T.I RESCUE

SEGURIDAD INFORMÁTICA

MESA DE AYUDA

www.tirescue.com
Info@tirescue.com.co
(57)315 259 2011

DISTINCIÓN EXCELENCIA

ISO 9001

Seguridad informática premium, respaldada por el reconocimiento internacional ISO 9001.

SC-CER900888

ISO 27001

Defendiendo Tus Datos con Rigor Internacional: Certificación ISO 27001.

SI-CER900889

ISO 20000-1

Excelencia en ciberseguridad, fundamentada en estándares mundiales de calidad.

TI-CER988544

ISO 22301

Continuidad del negocio sin interrupciones, conforme a estándares internacionales.

CO-CNCER988779

CUATRO CERTIFICACIONES ISO DEFINEN NUESTRA SUPERIORIDAD

Nuestro compromiso con la ciberseguridad trasciende la simple retórica. Es tangible y está validado por cuatro prestigiosas certificaciones **ISO: 9001, 27001, 20000-1 y 22301.** Estas no son solo acrónimos, sino un testimonio de nuestra dedicación para ofrecer servicios de primera clase. Representan nuestra promesa de calidad, seguridad, **eficiencia y resiliencia.** Al elegirnos, no solo está optando por un proveedor de ciberseguridad, sino por un aliado certificado que entiende y cumple con los más altos estándares internacionales.

COMPROMISO INTEGRAL: **MÁS ALLÁ DE LA SEGURIDAD BÁSICA**

Con nuestras certificaciones, garantizamos **calidad, seguridad de la información, excelencia en TI y continuidad del negocio**. Representan nuestro compromiso, profesionalismo e integridad. Elegirnos es optar por la ciberseguridad de élite y con respaldo.

icontec ISO 9001 SC-CER900888

icontec ISO / IEC 27001 SI-CER900889

icontec ISO / IEC 20000-1 TI-CER988544

icontec ISO 22301 CO-CNCER988779

IQNET CERTIFIED MANAGEMENT SYSTEM

PENTESTING AVANZADO

Certified Red Team Professional (CRTP)

Especialización en **Red Teaming** y ataques en **Active Directory**, validando técnicas avanzadas de explotación y escalamiento de privilegios en entornos empresariales.

Practical Network Penetration Tester (PNPT)

La certificación PNPT de TCM Security acredita habilidades en **pentesting real**, incluyendo explotación, escalamiento de privilegios y reportes profesionales.

Certified Ethical Hacker Master

Certificación en hacking ético y ciberseguridad ofensiva, validando habilidades en pruebas de penetración, análisis de vulnerabilidades y ataques controlados.

Cisco Ethical Hacker

Certificación en hacking ético y pruebas de penetración, con habilidades en análisis de vulnerabilidades, seguridad en redes y explotación de amenazas.

Hack The Box Pro Labs - Zephyr

Certificación avanzada en pentesting ofensivo, cubriendo ataques SQL, escalación de privilegios, explotación de aplicaciones web y movimiento lateral en redes.

Hack The Box Pro Labs - Offshore

Certificación en pentesting avanzado, con enfoque en ataques a Active Directory, evasión de protecciones, escalación de privilegios y tunneling.

Hack The Box Pro Labs - Rastalabs

Certificación en explotación de Active Directory, evasión de defensas, desarrollo de exploits y ataques de phishing, con enfoque en pentesting avanzado.

CERTIFICACIONES AVANZADAS

Certified Purple Team Analyst (CPTA V2)

Enfocado en **validar controles de seguridad** y mejorar la detección mediante ejercicios colaborativos.

Certified Cyber Defense Analyst (CCDA)

Enfocado en monitoreo, correlación de eventos y análisis de alertas para una detección

Certified Red Team Specialist V2 (CRTS V2)

Enfocado en evaluaciones ofensivas controladas: **reconocimiento, explotación y post-explotación.**

Certified Enterprise Lateral Movement Specialist

Certificación CELMS: **movimiento lateral en entornos empresariales** y técnicas de Active Directory.

