

Proceso:		Información, Documentación y Atención al Ciudadano										
Objetivo:		Gestionar y administrar los recursos y servicios de tecnologías de la información y las comunicaciones con el fin de administrar eficientemente todos los registros, documentos y archivos del Sanatorio de Contratación E.S.E. con el objetivo de atender de manera oportuna y eficaz los requerimientos de los usuarios; evaluando sus necesidades y expectativas tanto individuales como colectivas.										
Alcance:		Aplica a las actividades de atención de necesidades de los ciudadanos incluidas las solicitudes de atención en salud así como la recepción y la administración de la información y documentación a través de una óptima y moderna administración de los Sistemas de Información y Comunicaciones del Sanatorio de Contratación E.S.E.										
Fecha actualización:		12/04/2023										
Actualizado por:		Alejandrina Ruiz Rueda / Alvaro Gamboa Rojas									SEGUIMIENTO CUATRIMESTRAL AÑO 2026	
Referencia	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia	Descripción del Control	Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento Of. Control Interno	Observaciones 2 Cuatrim 2026
I	Afectación económica y reputacional	Fuga de información	Resultado de revelar información reservada y clasificada para beneficio propio o de un tercero	Posibilidad de incurrir en pérdida económica y/o reputacional debido a la fuga de información como resultado de revelar información reservada y clasificada para beneficio propio o de un tercero.	Corrupción	365	La oficina de Talento Humano implementa control de Seguridad de los recursos humanos (A.7).	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	Talento Humano	Implementado	24/08/2026	Para todo aspirante a un nuevo cargo se verifica los antecedentes Judiciales, Contraloría y Procuraduría. Así mismo su hoja de vida y soportes son cotejados con los requisitos establecidos en el manual de funciones para el cual se está postulando el candidato.
								Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Talento Humano y Gestión Contractual	30/10/2023	24/08/2026	El compromiso de confidencialidad y no divulgación de la información es firmado por todos los contratistas junto con los documentos soportes que hacen parte del CPS. Así mismo por los funcionarios nuevos que ingresan a la planta de personal de la entidad.
								La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Talento Humano y Gestión Contractual	30/10/2023	24/08/2026	El compromiso de confidencialidad y no divulgación de la información es firmado por todos los contratistas junto con los documentos soportes que hacen parte del CPS. Así mismo por los funcionarios nuevos que ingresan a la planta de personal de la entidad.
								Todos los empleados de la entidad, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	Talento Humano y Sistemas	30/11/2023	24/08/2026	Cuando el funcionario de planta ó contratista ingresa a la entidad se les da a conocer las políticas y procedimientos pertinentes a su cargo. Y cuando hay cambios o actualizaciones de los mismos se da a conocer a los funcionarios del área por parte del Jefe del proceso.
								Proteger los medios físicos que contienen información contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Sistemas y Comunicaciones	30/06/2023	24/08/2026	No se ha realizado traslado de información a través de un medio físico. La información se transfiere por correos electrónicos y a través de bases de datos de Eps o Ministerio de Salud las cuales se manejan a través de plataformas via internet.
								Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Control interno disciplinario	30/12/2023	24/08/2026	El Sanatorio de Contratación, en la planta de personal, no tiene creado el cargo para ejercer funciones del Comité Disciplinario. Y tampoco cuenta con funcionario encargado de dichas funciones. Por lo anterior, no está documentado el proceso disciplinario en caso de cometerse por parte de algun funcionario violación a la seguridad de la información.
							La oficina de Sistemas y Comunicaciones implementa control de acceso.	Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Sistemas y Comunicaciones	30/04/2023	24/08/2026	El 22 de agosto del 2024, se socializó en el Comité Institucional de Gestión y Desempeño: "La política de seguridad de la información" y el "Manual de creación y eliminación de usuarios de los sistemas de información". Los anteriores documentos están pendientes por actualizar.

