Ciberseguridad basada en ISO 27032:2012

Sisteseg Consulting Services

Bogotá

Colombia

Agenda

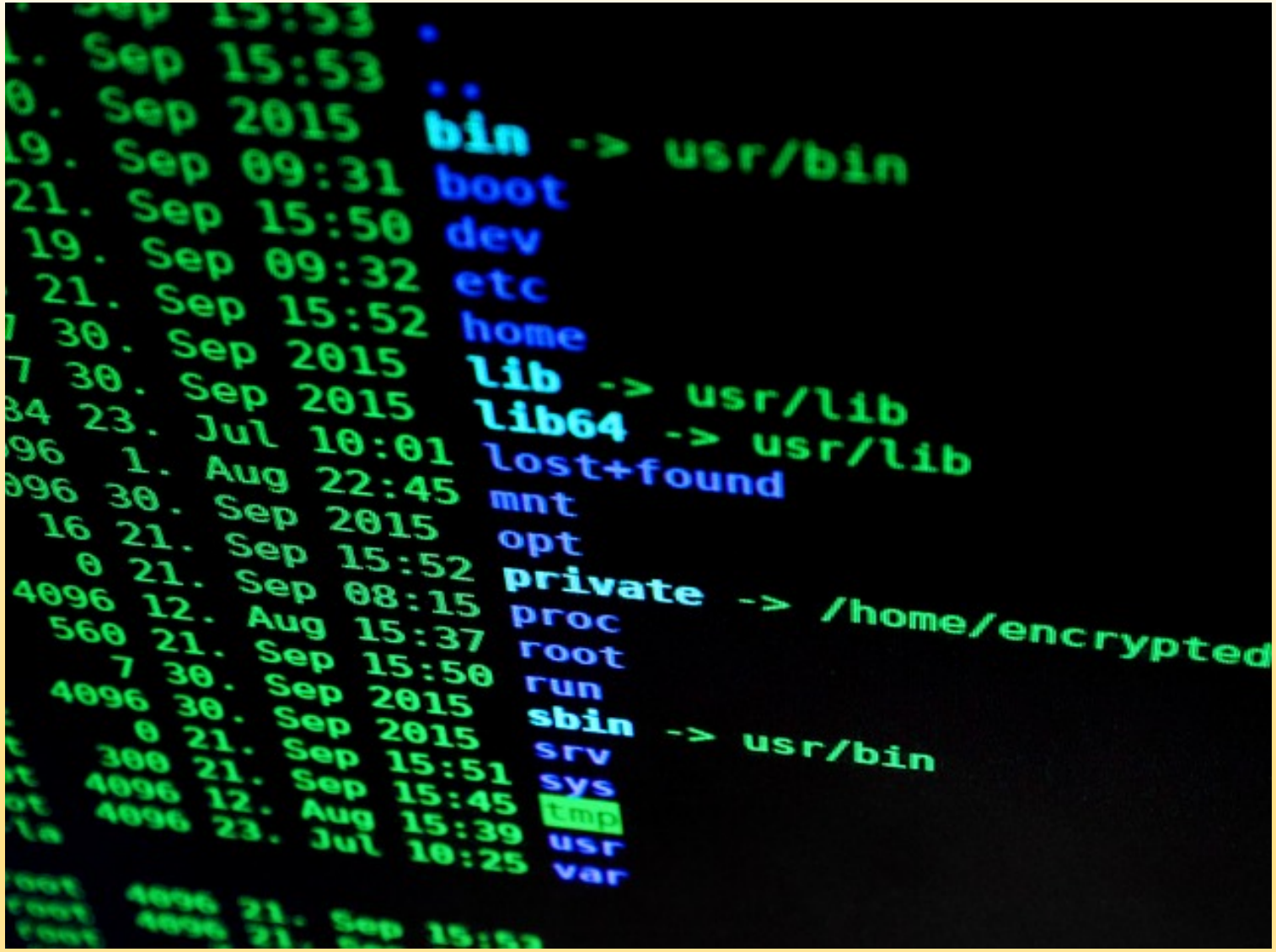
Por: Rodrigo Ferrer CISSP, CISA, QSA, ISO 27001 e ISO 22301, AMBCI, ABCP.

