FORM-01

MAPA DE RIESGO DE GESTIÓN - CORRUPCIÓN - SEGURIDAD DE LA INFORMACIÓN - FISCALES

PROCESO: GESTIÓN GERENCIAL Y PLANEACIÓN INSTITUCIONAL	CÓDIGO: GE-M-01	VERSIÓN: 07/04/2025	TIPO	PÁGINA: 1 DE 1

EVALUACIÓN DE RIESGO DE:	GESTIÓN DE LA INFORMACIÓN		
FECHA DE REVISIÓN Y APROBACIÓN:	1/02/2025	VIGENCIA:	2025
FECHA DE SEGUIMIENTO:	1-dic-25		

Identificación del riesgo								Análisis del riesgo inherente						Evaluación del riesgo - Valoración de los controles										Evaluación del riesgo - Nivel del riesgo residual					Plan de Acción					
Referencia	Proceso	Subproceso	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad Inherente	%	Criterios de Impacto	Impacto Inherente	%	Zona de Riesgo Inherente	No. Control	Descripción del Control	Afectación	Atributos: Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Probabilidad Residual	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento	Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Observaciones al Seguimiento	Estado
1	Gestión de Información	Seguridad de la Información	Económico y Reputacional	Brechas en controles de acceso	Políticas de seguridad débiles	Acceso no autorizado a información clínica de pacientes.	Pérdida de la confidencialidad	4380	Alta	80%	El riesgo afecta la imagen de la entidad a nivel nacional con efecto publicitario sostenido a nivel país	Catastrófico	100%	Extremo	1	Autenticación de doble factor	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	40%	Bajo	40%	Catastrófico	100%	Extremo	Reducir (mitigar)	Fortalecer controles de acceso y capacitar al personal. Listado de asistencia de capacitaciones - Evidencia	Líder TIC	1/01/2025	TRIMESTRAL	https://nuevosamaniedetalpagina.gov.co/capacitar-ciberseguridad-en-salud-enfocado-a-usuarios-de-la-informacion/ https://nuevosamaniedetalpagina.gov.co/capacitar-ciberseguridad-en-salud-enfocado-a-usuarios-de-la-informacion/	FINALIZADO
															2	Segmentación de acceso por perfil y rol	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	24,0%	Bajo	24%	Catastrófico	100%	Extremo	Reducir (mitigar)	Mapear funciones de cada cargo y configurar accesos en el software. Evidencia - Listado actualizado de roles y matriz de permisos						
															3	Monitoreo y alertas de accesos inusuales	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	14,4%	Moderado	14%	Catastrófico	100%	Extremo	Reducir (mitigar)	Configurar reglas de alerta en el sistema de información clínica y habilitar reportes periódicos. Log de alertas generadas y acciones correctivas documentadas. - Evidencia					PENDIENTE ACTUALIZACION SOFTWARE INDIGO	
2	Gestión de Información	Seguridad de la Información	Reputacional	Falta técnica en sistemas de respaldo	Falta de revisión de copias de seguridad	Pérdida de datos por fallo de respaldo.	Pérdida de la confidencialidad	240	Media	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	Copias de seguridad automáticas	Impacto	Correctivo	Manual	25%	Documentado	Continua	Con Registro	60%	Medio	60%	Moderado	45%	Moderado	Reducir (mitigar)	Implementar revisión mensual de copias de seguridad. Registro de revisión mensual - Evidencia	Líder TIC	1/01/2025	TRIMESTRAL	https://nuevosamaniedetalpagina.gov.co/copia-de-seguridad-backup/ https://nuevosamaniedetalpagina.gov.co/copia-de-seguridad-backup/	FINALIZADO
															2	Implementar una rutina mensual para verificar la integridad de las copias de seguridad mediante restauraciones de prueba. Éxito satisfactorio que los respaldos no están corruptos y que pueden recuperarse correctamente.	Impacto	Correctivo	Manual	25%	Documentado	Continua	Con Registro	0%	Muy Bajo	0%	Leve	0%	Bajo	Reducir (mitigar)	Programar restauraciones de pruebas en entornos controlados. Informes de pruebas de restauración archivados - Evidencia						
															3	Implementar una política de respaldos externos que incluya almacenamiento en una ubicación distinta a la sede principal o en la nube con cifrado y redundancia para garantizar la recuperación ante desastres locales.	Impacto	Correctivo	Manual	25%	Documentado	Continua	Con Registro	0%	Muy Bajo	0%	Leve	0%	Bajo	Reducir (mitigar)	Configurar sincronización automática de respaldos hacia nube certificada. Registro de sincronización en plataforma externa - Evidencia					Actualmente, la **ESE Carmen Emilia Ospina (HSCEO)** no cuenta con infraestructura de almacenamiento en nube para la sincronización de copias de seguridad. La gestión de la información institucional reposa en **servidores locales bajo la plataforma PAI PRIMA**, administrada internamente por el área de Tecnología de la Información y las Comunicaciones (TIC).	
