



Reuniones Científicas y Técnicas

Administración de la ciberseguridad en los sistemas contables actuales

**Comisión de Estudios sobre Sistemas de Registros,
su integridad y autenticidad documental**

Primera reunión: 2 de mayo de 2022

Doctora UBA. Área Contabilidad - Elsa Beatriz Suarez Kimura

Mag. en Seguridad Informática - Diego Sebastián Escobar

Comisión de Estudios sobre Sistemas de Registros, su integridad y autenticidad documental

**Reuniones mensuales 2dos. Martes
de cada mes 18,30 a 20hs**

Primera reunión: 2 de mayo de 2022



Reuniones Científicas y Técnicas



Administración de la ciberseguridad en los sistemas contables actuales

**Comisión de Estudios sobre Sistemas de Registros,
su integridad y autenticidad documental**

Primera reunión: 2 de mayo de 2022



Índice temático

Contexto actual y los objetivos de la actividad.

Ciberseguridad y el sistema de información contable.

Estándares y normativas utilizables/ aplicables en los sistemas contables.

Establecimiento de políticas, alcance del SGSI e inventario de Activos Informáticos.

Análisis de controles.

Reflexiones finales.



Gestión de la Ciberseguridad y el sistema de información contable

Sistema de Información Contable

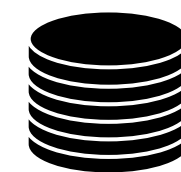
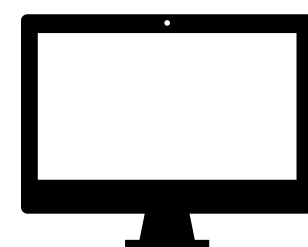
Segmento patrimonial