Certified Web Red Team Analyst

Explotación avanzada de vulnerabilidades, **escalamiento de privilegios**, validación de impacto y documentación de hallazgos para mejorar la seguridad en entornos empresariales.

Certified Red Team Analyst (CRTA)

Especialización en Red Teaming y ataques en Active Directory, aplicando **técnicas avanzadas** de explotación y escalamiento de privilegios en entornos empresariales.

Blue Team Fundamentals

Fundamentos de **Blue Team y defensa en ciberseguridad**, con enfoque en monitoreo de amenazas, respuesta a incidentes y gestión de vulnerabilidades para proteger infraestructuras críticas.

Tirescue.com

SOPORTE TÉCNICO PRESENCIAL Y/O REMOTO DE RESPUESTA RÁPIDA

¿Qué es la Mesa de ayuda **Nivel 1?**

Objetivo: Resolver problemas de configuración, dudas de software y errores de usuario **de forma inmediata.**

Alcance: Soporte técnico básico que **no requiere intervención física profunda en servidores o redes complejas.**

Dividimos el soporte en dos conceptos clave que determinan el uso del plan mensual:

Requerimientos ("Quiero algo nuevo"): Son solicitudes programadas o pedidos de cambio.

Ejemplos: Instalar un programa, crear un correo corporativo, configurar una firma.

Incidencias ("Algo no funciona"): Son fallos que impiden trabajar.

Ejemplos: El computador no conecta a internet, la impresora no imprime, se bloqueó la contraseña.

Mesa De Ayuda

¿Qué es la Mesa de ayuda **Nivel 2?**

Soporte técnico especializado para casos de mayor complejidad, que pueden involucrar cambios controlados de configuración, **administración de plataformas**, troubleshooting profundo y coordinación con áreas/proveedores. Aplica para tickets escalados desde Nivel 1 o que por su naturaleza requieren segundo nivel.

Requerimientos ("Quiero algo nuevo"): cambios avanzados o con impacto, que requieren validación técnica, permisos elevados, o tocar **plataformas/servidores/red.**

Ejemplo: Implementación de cambios en red (segmentación, VLAN, WiFi empresarial) o servicios internos.

Incidencias ("Algo no funciona"): Son fallos que **afectan la operación** y requieren diagnóstico profundo o intervención sobre **servicios críticos.**

Ejemplos: Problemas persistentes de conectividad (VPN, red corporativa, WiFi, DNS/DHCP).

Bronze

1 - 10 usuarios

- Servidores
- Mantenimientos
- Seguridad
- Backup
- Nivel 1
- Nivel 2

Requerimientos: 10
Incidentes: 3

$700.362 Mes

Usuario $80.000 Mes

Silver

11 - 25 usuarios

- Servidores
- Mantenimientos
- Seguridad
- Backup
- Nivel 1
- Nivel 2

Requerimientos: 25
Incidentes: 8

$1´260.652 Mes

Usuario $80.000 Mes

Valor requerimiento adicional

$60.000

Golden

25 - 40 usuarios

- Servidores
- Mantenimientos
- Seguridad
- Backup
- Nivel 1
- Nivel 2

Requerimientos: 45
Incidentes: 15

$1´890.978 Mes
Usuario $80.000 Mes

Diamond

41 - 100+

- Servidores
- Mantenimientos
- Seguridad
- Backup
- Nivel 1
- Nivel 2

Requerimientos: 70
Incidentes: 25

$2´661.376 Mes
Usuario $80.000 Mes

Valor incidencia adicional
$120.000

T.I RESCUE

SEGURIDAD INFORMÁTICA

IMPLEMENTACIÓN DE INFRAESTRUCTURA

www.tirescue.com
Info@tirescue.com.co
(57)315 259 2011

DISEÑO Y EJECUCIÓN DE INFRAESTRUCTURAS TI

En **TI Rescue**, nos enorgullecemos de nuestra dedicación a la **excelencia y la mejora continua**, lo cual está certificado y respaldado por nuestra adhesión a las **normas ISO.** Estas certificaciones son la piedra angular de nuestro compromiso con la calidad, la seguridad, la gestión eficiente y la resiliencia operativa

