WORKSHOP

GESTIÓN Y RESPUESTA DE CIBERATAQUES SIN MORIR EN EL INTENTO

Nahúm Deavila
Consultor en Ciberinteligencia

ROADMAP

1. ¿Cuál es el estándar común de seguridad?
2. Riesgos, amenazas y vulnerabilidades
3. Anatomía de un ciberataque
4. Respuesta a Incidentes Informáticos
5. Fortaleciendo los niveles de Ciberseguridad

El estado “común” de la Seguridad

- La seguridad **NO** es una prioridad
- No existen suficientes profesionales
- Las infraestructuras son un “Zoológico”
- No hay estrategias de monitoreo
- ¿Hay falta de **interés** o falta de **conocimiento**?

La seguridad **NO** es Prioridad...

1. La alta dirección no es consciente
2. El principio de las 3-D
3. ¿Cuál es el valor de tu información?
4. ¿Perdida de continuidad del negocio?
5. Es una **inversión** NO un gasto

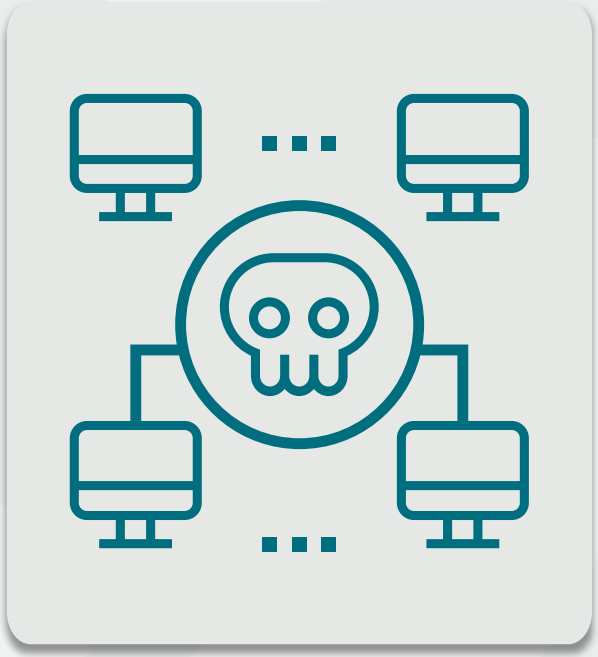
¿Soluciones?

Hablemos de Infraestructuras

Historias de terror

Componentes típicos en una infraestructura promedio:

- Diversidad de sistemas operativos
- Servicios por defecto
- Aspectos del antivirus
- Directorio activo obsoleto
- La segmentación de redes
- Actualizaciones y Backup