Segmento gerencial

Segmento ambiental y social



Soporte digital



Perspectivas de la Ciberseguridad

**Sistema de
información
contable**

**Plano
Técnico**

**Plano
Humano**

Organización

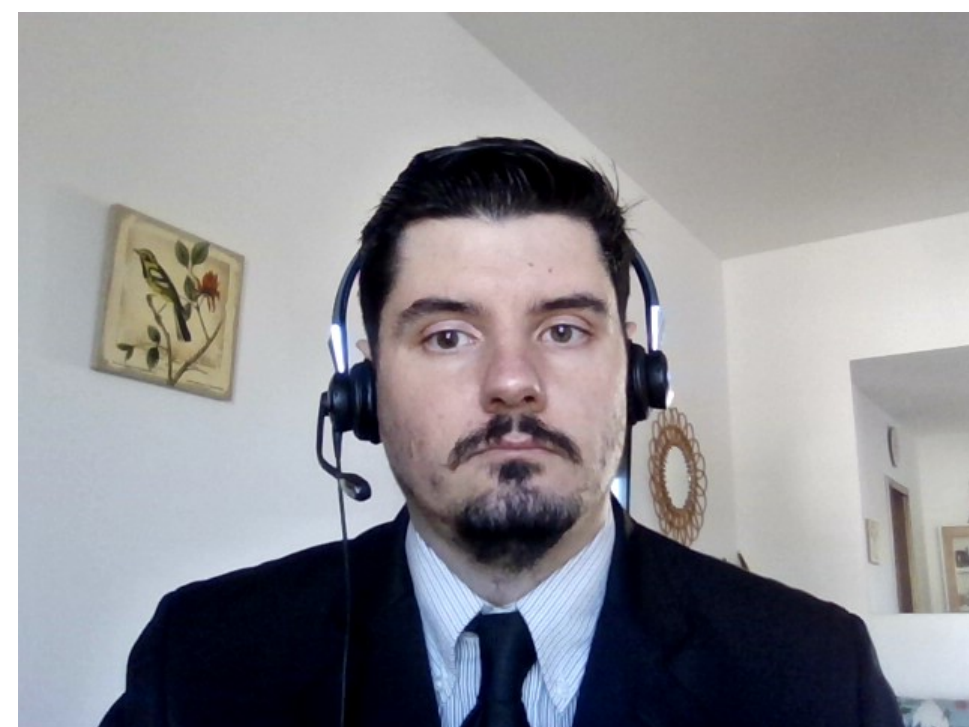
**Cumplimiento
Legal**



