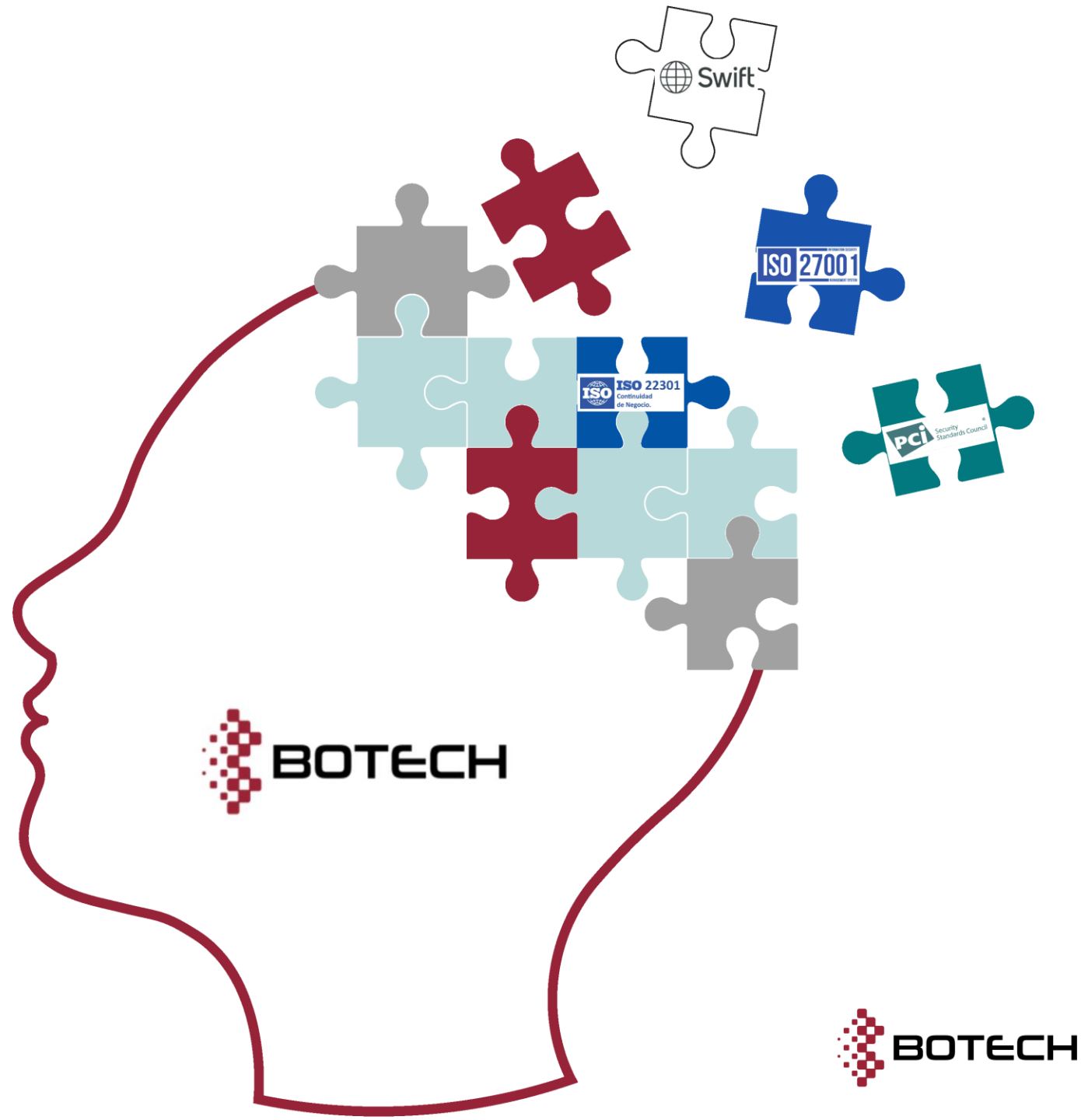


# Eficiencia en Procesos de Cumplimiento para Auditorias de TI





# ESTÁNDARES DE CERTIFICACIÓN







# PASOS CLAVE PARA EL CUMPLIMIENTO EFECTIVO

## DEFINIR UNA ESTRATEGIA

IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

## COLABORACIÓN ORGANIZACIONAL

FORMACIÓN DE UN EQUIPO DE TRABAJO CALIFICADO (INTER-ORGANIZACIONAL)