1. Introducción general
2. Pilares fundamentales
3. Modelo ISO 27032
4. El ciberespacio
5. Controles de ciberseguridad ISO 27032
6. Conclusiones

Introducción

Ciberespacio

- El ciberespacio es un ambiente en donde interactúan los seres humanos, el software y los servicios que en Internet se ofrecen (ISO 27032).



Amenazas

- Ataques de ingeniería social
- Malware
- Spyware
- Troyanos
- APT

Relaciones de ISO 27032

- La seguridad de la información
- La seguridad en las redes
- Seguridad en Internet
- Protección de la infraestructura crítica
- ISO 27001:2013
- ISO 27005:2018
- ISO 27002:2013
- ISO 31000:2018

Contexto de ISO 27032

- La seguridad en Internet y en el ciberespacio nos convoca a todos, la presencia actual de las organizaciones en este espacio crea unos beneficios para también unos riesgos.

Riesgos

- Exposición de información en las redes sociales.

Riesgos

El ciberespacio

Entorno virtual
ISO 27032

Personas

Organizaciones

Internet

Hardware y software

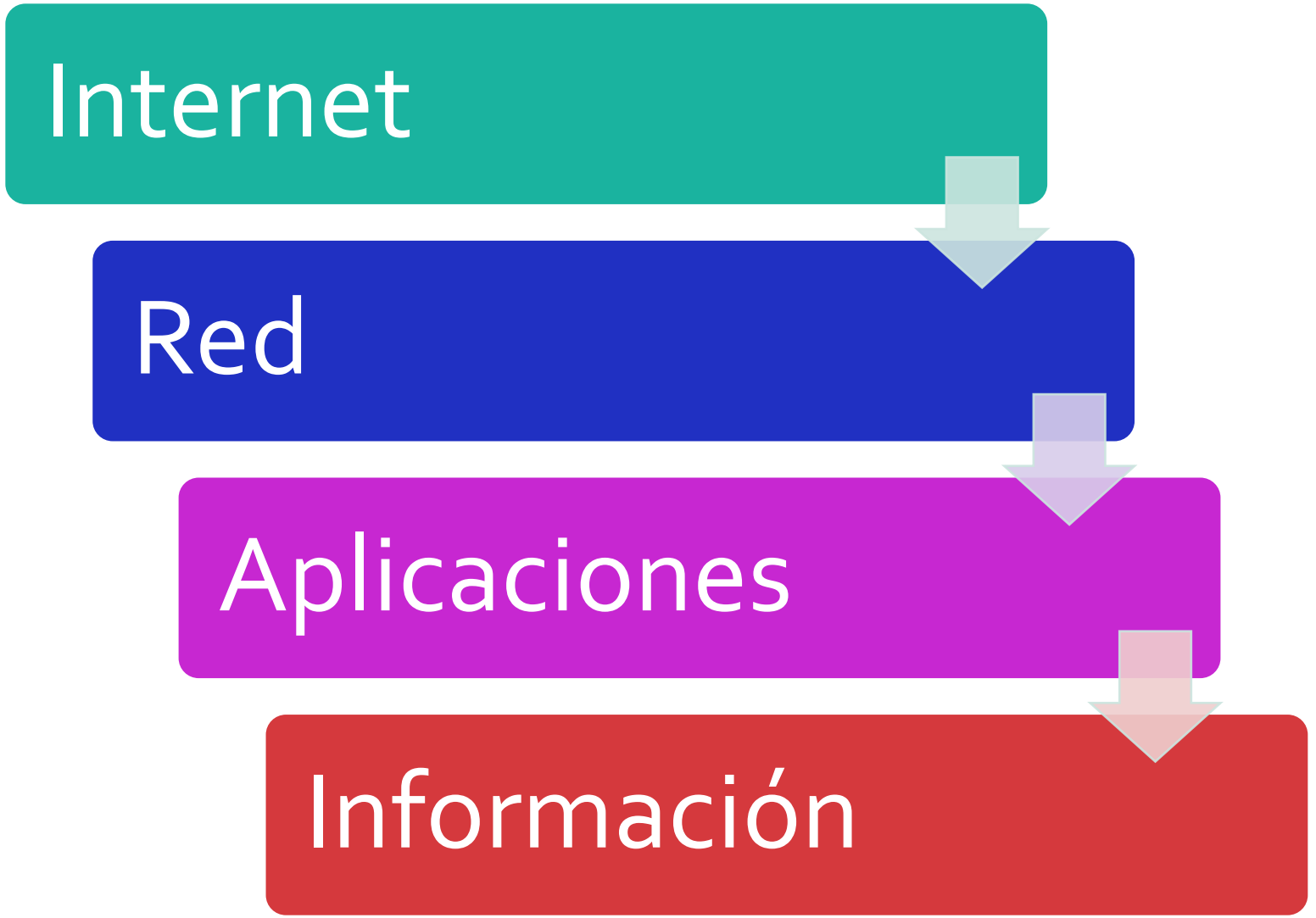
Redes

Pilares fundamentales

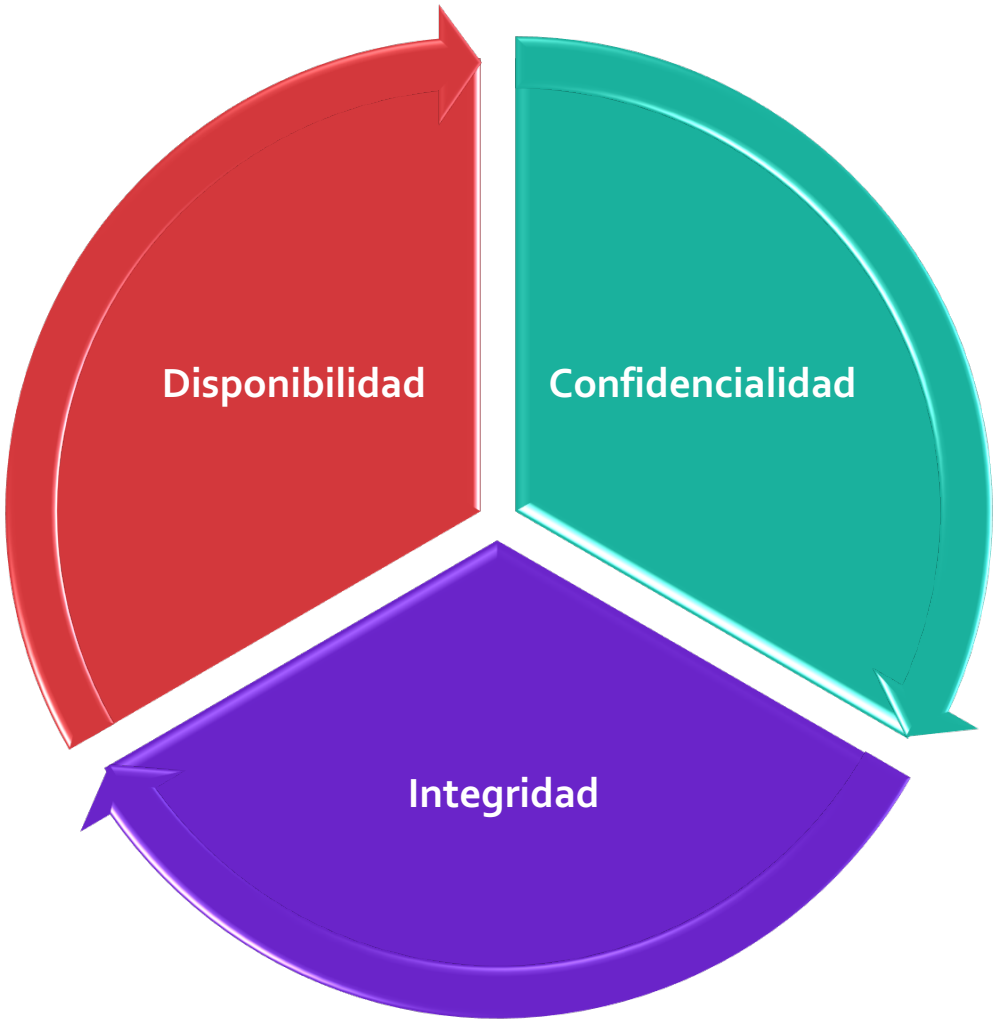
Ciberseguridad

ISO 27032

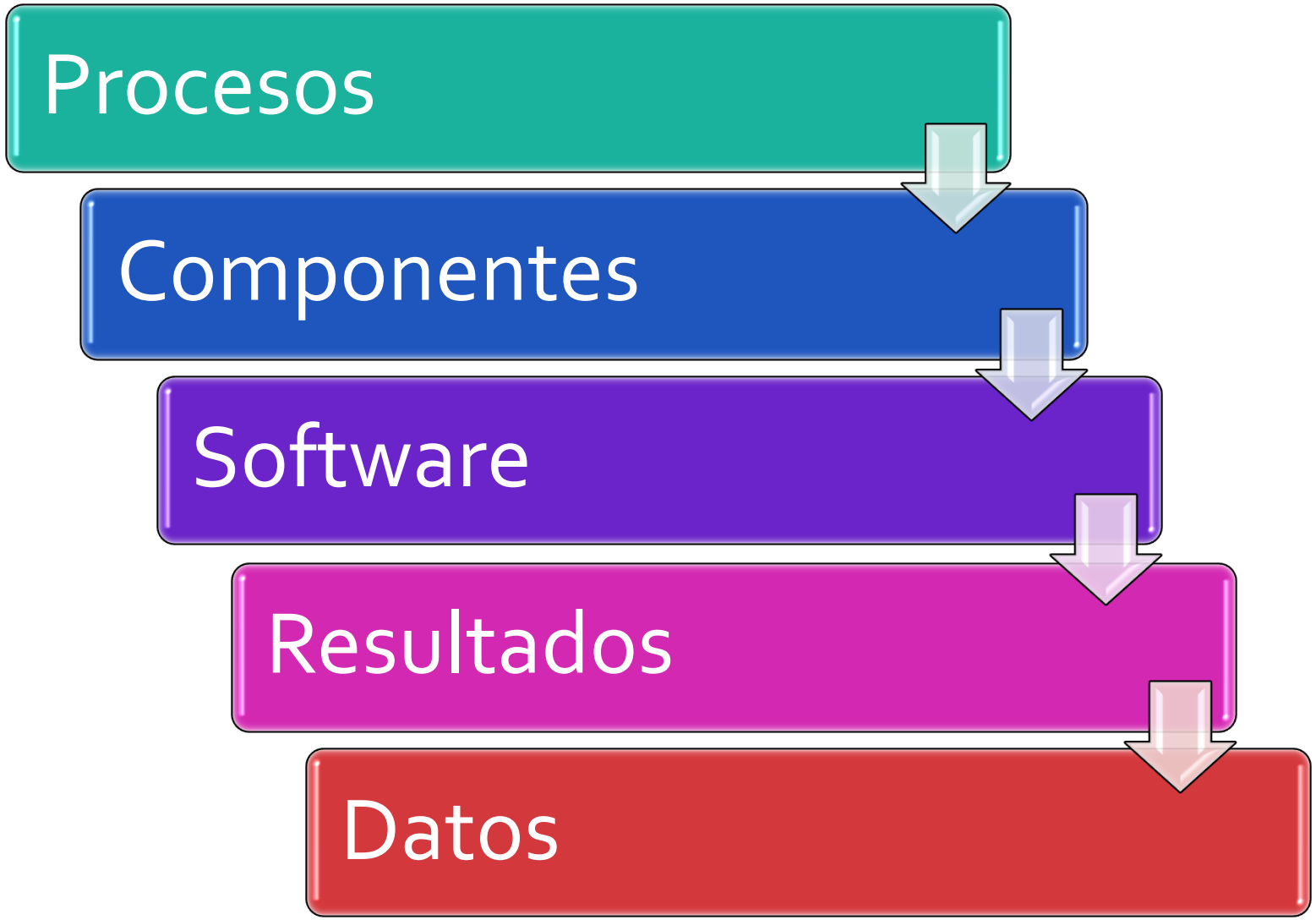
Seguridad en:



