



ESPE
ESCUELA POLITÉCNICA DEL EJÉRCITO
CAMINO A LA EXCELENCIA

“ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA EN LA RED DE ÁREA LOCAL (LAN), DE LA UNIDAD DE GESTIÓN DE TECNOLOGÍAS ESPE, PARA PERMITIR ESTABLECER UN PLAN DE DEFENSA Y PROTECCIÓN”

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

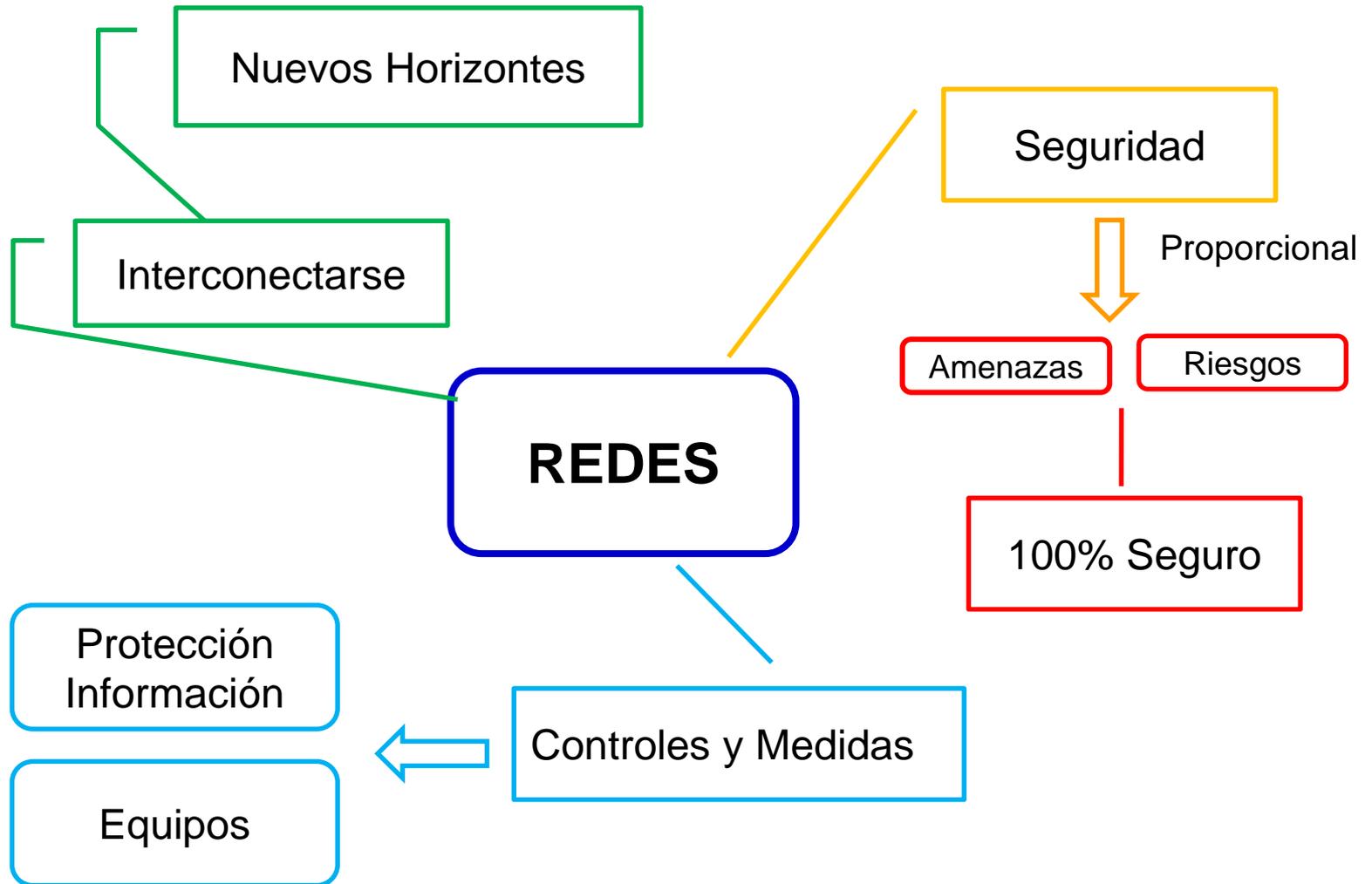
TECNÓLOGA EN COMPUTACIÓN:

