Compartiendo Información para la Ciberdefensa

- ¿Qué está pasando?
  - Caracterización del Cibercrimen
  - Datos concretos HOY
  - Expectativas
- Estrategias para la defensa
  - Métodos probados
  - Fortaleza de Buenas Prácticas
- Compartir la información como punto angular de la defensa
  - Mecanismos
  - Experiencias exitosas
  - Retos
- Reflexión Final

¿Qué está pasando?


Bitdefender
REAL-TIME MAP
Guerra cibernética
LEGEND
LIVE ATTACKS
LOCATIONS

Paul DeCoster Principal, Head of Practice – Risk, Legal, Com
Security (North America), Marlin Hawk

Ciberdelincuencia

- “Los ciberdelincuentes buscan constantemente **nuevos vectores de ataque** y disfrutan de esta ola de cambios. Sin embargo, para las personas encargadas de proteger a las empresas y los consumidores de estos ataques, **es un campo de batalla en constante cambio**.”

  “**No siguen las reglas**, y esto significa que pueden actuar de una manera mucho más ágil de lo que puede ser la contraparte.”.

Caracterización

Cibercrimen

Ciberhabilitado

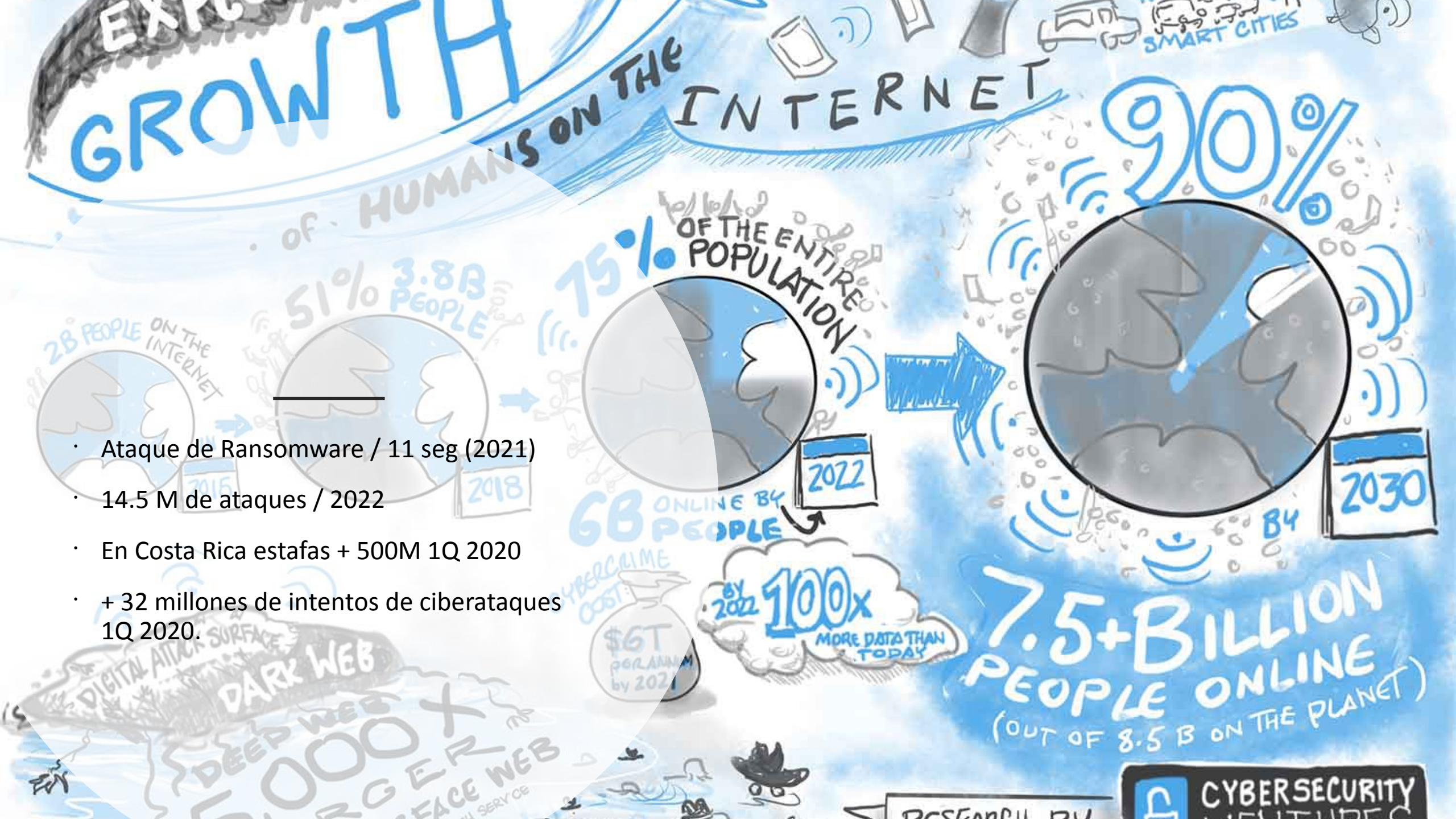
Crimen tradicional que se potencia mediante el uso de computadores o redes de computadoras.