Vulnerabilidades en Infraestructuras Corporativas

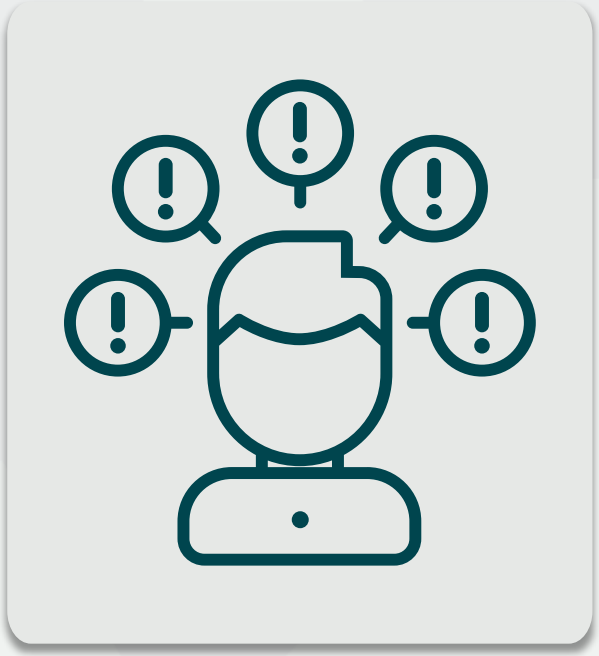
Vectores de compromiso inicial

Servicios expuestos en internet

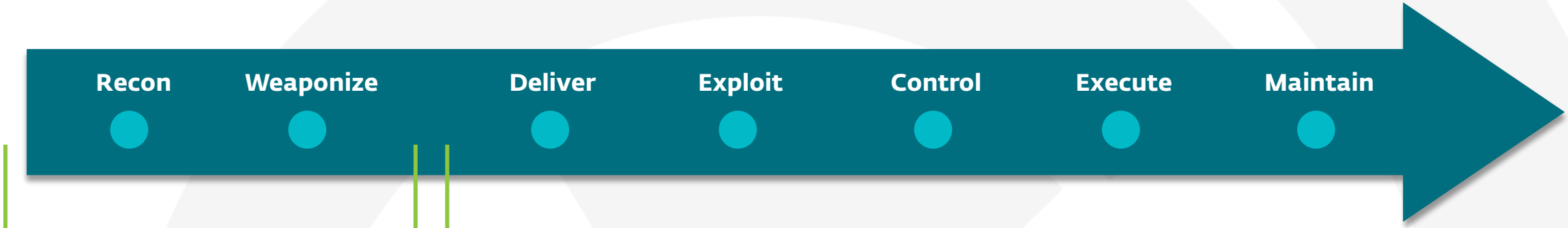
Interacción de un usuario final

Los principales dolores de cabeza para **Sysadmins**

- Carpetas compartidas (SMB)
- Escritorio remoto (RDP)
- Configuraciones por defecto
- Software desactualizado
- Aplicaciones o software sin testear
- Red sin segmentación
- Sin monitoreo de eventos
- Sin plan de respuesta a incidentes



Anatomía de un Ciberataque

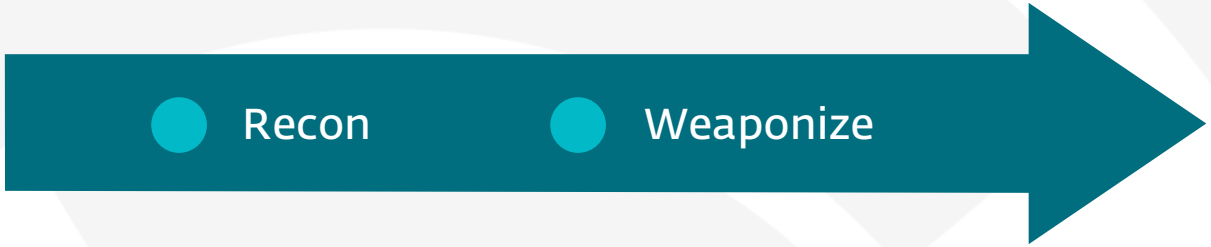


PRE-ATT&CK

- Priority Definition
- Planning, Direction
- Target Selection
- Information Gathering
- Technical, Paople, Organizational
- Weakness identification
- Technical, People, Organizational
- Adversary OpSec
- Establish & Maintain Infrastructure
- Personal Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

ATT&CK for Enterprise

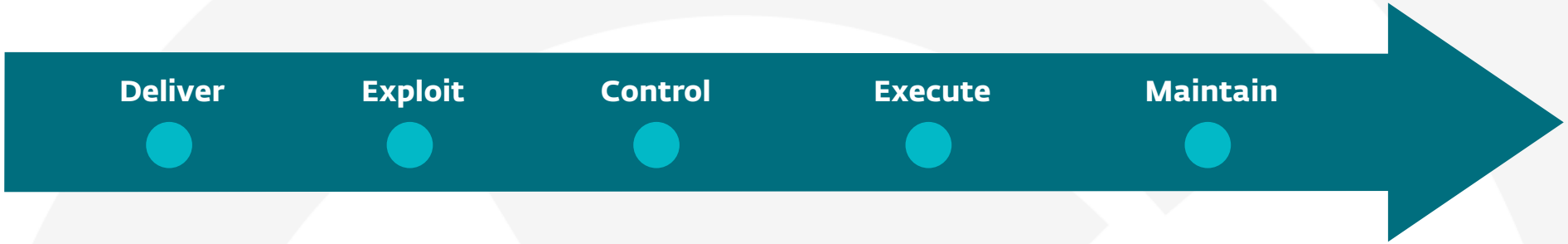
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Impact



PRE-ATT&CK

Priority Definition

- Planning, Direction ✔
- Target Selection ✔
- Information Gathering ✔
- Technical, Paople, Organizational ✔
- Weakness identification ✔
- Technical, People, Organizational ✔
- Adversary OpSec ✔
- Establish & Maintain Infrastructure ✔
- Personal Development ✔
- Build Capabilities ✔
- Test Capabilities ✔
- Stage Capabilities ✔



ATT&CK for Enterprise

- Initial Access ✔
- Execution ✔
- Persistence ✔
- Privilege Escalation ✔
- Defense Evasion ✔
- Credential Access ✔
- Discovery ✔
- Lateral Movement ✔
- Collection ✔
- Command and Control ✔
- Impact ✔