Autor: ORDÓÑEZ VEINTIMILLA DIANA JAZMÍN

Director: Ing. MOLINA PATRICIO



ANTECEDENTES

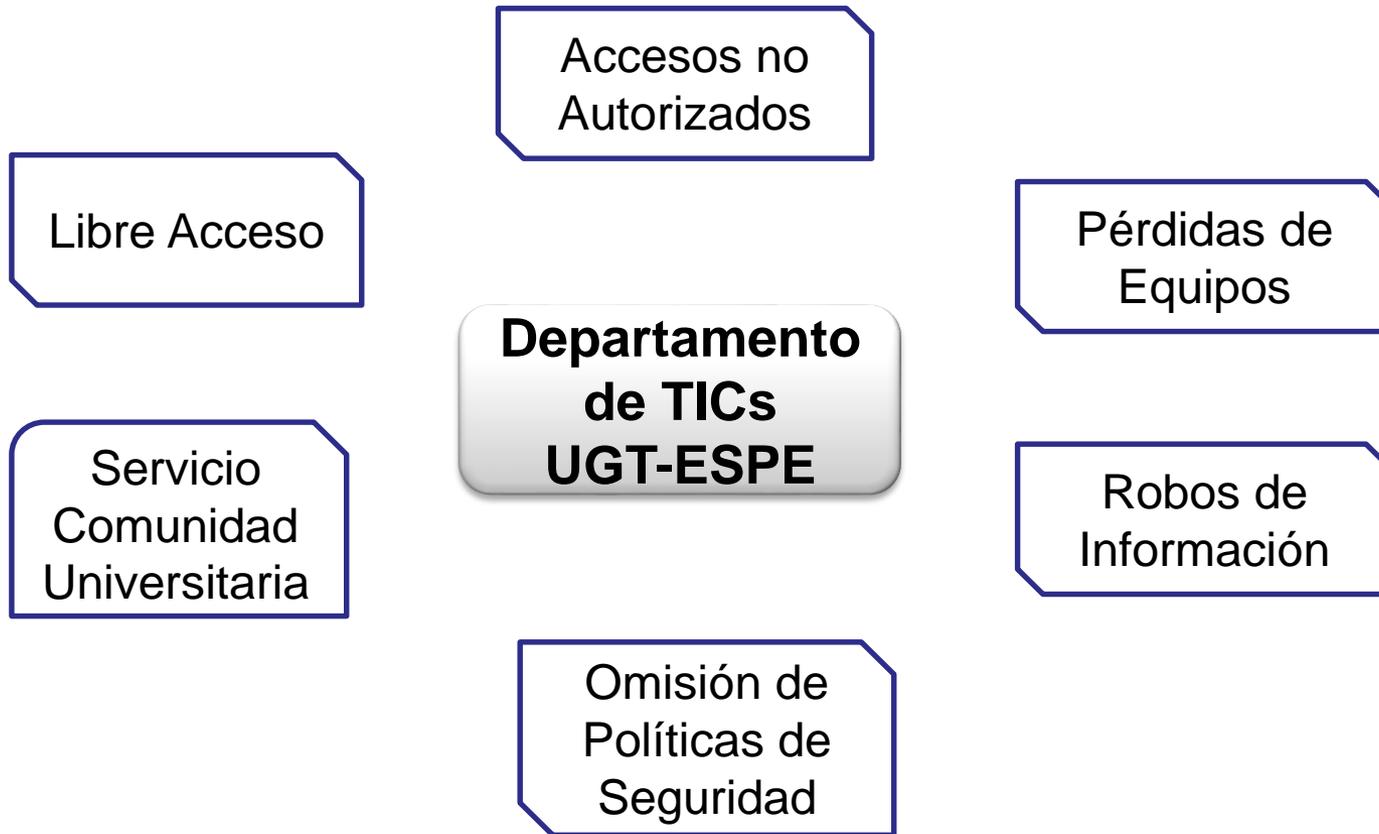


DATOS DE LA INSTITUCIÓN

La Unidad de Gestión de Tecnologías ESPE, se encuentra ubicada en el Sector la FAE, Cantón Latacunga, Provincia Cotopaxi, Dirección Av. Javier Espinoza N3-47 y Av. Amazonas, dedicada principalmente a actividades académicas, cuenta con una edificación adecuada, la misma que consta de tres plantas, divididas cada una en secciones, como laboratorios, aulas educativas, oficinas para el personal administrativo y de servicio, así como también el Departamento de TICs en el que principalmente va enfocado el proyecto.