Ciberdependiente

Crimen que depende del uso de computadores o redes de computadoras.

Estado del Cibercrimen

- ▲ 15% cada año
- **$6 trillion** USD 2021,
- Pone en *riesgo innovación e inversion TxD*
- Efecto Cibercrimen **>** Efecto desastres naturales en un año.
- **+** Rentable que el tráfico internacional de Drogas.
- ▲ APT Advanced Persistent Threat
- Source: Cybersecurity Ventures



- Ataque de Ransomware / 11 seg (2021)
- 14.5 M de ataques / 2022
- En Costa Rica estafas + 500M 1Q 2020
- + 32 millones de intentos de ciberataques 1Q 2020.

Estrategias para la Defensa

ESTRATEGIAS

- **Establecer un FW de Ciberseguridad formal**
- **Proveer conocimiento/conciencia, crear Cultura**
- **Monitoreo continuo de amenazas**
- **Evaluar y administrar las vulnerabilidades**
- **Administrar los riesgos de las cadenas de suministros**
- **Fortalecer la respuesta a incidentes**

Arquitecturas

- Modelo por capas
- Defensa en profundidad
- Zero Trust
- SASE (Secure Access Service Edge)

Buenas Prácticas

- ISO IEC 27001/ISO 27002
- NIST Cybersecurity Framework
- IASME Governance
- SOC 2
- CIS v7
- NIST 800-53
- COBIT
- COSO
- TC CYBER
- FedRAMP
- HIPAA
- GDPR

Compartir Información como punto angular de Defensa

Motivación

- **Toda** la comunidad es objeto de **ciberataques**
- La tasa y tipo de ciberataques sigue en **aumento**
- Los recursos para responder a los **desafíos** de la ciberseguridad son limitados
- La **cooperación** entre todas las partes interesadas es **esencial para la resiliencia digital**

mpartir información

Esquemas de cooperación

- CiSP (Cyber Security Information Sharing Partnership) "CiSP es una iniciativa conjunta de la industria y el gobierno creada para intercambiar información sobre amenazas cibernéticas en tiempo real, en un entorno seguro, confidencial y dinámico, aumentando la conciencia situacional y reduciendo el impacto en los negocios del Reino Unido". [36]

- US-CERT Especificaciones para el intercambio de información para ciberseguridad presenta "TAXII, STIX y CybOX [...] especificaciones técnicas impulsadas por la comunidad diseñadas para permitir el intercambio automatizado de información para la conciencia situacional de ciberseguridad, la defensa de la red en tiempo real y el sofisticado análisis de amenazas."

- ISAC (Information and Sharing Analysis Center) Tanto el Reino Unido (CPNI Information Exchanges) [37] como Holanda (NCSC ISAC) [38] utilizan el modelo del ISAC para facilitar el intercambio de información con partes públicas y privadas. El grupo de expertos de la Estrategia Nacional de Ciberseguridad de ENISA ha identificado el modelo ISAC como una buena práctica para el intercambio de información dentro de la UE [39, 40].

- **Mejores prácticas del GCCS Para la Conferencia Mundial sobre el Ciberespacio 2015 (GCCS2015), los Países Bajos presentaron un marco basado en las mejores prácticas holandesas en el intercambio de información sobre ciberseguridad [41].**