Referencia	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia	Descripción del Control	Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento Of. Control Interno	Observaciones 2 Cuatrimestre 2026
1	Afectación económica y reputacional	Fuga de información	Resultado de revelar información reservada y clasificada para beneficio propio o de un tercero	Posibilidad de incurrir en pérdida económica y/o reputacional debido a la fuga de información como resultado de revelar información reservada y clasificada para beneficio propio o de un tercero.	Corrupción	365	La oficina de Sistemas y Comunicaciones implementa control de acceso.	Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Sistemas y Comunicaciones	30/04/2023	24/08/2026	En el documento "Manual de creación y eliminación de usuarios de los sistemas de información", en la etapa 3: "Actualizar permisos en cuentas de usuarios" quedó contemplado que a través de la mesa de servicios se debe reportar a los líderes de proceso involucrados, vía correo electrónico, el listado de accesos a los sistemas de información que tiene el usuario objeto del traslado y solicitará la validación pertinente para confirmar si. Los accesos se deben mantener, algún acceso debe ser revocado, se debe adicionar un nuevo permiso de acceso. Los líderes de proceso involucrados deben reportar al correo mesadeservicios@sanatoriocontratacion.gov.co, las modificaciones requeridas para que el usuario solo cuente con los permisos de acceso mínimos para el desempeño de sus funciones. Pendiente por actualizar el Manual.
								Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Talento Humano y Sistemas y Comunicaciones	30/11/2023	24/08/2026	En el documento "Manual de creación y eliminación de usuarios de los sistemas de información", en la etapa 3: "Actualizar permisos en cuentas de usuarios" se encuentra el paso a paso del proceso de registro y cancelación de registros de usuarios. Pendiente por actualizar el Manual
								Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	Sistemas y Comunicaciones	30/04/2023	24/08/2026	En el documento "Manual de creación y eliminación de usuarios de los sistemas de información" está el paso a paso para registrar usuarios y su cancelación en los sistemas de información de la Institución" Pendiente por actualizar
								Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Sistemas y Comunicaciones	30/04/2023	24/08/2026	La Oficina de Gestión de Información y Tecnología restringirá las cuentas de usuario con acceso privilegiado a las plataformas tecnológicas, para ser accedidas solo por el personal autorizado y no deberán ser utilizadas para tareas rutinarias o periódicas del sistema o aplicación.
								Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	Sistemas y Comunicaciones	30/06/2023	24/08/2026	Se realiza periódicamente depuración de base de datos de usuarios administradores que estén activos e inactivos en el sistema
								Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	Talento Humano y Gestión Contractual	30/06/2023	24/08/2026	En el documento "Manual de creación y eliminación de usuarios de los sistemas de información" está el paso a paso en la etapa 2 - Cancelar cuenta de usuarios: para servidores públicos, contratistas y proveedores,
								Implementar Política sobre el uso de los servicios de red: Solo permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Sistemas y Comunicaciones	30/04/2023	24/08/2026	El uso de la red se encuentra restringido a sólo equipos de la Institución. Quien requiera conectarse a la red (funcionarios y/o contratistas) deben solicitar por medio de correo electrónico al área de Sistemas
								Implementar una política sobre el uso de controles criptográficos para la protección de la información.	Sistemas y Comunicaciones	30/04/2023	24/08/2026	Se está adecuando la red e infraestructura para implementar la política sobre controles criptográficos.
								Desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	Sistemas y Comunicaciones	30/04/2023	24/08/2026	Por la infraestructura de la red, en el Sanatorio de Contratación no se implementa las llaves criptográficas.
								Se debería adoptar una política de escritorio limpio y una política de pantalla limpia en las instalaciones de procesamiento de información.	Sistemas y Comunicaciones	30/04/2023	24/08/2026	A la fecha, la gran mayoría de usuarios no están aplicando la política de pantalla limpia. Se procederá de manera rígida y estricta por parte de l área de las TIC a bloquear el escritorio y eliminar carpetas que deberían estar en la carpeta de documentos.
								Hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	Sistemas y Comunicaciones	30/04/2023	24/08/2026	A la fecha el Sanatorio no cuenta con la infraestructura para realizar dicha labor.
								Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la entidad se deben acordar con estos y se deberían documentar.	Sistemas y Comunicaciones	30/04/2023	24/08/2026	Pendiente actualizar, la Política de seguridad y privacidad de la información, adoptada mediante Resolucion No. 446 de junio 2024.