3	Gestión de Información	Seguridad de la Información	Económico y Reputacional	Descarga de archivos maliciosos	Falta de capacitación y protección en equipos	Malware que afecte la disponibilidad de servicios médicos.	Pérdida de la confidencialidad	4380	Alta	80%	El riesgo afecta la imagen de la entidad a nivel nacional con efecto publicitario sostenido a nivel país	Catastrófico	100%	Extremo	1	Instalación de soluciones antivirus en todos los equipos de la organización, con actualizaciones automáticas y protección en tiempo real habilitada para detectar amenazas en tiempo de ejecución.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	48,0%	Medio	48%	Catastrófico	100%	Extremo	Reducir (mitigar)	Verificar instalación y habilitar actualizaciones automáticas en todos los dispositivos. Reportes de consola de administración del antivirus - Evidencia	Líder TIC	1/01/2025	TRIMESTRAL	https://nuevosamaniedetalpagina.gov.co/antivirus/	En curso
															2	Implementar políticas en los equipos para que solo personal autorizado pueda instalar software, reduciendo el riesgo de instalación de programas maliciosos o sospechosos.	Probabilidad	Detectivo	Automático	40%	Documentado	Continua	Con Registro	28,8%	Bajo	29%	Catastrófico	100%	Extremo	Reducir (mitigar)	Usar directivas de grupo (GPO) o herramientas de gestión centralizada (MDM/Intune). Registro de bloqueos o auditorías de software instalado. - Evidencia					https://nuevosamaniedetalpagina.gov.co/antivirus/	
															3	Realizar capacitaciones trimestrales al personal médico y administrativo sobre buenas prácticas de navegación, reconocimiento de correos fraudulentos (phishing) y manejo	Impacto	Correctivo	Manual	25%	Documentado	Continua	Con Registro	28,8%	Bajo	29%	Mayor	75%	Alto	Reducir (mitigar)	Capacitar al personal en prevención de ciberataques. Registro de asistencia - Evidencias					https://nuevosamaniedetalpagina.gov.co/capacitacion-area-tic/	
4	Gestión de Información	Seguridad de la Información	Económico y Reputacional	Error humano en envío de documentos	Falta de control en revisión de información	Divulgación accidental de información confidencial.	Pérdida de la confidencialidad	240	Media	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	Antes de enviar información sensible (como historias clínicas o datos personales) se debe revisar y validar la información obligatoria por parte del emisor y un segundo revisor autorizado.	Probabilidad	Detectivo	Manual	50%	Documentado	Continua	Con Registro	42,0%	Medio	42%	Moderado	60%	Moderado	Reducir (mitigar)	Implementar protocolo de doble revisión previa al envío de documentos sensibles. Formato o log de validación con doble persona - Evidencia.	Líder TIC	1/01/2025	TRIMESTRAL	https://nuevosamaniedetalpagina.gov.co/wp-content/uploads/sites/2/2025/01/%C3%B3rdenes-de-servicio-1.7.5.-%28Recuperado-0-%29.docx?wdOrigin=BROWSELINK&wdLOR=c7C7D7A0-7F8A-4F0A-A7D7-A7D7A0A7D7A0&ssr=1&web=1&wdenc=1&hid=1789204766_copia_de_pdf	FINALIZADO