Fases para implementar un proyecto de ciberseguridad

S G S I

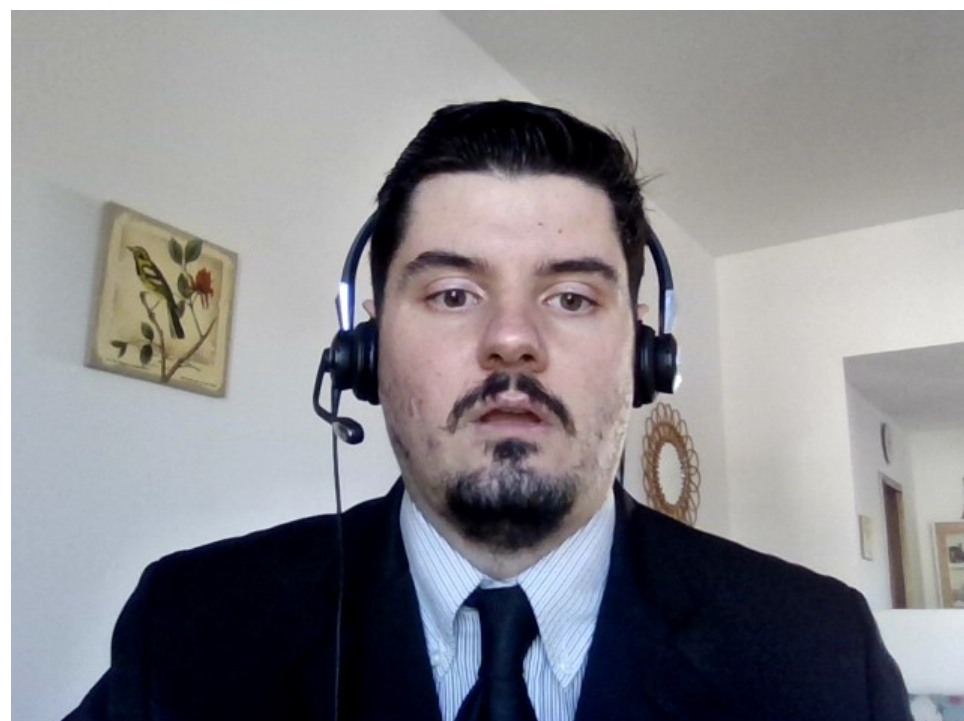
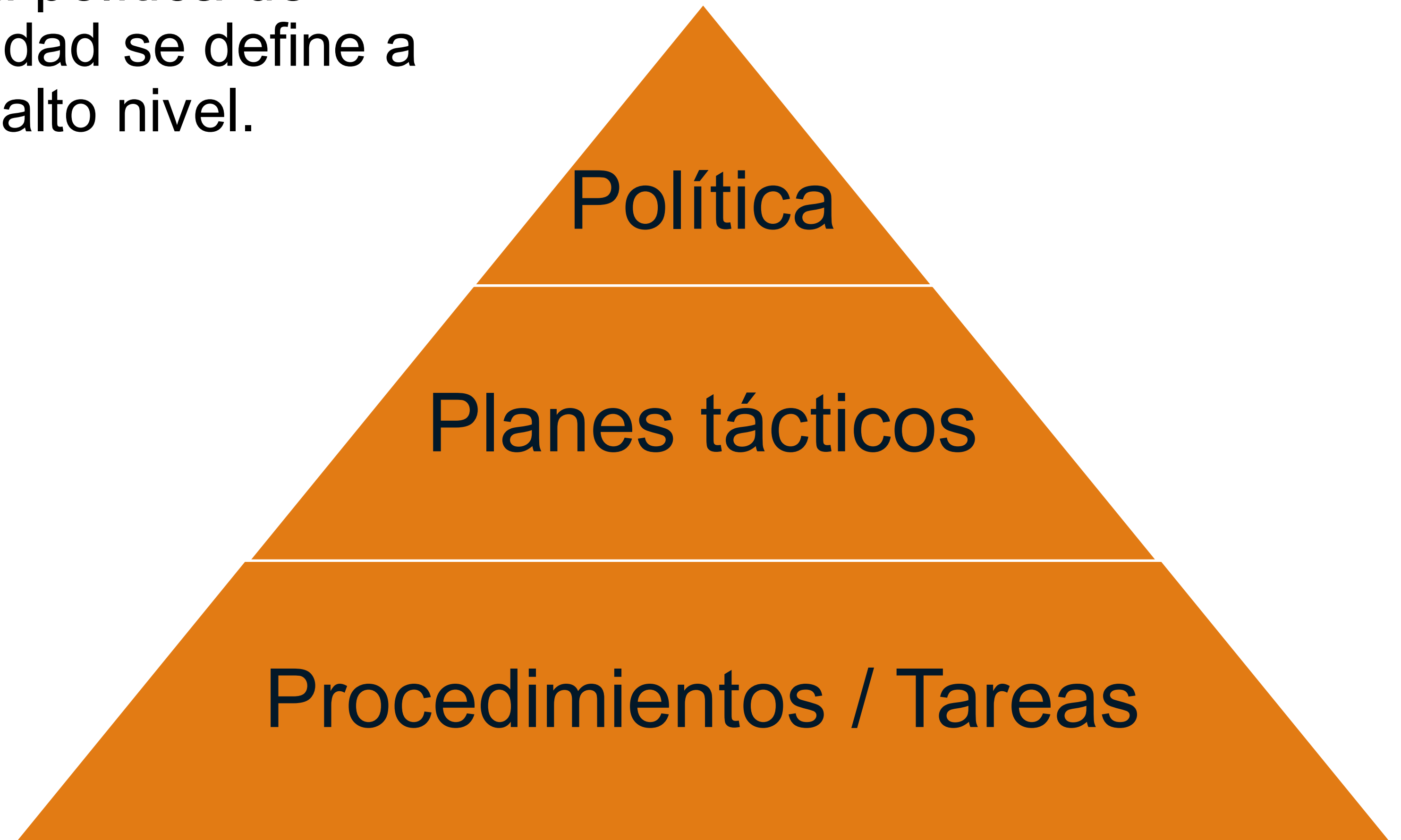
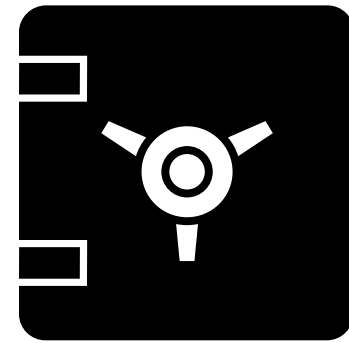
Sistema de Gestión de Seguridad de la Información



