

N°	ID EDT/WBS	Actividad	ID	Tiempo estimado	Tiempo estimado acumulado	Tiempo real	Tiempo real acumulado
1	1.1.1	Recopilar documentos y registros relevantes sobre los activos de la empresa	A1	3 días	3 días	2 días	2 días
2	1.2.1	Analizar la importancia de cada activo de información	A2	2 días	5 días	1 día	3 días
3	1.2.2	Documentar todos los activos de información crítica identificados	A3	3 días	8 días	3 días	6 días
4	1.3.1	Realizar un análisis exhaustivo de la infraestructura de TI	A4	4 días	12 días	4 días	10 días
5	1.3.2	Identificar puntos débiles en la red a través de herramientas de escaneo y vulnerabilidades	A5	2 días	14 días	2 días	12 días
6	1.4.1	Evaluación de impacto y probabilidad de cada riesgo identificado	A6	3 días	17 días	3 días	15 días
7	1.4.2	Priorizar los riesgos según su gravedad y probabilidad de ocurrencia	A7	2 días	19 días	2 días	17 días
8	1.5.1	Desarrollar estrategias y recomendaciones para mitigar los riesgos identificados	A8	3 días	22 días	3 días	20 días
9	1.5.2	Priorizar acciones de mitigación en función de la criticidad de los riesgos	A9	3 días	25 días	3 días	23 días
10	1.6.1	Desarrollar políticas de seguridad que aborden el acceso a datos, protección de información y respuesta a incidentes	A10	5 días	30 días	5 días	28 días
11	1.6.2	Obtener revisión y aprobación por parte de la gerencia	A11	3 días	33 días	3 días	31 días
12	1.7.1	Crear procedimientos operativos estándar para la implementación de políticas de seguridad	A12	4 días	37 días	4 días	35 días
13	1.7.2	Documentar pasos específicos que deben seguir los empleados	A13	3 días	40 días	3 días	38 días
14	1.8.1	Documentar los controles de acceso en los sistemas y aplicaciones	A14	2 días	42 días	2 días	40 días
15	1.9.1	Realizar pruebas exhaustivas para verificar la funcionalidad y seguridad de los controles de acceso implementados	A15	4 días	46 días	4 días	44 días
16	1.10.1	Diseñar plan detallado que describa cómo se realizarán las copias de seguridad	A16	3 días	49 días	3 días	47 días
17	1.11.1	Implementar procedimientos de copia de seguridad definidos en el plan	A17	4 días	53 días	4 días	51 días
18	1.12.1	Realizar pruebas para verificar la eficacia del plan de recuperación de datos	A18	3 días	56 días	3 días	54 días
19	1.13.1	Desarrollar material de capacitación que aborde las política y procedimientos establecidos	A19	4 días	60 días	3 días	57 días
20	1.14.1	Programar y coordinar sesiones de capacitación para el personal sobre las mejores prácticas de seguridad de la información	A20	3 días	63 días	1 días	58 días
21	1.15.1	Evaluar la efectividad de las sesiones de capacitación mediante la recopilación de retroalimentación y la realización de pruebas de conocimientos	A21	3 días	66 días	3 días	61 días