Nuestras implementaciones se guían por los más altos estándares globales ISO.

icontec ISO 9001 SC-CER900888

icontec ISO / IEC 27001 SI-CER900889

icontec ISO / IEC 20000-1 TI-CER988544

icontec ISO 22301 CO-CNCER988779

IQNET CERTIFIED MANAGEMENT SYSTEM

ÍNDICE
CONTENIDO

DOCUMENTACIÓN PREVIA A CONTRATACIÓN

Al iniciar el contrato, se enviará un **enlace** al cliente para que **cargue los documentos administrativos en un formulario**. Esta etapa permite recopilar la información necesaria antes de proceder con la implementación en nuestra infraestructura.

DOCUMENTOS ADMINISTRATIVOS

- Solicitud de RUT
- Solicitud de cámara de comercio
- Firma de contrato
- Envío de contrato de confidencialidad y anexo 14
- Firm de contrato de confidencialidad y anexo 14
- Envio plan de trabajo

FUNDAMENTOS DE LA DOCUMENTACIÓN ADMINISTRATIVA Y TÉCNICA

📌 **Objetivo Clave:** La documentación garantiza evidencia tangible del progreso y cumplimiento del proyecto.

📌 **Comunicación y Claridad:** Unifica la comprensión de objetivos y procesos entre todas las partes.

📌 **Cumplimiento Legal y Regulatorio:** Reduce el riesgo de incumplimiento y sanciones al demostrar conformidad con normativas.

DOCUMENTOS TÉCNICOS

- Envío de matriz de usuarios
- Envío matriz F-40
- Recepción matriz de usuarios
- Recepción de F-40
- Envío de documentos de capacitación
- Credenciales de acceso como administrador

PREPARACIÓN Y PLANIFICACIÓN

- **INVENTARIO DE EQUIPOS Y ANÁLISIS DE CONDICIONES Y CARACTERÍSTICAS**
- **INFORME DE NOVEDADES ENCONTRADAS Y REQUERIMIENTOS AL CLIENTE**
- **ACCIONES CORRECTIVAS ANTES DE LA IMPLEMENTACIÓN**

Estas tareas son fundamentales para garantizar que la fase de ejecución de la **implementación tecnológica pueda proceder sin contratiempos y con la mayor eficiencia posible**, alineándose estrechamente con las necesidades empresariales y las expectativas del cliente.

01. Inventario y Evaluación de Recursos TI

🔍 Identificación y análisis de hardware y software en uso.

⚙️ Evaluación de compatibilidad con nuevas soluciones.

🔄 Detección de necesidades de actualización o reemplazo.

02. Informe de Novedades y Requerimientos

💬 Comunicación con el cliente sobre hallazgos y desviaciones.

✅ Recomendaciones técnicas para ajustes.