ESCENARIOS

Exposición de Activos

- Zero Days
- Vulnerabilidades comunes
- Visibilidad en Internet

Ataques Dirigidos

- Campañas de Phishing
- Spear Phishing
- Crimen organizado

Compromiso Inicial

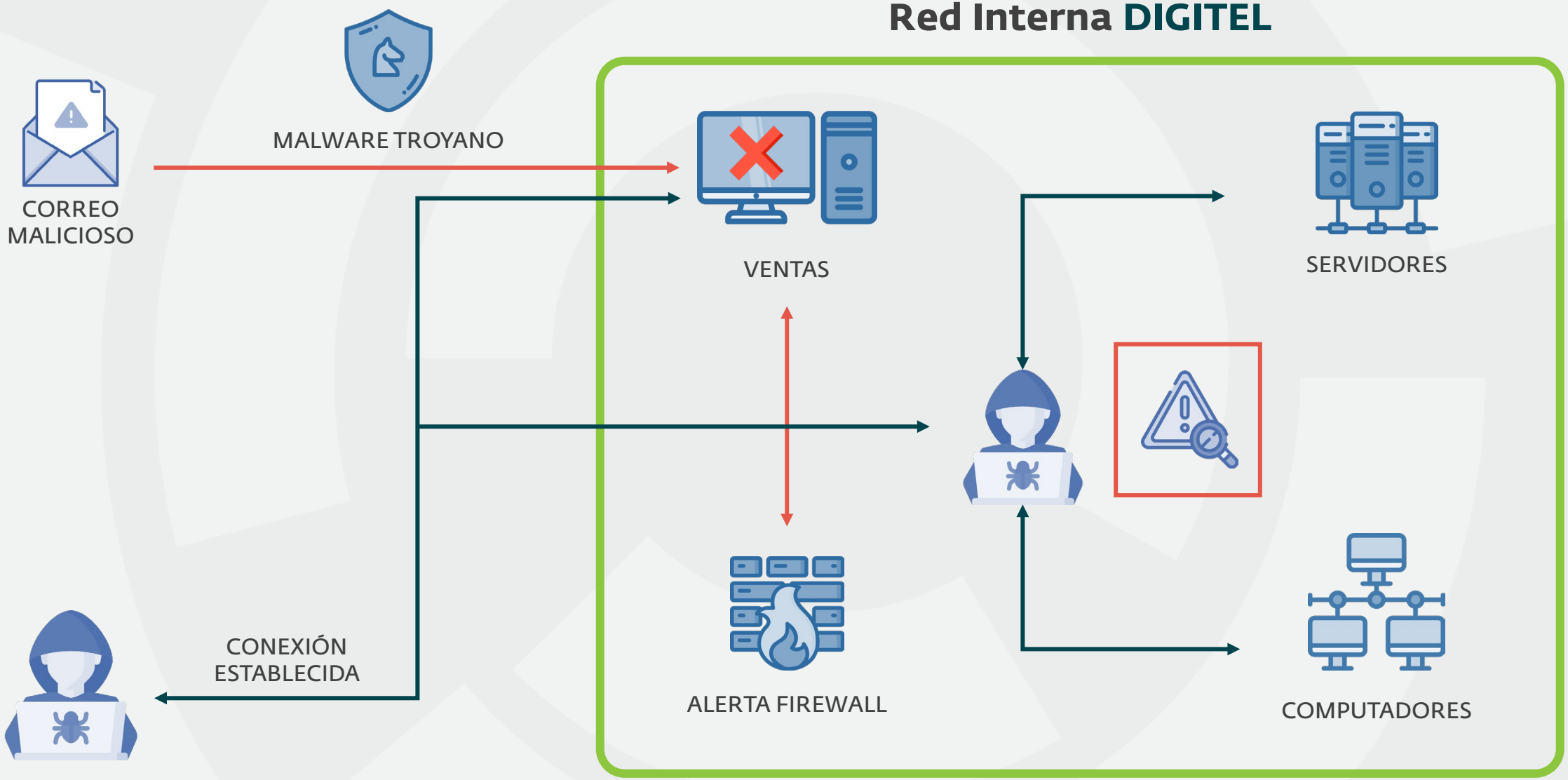
Acceso inicial
Spear-phishing

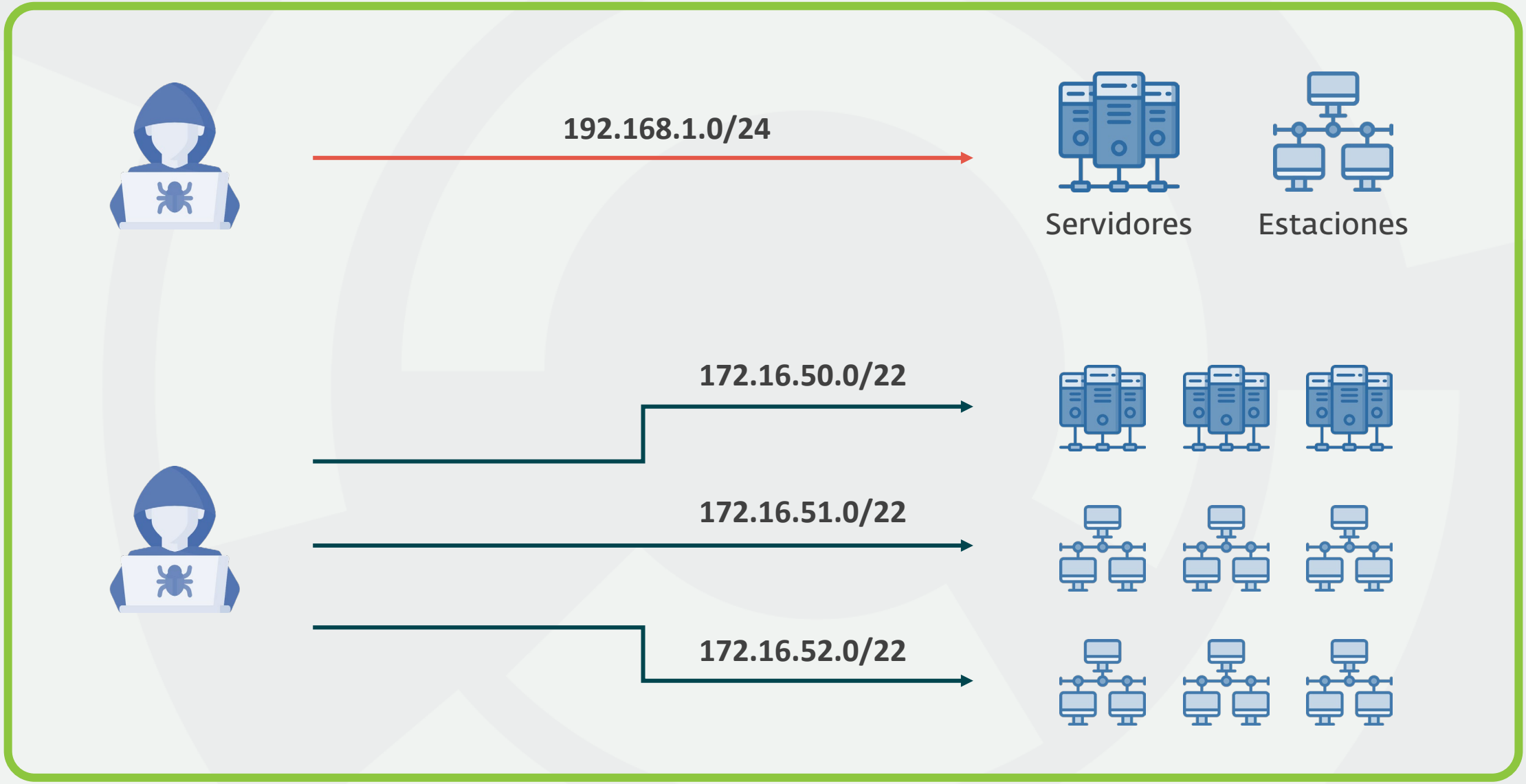
Servicios Remotos
Credenciales débiles

Vulnerabilidades
CVE públicos

Ciberataque a DIGITEL

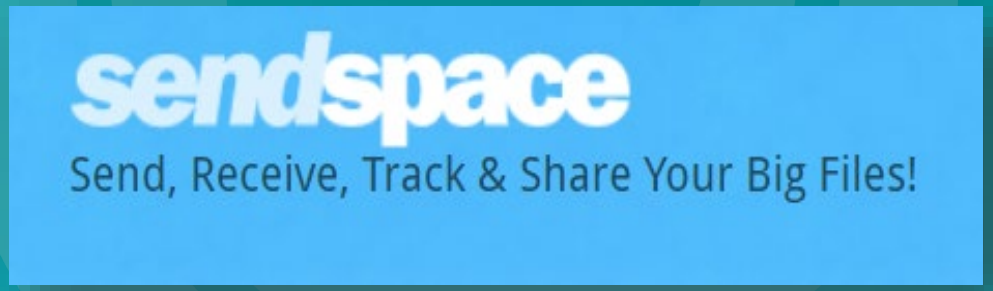
Red Interna DIGITEL





- Creación de persistencia
- Exfiltración de información
- Extracción de credenciales
- Escaneo de sistemas internos
- Movimientos laterales
- Evasión de sistemas de seguridad

Exfiltración de información



Persistencia en Windows

- Migración del proceso
- Inicio automático con Windows
- Manipulación de registro
- Creación de usuario(s) con privilegios
- Desactivación del Antivirus
- Modificación del Firewall

