

*transformamos*  
*nuestra visión en realidad...*

# Sociedad Información

# Estrategia de ciberseguridad en la Seguridad Social



# CONTENIDO



1. **Antecedentes**
2. El valor de la ciberseguridad
3. Líneas estratégicas ciberseguridad
4. Conclusiones

# Antecedentes

- Organización a nivel nacional
- Experiencia de 4 años en ciberseguridad
- Servicios de dos tipos:
  - Expresos de ciberseguridad
  - Asociados al servicio de comunicaciones

# CONTENIDO



1. Antecedentes
- 2. El valor de la ciberseguridad**
3. Líneas estratégicas ciberseguridad
4. Conclusiones

# Encuadre en las líneas de trabajo de la GISS (Gerencia de Informática de la SS)

- La ciberseguridad es un servicio transversal.
- Es un complemento de la seguridad.
- Asociado a varias líneas de trabajo de la GISS
  - *L1. Dar visibilidad a la SS como administración eficiente y avanzada*
  - *L4. Mejora de los servicios digitales al ciudadano*
  - *L8. Refuerzo del rol y la capacitación de la GISS en materia de transformación digital*
  - *L12. Renovación tecnológica*

# CONTENIDO



1. Antecedentes
2. El valor de la ciberseguridad
- 3. Líneas estratégicas ciberseguridad**
4. Conclusiones

# 1. Integración de los servicios de ciberseguridad

→ Colaboración entre empresas en la GISS y también con el CCN





## 2. Integración de herramientas de apoyo

- Usar las herramientas proporcionadas por el CCN.
  - En especial ANA y LUCIA.





# 3. Innovación en ciberseguridad

➔ Conocer y aprovechar ideas para mejorar la eficiencia y eficacia de los servicios de ciberseguridad



# 4. Indicadores de ciberseguridad

- Medidas flexibles y ágiles.
- El esfuerzo y los resultados
- Ayudan a defender el trabajo de ciberseguridad.

## Alerta temprana de ciberamenazas

Boletín de seguridad (Vulnerabilidades)	24
Alerta temprana de vulnerabilidades (CVE)	0
Aviso de seguridad	1
Notificación de Alerta de Amenaza (TO)	1
Alerta de Amenaza-(IOC) (TI)	1
Informe de Amenaza (T2)	0

## Feed de Ciberamenazas SIA

Feed de Ciberamenazas	0
-----------------------	---

## Identificación de actividades fraudulentas/ilegítimas

APKs fraudulentas/ilegítimas	5
Carding	0
Domínios defectados	8
Total dominios monitorizados	88
Fuga/Robo de Datos	17
Identities/Credenciales	0
Phishing	0
Phishing	0
Prospección manual en Fuentes abiertas	0

## Vigilancia en Fuentes abiertas

Hacktivismo: Campañas (DDoS, etc.)	0
Hacktivismo: Movimientos sociales	0
Reputación de Marca	0
Reputación de VIPs	0
Noticias relevantes	0

## Informes en suscripción

Informe de actividad del Servicio de Detección	1
Ciberboletín de noticias	1

## Concienciación

Informes (Fórum de concienciación)	0
------------------------------------	---



VIGILANCIA DIGITAL

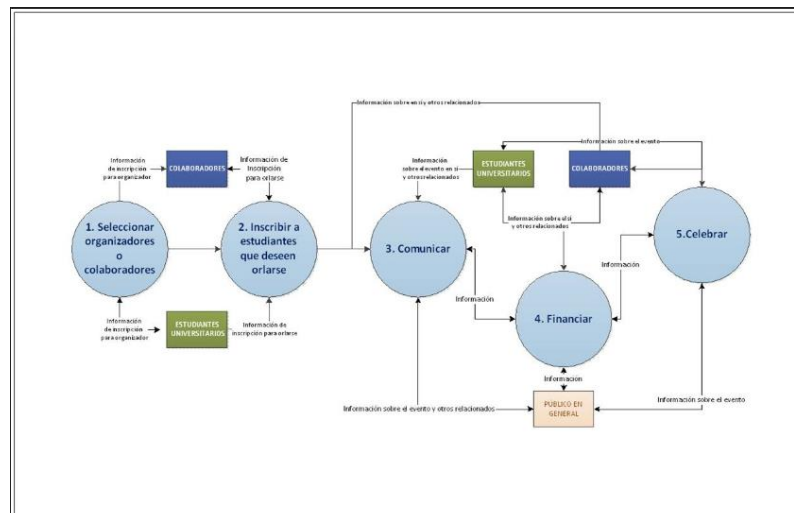
## 5. Detección eficiente de incidentes y vulnerabilidades

- Afinar las reglas de detección del SIEM
- Integrar las reglas SIEM con vigilancia digital y análisis de accesos a las bases de datos



# 6. Mejora de los procedimientos y proyectos de ciberseguridad

- ➔ Mantenerlos actualizados y documentados.
- ➔ Aumentar su beneficio o eficacia.
- ➔ Planificar los proyectos de ciberseguridad.



# CONTENIDO



1. Antecedentes
2. El valor de la ciberseguridad
3. Líneas estratégicas ciberseguridad
- 4. Conclusiones**

# La clave: La defensa en profundidad y resiliencia





*transformamos*  
*nuestra visión en realidad...*

**Gracias**