Política – Estructura organizativa –
Procedimientos - Procesos
Recursos necesarios

1 – Implementación de una Política de seguridad informática

La política de seguridad se define a alto nivel.



2 - Establecer el alcance del SGSI e identificar a los activos de información

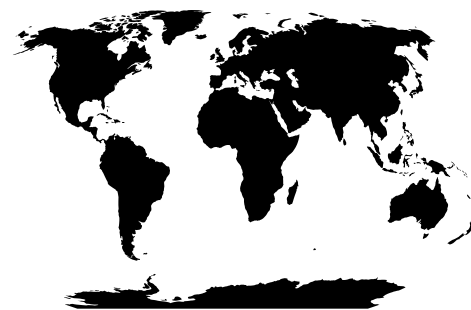
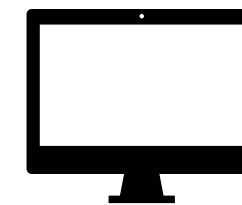
Procesos



Infraestructura de Software

Infraestructura de Hardware

Proveedores o servicios de terceros



Analizando:

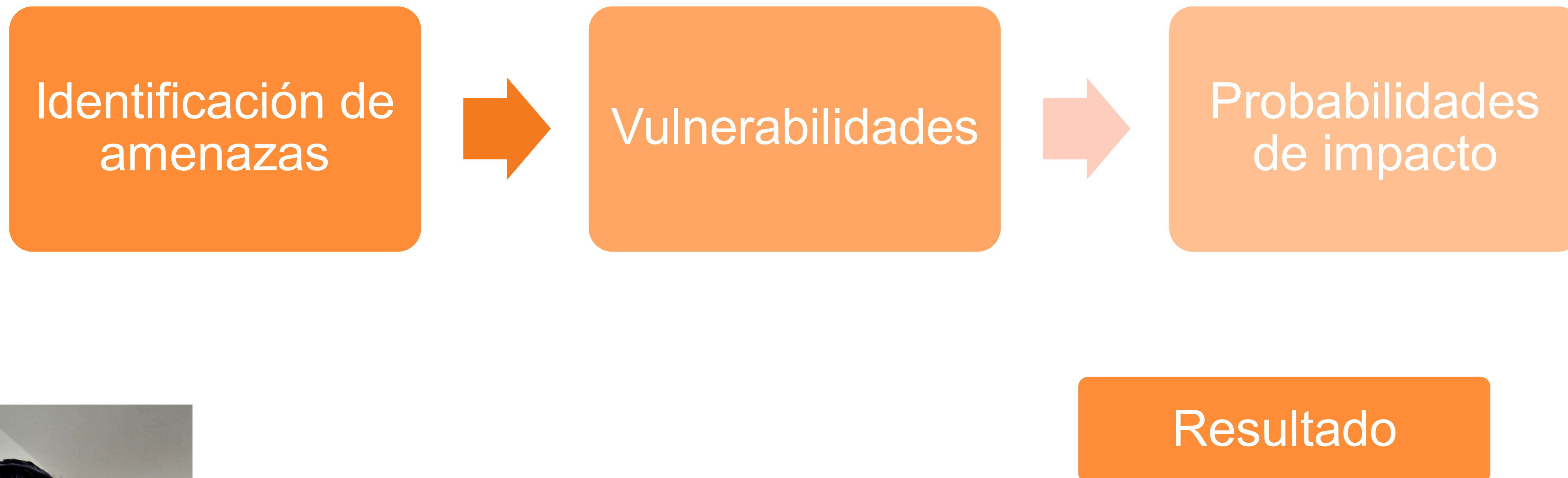
Clasificación

Responsables

Custodio



3 - Gestión de los riesgos



Evaluación de las vulnerabilidades, niveles de riesgos y la necesidad de aplicar medidas.

4 - Establecimiento de controles

En base a la
gestión de los
riesgos



Seleccionar los controles a implementar.

Implantar los procedimientos de monitoreo y controles.

**Ejemplos sobre amenazas
identificables en el SIC:**

Siniestros

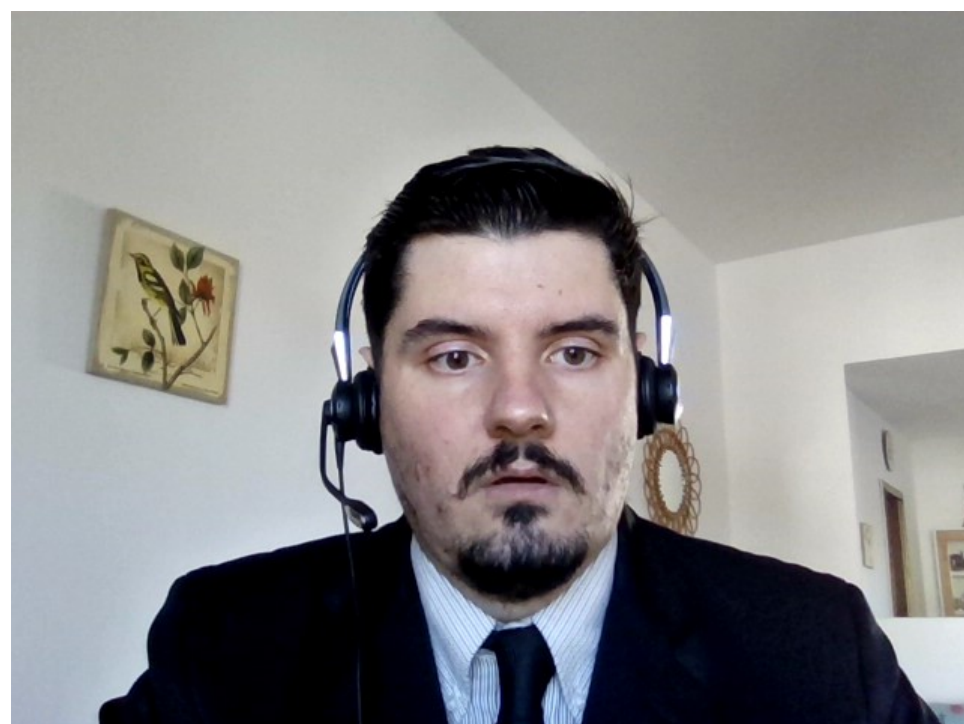
Catástrofes
naturales

Fuga de
información

Malware

Phishing

Ataques de
inyección SQL/
Denegación de
servicio (DoS)