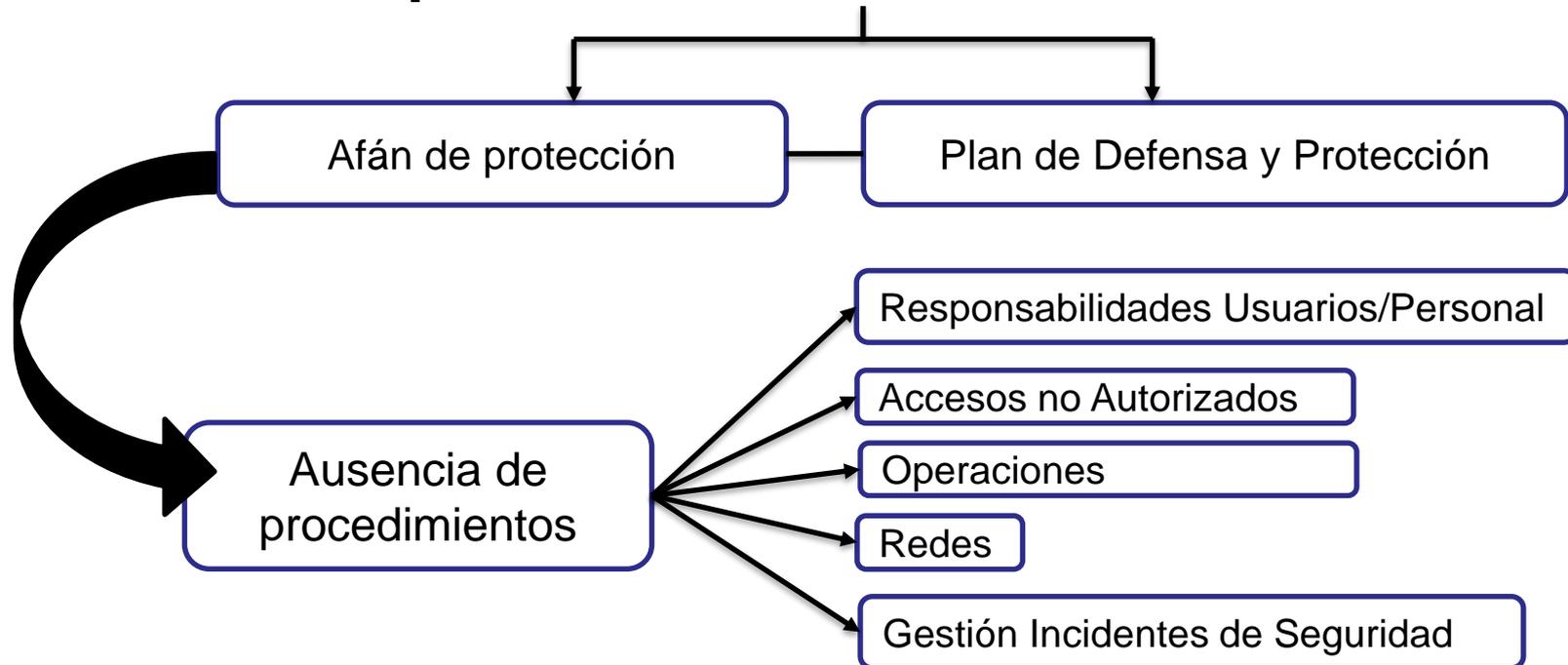
PLANTEAMIENTO DEL PROBLEMA

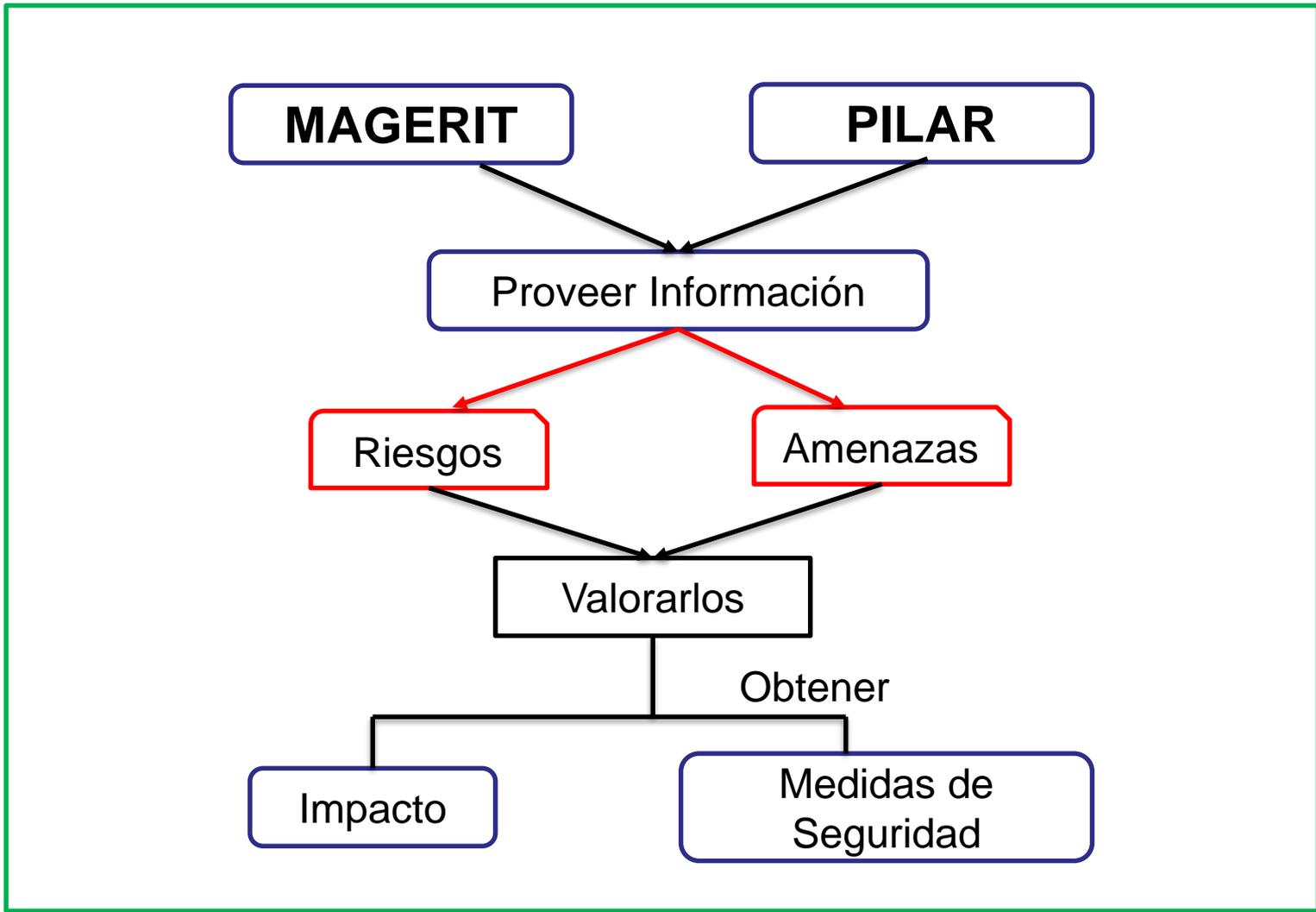


JUSTIFICACIÓN



Departamento de TICs de la UGT-ESPE





OBJETIVOS

OBJETIVO GENERAL

Analizar y evaluar riesgos de seguridad informática en la red de área local (LAN), de la unidad de gestión de tecnologías ESPE, para permitir establecer un plan de defensa y protección.