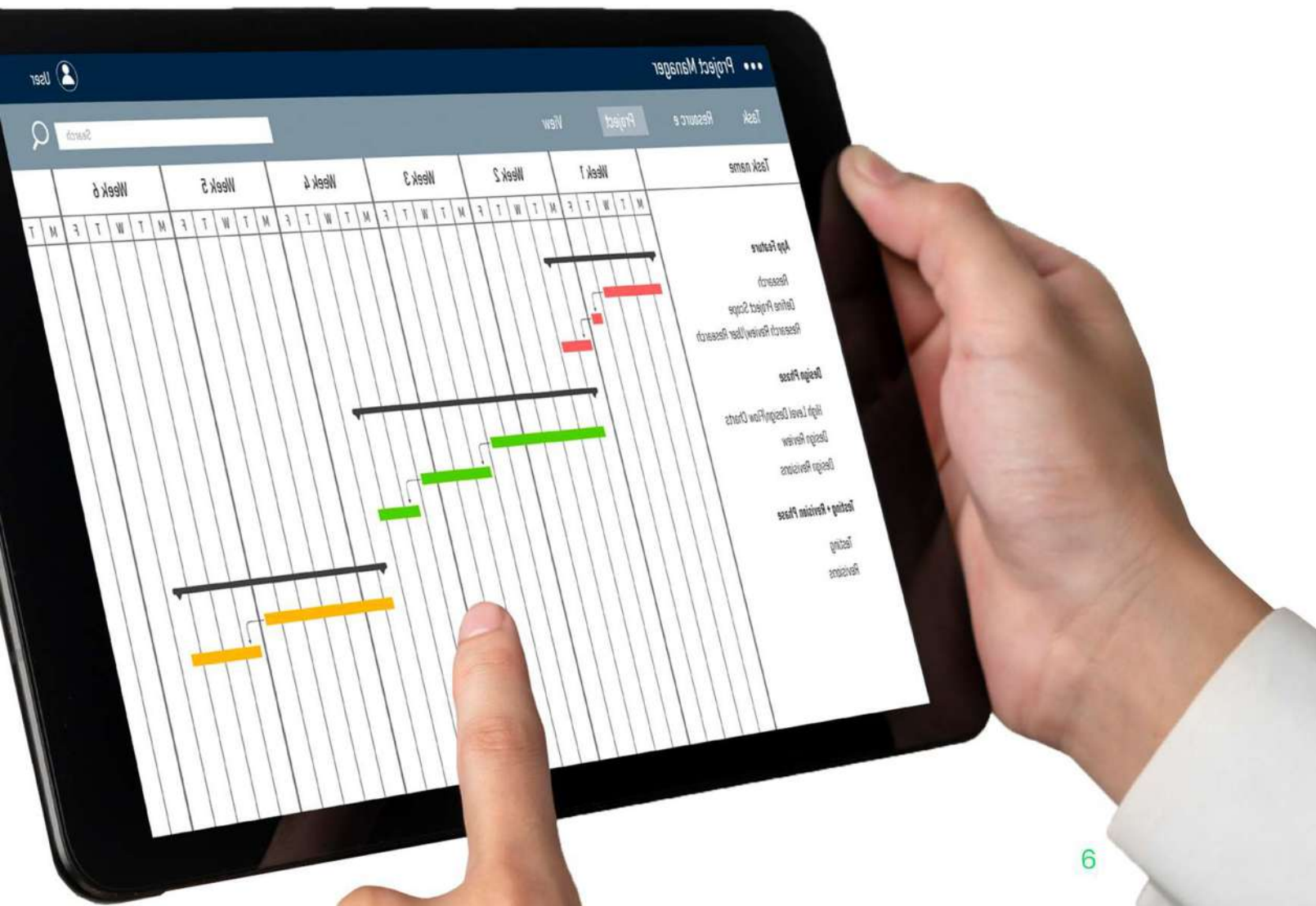
📄 Aprobación del cliente antes de proceder.

