertinencia en los procedimientos que desarrollan los procesos. - RESPONSABLES DEL PROCESO: Grado de autoridad y responsabilidad de los funcionarios frente al proceso. - COMUNICACIÓN ENTRE LOS PROCESOS: Efectividad en los flujos de información determinados en la interacción de los procesos.	Acta de Comité Técnico Consultivo para el Restablecimiento de Derechos Actas comités de adopciones Regional Actas comités Técnico de autorización Actas de Comité Técnico Consultivo de Coordinación de Autoridades Administrativas Actas del Comité Interinstitucional Consultivo para la Prevención de la Violencia Sexual y Atención Integral de los niños, niñas y Adolescentes Víctimas del Abuso Sexual Declaraciones de conformidad de una Adopción Internacional Documentación Equipos Móviles de Protección Integral EMPI Trabajo Infantil Documentación Unidades Móviles a Familias Víctimas de Desplazamiento Forzado Documento constitución de familias en Hogar Sustituto Informes Asistencia Técnica Informes de seguimiento pre y postadopción Instrumentos de Seguimiento de Lineamientos de alto valor nutricional AAVN Listado NNA Afectados por Uso Pornoyo Manipulación de Pólvora Acciones y Seguimiento Mecanismo de Aval Procesos de Adopciones Publicaciones en el espacio "Me Conoces" Reporte de familias en lista de espera Reportes Estrategias de acogimiento Resolución que aprueba Hogar Sustituto Valoraciones Psicosociales Resoluciones Ava Estudios Técnicos Instrumentos de supervisión para la verificación de cumplimiento de obligaciones a contratos de protección en las modalidades de Internado, Hogar Sustituto Entidad, Hogar Sustituto Unidad, Intervención de Apoyo - Apoyo Psicosocial y Apoyo Psicosocial Especializado	- Físico (Información Física) - Electrónico (Información Digital) - Físico - Electrónico	Modificación no autorizada de la información	Personal Talento y/o Factor Humano	Falta de conciencia en la custodia del activo Desconocimiento del manejo de la plataforma Share Point. Acceso no autorizado de usuarios por errores en la asignación de permisos	Pérdida de confidencialidad, integridad y disponibilidad los activos electrónicos priorizados del proceso que se gestionan en Share Point, por la modificación no autorizada de la información, debido a acceso no autorizado de usuarios por errores en la asignación de permisos, falta de conciencia en la custodia del activo y/o desconocimiento del manejo de la plataforma Share Point	Riesgo de Seguridad de la información	- Pérdida de reputacional - Incumplimientos legales - Llamados de Atención - Reprocesos - Sanciones	- Optimización de procesos	- SEDE NACIONAL. - PROTECCIÓN
24PSDG3	19/03/2024	SEDE DE LA DIRECCIÓN GENERAL	Protección	Liderar el diseño, actualización y desarrollo de planes, programas, proyectos y modalidades asegurando actuaciones oportunas y con calidad que restablezcan los derechos de los niños, niñas, adolescentes y jóvenes en situación de inobservancia, amenaza, vulneración o en conflicto con la ley	- TALENTO HUMANO: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional. - PROCESOS: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.	- 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, entre otros).	- INTERACCIONES CON OTROS PROCESOS: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o beneficiarios. - PROCEDIMIENTOS ASOCIADOS: Pertinencia en los procedimientos que desarrollan los procesos.	Actas comités de adopciones Regional Declaraciones de conformidad de una Adopción Internacional DERECHOS DE PETICIÓN, QUEJAS, RECLAMOS, DENUNCIAS Y SUGERENCIAS Documentación Unidades Móviles a Familias Víctimas de Desplazamiento Forzado HISTORIA DE ATENCIÓN Información de Niños, Niñas y Adolescentes atendidos en trámites de restablecimiento de derechos. Informes de seguimiento pre y postadopción Procesos de Adopciones Reporte de familias en lista de espera Respuesta de PQRS Solicitantes de adopción Solicitud Prueba ADN Valoraciones Psicosociales	- Físico (Información Física) - Físico - Electrónico	Acceso de colaboradores no autorizados a la ruta de Share Point	Talento y/o Factor Humano Lugar Personal	Desconocimiento del Procedimiento de Organización de Archivos, la Guía de Rotulación de la información y del procedimiento de préstamo y devolución de expedientes. Ausencia de controles de acceso físico a las áreas de archivo. Falta de conciencia acerca de la seguridad en la custodia de los activos. Ausencia de controles de acceso físico a las áreas de archivo.	