## PLAN DE TRABAJO

PLANEACIÓN DE AUDITORIAS DE TI

## CONSIDERAR APOYOS COMPLEMENTARIOS

CONTRATACIÓN DE SERVICIOS, HERRAMIENTAS, CONSULTORES, ETC QUE APOYEN AL CUMPLIMIENTO

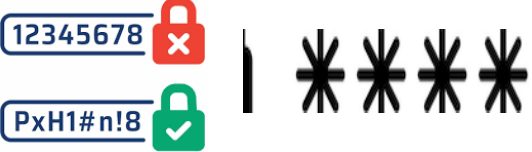




## CAPACITACIÓN

CAPACITAR AL PERSONAL QUE ESTA A CARGO DEL CUMPLIMIENTO

# DEFINIR UNA ESTRATEGIA: DEL SISTEMA DE GESTIÓN

<b>ALCANCE</b>  Determinar <b>alcance(s)</b> claro(s), para el alcance de certificación.  - Tecnología. - Procesos. - Infraestructura. - Personas.	<b>CONTEXTO</b>  Identificar el <b>contexto</b> organizacional y a <b>las partes interesadas</b> internas y externas que afecta al alcance.	<b>LÍDERAZGO</b>  Establecer una estructura de <b>liderazgo</b> que refleje las áreas impactadas dentro del Alcance.
<b>RIESGOS</b>  Contar con una <b>Gestión de Riesgos</b> integral.	<b>UNIFICAR</b>  Establecer un conjunto unificado de:  - Políticas. - Procedimientos. - Estándares - Guías.	<b>DESEMPEÑO</b>  Establecer métricas o indicadores de desempeño capaces de proveer mejora continua integral.

# COMPARATIVA ENTRE ESTÁNDARES

	Swift	ISO 27001	PCI DSS COMPLIANT	AICPA SOC
<b>CONTRASEÑAS</b> 	✓	✓	✓	✓
<b>AUTENTICACIÓN SEGURA - MFA</b> 	✓	✓	✓	✓
<b>ACTUALIZACIONES</b> 	✓	✓	✓	✓
<b>VULNERABILIDADES</b> 	✓	✓	✓	✓
<b>SEGURIDAD FÍSICA</b> 	✓	✓	✓	✓



