Matriz de Riesgos
ESE UNIVERSITARIA UNIVERSITARIA DEL ATLÁNTICO

Código:	
Fecha de emisión:	16/09/2024
Versión	Versión: 01

Identificación del Riesgo							Evaluación del Riesgo Inherente				
N°	Proceso	Descripción del Riesgo	Tipo de Riesgo	Causas	Consecuencias	Tipo de impacto	Probabilidad	Impacto	Nivel de riesgo	Clasificación de nivel de riesgo	Controles
1	TICs	Posibilidad de manipulación, filtración de información, eliminación o modificación de los sistemas de información y tecnológicos para alterar los registros, base de datos o documentos de la compañía, por parte de un trabjador en beneficio propio o de un tercero	Riesgo de Lavado de Activos y Financiación del Terrorismo (SARLAFT)	1. Desconocimiento de las normatividad 2. Información adulterada 3. Controles y barreras para prevencion de mitigacion de riesgos LAFT/COF ineficientes o inexistentes 4. Mala fe de trabajador que perpetua la acción	1. Investigaciones disciplinarias 2. Sanciones y compulsa de copias a autoridades competentes. 3. Posible perdida de información 4. Pérdida de recursos financieros 5. Daño a imagen institucional	Reputacional Económico Operativo Legal	3	3	9	MODERADO	1. Campañas semanales de sensibilización en seguridad y privacidad de la información a través de correos electrónicos masivos. 2. Implementación de control exhaustivo para la cuducidad de las contraseñas en el directorio activo de Windows, el sistema DG y correo institucional
2	TICs	Posibilidad de fallas en la continuidad de la operación en los sistemas de información y comunicaciones que integra la entidad	Riesgo Operacional (SARO)	1. Fallas en el Fluido eléctrico. 2. Caida del internet. 3. Falla en la conectividad. 4. Falla en los servidores 5. Falta espacio en el servidor. 6. Obsolencia de recursos tecnológicos 7. Fenómenos de fuerza mayor (Desastres). 8. Falla critica por parte de los proveedores tecnologicos (Software Dinamica, CLARO, etc) 9. Ataque cibernetico	1. Falla en la base de datos. 2. Colapso del Sistema. 3. Pérdida de información. 4. Lentitud del sistema. 5. Altos volúmenes de información que por tiempo no se da respuesta oportuna (No manejo de históricos). 6. Limitación del almacenamiento.	Reputacional Económico Operativo Legal	5	4	20	ALTO	1. Se proyecta la implementacion de un proveedor de servicio tercerizado que sirva de backup. 2. Se cuenta con un contrato vigente con la empresa FOCUS GROUP para arriendo de computadores quienes se encargan mantenimiento preventivo y correctivo a los equipos.
3	TICs	Posibilidad de perdidas o filtración de información por falta de seguridad informática, debidio a la ineficacia o inexistencia de procedimientos de seguridad de la información	Riesgo Operacional (SARO)	1. Vulnerabilidad en el acceso a los sistemas de información y/o comunicaciones 2. Falta de politicas y procedimientos de seguridad en los sistema de información y comunicaciones 3. Falta de aplicación de las politicas y procedimientos de seguridad establecidos. 4. Contraseñas inseguras 5. Sesiones activas despues del horario laboral o al dejar la estacion de trabajo	1. Pérdida o alteración de información. 2. Violación de Habeas Data. 3. Demandas por mal uso de la información. 4. Problemas con la confidencialidad e integralidad de la información. 5. Exposicion de informacion clasificada o reservada de la entidad	Reputacional Economico Legal	3	2	6	MODERADO	1. Socializar y difundir la Politica de Seguridad y Privacidad de la Información y Seguridad Digital en la ESE UNIVERSITARIA DEL ATLÁNTICO UNA, Resolución 0312 del 31 de julio de 2023. 2. Capacitación en responsabilidad, seguridad y privacidad de la información. 3. Implementación de controles de acceso a la plataforma DGH (Dinamica Gerencial Hospitalaria)
4	TICs	Posibilidad de no contar con las herramientas necesarias para identificar y tratar los riesgos de seguridad digital	Riesgo Operacional (SARO)	Falta de procedimientos de identificación y evaluación de riesgos	Materialización de riesgos por falta de seguimiento y planes de tratamiento	Reputacional Económico Operativo	3	2	6	MODERADO	1. Creación de matriz de riesgos para los procesos TICS de la Entidad. 2. Seguimiento al Plan de tratamiento de riesgos de seguridad y privacidad de la información la Entidad
5	TICs								0	BAJO	
6	TICs								0	BAJO	
7	TICs								0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	
									0	BAJO	

									0	BAJO	
									0	BAJO	
									0	BAJO	