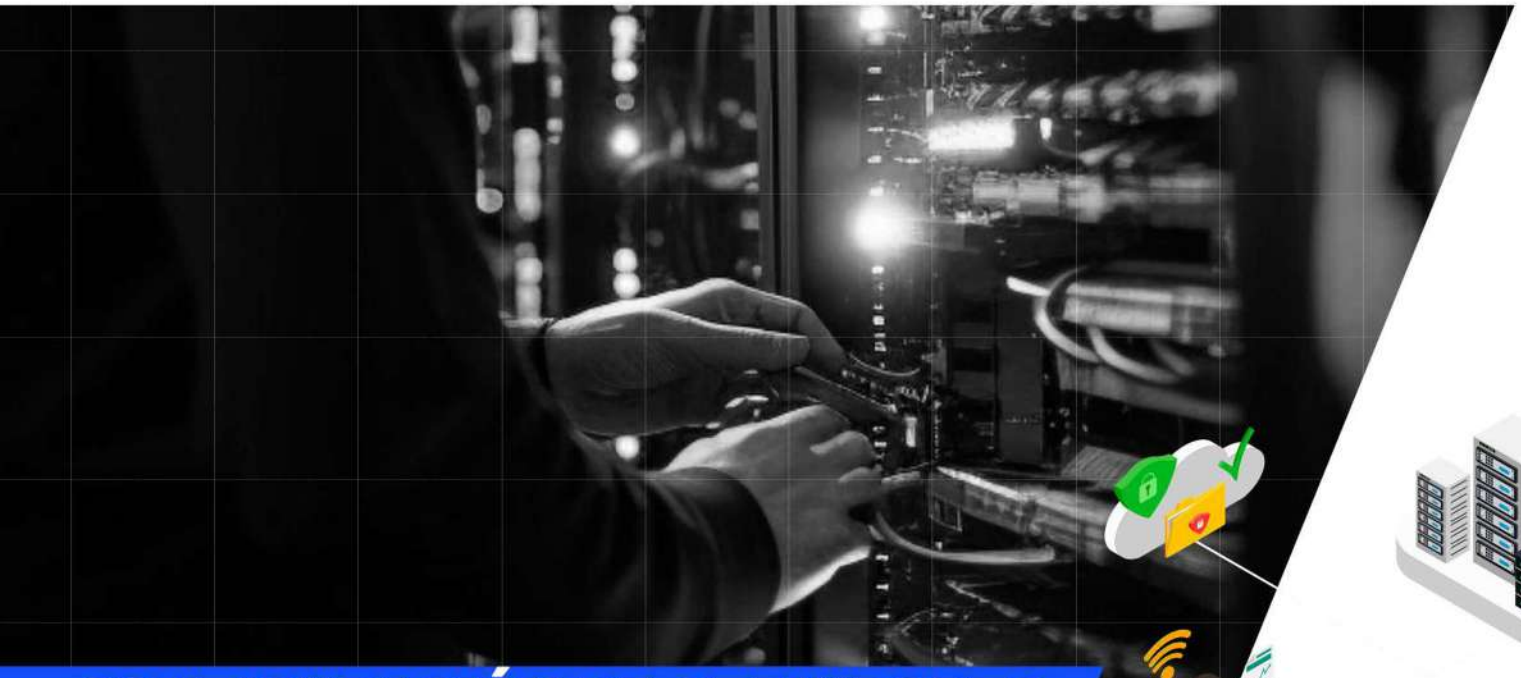
03. Acciones Correctivas Previas a la Implementación

🛠️ Solución de problemas de infraestructura y seguridad.

🔧 Reconfiguración y actualización de equipos y software.

📊 Optimización de procesos operativos para una base sólida.





CONFIGURACIÓN DE SERVIDORES E INFRAESTRUCTURA

- **INSTALACIÓN DE SERVIDOR O MÁQUINA VIRTUAL**
- **IMPLEMENTACIÓN DE ACTIVE DIRECTORY**
- **CREACIÓN DE USUARIOS EN DIRECTORIO ACTIVO**
- **INSTALACIÓN DE VPN EN EL SERVIDOR**
- **CREACIÓN DE ARCHIVOS VPN CON CONFIGURACIÓN PARA LOS EQUIPOS**

Al concluir la fase de "Configuración de Servidores e Infraestructura", una empresa se equipa con una infraestructura de TI fundamentalmente sólida y segura. **Los servidores y máquinas virtuales están activos y optimizados, Active Directory gestiona eficientemente las identidades y políticas**, y la red privada virtual brinda una conexión segura para el flujo ininterrumpido de las operaciones comerciales.

01. INSTALACIÓN DE SERVIDOR O MÁQUINA VIRTUAL

🖥️ Configuración de servidores físicos o virtuales como centros de datos o nodos de aplicación.