															2	Implementar el uso exclusivo de plataformas seguras y cifradas para el envío de información confidencial, evitando el uso de correo personal, redes sociales o pen drives no institucionales.	Probabilidad	Detectivo	Manual	50%	Documentado	Continua	Con Registro	0,0%	Muy Bajo	0%	Mayor	75%	Alto	Reducir (mitigar)	Configurar y capacitar el uso de plataformas seguras (correo cifrado, portales internos). Log del sistema de mensajería y trazabilidad de envíos - Evidencia					https://nuevosamaniedetalpagina.gov.co/capacitacion-area-tic/	
															3	Capacitación obligatoria y periódica a todo el personal sobre políticas institucionales de manejo de información confidencial, con énfasis en errores comunes y sus consecuencias legales y éticas.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	25,2%	Bajo	25%	Moderado	60%	Moderado	Reducir (mitigar)	Desarrollar e impartir capacitación sobre manejo y confidencialidad de la información. Registro de asistencia - Evidencia					https://nuevosamaniedetalpagina.gov.co/capacitar-capacitaciones-sobre-manejo-y-seguridad-y-privacidad-de-la-informacion/	
5	Gestión Documental	Gestión Documental	Económico y Reputacional	Documentos mal clasificados o extraviados por errores humanos	Falta de procedimiento estandarizado para almacenamiento y control de archivos físicos	Pérdida de documentos físicos relevantes como historias clínicas o actas administrativas	Pérdida de la confidencialidad	240	Media	60%	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal	Mayor	80%	Alto	1	Todos los documentos relevantes (historias clínicas, actas, resoluciones) se registran con un código único en un sistema de control físico (manual o digital), que permite su trazabilidad y localización rápida.	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	30,0%	Bajo	30%	Mayor	80%	Alto	Reducir (mitigar)	Diseñar un formato de registro de documentos con numeración única - Evidencia del seguimiento Capacitar al personal de archivo en el uso del formato y el sistema de codificación - Actas de asistencia Evidencia	Líder TIC - Gestión Documental	1/01/2025	TRIMESTRAL	https://nuevosamaniedetalpagina.gov.co/wp-content/uploads/sites/2/2025/01/%C3%B3rdenes-de-servicio-1.7.5.-%28Recuperado-0-%29.docx?wdOrigin=BROWSELINK&wdLOR=c7C7D7A0-7F8A-4F0A-A7D7-A7D7A0A7D7A0&ssr=1&web=1&wdenc=1&hid=1789204766_copia_de_pdf https://nuevosamaniedetalpagina.gov.co/wp-content/uploads/sites/2/2025/01/%C3%B3rdenes-de-servicio-1.7.5.-%28Recuperado-0-%29.docx?wdOrigin=BROWSELINK&wdLOR=c7C7D7A0-7F8A-4F0A-A7D7-A7D7A0A7D7A0&ssr=1&web=1&wdenc=1&hid=1789204766_copia_de_pdf https://nuevosamaniedetalpagina.gov.co/wp-content/uploads/sites/2/2025/01/%C3%B3rdenes-de-servicio-1.7.5.-%28Recuperado-0-%29.docx?wdOrigin=BROWSELINK&wdLOR=c7C7D7A0-7F8A-4F0A-A7D7-A7D7A0A7D7A0&ssr=1&web=1&wdenc=1&hid=1789204766_copia_de_pdf	FINALIZADO
															2	Se implementa un sistema de control de préstamos de historias clínicas físicas, ya sea electrónico (que registran quién accede, cuándo, y para qué solicita un documento, exigiendo devolución en tiempo definido.	Probabilidad	Detectivo	Manual	30%	Documentado	Continua	Con Registro	17,6%	Muy Bajo	18%	Moderado	60%	Moderado	Reducir (mitigar)	Crear una política interna de préstamos de documentos. Establecer un procedimiento de control con responsables y tiempo límite. Auditar mensualmente los movimientos registrados - Evidencia					https://nuevosamaniedetalpagina.gov.co/wp-content/uploads/sites/2/2025/01/%C3%B3rdenes-de-servicio-1.7.5.-%28Recuperado-0-%29.docx?wdOrigin=BROWSELINK&wdLOR=c7C7D7A0-7F8A-4F0A-A7D7-A7D7A0A7D7A0&ssr=1&web=1&wdenc=1&hid=1789204766_copia_de_pdf https://nuevosamaniedetalpagina.gov.co/wp-content/uploads/sites/2/2025/01/%C3%B3rdenes-de-servicio-1.7.5.-%28Recuperado-0-%29.docx?wdOrigin=BROWSELINK&wdLOR=c7C7D7A0-7F8A-4F0A-A7D7-A7D7A0A7D7A0&ssr=1&web=1&wdenc=1&hid=1789204766_copia_de_pdf	
