

FECHA DE ACTUALIZACION:		2024					MACROPROCESO	PROCESO SISTEMAS DE INFORMACION												
PROCESO	RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD	CONSECUENCIA	VALORACION DEL ACTIVO	VALORACION DEL RIESGO SIN CONTROLES			CONTROLES	VALORACION DEL RIESGO DESPUES DE CONTROLES			TRATAMIENTO					
								PROBABILIDAD	IMPACTO	SEVERIDAD		PROBABILIDAD	IMPACTO	SEVERIDAD	OPCIONES DE MANEJO	ACCIONES	RESPONSABLE DE LAS ACCIONES	FECHA DE IMPLEMENTACION		MEDIO DE EVIDENCIA
														INICIO	FINAL					
GESTION DE SISTEMAS DE INFORMACION	R1 Posibilidad de perder completitud, exactitud y la coherencia de datos de las bases de datos por vulneración de datos reservados debido a contraseñas no seguras, ausencia de mecanismos de autenticación, ausencia de bloques de sesión y ausencia de políticas de control de acceso.	Bases de datos	INFORMACION	Modificaciones no autorizadas Vulneración de datos reservados	V1. Contraseñas no seguras V2. Ausencia de mecanismos de autenticación de usuarios V3. Ausencia de bloques de sesión V4. Ausencia de políticas de control de acceso	Legales Económicas Inadecuada toma de decisiones Error en la recepción y envío de comunicaciones oficiales Afectación de la imagen y reputación	ALTO	80% Alta	80% Mayor	ALTO	Control 1: (V4) El ingeniero de sistemas encargado de realizar la auditoría de seguridad de la información, verifica que los colaboradores estén aplicando las buenas prácticas de seguridad y privacidad de la información, a través de una evaluación de conocimientos y de un cuestionario de verificación en los puestos de trabajo de las sedes auditadas. Control 2: (V2) El Sistema de gestión de base de datos relacional SQL Server verifica que los roles y derecho de acceso de los usuarios sean los correctos para el acceso a las bases de datos a través del inicio de sesión del usuario y contraseña asignados. Control 3: (V3) El administrador de directiva de grupos del directorio activo de manera automática bloquea los usuarios que han intentado acceder más de tres veces con la contraseña errónea a través de la política del directorio activo implementada. Control 4: (V1) El administrador de directiva de grupos del directorio activo de manera automática valida que las contraseñas creadas contengan combinación de mínimo 8 caracteres a través de la política de contraseñas seguras del directorio activo implementada. Control 5: (V2) Asignación de perfiles a las bases de datos por custodios de la información y seguimiento.	4% Muy baja	80% Mayor	ALTO	MITIGAR EL RIESGO (Tomar correctivos en caso de materialización del riesgo, toda vez que la probabilidad de ocurrencia es muy baja de acuerdo a los controles preventivos aplicados en la Entidad)	1. Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	1. Líder del proceso Oficina Control Interno	Semestralmente		Actas e Informes
GESTION DE SISTEMAS DE INFORMACION	R2 Posibilidad de pérdida de la confidencialidad y disponibilidad de la información por falla de los equipos de cómputo, mal funcionamiento de los equipos e infección por virus informático, debido a mantenimiento insuficiente, ausencia de reposición tecnológica, falta de equipos de refrigeración y/o inconvenientes por humedad, polvo o suciedad, descarga y uso no controlado de software, ausencia de virus, uso inadecuado de equipos de cómputo	Servidores Computadores de escritorio y portátiles Unidad NAS de almacenamiento	HARDWARE	Falla de los equipos de cómputo Mal funcionamiento de los equipos Infección por virus informático (Spyware/Malware)	V1. Mantenimiento insuficiente V2. Ausencia de reposición tecnológica V3. Falta de equipos de refrigeración y/o inconvenientes por humedad (o al Polvo y Suciedad) V4. Descarga y uso no controlado de software V5. Ausencia de antivirus V6. Uso inadecuado de equipos de cómputo	Legales Económicas Insatisfacción de usuarios y sus familias por la no atención No continuidad en el proceso de atención integral en salud y procesos de apoyo a través de la herramienta SIOS Eventos adversos	ALTO	100% Muy Alta	80% Mayor	ALTO	Control 1: (V1) El supervisor del contrato de mantenimiento preventivo y correctivo de equipos de comunicaciones y sistemas verifica que se haya ejecutado el mantenimiento por parte del contratista a través del informe que envía el proveedor y la firma del registro a satisfacción de los mantenimientos por parte de los técnicos de sistemas. Control 2: (V2) El jefe de la Oficina Asesora de Comunicaciones y Sistemas elabora y ejecuta el plan de adquisiciones de nuevas tecnologías con los recursos asignados para compra de equipos asignados en el presupuesto. Control 