02. IMPLEMENTACIÓN DE ACTIVE DIRECTORY

📂 Configuración del servicio de directorio para controlar accesos y políticas en la red.

03. CREACIÓN DE USUARIOS EN DIRECTORIO ACTIVO

👥 Registro y configuración de cuentas de usuario para autenticación y autorización.

04. INTALACIÓN DE VPN EN EL SERVIDOR

🔒 Configuración de una Red Privada Virtual (VPN) para accesos remotos seguros.

05. CREACIÓN DE ARCHIVOS VPN CON CONFIGURACIÓN PARA LOS EQUIPOS

📑 Generación de configuraciones VPN personalizadas para cada usuario y equipo.

GESTIÓN DE SEGURIDAD

- CREAR E IMPLEMENTAR POLÍTICAS DE SEGURIDAD
- IMPLEMENTACIÓN DE PERMISOS SEGÚN FI-40
- INSTALACIÓN DE ANTIVIRUS
- HABILITAR BITLOCKER EN LOS EQUIPOS

Fortalecemos la seguridad de TI con políticas avanzadas, control de accesos FI-40 y cifrado BitLocker. Garantizamos protección contra intrusiones digitales y amenazas virtuales con soluciones antivirus avanzadas, asegurando la integridad de los sistemas y dispositivos ante cualquier contingencia.

01. Creación e Implementación de Políticas de Seguridad

🛡️ Establecimiento de normas y protocolos para proteger la información contra accesos no autorizados y ciberamenazas.

02. Implementación de Permisos según FI-40

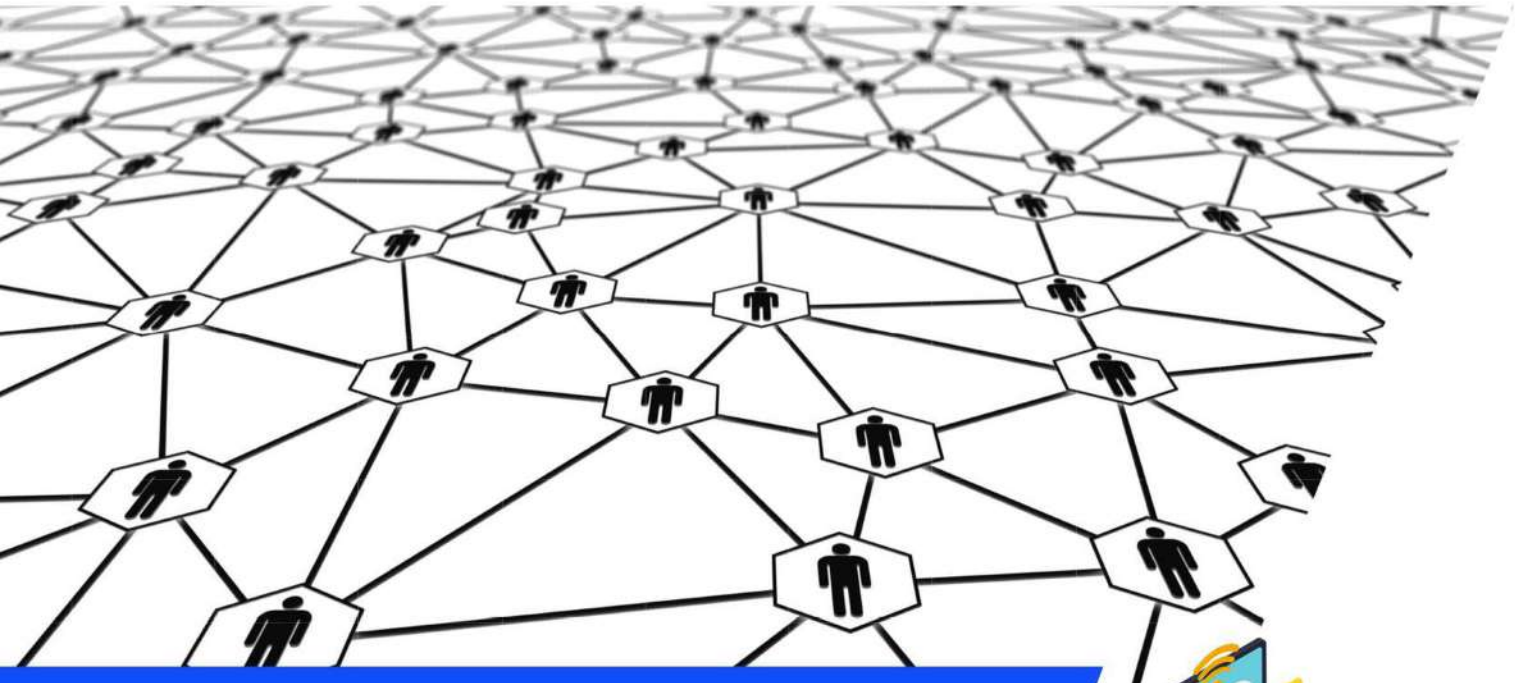
🔑 Configuración de directrices para gestionar accesos y permisos bajo el estándar FI-40.