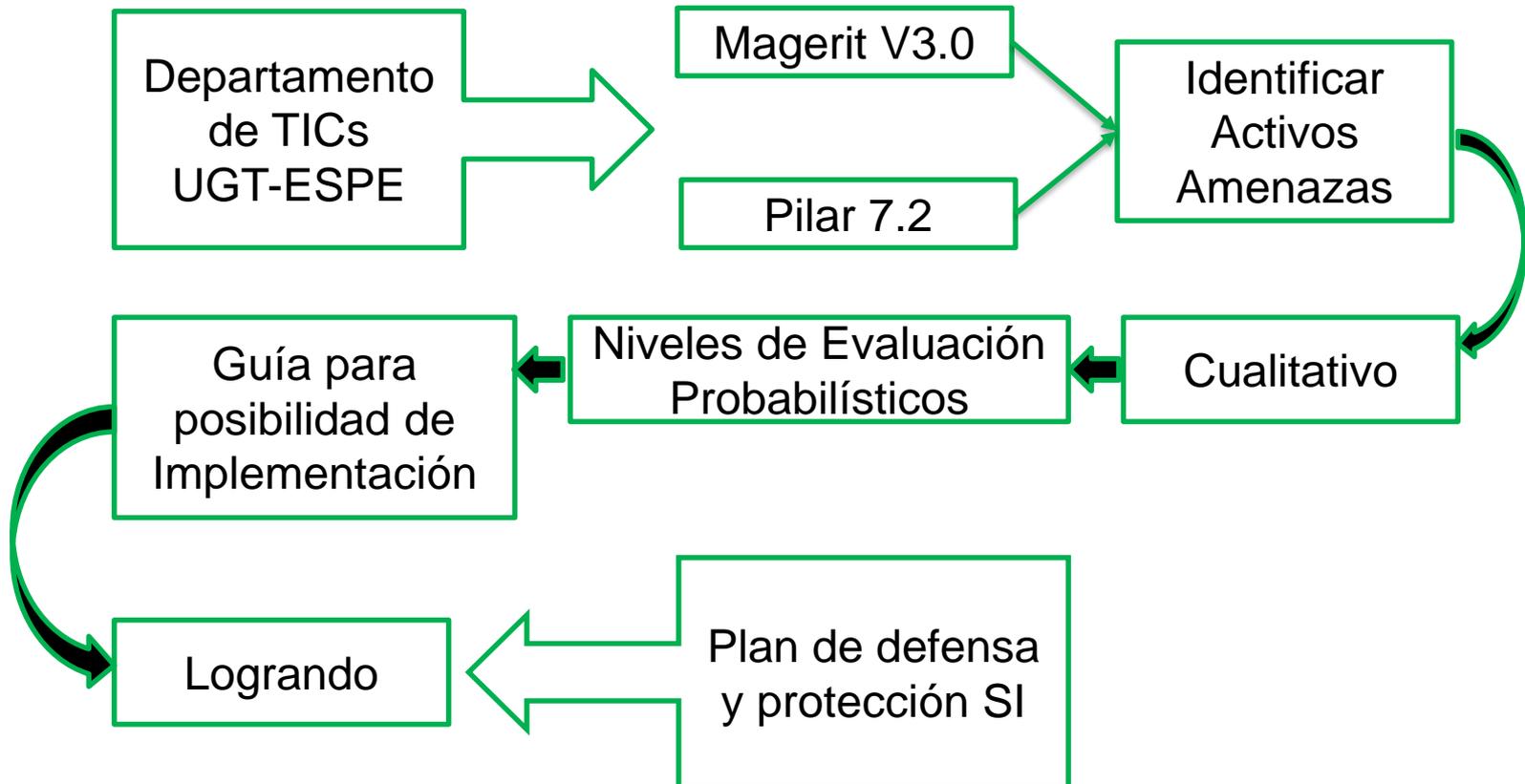
OBJETIVOS ESPECÍFICOS

- Identificar los requerimientos de la metodología Magerit y la herramienta Pilar, especificando las características de operación necesarias, para la realización del análisis de riesgos.
- Establecer un análisis de carácter cualitativo en los activos más críticos de la red LAN de la institución, para la identificación y valoración de amenazas.
- Proponer un plan de defensa y protección de seguridad informática para la red LAN de la Unidad de Gestión de Tecnologías ESPE, proporcionando lineamientos para precautelar la seguridad de la información, y toma de acciones para salvaguardar la integridad de los activos de la misma.



