N.	ID EDT/WBS	Actividad	Descripción	Identificador	Predecesoras	Duración (días)	Tm	To	Tp
1	1.1.1	Recopilar documentos y registros relevantes sobre los activos de la empresa	Reunir y revisar documentos, registros y otros materiales relacionados con los activos de información de la empresa, como contratos, informes financieros, políticas internas, entre otros	A1	-	3	3	2	4
2	1.2.1	Analizar la importancia de cada activo de información	Evaluar la relevancia y el valor de cada activo de información identificado en función de su impacto en los objetivos y operaciones de la empresa	A2	A1	3	3	2	4
3	1.2.2	Documentar todos los activos de información crítica identificados	Registrar y documentar de manera detallada todos los activos de información crítica identificados durante el proceso de análisis y evaluación	A3	A2	4	4	3	5
4	1.3.1	Realizar un análisis exhaustivo de la infraestructura de TI	detallada de la infraestructura de tecnología de la información de la empresa para identificar posibles vulnerabilidades y riesgos de	A4	-	4	4	3	5
5	1.3.2	Identificar puntos débiles en la red a través de herramientas de escaneo y vulnerabilidades	Utilizar herramientas de escaneo y análisis de vulnerabilidades para identificar y evaluar posibles puntos débiles en la red de la empresa	A5	A4	2	2	1	3
6	1.4.1	Evaluación de impacto y probabilidad de cada riesgo identificado	Evaluar el impacto potencial y la probabilidad de ocurrencia de cada riesgo identificado durante el análisis de vulnerabilidades y riesgos	A6	A3, A5	3	3	2	4
7	1.4.2	Priorizar los riesgos según su gravedad y probabilidad de ocurrencia	Clasificar y priorizar los riesgos identificados en función de su gravedad, impacto y probabilidad de ocurrencia para centrarse en los más críticos primero	A7	A6	2	2	1	3
8	1.5.1	Desarrollar estrategias y recomendaciones para mitigar los riesgos identificados	Elaborar estrategias y recomendaciones específicas para abordar y mitigar los riesgos identificados, incluyendo medidas preventivas y correctivas	A8	A7	3	3	2	4
9	1.5.2	Priorizar acciones de mitigación en función de la criticidad de los riesgos	Determinar y priorizar las acciones necesarias para mitigar los riesgos identificados, asignando recursos y estableciendo plazos para su implementación	A9	A8	3	3	2	4
10	1.6.1	Desarrollar políticas de seguridad que aborden el acceso a datos, protección de información y respuesta a incidentes	detalladas que establezcan las reglas y procedimientos para proteger los activos de información de la empresa y responder a posibles incidentes	A10	A3, A9	5	5	4	6
11	1.6.2	Obtener revisión y aprobación por parte de la gerencia	Presentar las políticas de seguridad desarrolladas para su revisión y aprobación por parte de la alta dirección de la empresa.	A11	A10	2	2	1	3
			Desarrollar procedimientos detallados y estándar para						

12	1.7.1	Crear procedimientos operativos estándar para la implementación de políticas de seguridad	implementar las políticas de seguridad aprobadas, especificando los pasos y responsabilidades correspondientes.	A12	A11	4	4	3	5
13	1.7.2	Documentar pasos específicos que deben seguir los empleados	Registrar y documentar los pasos específicos que deben seguir los empleados para cumplir con las políticas y procedimientos de seguridad establecidos.	A13	A12	3	3	2	4
14	1.8.1	Documentar los controles de acceso en los sistemas y aplicaciones	Registrar y documentar los controles de acceso implementados en los sistemas y aplicaciones de la empresa para proteger los activos de información.	A14	A10, A13	5	5	4	6
15	1.9.1	Realizar pruebas exhaustivas para verificar la funcionalidad y seguridad de los controles de acceso implementados	Realizar pruebas exhaustivas y simulaciones para verificar la efectividad y seguridad de los controles de acceso implementados en los sistemas y aplicaciones.	A15	A14	5	5	4	6
16	1.10.1	Diseñar plan detallado que describa como se realizarán las copias de seguridad	Elaborar un plan detallado que describa los procedimientos y la programación para realizar copias de seguridad de los datos de la empresa.	A16	A4, A15	2	2	1	3
17	1.11.1	Implementar lo procedimientos de copia de seguridad definidos en el plan	Poner en práctica los procedimientos de copia de seguridad definidos en el plan para garantizar la protección y disponibilidad de los datos de la empresa.	A17	A16	3	3	2	4
18	1.12.1	Realizar pruebas para verificar la eficacia del plan de recuperación de datos	Realizar pruebas y simulaciones para verificar la efectividad y eficacia del plan de recuperación de datos en caso de fallos del sistema o incidentes de seguridad.	A18	A17	2	2	1	3
19	1.13.1	Desarrollar material de capacitación que aborde las política y procedimientos establecidos	Crear materiales de capacitación, como manuales y presentaciones, que aborden las políticas y procedimientos de seguridad establecidos para el personal de la empresa.	A19	A10, A18	3	3	2	4
20	1.14.1	Programar y coordinar sesiones de capacitación para el personal sobre las mejores prácticas de seguridad de la información	Organizar y coordinar sesiones de capacitación para el personal de la empresa sobre las mejores prácticas de seguridad de la información y el uso adecuado de los sistemas y datos.	A20	A19	2	2	1	3
21	1.15.1	Evaluar la efectividad de las sesiones de capacitación mediante la recopilación de retroalimentación y la realización de pruebas de conocimientos.	Evaluar la efectividad de las sesiones de capacitación mediante la recopilación de retroalimentación del personal y la realización de pruebas de conocimientos para verificar la comprensión y aplicación de los conceptos de seguridad de la información.	A21	A20	2	2	1	3
						Estimación total (días)			65