03. Instalación de Antivirus

🛠️ Implementación de software de seguridad para detectar, prevenir y eliminar malware.

04. Habilitación de BitLocker

🔒 Activación del cifrado de disco para proteger datos ante pérdida o robo de hardware.



ADMINISTRACIÓN DE REDES

- **ENVIO DE CRONOGRAMA PARA MIGRACIÓN DE EQUIPOS**
- **RECEPCIÓN DE APROVADO**
- **INICIO DE MIGRACIÓN DE EQUIPOS AL DOMINIO**
- **CREAR UNIDAD DE RED POR POLÍTICA (USUARIOS)**

Al culminar la fase de "Administración de Redes", se ha logrado una transición coordinada y aprobada de equipos a una infraestructura de red modernizada. La cuidadosa ejecución del cronograma de migración significa que **los dispositivos ahora operan bajo un dominio unificado que mejora la seguridad y simplifica la administración de usuarios.**

01. Envío de Cronograma para Migración de Equipos

📅 Planificación y Comunicación:
Detallamos un calendario para la transferencia organizada de sistemas y datos a la nueva infraestructura.

02. Recepción de Aprobado

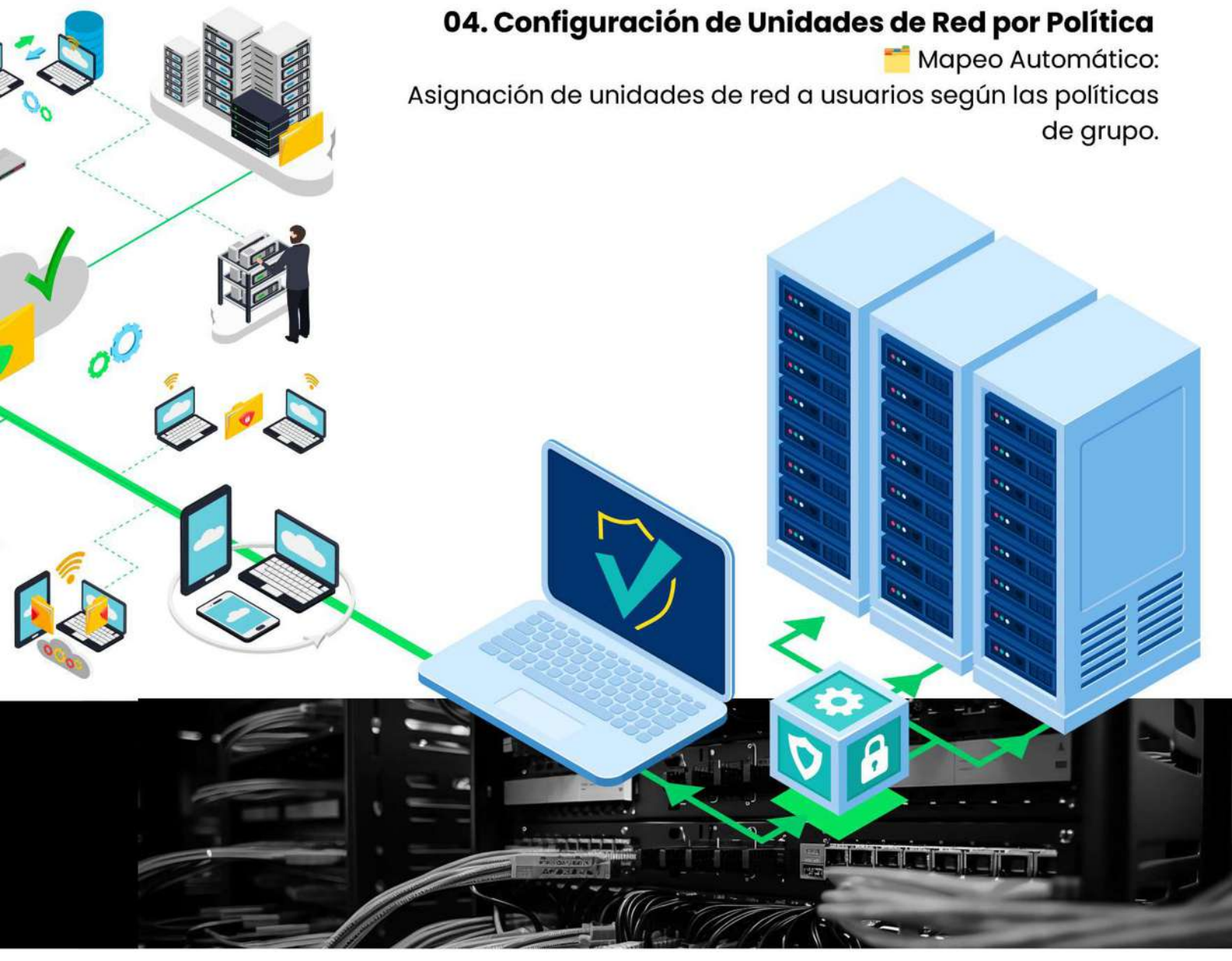
✅ Confirmación del Cliente:
Obtención del consentimiento formal para proceder con las etapas planificadas.

03. Inicio de Migración al Dominio