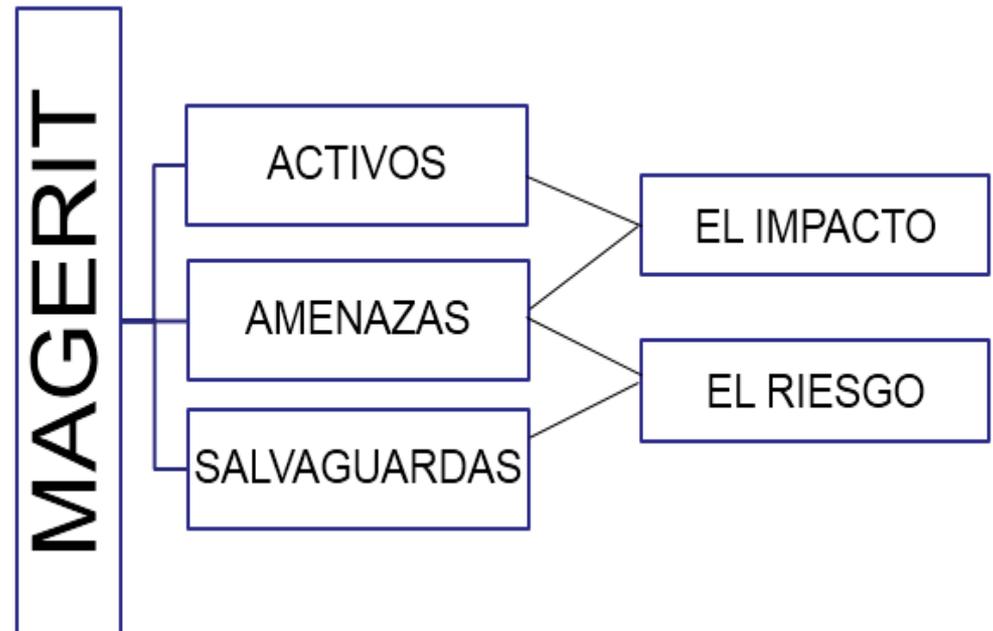
ALCANCE

Realizar un Análisis y Evaluación de Riesgos



METODOLOGÍA MAGERIT V3.0

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, que permite: estudiar los riesgos que soporta un sistema de información y el entorno asociado a él.



VALORACIÓN ACTIVOS

*Impacto = valor * degradación*

*Riesgo = impacto * degradación*

VALORACIÓN AMENAZAS

Identificadas por la Frecuencia de ocurrencia y el grado de degradación que cause.

SALVAGUARDAS

Medidas de protección frente a las amenazas localizadas.



ACTIVOS

Software

- Sistema Operativo Linux

Hardware

- Firewall
- Switch Core HP
- Switch de Distribución Linksys
- Switch de Acceso Dlink
- Router Cisco
- Router Mikrotik
- Servidor Linux
- Switch Capa 2

Equipamiento Auxiliar

- Rack Comunicación TICs
- UPS 6KVA

Instalaciones

- Cuarto de Comunicaciones TIC's

Personal

- Administrador de Red
- Soporte Técnico



EAR/PILAR

Entorno de Análisis de Risgos (EAR) Pilar: PILAR conjuga los activos dentro un sistema con las amenazas posibles, calcula los riesgos y permite incorporar salvaguardas para reducir el riesgo a valores residuales aceptables. Esto permite fundamentar la confianza en el sistema.

