Referencia	TIPO DE RIESGO	FACTOR DE RIESGOS /TIPO DE ACTIVOS DE LA INFORMACIÓN	DESCRIPICÓN / VULNERAVILIDAD	CAUSA INMEDIATA	CAUSA RAÍZ	DESCRIPCIÓN DEL RIESGO	CLASIFICACIÓN DEL RIESGO	FRECUENCIA CON LA CUAL SE REALIZA LA ACTIVIDAD	PROBABILIDAD INHERENTE	%	CLASIFICACIÓN	CRITERIOS DE IMPACTO	IMPACTO INHERENTE	%	ZONA DE RIESGO INHERENTE	NO. CONTROL	DESCRIPCIÓN DEL CONTROL	ATRIBUTOS						
																		Tipo	Afectación	Implementación	Calificación	Documentación	Frecuencia	Evidencia
1	Seguridad_de_la_Información	HARDWARE	Ausencia de esquemas de reemplazo periódico	falta de presupuesto para mantener un stop disponible.	FALTA DE EQUIPOS Y TECNOLOGIA IDONEA Y SUFICIENTE.	Falta de equipos de tecnología idónea y suficiente	Fallas Tecnologicas	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	Media	60%	Afectación_Económica_o_presupuestal	Entre 10 y 50 SMLMV	Menor	40%	Moderado	1	La alta Dirección debe proveer los recursos necesarios para garantizar el SGSI.	Preventivo		Manual	40%	Sin Documentar	Aleatoria	Con Registro
																2								
																3								
1	Seguridad_de_la_Información	HARDWARE	Mantenimiento insuficiente		FALTA DE MANTENIMIENTO DE EQUIPOS	FALTA DE REALIZACION DE MANTENIMIENTO A LOS EQUIPOS	Fallas Tecnologicas	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	Baja	40%	Afectación_Económica_o_presupuestal	Entre 10 y 50 SMLMV	Menor	40%	Moderado	1	Llevar a cabo la ejecucion del plan de mantenimiento preventivo.	Preventivo		Manual	40%	Documentado	Continua	Con Registro
																2	Seguimiento a la ejecucion del plan de mantenimiento, el cual se debe cumplir como requisito para los entes de control.	Detectivo		Manual	30%	Documentado	Aleatoria	Con Registro
																3								
																4								
1	Seguridad_de_la_Información	INFORMACIÓN	probabilidad de perdida de información de las bases de datos de la institución.	falla en los discos duros.	No contar con un plan de contingencia que incluya replica en línea de los servidores de la ESE HOSPITAL DEL SARARE en un sitio alterno.	Ausencia de mecanismos de identificación y autenticación puede ocacionar abuso de derchos y error en el uso lo que causaría perdida de confiedencialidad en el software o posibilidad de acceso a S.O, manejadores de Bases de Datos y/o software institucional, sin ningun tipo de restricción.	Fallas Tecnologicas	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	Baja	40%	Afectación_Económica_o_presupuestal	Entre 10 y 50 SMLMV	Menor	40%	Moderado	1	Personal de soporte técnico realiza el mantenimiento al directorio activo.	Preventivo		Manual	40%			
																2	El profesional universitario parameteriza el acceso a las aplicaciones con criterios de contraseñas fuertes.	Preventivo		Manual	40%			
																3	El profesional universitario parameteriza el acceso a las bases de datos con criterios de contraseñas fuertes	Preventivo		Manual				
																4	Seguridad Perimetral UTM a través del FORTINET.	Preventivo		Automático	50%		Continua	Con Registro
	Seguridad_de_la_Información	RED	Indisponibilidad de los: Canales (WAN, LAN), Servidores y correo electrónico.	Conexión deficiente de la fibra optica y de cableado estructurado.	Indisponibilidad de los: Canales (WAN, LAN), Servidores y correo electrónico.	Interrupciones que afectan la funcionalidad de canales, servidores, software operacional y correo electrónico de forma parcial.	Fallas Tecnologicas	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	Media	60%	Afectación_Económica_o_presupuestal	Entre 10 y 50 SMLMV	Menor	40%	Moderado	1	Seguimiento a los mecanismos de alta disponibilidad implementados sobre los servicios de canales de datos, servidores y correo electrónico	Preventivo		Manual	40%			
																2	Seguridad Perimetral UTM a través del FORTINET.	Preventivo		Automático	50%		Continua	Con Registro
																3								
																4								