Plan: Plan de Seguridad y Tratamiento de Riesgos de la Información 2024
Vigencia: 2024
Aprobado por: Acta No. 001 de 2024 de Comité de Gestión y Desempeño del Sanatorio de Contratación E.S.E.

				META PROGRAMADA PARA EL TRIMESTRE				AVANCE ALCANZADO					
NOMBRE DEL PLAN	ÁREA TEMÁTICA - SUBCOMPONENTE	ACTIVIDAD / CONTROL A IMPLEMENTAR	PRODUCTO	1	2	3	4	1	2	3	4	OBSERVACIONES 3° TRIM	RESPONSABLE
Plan de Seguridad y Tratamiento de Riesgos de la Información	Controles establecidos para los riesgos identificados	Capacitar a los empleados y contratistas en la toma de conciencia y actualizacion regular en las políticas de seguridad de la información y procedimientos relacionados a su cargo.	Capacitación en seguridad de la información.		100%			_	0%	100%		El 27 de agto del 2024 se socializó la Política de seguridad de la Información, en la cual, se habló sobre los roles y responsabilidades que tenemos como funcionarios frente a la información institucional que manejamos	Sistemas
		Establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Documentar política de control de acceso implementada.		100%			_	100%	_		N/A	Sistemas
		Documentar e implementar un proceso formal de registro y cancelación de usuarios, para posibilitar la asignación de los derechos de acceso.	Procedimiento documentado e implementado	50%	100%			25%	100%	_		N/A	Sistemas
		Documentar e implementar la política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	Política aprobada e implementada.			100%		_	_	50%		Se cuenta con el borrador de la política de escritorio y pantalla limpia y está pendiente de ser socializado y aprobado por el Comité de Gestión y Desempeño	Sistemas
		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.	Copias de seguridad.	100%	100%	100%	100%	100%	100%	100%		Se realizan las copias de seguridad del Sistema Gd (Software)	Sistemas
		Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Pruebas a los sistemas de información realizadas / Pruebas a los sistemas de información programadas		100%	100%	100%	_	0%	0%		Actualmente no se puede realizar pruebas a los sistemas de información ya que no hay exigencia al personal para manejar los controles que se establecen o programan en el Software, por parte de los lideres de los procesos y Gerencia.	Sistemas
		Identificar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Análisis de cambios realizados / Cambios presentados en el periodo	100%	100%	100%	100%	100%	100%	100%		Afecta la seguridad de la información el NO contar con licencia activa de antivirus. Situación que ha sido informada por el Ingeniero encargado de Sistemas a Gerencia y al Comité de Gestión y Desempeño	Sistemas

				META PROGRAMADA PARA EL TRIMESTRE				AVANCE ALCANZADO					
NOMBRE DEL PLAN	ÁREA TEMÁTICA - SUBCOMPONENTE	ACTIVIDAD / CONTROL A IMPLEMENTAR	PRODUCTO	1	2	3	4	1	2	3	4	OBSERVACIONES 3° TRIM	RESPONSABLE
Plan de Seguridad y Tratamiento de Riesgos de la Información	Controles establecidos para los riesgos identificados	Documentar e implementar controles de prevención, de detección y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Procedimiento documentado e implementado	50%	100%			0%	0%	0%		Actividad no realizada	Sistemas
		Documentar e implementar procedimientos para controlar la instalación de software en sistemas operativos.	Procedimiento documentado e implementado	50%	100%			50%	0%	0%		No hay documentos donde estén los procedimientos para controlar la instalación de software en los sistemas operativos de la entidad.	Sistemas
		Diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	plan de contingencia contra riesgos		33%	66%	100%	_	0%	0%		No se cuenta con plan de contingencia contra riesgos o desastres naturales, ataques maliciosos o accidentes	Sistemas
		Mantener en optimas condiciones de funcionamiento los equipos tecnológicos.	Ejecución del plan de mantenimiento de equipos tecnológicos	25%	50%	75%	100%	25%	50%	60%		El plan de mantenimiento de equipos de computo se elaboró en Julio 2024, sin embargo, sólo se realiza mantenimiento preventivo ya que para realizar el correctivo se requiere de recursos presupuestales para compras de componentes que se requieren cambiar en los equipos.	Sistemas