3: (V3) El equipo de aire acondicionado mantiene condiciones ambientales precisas para la integridad de los servidores que permite el cuidado y funcionamiento de los equipos que allí se encuentran. Control 4: (V4) Las políticas de seguridad de la información implementadas administran la infraestructura de hardware y software controlando el acceso y uso a los recursos informáticos y se lo hace a través del directorio activo y del antivirus. Control 5: (V5) El personal técnico en sistemas verifica que el antivirus se encuentre instalado y actualizado y así detecta, evita y elimina malware comparando cada archivo del disco duro con un diccionario de virus ya conocidos. Si cualquier pieza de código en un archivo del disco duro coincide con el virus conocido en el diccionario, el software antivirus entra en acción, llevando a cabo una de las acciones posibles. Control 6: (V6) El personal técnico en redes realiza la capacitación y evaluación sobre uso adecuado de equipos informáticos y adherencia a las guías rápidas de uso Control 7: (V2) El jefe de oficina de comunicaciones y sistemas realiza seguimiento y medición del indicador relacionado con la proporción de ejecución presupuestal para la adquisición y renovación de tecnología	4% Muy baja	80% Mayor	ALTA	MITIGAR EL RIESGO (Tomar correctivos en caso de materialización del riesgo, toda vez que la probabilidad de ocurrencia es muy baja de acuerdo a los controles preventivos aplicados en la Entidad)	1. Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	Líder del proceso Oficina Control Interno	Semestralmente		Actas e informes
GESTION DE SISTEMAS DE INFORMACION	R3 Posibilidad de pérdida de confidencialidad y disponibilidad de la información por falla de la conectividad, falla de las telecomunicaciones y espionaje remoto, debido a la ausencia de cumplimiento de los niveles de servicio por parte del proveedor, ausencia de equipos para la protección externa y conexiones de red sin protección.	Switches Acces Point Cableado Fibra Óptica Cableado Estructurado Fornigate	REDES	Falla de la conectividad Falla de las telecomunicaciones Espionaje Remoto (Hackers)	V1. Ausencia de cumplimiento de los niveles de servicio por parte de proveedor. V2. Ausencia de equipos para la protección externa V3. Conexiones de red sin protección	Pérdida de la información durante la contingencia (Historia Clínica) Pérdida de tiempo operacional Pérdida de datos al momento de la caída del servicio	ALTA	100% Muy Alta	80% Mayor	ALTO	Control 1: (V1) El jefe de la Oficina Asesora de Comunicaciones y Sistema verifica el cumplimiento del servicio de conectividad e internet a través del acuerdo de nivel de servicios establecido en el contrato con el proveedor. Control 2: (V1) La herramienta PRTG monitorea los niveles de servicios de conectividad e internet a través del indicador del informe mensual suministrado por el software donde se establecen las caídas de los servicios. Control 3: (V2,V3) El equipo FORTIGATE es un dispositivo de seguridad perimetral que controla amenazas emergentes detectando prevención de intrusos, bloqueo a sitios web maliciosos, amenazas de malware a través del firewall.	22% Baja	80% Mayor	ALTO	MITIGAR EL RIESGO	1. Solicitar al proveedor las vulnerabilidades de software malicioso presentadas y las acciones de mitigación implementadas en Firewall 2. Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	1. Jefe oficina sistemas de información 2. Líder del proceso Oficina Control Interno	1. 1/07/2024 1. 31/12/2024	2. Semestralmente	1. Oficio solicitud e informe enviado por el proveedor 2. Actas e informes

FECHA DE ACTUALIZACION:		2024					MACROPROCESO	PROCESO SISTEMAS DE INFORMACION												
PROCESO	RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD	CONSECUENCIA	VALORACION DEL ACTIVO	VALORACION DEL RIESGO SIN CONTROLES			CONTROLES	VALORACION DEL RIESGO DESPUES DE CONTROLES			TRATAMIENTO					
								PROBABILIDAD	IMPACTO	SEVERIDAD		PROBABILIDAD	IMPACTO	SEVERIDAD	OPCIONES DE MANEJO	ACCIONES	RESPONSABLE DE LAS ACCIONES	FECHA DE IMPLEMENTACION		MEDIO DE EVIDENCIA
								ALTA	80% Alta	80% Mayor	ALTO	4% Muy Baja	80% Mayor	ALTO				INICIO	FINAL	
