Plan: Plan de Seguridad y Tratamiento de Riesgos de la Información 2023

Vigencia: 2023

Aprobado por: Acta No. 001 de 2023 de Comité de Gestión y Desempeño del Sanatorio de Contratación E.S.E.

NOMBRE DEL PLAN	ÁREA TEMÁTICA - SUBCOMPONENTE	ACTIVIDAD / CONTROL A IMPLEMENTAR	PRODUCTO	META PROGRAMADA PARA EL TRIMESTRE				AVANCE ALCANZADO				OBSERVACIONES PRIMER TRIMESTRE	RESPONSABLE
				1	2	3	4	1	2	3	4		
Plan de Seguridad y Tratamiento de Riesgos de la Información	**Controles establecidos para los riesgos identificados**	Establecer los acuerdos contractuales con empleados y contratistas, de sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Actualización modelos contratos	100%				0%				Actividad aún no realizada	Talento Humano y Gestión Contractual
		Todos los empleados de la organización, 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.	Capacitación en seguridad de la información.		100%			-				No aplica para el trimestre en estudio	Talento Humano y Sistemas
		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.	Procedimiento documentado e implementado		50%	100%		-				No aplica para el trimestre en estudio	Control interno disciplinario y Jurídica
		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.	política de control de acceso implementada.		100%			-				No aplica para el trimestre en estudio	Sistemas
		Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	informe de usuarios habilitados	50%	100%			50%				Se realiza depuracion del sistema y se actualizan los perfiles de acceso de cada uno de los usuarios autorizados.	Sistemas
		Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Procedimiento documentado e implementado	50%	100%			10%				Se esta trabajando en el diseño del formato para su posterior aprobación.	Talento Humano y Sistemas
		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.	Procedimiento documentado e implementado	50%	100%			20%				Para el acceso a los sitemas de la entidad se asignan contraseñas seguras a cada uno de los usuarios autorizados y se actualizan los derechos de acceso según la rotación de usuarios. Proceso pendiente de documentar.	Talento Humano y Sistemas

NOMBRE DEL PLAN	ÁREA TEMÁTICA - SUBCOMPONENTE	ACTIVIDAD / CONTROL A IMPLEMENTAR	PRODUCTO	META PROGRAMADA PARA EL TRIMESTRE				AVANCE ALCANZADO				OBSERVACIONES PRIMER TRIMESTRE	RESPONSABLE
				1	2	3	4	1	2	3	4		
Plan de Seguridad y Tratamiento de Riesgos de la Información	**Controles establecidos para los riesgos identificados**	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Procedimiento documentado e implementado	50%	100%			20%				Los usuarios normales no tienen permiso para asignarse decrechos de acceso priviligiado solo los administradores del sistema (encargados de sistemas), proceso pendiente de documentar.	Sistemas
		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.	Procedimiento documentado e implementado	50%	100%			30%				Todo empleado al finalizar su vinculo con la entidad es deshabitado del sistema y se actualizan contraseñas de ingreso a los correos institucionales y plataformas a las que tuvise acceso. Proceso pendiente de documentar.	Talento Humano y Sistemas
		Desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	política aprobada e implementada.			100%		-				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
		Se debería adoptar una 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%		-				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
		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%				Los backup se realizan diariamente (automatico) y un backup manual semanal. Está pendiente la documentación de la política	Sistemas y Comunicaciones
		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%	-				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
		Se deberían controlar 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%	0%				Se debe crear un formato de control de cambios en los sistemas de procesamiento de información	Sistemas y Comunicaciones

NOMBRE DEL PLAN	ÁREA TEMÁTICA - SUBCOMPONENTE	ACTIVIDAD / CONTROL A IMPLEMENTAR	PRODUCTO	META PROGRAMADA PARA EL TRIMESTRE				AVANCE ALCANZADO				OBSERVACIONES PRIMER TRIMESTRE	RESPONSABLE
				1	2	3	4	1	2	3	4		
		Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	Acciones de mejora implementadas / Acciones de mejora identificadas auditoria				100%	-				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
Plan de Seguridad y Tratamiento de Riesgos de la Información	**Controles establecidos para los riesgos identificados**	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.	Procedimiento documentado e implementado	50%	100%			30%				Se cuenta con antivirus (control detectivo); en preventivo tenemos firewall, y en correctivo contamos con restauración de backus	Sistemas y Comunicaciones
		Implementar procedimientos para controlar la instalación de software en sistemas operativos.	Procedimiento documentado e implementado	50%	100%			30%				Se maneja un usuario administrador protegido con contraseña en todos los equipos de la entidad, el cual impide que se instale o se manipule el software sin la autorización del administrador.(encargados de sistemas).	Sistemas y Comunicaciones
		Elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Registro de fallas y eventos realizados / Fallas y eventos presentados en el periodo	100%	100%	100%	100%	100%				Periodicamente se revisa el sistema de información de los registros de usuarios	Sistemas y Comunicaciones
		Identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.	Actualuzacion activos de la información			100%		-				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
		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 organización.	Procedimiento documentado e implementado	50%	100%			0%				Actrividad no realizada	Sistemas Integrados de Gestión
		Diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	plan de contingencia contra riesgos		33%	66%	100%	-				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
		Los equipos se mantienen correctamente para asegurar su disponibilidad e integridad continuas.	Ejecución del plan de mantenimiento de equipos tecnológicos	25%	50%	75%	100%	25%				Los equipos reciben mantenimiento permanente dando cumplimiento al respectivo plan.	Sistemas y Comunicaciones