5 – Documentación, auditoría y mejora del SGSI

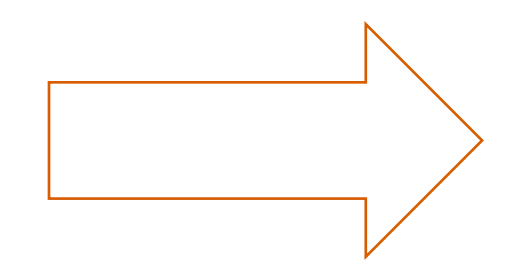
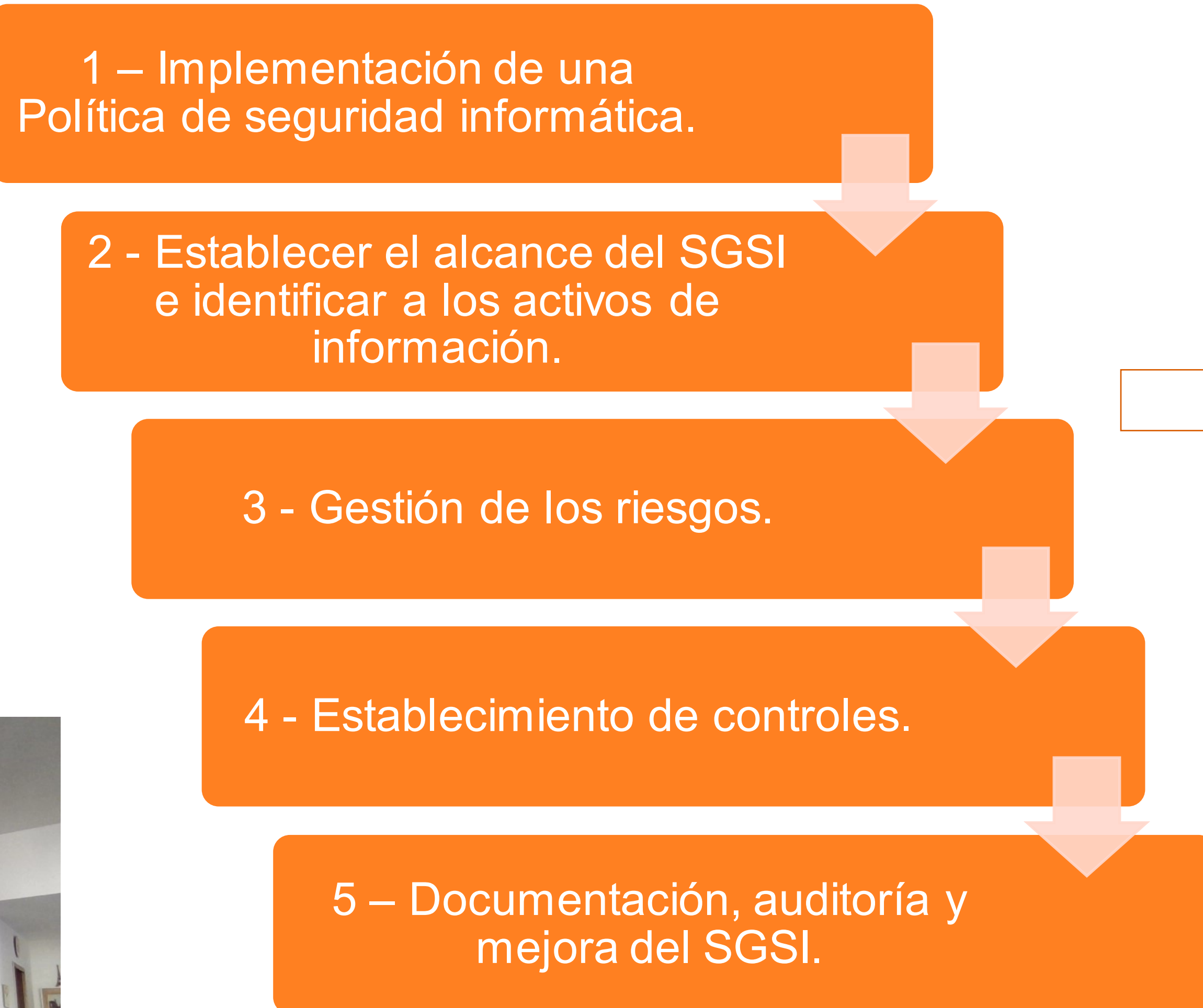
A. Documentar los planes, normas y procedimientos.