Referencia	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia	Descripción del Control	Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento Of. Control Interno	Observaciones 2 Cuatrim 2026
1	Afectación económica y reputacional	Fuga de información	Resultado de revelar información reservada y clasificada para beneficio propio o de un tercero	Posibilidad de incurrir en pérdida económica y/o reputacional debido a la fuga de información como resultado de revelar información reservada y clasificada para beneficio propio o de un tercero.	Corrupción	365	La oficina de Sistemas y Comunicaciones implementa control de Seguridad de las operaciones.	Los coordinadores de área, deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	Sistemas y Comunicaciones	30/04/2023	24/08/2026	El encargado de las TIC , ya tiene organizada el área de cartera y facturación en cuanto al almacenamiento en red de dichas dependencias.
								Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Sistemas y Comunicaciones	30/04/2023	24/08/2026	El encargado de las TIC , revisa todas las noches, la red y los procesos del servidor.
								Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	Todos los procesos	Permanente	24/08/2026	Los procedimientos de operación que han sido documentados se encuentran en el drive del Sistema Integrado de gestión y en las respectivas oficinas que hacen uso del mismo, sin embargo, se encuentra pendiente actualizar procedimientos de las diferentes áreas.
								Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Sistemas y Comunicaciones	30/06/2023	24/08/2026	Se cuenta con antivirus (control detectivo) sólo en los equipos que tienen licencia. Pendiente parametrizar el antivirus en cada equipo
								Implementar procedimientos para controlar la instalación de software en sistemas operativos.	Sistemas y Comunicaciones	30/06/2023	24/08/2026	Toda instalación de Software está controlada para directrices de usuarios con dominio
							La oficina de Sistemas y Comunicaciones implementa Gestión de incidentes de seguridad de la información	Elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Sistemas y Comunicaciones	30/06/2023	24/08/2026	Contamos con la CSIRT (desde noviembre 2025), el cual, monitorea la infraestructura de la red.
								Obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Sistemas y Comunicaciones	30/06/2023	24/08/2026	Contamos con la CSIRT (desde noviembre 2025), el cual, monitorea la infraestructura de la red.
2	Afectación económica y reputacional	Pérdida de información	Debido al deterioro del medio de conservación (físico y/o digital) o extravío del documento.	Posibilidad de incurrir en pérdida económica y/o reputacional debido a la pérdida de información como resultado del deterioro del medio de conservación (físico y/o digital) o extravío del documento.	Ejecución y administración de procesos	500	El Comité Institucional de Gestión y Desempeño Identifica los activos organizacionales y define las responsabilidades de protección apropiadas.	Identificar los activos asociados con la información y las instalaciones de procesamiento de información y elaborar y mantener un inventario de estos activos.	Sistemas y Comunicaciones	31/08/2023	24/08/2026	Ya se tienen identificados los activos de información y el inventario de equipos.
								Desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la entidad	Sistemas Integrados de Gestión	Permanente	24/08/2026	Se está empezando a implementar en las áreas financieras, sin embargo, aún no se encuentra documentado el procedimiento de etiquetado de la información.
							La oficina de Sistemas y Comunicaciones implementa gestión de medios removibles.	Implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la entidad.	Sistemas y Comunicaciones	31/08/2023	24/08/2026	A la fecha no se han elaborado éstos procedimientos.
							La oficina de Sistemas y Comunicaciones implementa política de copias de respaldo.	Hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	Sistemas y Comunicaciones	30/04/2023	24/08/2026	A la fecha el Sanatorio no cuenta con la infraestructura para realizar dicha labor.
							La oficina de Sistemas y Comunicaciones implementa Gestión de incidentes de seguridad de la información	Elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Sistemas y Comunicaciones	30/06/2023	24/08/2026	Contamos con la CSIRT (desde noviembre 2025), el cual, monitorea la infraestructura de la red.
								Obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la entidad a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Sistemas y Comunicaciones	30/06/2023	24/08/2026	Los equipos se mantienen con las debidas actualizaciones y con el monitoreo de la CSIRT

Referencia	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia	Descripción del Control	Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento Of. Control Interno	Observaciones 2 Cuatrim 2026
2	Afectación económica y reputacional	Fuga de información	Debido al deterioro del medio de conservación (físico y/o digital) o extravío del documento.	Posibilidad de incurrir en pérdida económica y/o reputacional debido a la pérdida de información como resultado del deterioro del medio de conservación (físico y/o digital) o extravío del documento.	Ejecución y administración de procesos	500	Los líderes de los procesos previenen el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	Realizar capacitación en transferencias documentales al personal.	Sistemas y Comunicaciones	1/04/2023	24/08/2026	En el período de estudio no se han realizado capacitaciones sobre transferencias documentales
								Diseñar y aplicar plan protección física contra desastres naturales, ataques maliciosos o accidentes.	Sistemas y Comunicaciones	30/08/2023	24/08/2026	Contra desastres naturales no se cuenta con protección. Sólo se cuenta con antivirus (no en todos los equipos). No se cuenta con los dispositivos requeridos para almacenamiento de información (servidores). Se cuenta con la configuración en el dispositivo de comunicación interno que actúa como firewall.
								Los equipos se mantienen correctamente para asegurar su disponibilidad e integridad continuas.	Sistemas y Comunicaciones	Implementado	24/08/2026	En la vigencia 2026 no se ha cumplido con el cronograma de mantenimiento físico de computadores debido a falta de insumos y repuestos, para ejecutar dicha labor.
*Nota: La columna referencia se sugiere para mantener el consecutivo de riesgos, así el riesgo salga del mapa no existirá otro riesgo con el mismo número. Una entidad puede ir en el riesgo 150 pero tener 70 riesgos, lo que permite llevar una traza de los riesgos. Esta información la debe administrar la oficina asesora de planeación o Gerencia de Riesgos.												

Fuente: Adaptado de Curso Riesgo Operativo Universidad del Rosario por Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.