PLAN DE SEGURIDAD INFORMÁTICA

Plan de Seguridad Informática:

El Plan de Seguridad Informática proporciona pautas necesarias para gestionar de manera correcta la seguridad tanto de la información, como el uso de los activos, proponiendo ideas para mejorar en el momento de su implementación.



SITUACIÓN ACTUAL RED LAN UGT-ESPE

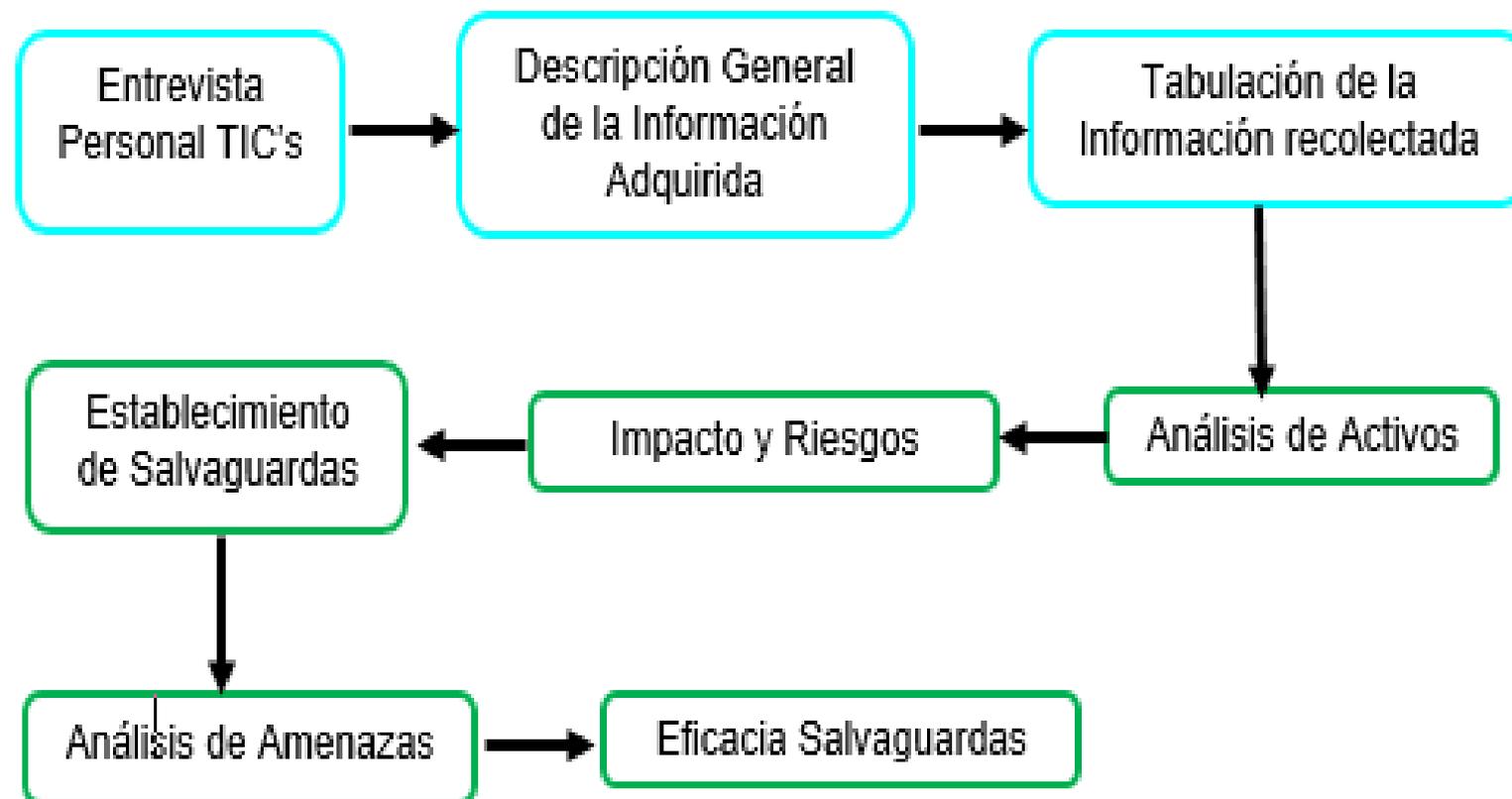
Institución	Número plantas (Edificio)	Número de Áreas	Número de Usuarios	Número de PCs		Responsable
				Desktop	Laptop	
Unidad de Gestión de Tecnologías ESPE	3	9	90	30	60	Sgop. Luis Santana