Pérdida de integridad, disponibilidad y confidencialidad de la información de los activos de información físicos priorizados del proceso, debido al incumplimiento de los procedimientos para la gestión documental, por falta de conciencia en la seguridad de la información de los colaboradores acerca de la custodia de los activos, la ausencia de controles de acceso físico a las áreas de archivo o desconocimiento del Procedimiento de Organización de Archivos, la Guía de Rotulación de la Información y del procedimiento de préstamo y devolución de expedientes.	Riesgo de Seguridad de la información	- Pérdida de reputacional - Incumplimientos legales - Llamados de Atención - Reprocesos - Sanciones	- Optimización de procesos	- SEDE NACIONAL. - PROTECCIÓN
24PSDG4	19/03/2024	SEDE DE LA DIRECCIÓN GENERAL	Protección	Liderar el diseño, actualización y desarrollo de planes, programas, proyectos y modalidades asegurando actuaciones oportunas y con calidad que restablezcan los derechos de los niños, niñas, adolescentes y jóvenes en situación de inobservancia, amenaza, vulneración o en conflicto con la ley	- FINANCIEROS: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada. - TALENTO HUMANO: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional. - PROCESOS: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento. - TECNOLOGÍA: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información - ESTRATÉGICOS: Direccionamiento estratégico, planeación institucional,	- ECONÓMICOS Y FINANCIEROS: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia. - POLÍTICOS: Cambios de gobierno, legislación, políticas públicas, regulación. - SOCIALES Y CULTURALES: Demografía, responsabilidad social, orden público. - TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno digital. - AMBIENTALES: Emisiones y residuos,	- DISEÑO DEL PROCESO: Claridad en la descripción del alcance y objetivo del proceso. - INTERACCIONES CON OTROS PROCESOS: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o beneficiarios. - TRANSVERSALIDAD: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos del ICBF - PROCEDIMIENTOS ASOCIADOS: Pertinencia en los procedimientos que desarrollan los procesos.	Base de datos población víctima de desplazamiento forzado - SIUM, estrategia unidades móviles	- Software	E Falta de conciencia acerca de la seguridad de la información por parte de los profesionales de apoyo o referentes de cada regional a los archivos fuentes y a SIUM (Sistema de Información de Unidades Móviles).	Talento y/o Factor Humano Personal	Persona mal intencionado Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad Falta de conciencia acerca de la custodia de la información por parte de los profesionales de apoyo o referentes de cada regional de los archivos fuentes y al SIUM (Sistema de Información de Unidades Móviles)	Pérdida de integridad, confidencialidad y disponibilidad de la información de Base de datos población víctima de desplazamiento forzado - SIUM y estrategia unidades móviles (Sistema de Información de Unidades Móviles) por la falta de conciencia acerca de la custodia de la información por parte de los profesionales de apoyo o referentes de cada regional de los archivos fuentes y al SIUM (Sistema de Información de Unidades Móviles), debido a la ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad y persona mal intencionado	Riesgo de Seguridad de la información	- Pérdida de reputacional - Incumplimientos legales - Llamados de Atención - Reprocesos - Sanciones	- Optimización de procesos	- SEDE NACIONAL. - PROTECCIÓN

2. ANÁLISIS / 3. VALORACIÓN / 4. MANEJO

ID	PROBABILIDAD	IMPACTO	NIVEL ANTES DE CONTROLES	DESCRIPCIÓN DE LOS CONTROLES ACTUALES	Diseño	Ejecución	Efectividad	El control ayuda a disminuir la probabilidad	El control ayuda a disminuir el impacto	PROBABILIDAD	NIVEL ANTES DE CONTROLES	NIVEL DE RIESGO (Después de Controles)	OPCIONES TRATAMIENTO	CONTROLES ANEXO A ISO 27001:2013	PRIORIDAD	MATERIALIZACIÓN	OBSERVACIONES	PRECEDE