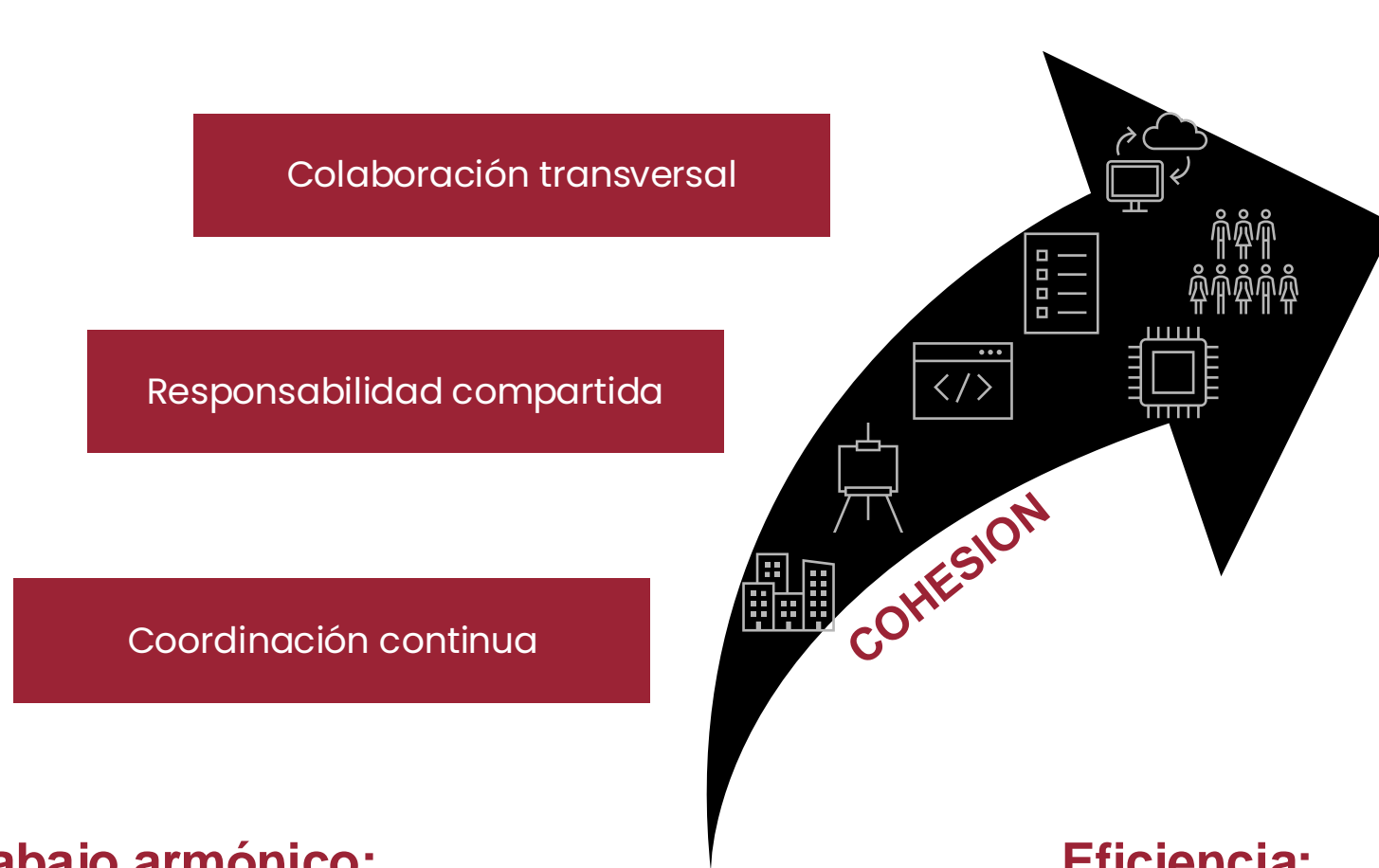
# TIPS PARA EL PROGRAMA DE AUDITORIA



- Considerar plazos de certificación.
- Periodicidades de actividades o tareas recurrentes.
- Disponibilidad de recursos que participan en las sesiones de auditoría.
- Oficina de cumplimiento o personal encargado de coordinar las auditorías.
- Liderazgo en la toma de decisiones.
- Concentración y resguardo de evidencias (Integridad de las evidencias).
- Considerar plazos adecuados para capacitar a los recursos.
- Al finalizar los ciclos de auditoría, revisar las lecciones aprendidas.



# COLABORACIÓN ORGANIZACIONAL



**Trabajo armónico:**  
Alineación interdepartamental de expectativas y responsabilidades

**Eficiencia:**  
Todas las áreas claves controlan su información y evidencias.

# CONSIDERAR APOYOS COMPLEMENTARIOS



**PROVEEDORES  
DE SERVICIO DE NUBE**



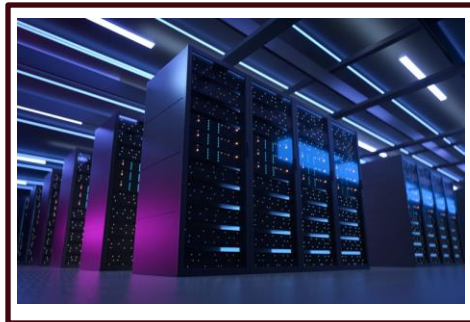
**PROVEEDORES  
DE SERVICIO**



**CONSULTORES  
CALIFICADOS**



**CALL CENTERS**



**CENTROS DE DATOS  
CERTIFICADOS**



**HERRAMIENTAS O  
EQUIPOS CALIFICADOS**



**HERRAMIENTAS DE  
SEGUIMIENTO DE AUDIT**

**Sin  
capacitación**



**Con  
capacitación**



# CAPACITAR AL PERSONAL (BENEFICIOS)

- Interacción con otros expertos.
- Discusión y colaboración en grupos.
- Certificación más efectiva.
- Reducción del tiempo para obtener certificaciones.
- Conocimiento acelerado sobre lo que las normas y estándares.



**empresa que invierte en  
tecnología e infraestructura**



**empleado sin  
capacitación  
cae en un  
phishing**

# AUDITORÍA



Lo que mis amigos piensan que hago



Lo que mi mamá piensa que hago



Lo que la sociedad piensa que hago



Lo que los socios piensan que hago



Lo que yo creo que hago



Lo que realmente hago

# ¿Preguntas?

***Christian Calderón***  
[ccalderon@botech.info](mailto:ccalderon@botech.info)



[www.botech.info](http://www.botech.info)