Movimientos Laterales

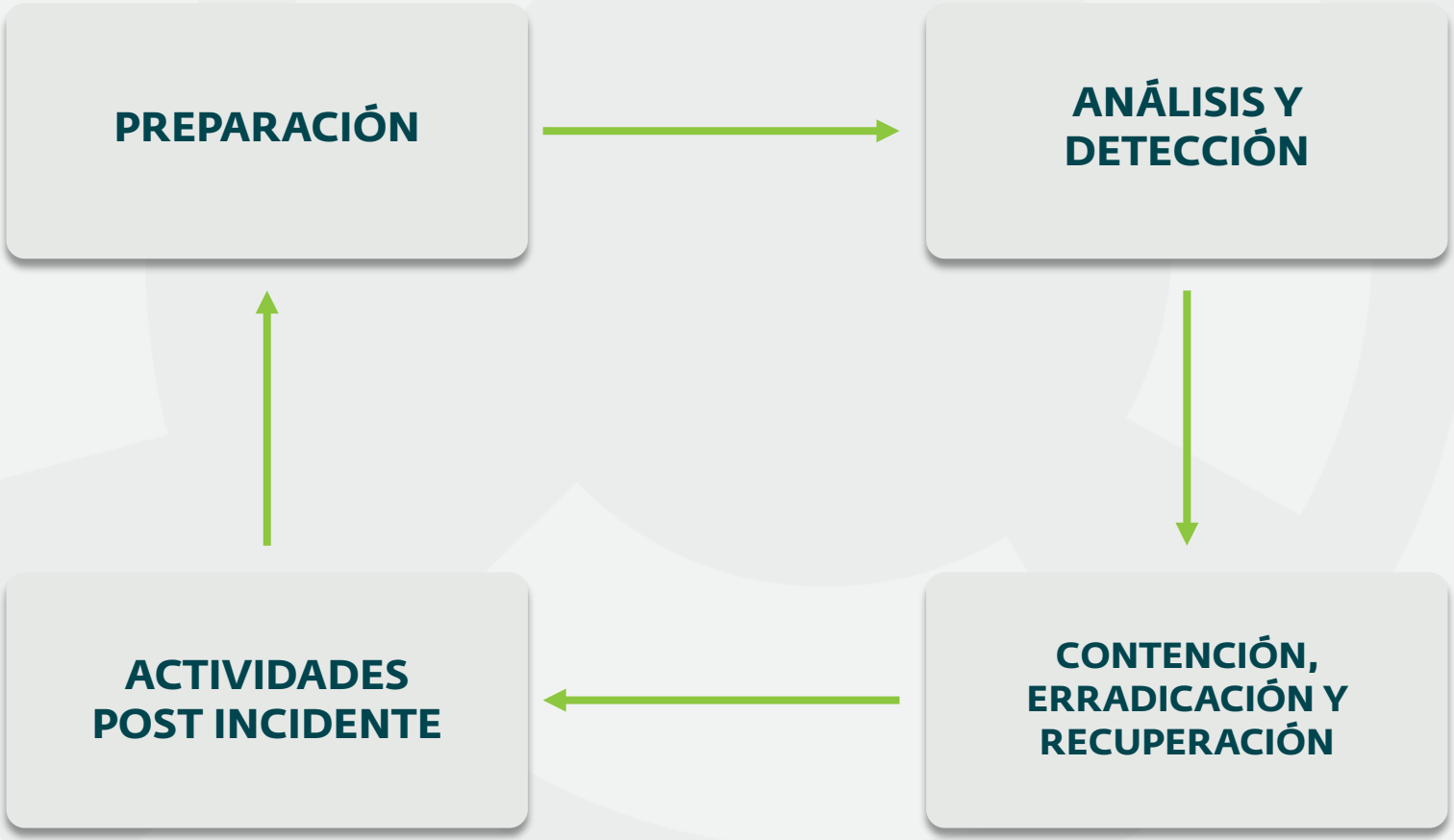
Carpetas Compartidas (SMB)

¿Qué tan preparado estas para un Ciberataque?

¿Soy Ciber resiliente?

- Conozco el funcionamiento de mi infraestructura
- Tengo documentación de seguridad
- Implemento mi documentación
- Realizo pruebas periódicamente
- Cuento con profesionales en seguridad