															3	Los documentos se almacenan en condiciones adecuadas (estanterías, contenedores, con humedad, temperatura adecuada) y con protección contra deterioro físico, incendios o inundaciones.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	16,5%	Muy Bajo	16%	Mayor	80%	Alto	Reducir (mitigar)	Evaluar el estado actual del archivo (diagnóstico) y crear un plan de mejoramiento. Remitir seguimiento - Evidencia. Instalar señalización y normas de conservación. Remitir evidencia - Evidencia					https://nuevosamaniedetalpagina.gov.co/programa-de-gestion-documental/	
6	Gestión Documental	Gestión Documental	Reputacional	Ingreso de personal no autorizado a zonas de archivo o acceso digital sin credenciales adecuadas	Falta de control de accesos físicos y digitales	Acceso no autorizado a historias clínicas o documentos personales	Pérdida de la confidencialidad	96	Media	60%	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal	Mayor	80%	Alto	1	Se restringe el acceso físico al archivo mediante cerraduras con llave, tarjeta o código, permitiendo la entrada solo al personal autorizado. Se lleva un registro diario de accesos.	Probabilidad	Preventivo	Manual	40%	Documentado	Diaria	Con Registro	36,0%	Bajo	36%	Mayor	80%	Alto	Reducir (mitigar)	Instalar cerraduras electrónicas o control de ingreso físico. Elaborar un listado actualizado de personal autorizado. Implementar bitácora de ingreso firmada. Remitir Evidencias.	Líder TIC - Gestión Documental	1/01/2025	TRIMESTRAL	https://nuevosamaniedetalpagina.gov.co/actualizar-auditorias-conforme-al-plan-de-accion-de-la-vigencia-de-acuerdo-a-la-nueva-estructura-funcional-del-software-indigo/	FINALIZADO
															2	Se asegura que el sistema digital de historias clínicas solo sea accedido mediante credenciales personalizadas (usuario y contraseña) y en ciertos casos con doble autenticación (2FA).	Probabilidad	Preventivo	Manual	40%	Documentado	Diaria	Con Registro	36,0%	Bajo	36%	Mayor	80%	Alto	Reducir (mitigar)	Configurar roles y permisos en el sistema de historia clínica. Establecer política de renovación de contraseñas cada 90 días. Activar autenticación de doble factor para accesos externos o privilegiados.						
															3	El personal que maneja información sensible recibe capacitación periódica sobre normativas de protección de datos, ética en el manejo de historias clínicas y consecuencias legales de la violación de la confidencialidad.	Probabilidad	Preventivo	Manual	40%	Documentado	Mensual	Con Registro	36,0%	Bajo	36%	Mayor	80%	Alto	Reducir (mitigar)	Programar capacitaciones trimestrales con el área jurídica o de seguridad de la información. Remitir evidencia de las actas de asistencia					https://nuevosamaniedetalpagina.gov.co/capacitaciones-sobre-habeas-y-manejo-documentos/	