24PSDG1	Muy Baja	Mayor	Alto (Muy Baja - Mayor)	NOMBRE: Realizar la asignación de usuarios de acuerdo con el procedimiento de asignación de usuarios RESPONSABLE: Profesional Especializado PERIODICIDAD: Cuando ocurra PROPÓSITO: Realizar la activación y desactivación de usuarios oportunamente garantizando que se cuente con las autorizaciones respectivas. OBSERVACIÓN O DESVIACIÓN: Informar a MIS las solicitudes pendientes para que se gestionen EVIDENCIA: Reporte de la activación de usuarios de SIM - Casos registrados en MIS. TIPO DE CONTROL: Detectivo NATURALEZA DEL CONTROL: Semiautomático CONTROL DOCUMENTADO: SÍ	Fuerte (3)	Fuerte (3)	Efectivo	Directamente	No disminuye	Muy Baja	Alto (Muy Baja - Mayor)	Alto (Muy Baja - Mayor)	Mitigar el riesgo	A.8.1. Responsabilidad por los Activos. - A.8.1.3. Uso Aceptable de los Activos. A.7.2. Durante la ejecución de empleo. - A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la información.	2 - De 4 a 8 meses	Activar el procedimiento de atención a incidentes de seguridad de la información para materializar el riesgo, realizar la revaloración del riesgo.		23PSDG1
24PSDG2	Media	Moderado	Moderado (Media - Moderado)	NOMBRE: 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 las partes interesadas. OBSERVACIÓN O DESVIACIÓN: Brindar asesoría y acompañamiento que tiene como fin fortalecer el conocimiento, las competencias y habilidades de las partes interesadas. Se encuentra documentado en el Procedimiento Asistencia Técnica. EVIDENCIA: Listados de Asistencia. TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Manual CONTROL DOCUMENTADO: SÍ NOMBRE: Responder a las solicitudes de permisos en la carpeta de SharePoint RESPONSABLE: Profesional Especializado PERIODICIDAD: Cuando ocurra (se reportarán las evidencias de cumplimiento conforme al PSGSI) PROPÓSITO: Asignar privilegios de acceso a las carpetas creadas para el almacenamiento de la información final del proceso. OBSERVACIÓN O DESVIACIÓN: Revisión de los permisos de los/las colaboradores que hacen parte del proceso. EVIDENCIA: Correos electrónicos TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Manual CONTROL DOCUMENTADO: SÍ	Fuerte (3)	Fuerte (3)	Efectivo	Directamente	No disminuye	Media	Moderado (Media - Moderado)	Moderado (Muy Baja - Moderado)	Mitigar el riesgo	A.9.1. Requisitos del Negocio para Control de Acceso. - A.9.1.1. Política de Control de Acceso. A.9.2. Gestión de Acceso de Usuarios. - A.9.2.5. Revisión de los derechos de acceso de usuarios.	2 - De 4 a 8 meses	Activar el procedimiento de atención a incidentes de seguridad de la información para materializar el riesgo, realizar la revaloración del riesgo.	La valoración del riesgo continua como la 2023	23PSDG2
24PSDG3	Media	Moderado	Moderado (Media - Moderado)	NOMBRE: Solicitar a través de préstamo de carpeta de adopciones RESPONSABLE: Profesional PERIODICIDAD: Manual PROPÓSITO: Realizar el seguimiento al préstamo de las carpetas de adopciones OBSERVACIÓN O DESVIACIÓN: Informar al jefe inmediato EVIDENCIA: Copia de préstamo de carpetas TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Manual CONTROL DOCUMENTADO: SÍ	Fuerte (3)	Fuerte (3)	Efectivo	Directamente	No disminuye	Media	Moderado (Media - Moderado)	Moderado (Muy Baja - Moderado)	Mitigar el riesgo	A.11.1. Áreas Seguras. - A.11.1.3. Seguridad de oficinas, recintos e instalaciones. A.8.1. Responsabilidad por los Activos - A.8.1.3. Uso Aceptable de los Activos.	2 - De 4 a 8 meses	Activar el procedimiento de atención a incidentes de seguridad de la información para materializar el riesgo, realizar la revaloración del riesgo.	La valoración del riesgo continua como la 2023	23PSDG3
24PSDG4	Muy Baja	Moderado	Moderado (Muy Baja - Moderado)	Realizar Asistencia Técnica a los profesionales de apoyo o referentes de cada regional de ICBF. Especialmente en lo referente a la concientización de uso de información reservada (base de datos y claves) la cual no puede ser compartida. RESPONSABLE: Profesional Especializado PERIODICIDAD: Cuando ocurra PROPÓSITO: Lograr sensibilizar a los profesionales de apoyo y referentes de cada regional en el uso del Sistema de Información de Unidades Móviles SIUM el cual está encriptado. OBSERVACIÓN O DESVIACIÓN: Llamado de atención a los profesionales de apoyo o referentes de cada regional del ICBF debido a incumplimiento de las obligaciones contractuales.	Fuerte (3)	Fuerte (3)	Efectivo	Directamente	No disminuye	Muy Baja	Moderado (Muy Baja - Moderado)	Moderado (Muy Baja - Moderado)	Mitigar el riesgo	A.7.2. Durante la ejecución de empleo. - A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la información.	2 - De 4 a 8 meses	Activar el procedimiento de atención a incidentes de seguridad de la información para materializar el riesgo, realizar la revaloración del riesgo.	La valoración del riesgo continua como la 2023	23PSDG4