B. Revisión y auditoría interna del proyecto.

C. Implementar recomendaciones.



¿Qué estándares, normativas y buenas prácticas se encuentran disponibles?

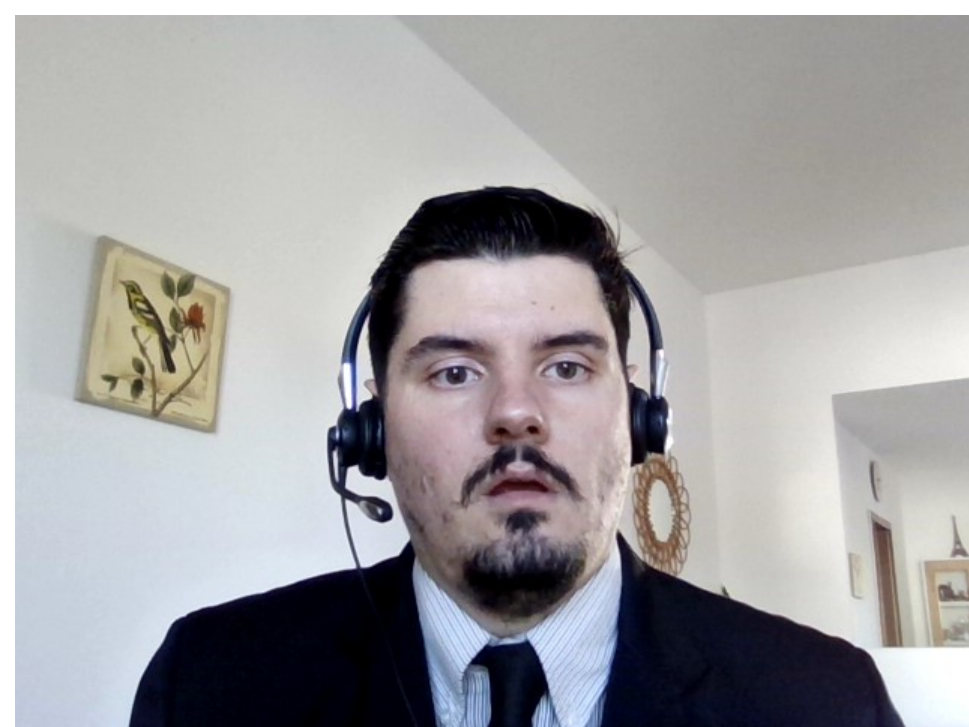
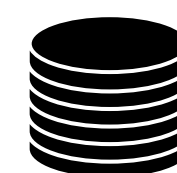
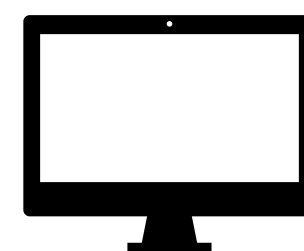


Legislación de Datos Personales.



Reflexiones finales

**Sistema de
información
contable**



consejo

THANK YOU

GRACIAS
ARIGATO
SHUKURIA
JUSPAXAR
DANKSCHEEN
TASHAKKUR ATU
SUKSAMA
EKHMET
MEHRBANI
PALDIES
BOLZIN
MERCICI
BIYAN
SHUKRIA
TINGKI
YAQHANYELAY
TASHAKKUR ATU
SUKSAMA
EKHMET
MEHRBANI
PALDIES
BOLZIN
MERCICI
GRACIAS
ARIGATO
SHUKURIA
JUSPAXAR
DANKSCHEEN
TASHAKKUR ATU
SUKSAMA
EKHMET
MEHRBANI
PALDIES
BOLZIN
MERCICI
BIYAN
SHUKRIA
TINGKI
YAQHANYELAY
TASHAKKUR ATU
SUKSAMA
EKHMET
MEHRBANI
PALDIES
BOLZIN
MERCICI