Seguridad de la información

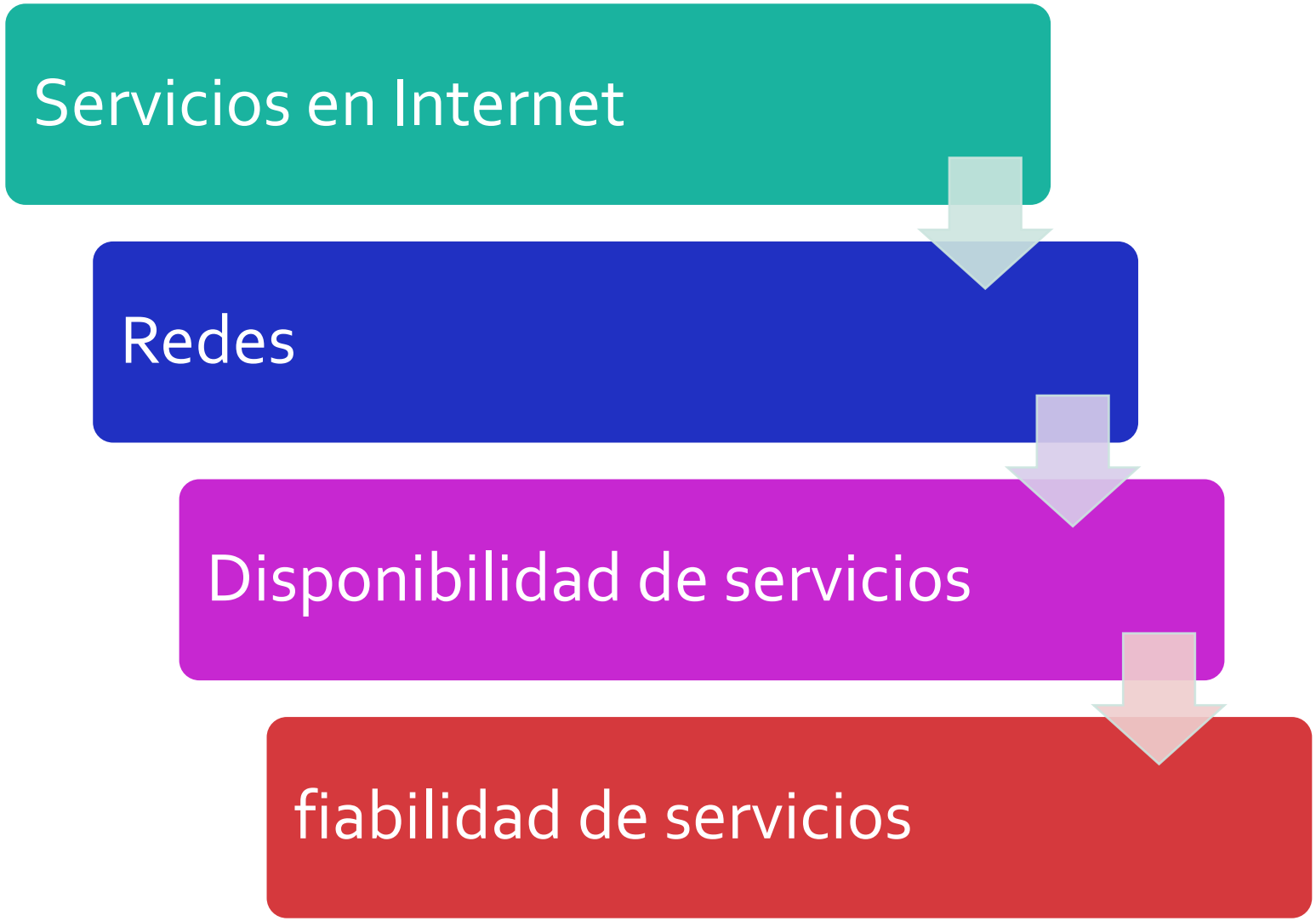


Seguridad en Aplicaciones



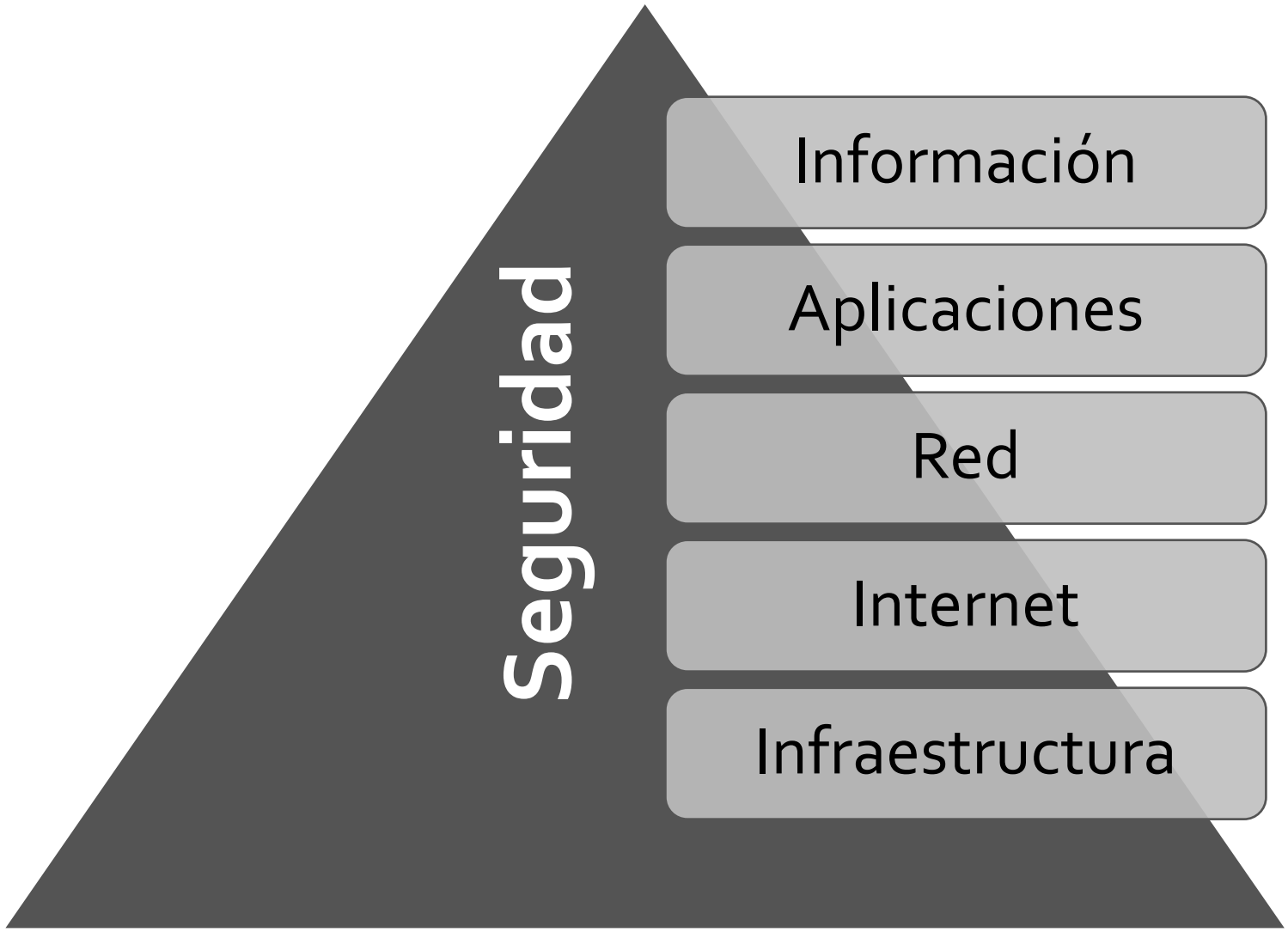
Seguridad en la red

Seguridad en Internet



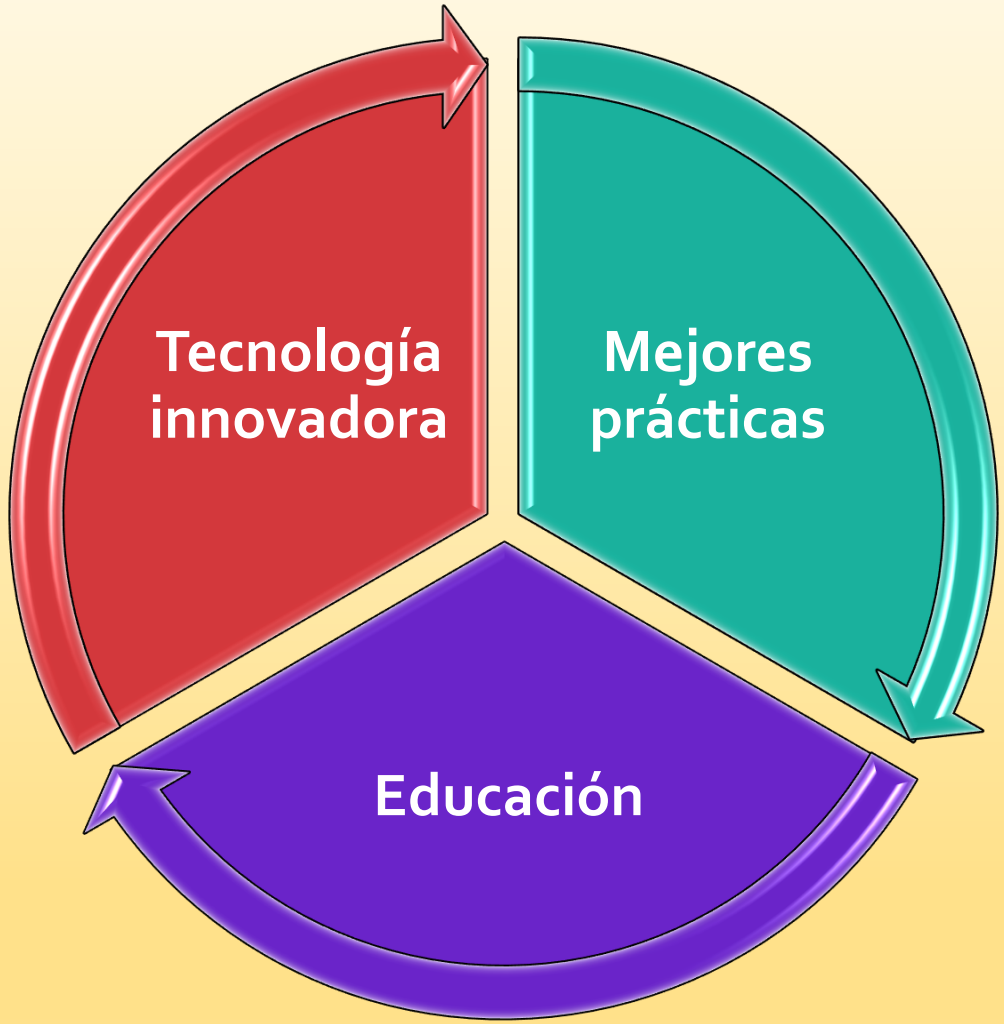
Modelo ISO 27032

Relación de la ciberseguridad con otros ámbitos



Modelo general ISO 27032

Controlar los riesgos



El ciberespacio

Partes interesadas

- El ciberespacio no pertenece a nadie, todos podemos participar.
- Las partes interesadas se dividen en:
  - Los consumidores, como personas y organizaciones
  - Los proveedores de servicios

Activos en el ciberespacio

- La información
- El software
- Hardware