GESTION DE SISTEMAS DE INFORMACION	R6 Posibilidad de pérdida de confidencialidad y disponibilidad de la información por fuga de información, inundaciones y pérdida de información. Debido a la ausencia de controles de acceso físico, susceptibilidad a la humedad, el polvo y la suciedad y falta de copias de respaldo.	Archivos electrónicos y digitales Documentos físicos y comunicaciones oficiales	Información	Fuga de información Inundaciones Pérdida de información	V1. Ausencia de Controles de acceso físico V2. Susceptibilidad a la humedad el polvo y la suciedad V3. Falta de copias de respaldo	Legales Económicas Imagen Reputación	ALTA	80% Alta	80% Mayor	ALTO	Control 1: (V2) El dispositivo termo higrometro mide la temperatura y humedad de los archivos de historia clínica, a través del formato de registro definido para tal fin se llevan los datos históricos de la medición. Control 2: (V2) El personal de aseo realiza limpieza y desinfección de las áreas de archivo y registra en el formato de limpieza y desinfección estandarizado por la empresa Control 3: (V1) El profesional Universitarios de Salud y Seguridad en el trabajo implementó la señalización a los espacios físicos de los archivos, data center y oficinas de la empresa mediante avisos preventivos de acceso al personal interno y externo. Control 4: (V1) El jefe de la oficina Asesora de comunicaciones y Sistemas gestionó la instalación de una puerta electrónica con clave de acceso al datacenter de la empresa, la clave de acceso es manejada solo por el personal de ingenieros de la oficina. Control 5: (V1) La cámara de video vigilancia instalada en el datacenter permite controlar el acceso del personal técnico a través de las grabaciones realizadas en el DVR.	4% Muy Baja 80% Mayor ALTO	MITIGAR EL RIESGO	1. Verificación semestral del cumplimiento de las actividades propuestas en el documento sistema integrado de conservación SIC 2. Se valida mensualmente que los usuarios realicen la copia de seguridad en el espacio asignado en la unidad de almacenamiento del datacenter. Se lleva un registro de que usuarios realizaron copia y quienes no, con el fin de recordar a los usuarios de la importancia de las copias de seguridad y evitar pérdidas de información. 3. Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	1. y 2. Profesional Universitario Sistemas 2. Técnico de sistemas 3. Lider del proceso Oficina Control Interno	1. y 2 1/07/2024 1. y 2 2.31/12/2024	1. y 2 2.31/12/2024	1. y 2 Indicador de copias de seguridad MIIPS 3. Actas e Informes		
GESTION DE SISTEMAS DE INFORMACION	R7 Posibilidad de afectación de credibilidad e imagen institucional por la desinformación a los grupos de interés. Debido a difusión de noticias falsas, información incompleta entregada por la Empresa, inoportunidad en la entrega de la información, ausencia de medios y canales de comunicación	Piezas audiovisuales: Vídeos, Post, Banners, Comunicados de prensa, programas radiales. Afiches.	Información	Desinformación a los grupos de interés	V1: Difusión de noticias falsas V2 Información incompleta entregada por la Empresa V3: Inoportunidad en la entrega de la información V4: Ausencia de medios y canales de comunicación (arreglar)	Crisis comunicacional Insatisfacción de las partes interesadas Pérdida de Reputación e Imagen Perdidas económicas	ALTA	80% Alta	60% Moderado	ALTO	Control 1: V1, V2: El técnico operativo realiza la capacitación del protocolo de comunicación de crisis mediática, reputacional o informativa que permite a los funcionarios abordar situaciones de crisis comunicacional Control 2: V4 La empresa, tiene implementados y adoptados canales de comunicación de manera oficial para asegurar la comunicación de la información institucional hacia las partes interesadas. Control 3: V(1) El grupo de comunicaciones, anualmente, realiza o actualiza la matriz de comunicaciones para brindar información institucional a las partes interesadas	17% Muy Baja 60% Moderado MODERADO	MITIGAR EL RIESGO	1. Realizar el procedimiento para la estandarización de la entrega de información a las partes interesadas. 2. Socializar el procedimiento para la estandarización de la entrega de información a las partes interesadas a todo el personal de la entidad 3. Aplicar el procedimiento para la estandarización de la entrega de información a las partes interesadas 4. Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	1 y 2 Técnico operativo - Comunicaciones y sistemas 3. Todo el personal 4. Lider del proceso Oficina Control Interno	1. Julio 2024 2. Septiembre 2024 3. Permanente 4. Semestralmente	1. Agosto 2024 2. Octubre 2024	1. Procedimiento aprobado 2. Circular Listas de asistencia piezas audiovisuales. 3. Documentos registros. Comunicados de prensa y piezas audiovisuales. 4. Actas e Informes		
ELABORO						REVISO						APROBO (Lider de Proceso)								
ARVEY VALLEJO - Jefe Oficina Sistemas de informacion y comunicacion						JAIME SANTACRUZ S.- Responsable Tipologia Administrativa						(Aprobado mediante acta No 4 del 14 de agosto comité coordinador de control interno)								