MATRIZ DE RESPONSABILIDADES DEL EQUIPO

N	ID	DESCRIPCIÓN DE LA TAREA	RESPONSABLE	NOMBRE
1.		IDENTIFICACIÓN DE ACTIVOS		
1.1		INVENTARIO DE ACTIVOS		
1	1.1.1	Inventarios de activos	Administrador de Redes e Infraestructura de T.I	Omar Ciriaco Esquivel
2	1.1.2	Priorización de activos de información	Administrador de Redes e Infraestructura de T.I	Omar Ciriaco Esquivel
1.2		ANALISIS Y PRIORIZACION DE ACTIVOS		
1	1.2.1	Analizar la importancia de cada activo de información	Administrador de Redes e Infraestructura de T.I	Omar Ciriaco Esquivel
2	1.2.2	Documentar todos los activos de información crítica identificados	Administrador de Redes e Infraestructura de T.I	Omar Ciriaco Esquivel
2.		EVALUACIÓN DE RIESGOS Y VULNERABILIDADES		
2.1		Informe de identificación de riesgos y vulnerabilidades		
1	2.1.1	Realizar un análisis exhaustivo de la infraestructura de TI	Jefe de Proyecto	Daniel Gonzales Castillo
2	2.1.2	Identificar puntos débiles en la red a través de herramientas de escaneo y de vulnerabilidades	Jefe de Proyecto	Daniel Gonzales Castillo
2.2		Informe de análisis y priorización de riesgos		
1	2.2.1	Evaluación de impacto y probabilidad de cada riesgo identificado	Jefe de Proyecto	Daniel Gonzales Castillo
2	2.2.2	Priorizar los riesgos según su gravedad y probabilidad de ocurrencia.	Jefe de Proyecto	Daniel Gonzales Castillo
2.3		Informe de recomendaciones de mitigación		

1	2.3.1	Desarrollar estrategias y recomendaciones para mitigar los riesgos identificados	Jefe de Proyecto	Daniel Gonzales Castillo
2	2.3.2	Priorizar las acciones de mitigación en función de la criticidad de los riesgos	Jefe de Proyecto	Daniel Gonzales Castillo
3.		POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD		
3.1		Políticas de seguridad		
1	3.1.1	Desarrollar políticas de seguridad que aborden el acceso a datos, protección de información y respuesta a incidentes	Desarrollador de Politicas	Milagros Soto Obregon
2	3.1.2	Obtener revisión y aprobación por parte de la gerencia	Coordinador de Cumplimiento	Milagros Soto Obregon
3.2		Manual de procedimientos de seguridad documentados		
1	3.2.1	Crear procedimientos operativos estándar para la implementación de politicas de calidad	Coordinador de Cumplimiento	Milagros Soto Obregon
2	3.2.2	Documentar pasos especificos que deben seguir los empleados	Coordinador de Cumplimiento	Milagros Soto Obregon
4.		IMPLEMENTACIÓN DE CONTROLES DE ACCESO Y AUTENTICACIÓN		
4.1		Politicas y procedimientos de control de accesos		
1	4.1.1	Documentar los controles de acceso en los sistemas y aplicaciones	Analista de Seguridad de la Informacion	James Huanuco Vicuña
4.2		Plan de gestión de accesos y monitoreo		
1	4.2.1	Documentar monitoreo de la funcionalidad y seguridad de los controles de acceso implementados	Analista de Seguridad de la Informacion	James Huanuco Vicuña
5.		PLAN DE COPIAS DE SEGURIDAD Y RECUPERACIÓN DE DATOS		
5.1		Plan de copias de seguridad		
1	5.1.1	Diseñar plan detallado que describa cómo se realizarán las copias de seguridad	Ingeniero de Sistemas	Antony Vasquez Leiva

5.2		Informe de pruebas de recuperación de datos		
1	5.2.1	Realizar pruebas periódicas para verificar la eficacia del plan de recuperación de datos	Ingeniero de Sistemas	Antony Vasquez Leiva
6.		CAPACITACIÓN DEL PERSONAL		
6.1		Material de capacitación		
1	6.1.1	Desarrollar material de capacitación que aborde las políticas y procedimientos establecidos	Coordinador de Capacitacion	Miguel Yauricasa Mendoza
6.2		Sesiones de capacitación programadas y coordinadas		
1	6.2.1	Programar y coordinar sesiones de capacitación para el personal sobre las mejores prácticas de seguridad de la información	Coordinador de Capacitacion	Miguel Yauricasa Mendoza
6.3		Formulario de evaluación de la efectividad de la capacitación		
1	6.3.1	Evaluar la efectividad de las sesiones de capacitación mediante la recopilación de retroalimentación y la realización de pruebas de conocimientos.	Coordinador de Capacitacion	Miguel Yauricasa Mendoza