- Los servicios
- Las personas
- Activos intangibles

Metas de la ciberseguridad ISO 27032

Controles de ciberseguridad ISO 27032

Controles de aplicación

- Presentar políticas empresariales
- Manejo de sesiones web
- Evitar ataques de scripting
- Revisar código
- Servicios autenticados y seguros

Protección de servidores

- Usar estándares de configuración
- Actualizaciones periódicas
- Generar registros (logs)
- Uso de antivirus y antispyware
- Análisis de vulnerabilidades
- Revisiones periódicas de malware

Controles de usuario final

- Instalar actualizaciones (OS)
- Aplicaciones actualizadas
- Uso de antivirus y antispyware
- Bloqueadores de scripts
- Bloquear ventanas emergentes
- Filtros de phishing
- Uso de firewall personal

Controles para la ingeniería social

- Políticas de seguridad
- Clasificación de la información
- Sensibilizaciones
- Controles técnicos aplicables

Conclusiones

Finalmente…

- El ciberespacio en un ambiente muy complejo.
- Diferentes niveles de seguridad en el ciberespacio.
- Hay un proliferación de malware.
- Se debe mejorar la gestión de incidentes
- Seguridad en los proveedores de servicio
- Se debe proteger:
  - La información
  - Las redes
  - La Internet
  - Y la infraestructura crítica de información (CIIP)

Ciberseguridad basada en ISO 27032:2012
FIN