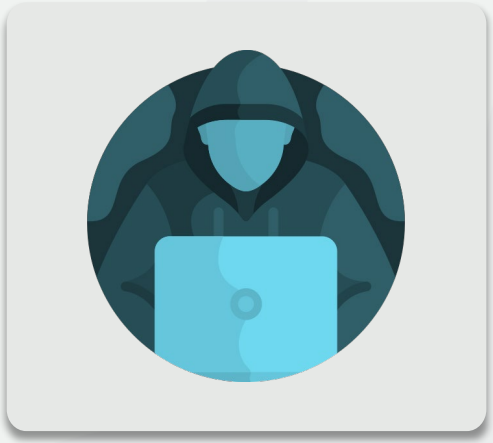
El ciclo adecuado



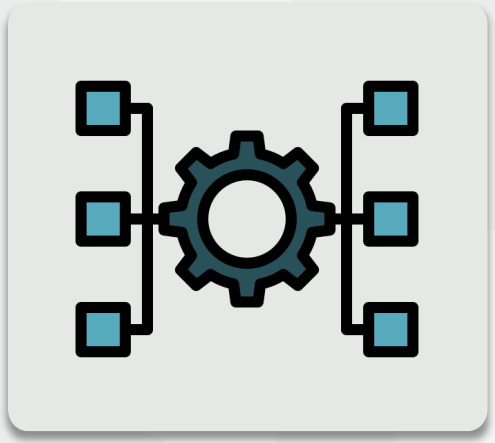
Antes del Incidente

- Gestión de activos
- Documentación necesaria
- Sensibilización a usuarios
- Simulacros
- Monitoreo de sistemas
- Gestión de riesgos

No olvides...



- Pruebas de Ethical Hacking
- Análisis de vulnerabilidades
- Gestión de vulnerabilidades



- Aplicaciones web
- Software a medida
- Infraestructura general

Llego el día esperado...

Identificar el ataque

Inicio los protocolos

Recupero los sistemas

Verifico el protocolo

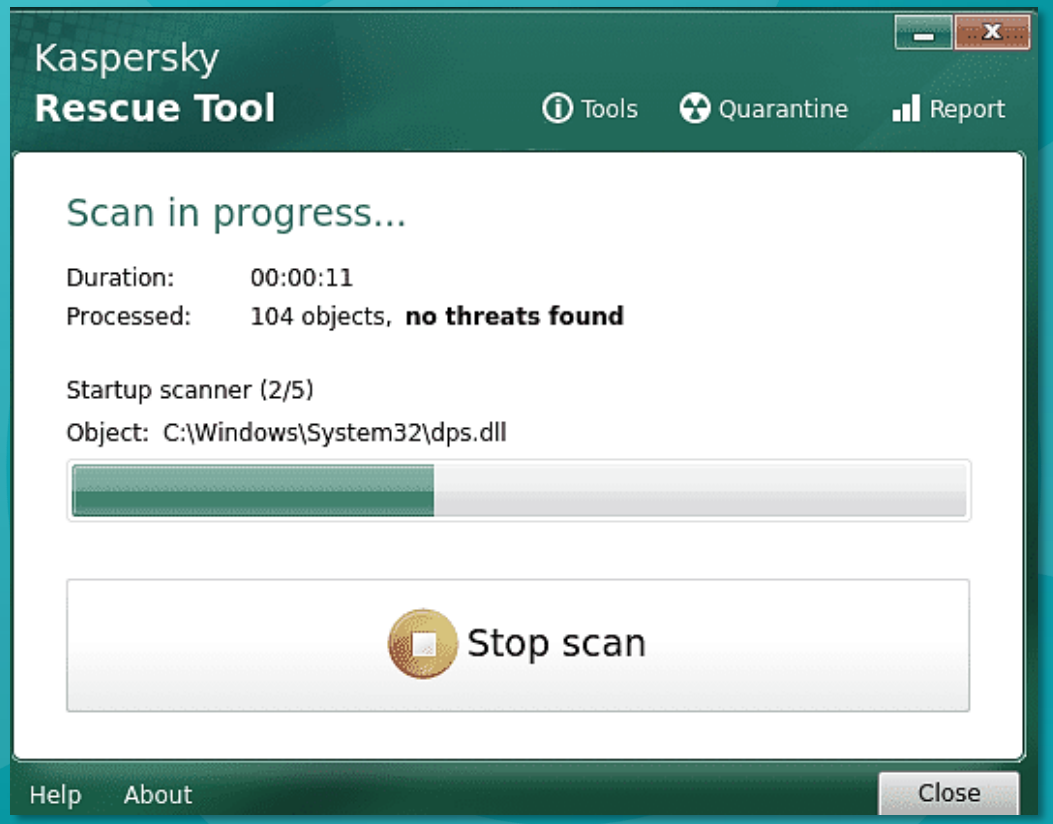
Actividades en Incidente

1. Evaluación inicial
2. Respuesta inicial
3. Recopilación de pruebas forenses
4. Implementar solución temporal
5. Enviar comunicaciones
6. Consultar a las autoridades
7. Implementar soluciones permanentes
8. Determinar el impacto en el negocio

Protocolo de Respuesta

1. Desconexión total de Internet (NO apagues equipos)
2. Limpieza a bajo nivel con herramienta (Kaspersky Rescue Tool)
3. Activar la visualización de carpetas ocultas
4. Desactivar las unidades de red del sistema
5. Verificar las carpetas compartidas (permisos)
6. Verificación de usuarios del sistema
7. Eliminar archivos cifrados
8. Instalación o activación de Antivirus
9. Escanear el sistema con el antivirus
10. Conectar el equipo a Internet

Kaspersky Rescue Tool



- ISO liviana para Bootear
- Escaneo a unidades
- Eliminación de malware

¿Se debe denunciar?