💻 Transferencia de Equipos:
Migración de computadoras y dispositivos al dominio gestionado por Active Directory.

04. Configuración de Unidades de Red por Política

🗂️ Mapeo Automático:
Asignación de unidades de red a usuarios según las políticas de grupo.



MANTENIMIENTO Y RESPALDO

- PROPUESTA MANTENIMIENTOS PREVENTIVOS
- RESPALDO DE INFORMACIÓN DEL CLIENTE
- MIGRACIÓN DE INFORMACIÓN DEL CLIENTE AL SERVIDOR

El mantenimiento preventivo maximiza el rendimiento y vida útil de los sistemas, reduciendo tiempos de inactividad. Los respaldos y migraciones protegen la información crítica, garantizando su seguridad y disponibilidad ante cualquier imprevisto.

01. Mantenimiento Preventivo

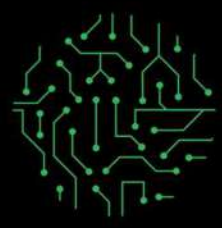
🛠️ Planificación y ejecución de inspecciones regulares para evitar fallas y maximizar la disponibilidad del sistema.

02. Respaldo de Información del Cliente

🔄 Implementación de copias de seguridad que garantizan la integridad y recuperación de los datos.

03. Migración de Información al Servidor

📂 Traslado seguro y eficiente de los datos del cliente a la nueva infraestructura.



T.I RESCUE

SEGURIDAD INFORMATICA

WWW.TIRESCUE.COM

Expertos en Ciberseguridad