Plan: Plan de Seguridad y Tratamiento de Riesgos de la Información 2022

Vigencia: 2022

Aprobado por: Acta No. 1 de 2022 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	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	50%	100%			50%				Para todo aspirante a un nuevo cargo se verifica los antecedentes Judiciales, Contraloria y Procuraduria	Talento Humano y Gestión Contractual
		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.	Actualización modelos contratos	50%	50%			50%				Elaborar un oficio para talento humano, procesos contractuales y juridica donde se sugiera agregar una clausula en los contratos de empleados y contratistas que incluya el manejo y apropiación de la seguridad de la información y acuerdos de propiedad intelectual. "Carta de compromiso de confidencialidad de la información"	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%			N/A				No aplica para el trimestre en estudio	Talento Humano y Sistemas
		Proteger los medios físicos que contienen información contra acceso no autorizado, uso indebido o corrupción durante el transporte.	protocolo implementado.	100%				100%				No se ha realizado traslado de información a través de un medio físico	Sistemas y Comunicaciones
		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	N/A	50%	100%		50%				No aplica para el trimestre en estudio	Control interno disciplinario
		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.	N/A	100%			N/A				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
		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	N/A	100%			N/A				No aplica para el trimestre en estudio	Sistemas y Comunicaciones

NOMBRE DEL PLAN	ÁREA TEMÁTICA - SUBCOMPONENTE	ACTIVIDAD / CONTROL A IMPLEMENTAR	PRODUCTO	META PROGRAMADA PARA EL TRIMESTRE				AVANCE ALCANZADO				OBSERVACIONES	RESPONSABLE
				1	2	3	4	1	2	3	4		
		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%			30%				Verbalmente se está realizando, aún no se ha documentado el proceso formal de registro y cancelación de registros de usuarios	Talento Humano y Sistemas y Comunicaciones
Plan de Seguridad y Tratamiento de Riesgos de la Información	**Controles establecidos para los riesgos identificados**	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%			30%				A la fecha se realiza de forma verbal donde se asigna el usuario al funcionario. Faltaria elaborar el formato para solicitud de creación de usuario ó para revocar los derechos de acceso	Sistemas y Comunicaciones
		Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Procedimiento documentado e implementado	50%	100%			50%				Se realiza depuración de base de datos de usuarios administradores que estén activos e inactivos en el sistema	Sistemas y Comunicaciones
		Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	Procedimiento documentado e implementado	50%	100%			20%				No se ha establecido la "Política de control de acceso al sistema de información"	Sistemas y Comunicaciones
		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%			50%				Cuando el funcionario cambia de dependencia o sale de la Institución se le desactiva el usurio de acceso al Software Institucional., labor desarrollada desde el área de Sistemas.	Talento Humano y Gestión Contractual
		Establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	política aprobada e implementada.	N/A		100%		N/A				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
		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.	política aprobada e implementada.	N/A		100%		N/A				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
		Implementar una política sobre el uso de controles criptográficos para la protección de la información.	política aprobada e implementada.	N/A		100%		N/A				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
		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.	N/A		100%		N/A				No aplica para el trimestre en estudio	Sistemas y Comunicaciones

NOMBRE DEL PLAN	ÁREA TEMÁTICA - SUBCOMPONENTE	ACTIVIDAD / CONTROL A IMPLEMENTAR	PRODUCTO	META PROGRAMADA PARA EL TRIMESTRE				AVANCE ALCANZADO				OBSERVACIONES	RESPONSABLE
				1	2	3	4	1	2	3	4		
		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.	N/A		100%		N/A				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
Plan de Seguridad y Tratamiento de Riesgos de la Información	**Controles establecidos para los riesgos identificados**	Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	política aprobada e implementada.	50%	100%			10%				Pendiente elaborar la política y procedimientos de transferencia de la información	Sistemas y Comunicaciones
		Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deberían documentar.	Acto administrativo adoptado	N/A		100%		N/A				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
		Los directores deberían 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.	Cumplimiento matriz de información	100%	100%	100%	100%	100%				Los encargados de cada dependencia revisan de manera permanente la seguridad de la información	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	N/A	100%	100%	100%	N/A				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
		Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	Procedimientos implementados / Procedimientos identificados proceso	N/A	33%	66%	100%	N/A				No aplica para el trimestre en estudio	Todos los procesos
		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	Análisis de cambios realizados / Cambios presentados en el periodo	100%	100%	100%	100%	50%				Se debe crear un formato de control de cambios en los sistemas de procesamiento de información	Todos los procesos

NOMBRE DEL PLAN	ÁREA TEMÁTICA - SUBCOMPONENTE	ACTIVIDAD / CONTROL A IMPLEMENTAR	PRODUCTO	META PROGRAMADA PARA EL TRIMESTRE				AVANCE ALCANZADO				OBSERVACIONES	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	N/A			100%	N/A				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
		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%			50%				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%			50%				Se cuenta con bloqueos de contraseña para instalaciones de software en los computadores de la Institución	Sistemas y Comunicaciones
Plan de Seguridad y Tratamiento de Riesgos de la Información	**Controles establecidos para los riesgos identificados**	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%				Perioidicamente se revisa el sistema de información de los registros de usuarios	Sistemas y Comunicaciones
		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.	Vulnerabilidades gestionadas / Vulnerabilidades presentadas en el periodo	100%	100%	100%	100%	100%				Se revisa constantemente la interfaz de antivirus donde se encuentra el informe de riesgos a los cuales estamos expuestos	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%		N/A				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%			50%				El Sanatorio de Contratación cuenta con tablas de retención documental	Sistemas Integrados de Gestión
		Implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Procedimiento documentado e implementado	N/A	50%	100%		N/A				No aplica para el trimestre en estudio	Sistemas y Comunicaciones
		Diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	plan de contingencia contra riesgos	N/A	33%	66%	100%	N/A				No aplica para el trimestre en estudio	Sistemas y Comunicaciones

NOMBRE DEL PLAN	ÁREA TEMÁTICA - SUBCOMPONENTE	ACTIVIDAD / CONTROL A IMPLEMENTAR	PRODUCTO	META PROGRAMADA PARA EL TRIMESTRE				AVANCE ALCANZADO				OBSERVACIONES	RESPONSABLE
				1	2	3	4	1	2	3	4		
		Los equipos se mantienen correctamente para asegurar su disponibilidad e integridad continuas.	Ejecución del plan de mantenimiento de equipos tecnológicos	25%	50%	75%	100%	50%				Los equipos reciben mantenimiento permanente.	Sistemas y Comunicaciones

30 DE MARZO DEL 2022

Dr. FREDY EDUARDO FONSECA SUAREZ

GERENTE SANATORIO DE CONTRATACION ESE