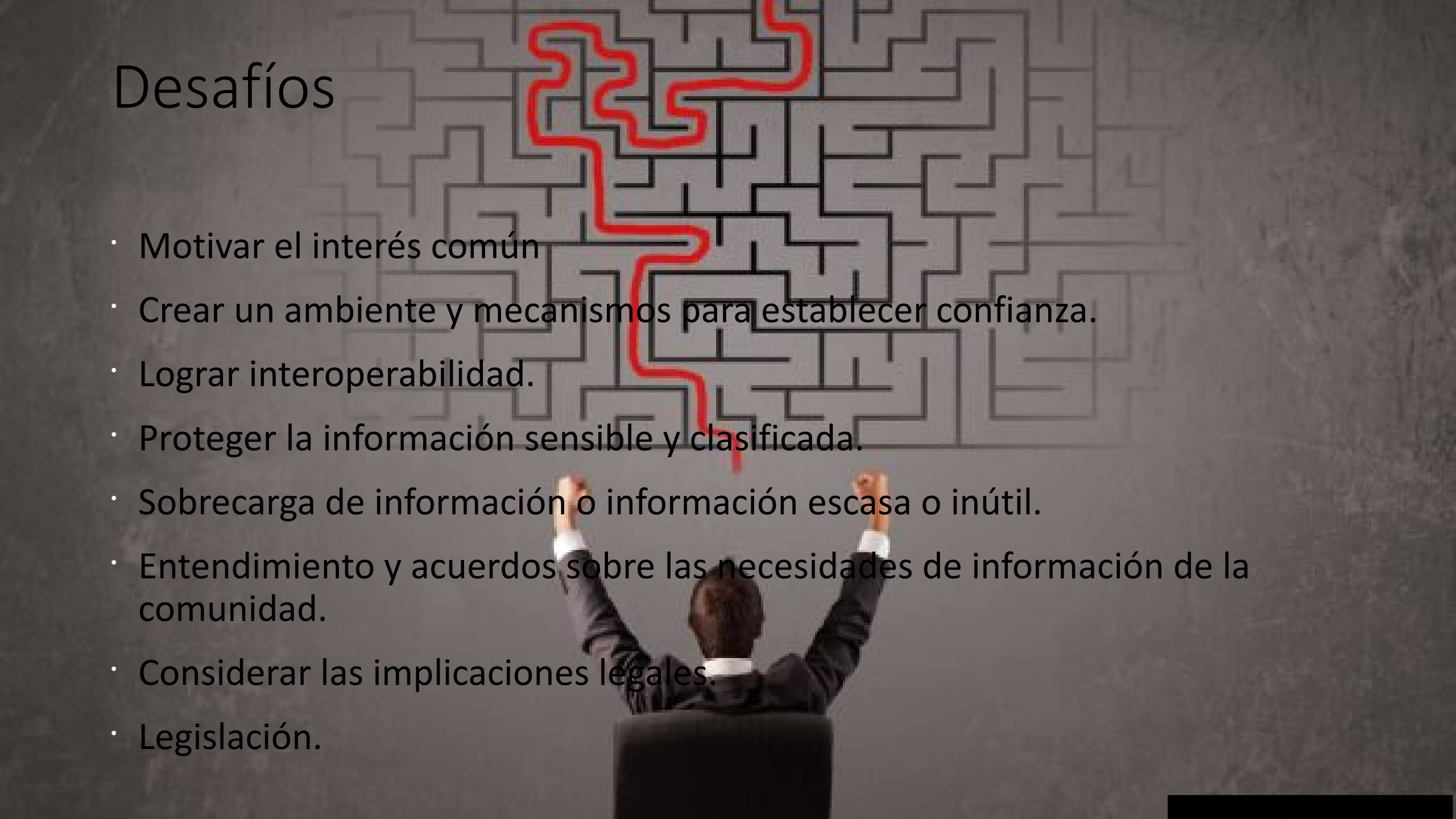
- ISAO (Information Sharing and Analysis Organization) El modelo ISAO [33, 34, 35] está en uso en los Estados Unidos para el intercambio independiente de información sobre ciberseguridad.

- ECHO European network of Cybersecurity centres and competence HUB for Innovation and Operations. 2019.

Experiencias Exitosas

Casos de Uso	Dimensiones				
	Tipo de colaboración	Nivel de los participantes	Sector	Arquetipo	# de afiliados
CPNI.UK y el IE (Information Exchanges)					
FS-ISAC					
Projecto Griffin					
NIS-P					

Desafíos



- Motivar el interés común
- Crear un ambiente y mecanismos para establecer confianza.
- Lograr interoperabilidad.
- Proteger la información sensible y clasificada.
- Sobrecarga de información o información escasa o inútil.
- Entendimiento y acuerdos sobre las necesidades de información de la comunidad.
- Considerar las implicaciones legales.
- Legislación.

Recomendaciones

CSIS (2015)

- Analizar si aplican o no acuerdos para compartir la información en función del perfil de riesgos.
- Compartir entre organizaciones privadas puede aliviar preocupaciones sobre la privacidad.
- Proteger la información personal.
- Construir sobre esfuerzos existentes y mecanismos para compartir información.
- Determinar procedimientos directos y rápidos para compartir con las entidades y sector privado información sobre amenazas.

---///Referencias///---

- https://scholarspace.manoa.hawaii.edu/bitstream/10125/59
- https://studenttheses.universiteitleiden.nl/access/item%3A2
- https://cams.mit.edu/wp-content/uploads/2017-06.pdf
- https://www.enisa.europa.eu/topics/national-cyber-security-
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP
- https://www.researchgate.net/profile/Eric_Luiijf/publication/