



MATRIZ PLAN DE TRATAMIENTO DE
RIESGOS DE SEGURIDAD DE LA
INFORMACIÓN

DIRECCIÓN TICS

FECHA: ENERO 2023

N°	RIESGO	CAUSA DEL RIESGO	EFECTO DEL RIESGO	CONTROLES		DESCRIPCIÓN DEL CONTROL	SEVERIDAD		FRECUENCIA		DETECCIÓN		NIVEL DE CRITICIDAD	ACCIONES PREVENTIVAS O DE MEJORA
				SI	NO									
1	Indisponibilidad del sistema DGH.	Caída por fluido eléctrico, colección de la red, sistema operativo, virus, control de acceso no autorizado.	Inconveniencia de la atención, pérdida de recursos, pérdida de información.		X	Recurso humano disponible, ups, plan de contingencia, antivirus.	Menor	2	Frecuente	4	Alta	4	70	Trazadas en el plan de acción y la capacitación del sistema DGH.
2	Inconsistencia en la Información	Validación de la información.	Toma de decisiones erróneas.	X		Auditoría Médica, administrativa.	Mayor	4	Frecuente	4	Baja	7	50	Trazadas en el plan de acción y la capacitación del sistema DGH.
3	Sistematización de los procesos	Ausencia de un sistema integral	Débil integralidad entre los procesos.		X	Auditoría Médica, administrativa.	Mayor	4	Frecuente	4	Baja	7	30	Trazadas en el plan de acción y la capacitación del sistema DGH.
4	Inconveniencia a la solicitud de la capacitación de funcionarios sobre el sistema DGH	Disponibilidad de tiempo, disponibilidad de recursos.	Desactualización, ingreso o ausencia de información pertinente.	X		Evaluación del conocimiento.	Menor	2	Frecuente	4	Baja	7	70	Trazadas en el plan de acción y PETI y la capacitación del Sistema DGH.
5	Débil conocimiento de los funcionarios en el sistema DGH.	Plan de capacitación continua.	Débil integralidad de la información	X		Evaluación del conocimiento.	Menor	2	Ocasional	3	Baja	7	70	Trazadas en el plan de acción y PETI y la capacitación del Sistema DGH.
6	Debilidad en la aplicación y socialización de la seguridad de la información.	Aplicación de las políticas de seguridad de la información.	Uso inadecuado, pérdida o fuga de la información.		x	Manual de políticas de seguridad de la información.	Mayor	4	Frecuente	4	Alta	4	50	Trazadas en el Plan Estratégico de tecnologías de la información PETI.
7	A causa de la no existencia de la política de seguridad aprobada por la gerencia, en consecuencia, no ha sido socializada, los funcionarios pueden incurrir en acciones que afecten la seguridad de la información.	No se encuentra implementada al 100% la política de la seguridad de la información en la E.S.E. UNA.	Uso inadecuado de la información, generación de quiebres que pueden atentar contra la información de la E.S.E UNA.		X	Se requiere aumentar el alcance de la seguridad de la información de la E.S.E UNA.	Mayor	4	Frecuente	4	Alta	4	70	Programada en el PETI
8	Debido a la falta unificación de criterios y la implementación de un protocolo que regule la entrega de la información contenidas en las bases de datos, se corre el riesgo de fuga y divulgación de la	Unificación de criterios y implementación de un protocolo, uso y procesamiento de la información de salida de las bases de datos de la E.S.E. UNA.	Fuga y divulgación de la información.		X	Se requiere planear, desarrollar e implementar el protocolo de uso de BD.	Mayor	4	Ocasional	3	Baja	7	50	Pendiente por desarrollar.



MATRIZ PLAN DE TRATAMIENTO DE
RIESGOS DE SEGURIDAD DE LA
INFORMACIÓN

DIRECCIÓN TICS

FECHA: ENERO 2023

	información confidencial e interna.													
9.	A causa en las fallas presentadas al momento de crear, modificar o deshabilitar un usuario, por la notificación correcta y a tiempo por parte de Talento Humano y Asistencial.	Inconsistencia en la información por usuarios que ya no se encuentran en la institución o no cuentan con la autorización escrita.	Riesgo de pérdida de información, acceso por personal que debería estar inhabilitados.		X	Se creo un formato de creación, modificación y eliminación de usuario.	Mayor	4	Frecuente	4	Alta	4	50	

CRITERIOS PARA LA EVALUACIÓN DEL RIESGO

PROBABILIDAD					
CASI SEGURO (5)					
FRECUENTE (4)					
OCASIONAL (3)					
RARO (2)					
REMOTA (1)					
	INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
	IMPACTO				