- ¿Cuál es el valor de la información cifrada?
- ¿Qué sucede si se filtra la información?
- ¿Es una infraestructura critica?
- Aspectos legales con clientes y proveedores
- ¿Se debe pagar rescate?

¿Vale la pena investigar?

- ¿Cuál es el objetivo de la investigación?
- ¿Existen sospechas de un Insider?
- ¿Por qué SI debería hacerlo?
- ¿Quiénes deberían realizarla?
- ¿Qué espero de los resultados?

Actividades POST Incidente

1. Definir la nueva estrategia de seguridad
2. Sensibilizar a los usuarios
3. Monitorear la infraestructura
4. Recuperar la normal operatividad
5. Iniciar la nueva preparación a incidentes

¿Cuál es el Principal Problema?

Infraestructura Segura

¿Qué debería tener?

1. Segmentación correcta de red
2. Copias de seguridad eficientes
3. Sistemas de Ciberseguridad
4. Personal capacitado
5. Departamento especializado

Centro de Operaciones en Seguridad (SOC)

- Prevención de amenazas y ataques
- Análisis y monitorización
- Defensa ante ciberataques
- Mejora continua en ciberseguridad

Sistemas en Ciberseguridad

Soluciones Open Source

1. Honeypot de alta interacción
2. Plataforma de Gestión de Incidentes
3. Plataforma de Gestión de Amenazas
4. Plataforma de Inteligencia de Amenazas
5. Plataforma de Análisis de Amenazas
6. Gestión de eventos y seguridad (SIEM)

Preparación para Futuros Incidentes

Guía rápida

1. Plan de respuesta a incidentes
2. Clasifica, monitorea y prueba
3. Ten un equipo capacitado
4. Sensibiliza periódicamente
5. Prioriza las copias de seguridad

GRACIAS

#Bogotá territorio inteligente

Jueves 04 de agosto de 2022
9:00 a.m. a 10:30 am

COMPARTIC BOGOTÁ GOBIERNO Y SEGURIDAD DIGITAL

Plan Estratégico de Tecnologías de la Información - PETI

ALCALDÍA MAYOR DE BOGOTÁ D.C. | ALTA CONSEJERÍA DISTRITAL DE TIC | BOGOTÁ

Tema:

PETI

FECHA: agosto 04, 2022 9:00am

- **9:00 Apertura y presentación de la Alta Consejería Distrital de TIC**
  - Estrategia de la Oficina de Alta Consejería TIC
  - Objetivos de las sesiones de ComparTIC
  - Mensajes del Plan Estratégico de Tecnologías de la Información - PETI
- **9:20 Presentación del Grupo de Energía de Bogotá**
  - Beneficios, recomendaciones y experiencias.
  - Mayor reto y cómo lo solucionaron.
- **10:00 Preguntas por parte de las entidades y/o asistentes**
  - Lineamientos
  - Agenda de talleres de ComparTIC – Gobierno Digital 2022
- **10:29 Cierre del evento**

Tema:

PETI

FECHA: agosto 04, 2022 9:00am

Grupo de Energía de Bogotá

José Fernando Galvis Panqueva

Gerente de tecnología

jgalvis@geb.com.co

Oficina de Alta Consejería Distrital de TIC

Nicolás Sánchez Barrera

nsanchez@alcaldiabogota.gov.co

Jaime Leonardo Acosta Diaz

jlacosta@alcaldiabogota.gov.co

Tema:

PETI

FECHA: agosto 04, 2022 9:00am

Estrategia

Oficina de Alta Consejería Distrital de TIC

Buscamos consolidar a Bogotá como un Territorio Inteligente

Se consolida a través de la implementación de un Gobierno Abierto en Bogotá

GOBIERNO ABIERTO DE BOGOTÁ

Lo hacemos a partir del aprovechamiento estratégico de tecnología, datos e innovación a través de proyectos concretos en el Distrito

ALTA CONSEJERÍA DISTRITAL DE TIC | BOGOTÁ

Tema:

PETI

FECHA: agosto 04, 2022 9:00am

ALCALDÍA MAYOR DE BOGOTÁ D.C. | ALTA CONSEJERÍA DISTRITAL DE TIC | BOGOTÁ

ComparTIC

Conocer **cómo hacen otras** entidades **para mejorar la calidad** de vida de los ciudadanos

Aprender a utilizar la tecnología como un medio para facilitar el día a día de las ciudadanas y los ciudadanos