INVENTARIO ACTIVOS DE RED LAN UGT-ESPE

Cant	Activo	Descripción	Categoría	Ubicación	Responsable TICs
3	Router CISCO	Enlace WAN	Capa 3	Rack Comunicación	Sgop. Luis Santana
		Backup			
1	Router Mikrotik	Gestión WLAN Gestión WAN	Capa 3	Rack Comunicación	Sgop. Luis Santana
2	Switch 24 puertos	Wireless Administrable	Capa 3	Rack Comunicación	Sgop. Luis Santana
			Capa 2		
3	Switch 24 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana
3	Switch 16 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana
1	Rack	Servidores		Gabinete Cerrado TIC's	Sgop. Luis Santana
1		Firewall FortiGuard		BACO UGT-ESPE TICs	Sgop. Luis Santana
1	UPS 6KVA	Energía Respaldo TIC's		TICs	Sgop. Luis Santana
1	Servidor Linux	Servicio Proxy Permisos Acceso RED		TICs	Sgop. Luis Santana
1	Sistema Operativo Linux	Sistema Operativo Linux		TICs	Sgop. Luis Santana

Elaboración del Análisis de Riesgos de la red LAN de la Unidad de Gestión de Tecnologías ESPE





E S P E
ESCUELA POLITÉCNICA DEL EJÉRCITO
CAMINO A LA EXCELENCIA



E S P E
ESCUELA POLITÉCNICA DEL EJÉRCITO
CAMINO A LA EXCELENCIA



E S P E
ESCUELA POLITÉCNICA DEL EJÉRCITO
CAMINO A LA EXCELENCIA



ESPE
ESCUELA POLITÉCNICA DEL EJÉRCITO
CAMINO A LA EXCELENCIA



ESPE
ESCUELA POLITÉCNICA DEL EJÉRCITO
CAMINO A LA EXCELENCIA

CONCLUSIONES

- Los requerimientos de las herramientas, fueron identificadas y especificadas según sus características operacionales, dando lugar al desarrollo exitoso de las actividades planteadas para el análisis de los riesgos de activos de red de la institución.
- La Metodología Magerit, aplicada en el proyecto de investigación ayudó de manera principal a la protección de los equipos informáticos, la misma que fue establecida según las dimensiones de seguridad, disponibilidad, integridad, confidencialidad, apoyando a la disposición de los servicios y mantenimiento.
- El desarrollo del plan de defensa y protección, efectuado, a partir del análisis de los activos de la red LAN de la Unidad de Gestión de Tecnologías ESPE, es pieza fundamental en la prevención de incidentes, el cual ayuda a mejorar la seguridad del uso adecuado de los recursos informáticos. Obteniendo la reducción significativa entre el 75% al 80% de ocurrencia de amenazas; y asegurando de mejor manera la gestión de la seguridad en la Institución, en función del tratamiento de los riesgos de mayor importancia



RECOMENDACIONES

- Se recomienda la utilización de metodologías, referentes a seguridad informática, en las que se pueda identificar riesgos recurrentes para de esta manera ayudar a reducirlos.
- Es recomendable contar con herramientas de análisis y gestión de riesgos como Pilar porque en el caso de suscitarse una amenaza da una respuesta eficaz, para minimizar los riesgos de degradación en los activos de una red
- Mantener actualizadas las políticas de seguridad de la información en el Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, para precautelar la integridad de cada uno de los recursos informáticos, basándose en procedimientos que ayuden a incrementar la protección de los equipos.
- Verificar de manera constante la evolución de herramientas de seguridad informática y por consiguiente el surgimiento de nuevas amenazas en general, para tratar de evitarlas o aplicar la solución más efectiva.