Implementar los lineamientos no es el objetivo final. Debemos **aprender a generar valor a partir de su implementación**

Primer jueves de cada mes
9:00 am a 10:30 am
Gobierno Digital
nsanchez@alcaldiabogota.gov.co

Último Jueves de cada mes
10:00 am a 11:30 am
Seguridad Digital
jcmancipe@alcaldiabogota.gov.co

Tema:

PETI

FECHA: agosto 04, 2022 9:00am

Plan Estratégico de TI

Grupo Energía Bogotá

Mensajes

1. La Planeación Estratégica de TI debe estar pensada en ***transformar, innovar, adoptar nuevas tecnologías*** para que la tecnología se vuelva **un instrumento que genere gran valor a la entidad**. Esto se logra **entendiendo las necesidades de las áreas misionales** y buscando oportunidades en las nuevas tecnologías.

2. Los proyectos del PETI **deben ser priorizados y llevarse al Plan de Acción Institucional** para que puedan ser ejecutados. El rol del jefe TIC debe ser entendido como **el encargado de liderar la transformación digital de cada entidad.**

3. La Transformación Digital se logra entendiendo cuáles son las transformaciones que puedo generar para mejorar **1. La calidad de vida de los usuarios de la entidad, 2. La eficiencia de los procesos de la entidad 3. Las habilidades tecnológicas de los colaboradores de la entidad**. Siempre pensando la tecnología como un medio para lograr esas transformaciones y no como un fin.

Tema:

PETI

FECHA: agosto 04, 2022 9:00am

Lineamientos Plan Estratégico de TI

Decreto 612 de 2018	• Por el cual se fijan las directrices para la integración de los planes institucionales (PETI) al plan de acción de la entidad
Decreto 767 de 2022 – Política de Gobierno Digital	• Se establece que los proyectos de Transformación deben quedar integrados al PETI
Decreto 1263 de 2022 – Lineamientos TD	• Reitera que los proyectos de TD deben ser integrados al PETI

Tema:

PETI

FECHA: agosto 04, 2022 9:00am

Grupo de Energía de Bogotá

José Fernando Galvis Panqueva

Gerente de tecnología

jgalvis@geb.com.co

Oficina de Alta Consejería Distrital de TIC

Nicolás Sánchez Barrera

nsanchez@alcaldiabogota.gov.co

Jaime Leonardo Acosta Diaz

jlacosta@alcaldiabogota.gov.co

Tema:

PETI

FECHA: agosto 04, 2022 9:00am

PREGUNTAS DE ENTIDADES Y ASISTENTES

Tema:

PETI

FECHA: agosto 04, 2022 9:00am

ComparTIC Bogotá: Gobierno Digital

primer jueves del mes de 9:00 a.m. a 10:30 a.m., de la siguiente manera:

- **22 de febrero:** Acuerdo Marco de Precios Nube Pública IV
- **22 de marzo:** Accesibilidad, Usabilidad y Transparencia
- **05 de mayo:** Arquitectura Empresarial
- **02 de junio:** Desarrollo de software DevOps
- **07 de julio:** Desarrollo de Software
- **04 de agosto:** Planeación estratégica de Tecnologías de la Información y las Comunicaciones
- **01 de septiembre:** Internet de las cosas (IoT)
- **06 de octubre**: Servicios Ciudadanos Digitales
- **03 de noviembre:** Servicios centrados en el usuario
- **01 de diciembre:** Analítica

ComparTIC Bogotá: Seguridad Digital

Último jueves del mes de 10:00 a.m. a 11:30 a.m., con los siguientes temas:

- **24 de febrero:** Seguridad Digital – Modelo de Seguridad y Privacidad de la Información
- **24 de marzo:** Plan Distrital de Protección de Datos Personales
- **28 de abril:** Riesgos de seguridad digital
- **26 de mayo:** Seguridad en el teletrabajo o trabajo en casa
- **30 de junio:** Taller de buenas prácticas en seguridad de sitios Web
- **28 de julio:** Plan Estratégico de Seguridad de la Información - PESI
- **25 de agosto:** Riesgos de ciberseguridad en IoT
- **29 de septiembre:** Taller de Hacking ético e Ingeniería Social
- **27 de octubre:** Gestión de incidentes de seguridad de la información
- **24 de noviembre:** Servicios seguros en continuidad del

2022

Alta Consejería Distrital de TIC
Secretaría General - Alcaldía Mayor de Bogotá
Tel: 601 3813000, ext. 2001
Bogotá, Colombia: Carrera 8 # 10 – 65
tic.bogota.gov.co

@ConsejeriaTIC

ALCALDÍA MAYOR DE BOGOTÁ D.C.
ALTA CONSEJERÍA DISTRITAL DE TIC
BOGOTÁ