

El pasado, el presente y la incertidumbre en la gestión del Estado en la Soberanía Digital

Expositor: Mgs. Eddy G. Chumania ñ.

PROJECT MANAGER & GRC SENIOR ADVISOR

- Ingeniero en Sistemas por la ESPE;
- Becado Instituto Ciberseguridad – León España (INCIBE) Programa de Excelencia en Ciberseguridad – CICTE –OEA
- MSC. Administración y Marketing (Universidad Indoamerica)
- Master Universitario en Inteligencia Artificial (UNIR).

Certificacione

- Certified Information Security Manager. CISM
- Lead Auditor ISO/IEC 27001:2022
- CEH Certified Ethical Hacker – EC COUNCIL
- Certificate of Cloud Security Knowledge (CCSK)
- Certificate of Cloud Auditing Knowledge (CCAK)
- Delegado de Protección de Datos Personales - AECI

Áreas de Trabajo

Dirección General de Inteligencia del Comando Conjunto de las FF.AA.

Centro de Respuestas a Incidentes de Seguridad Informática de las FF.AA. (CSIRT-FF.AA.)

Comando de Ciberdefensa de la FF.AA. (COCIBER)

Economía Popular y Solidaria, Retail, Seguros, Petróleo y Gas, Educación, Call Center, Telecomunicaciones, Desarrollo de SW, Salud, Sector Público (Gobierno)

Experiencia

Más de 30 años de experiencia específica en áreas de Seguridad de la Información, desarrollando diferentes actividades en sub ramas como:

- Auditor de TICs
- Oficial de Seguridad de la Información
- Perito Criminalístico Informático Forense
- Ingeniero Preventa
- Consultor Senior en Seguridad de la Información
- Docente Universitario de pregrado y posgrado.
- Project Manager Comando de Ciberdefensa
- Project Manager CSIRT-FF.AA.

Involucrado en proyectos en países como:

Aportes Ecuador, Colombia, Chile, Brasil, México, Puerto Rico, USA, España, Generación y revisión de proyectos normativos regulatorios:

- Esquema Gubernamental de Seguridad de la Información EGSI V2
- Ley Orgánica de Protección de Datos Personales
 - Reglamento de la LOPDP
- Actualización de la Norma de Riesgo Operativo de la Super de Bancos - ámbito de Seguridad de la Información
- Actualización de la norma de Seguridad de La Información
- Ley de Seguridad Digital



Legaltech and cybersecurity

TEMARIO

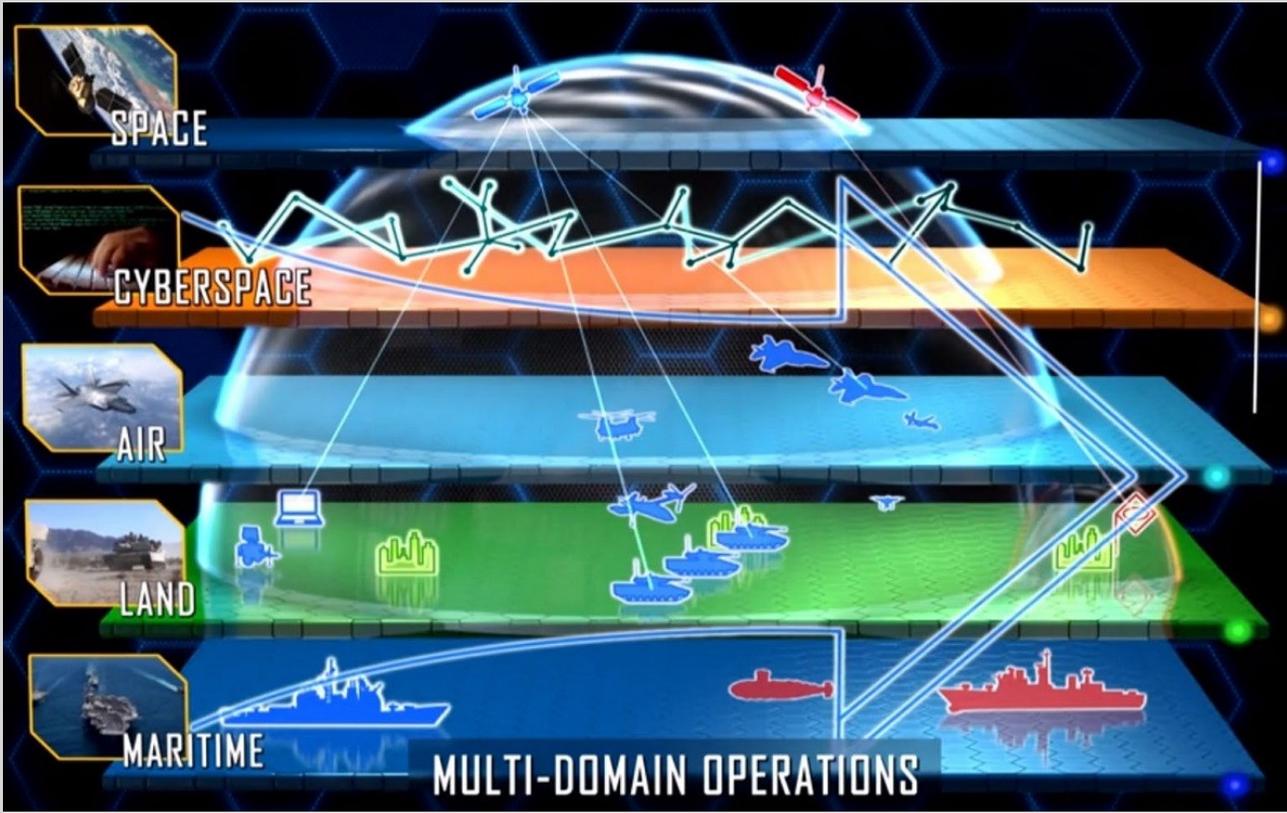
1. Normativa legal
2. Seguridad de la información
3. Ciberseguridad
4. Ciberdefensa
5. Ciberamenazas (aspectos negativos)
6. Infraestructura críticas
7. Disciplinas asociadas
8. Operaciones de Ciberdefensa
9. Tácticas, técnicas y procedimientos
10. Fuerza ciberespacial



NORMATIVA LEGAL



CIBERESPACIO



- **Ciberespacio**

- Es un entorno complejo basado en tecnologías digitales que proveen un lugar global para la interacción digital entre las personal incluyendo interacciones formales e informales con entidades públicas y privadas.

El ciberespacio se considera público pero con variedad de elementos que son parte de entidades privadas

La interacción del ciberespacio incluye:

ISO/IEC 27100:2020 - Information technology - Cybersecurity - Overview and concepts

Compartir

Intercambiar

Procesar

Recibir



Ciberespacio como dominio de operaciones.

- The NATO Warsaw Summit, held on 8 – 9 July 2016
- Cyber defence is part of NATO's core task of collective defence the Allies now 'recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea'.
 - <https://ccdcoe.org/incyber-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/>
- **Atractivo de uso del ciberespacio**
 - Abaratamiento
 - Circulación libre y anonimato (perfiles falsos)
 - Sin límites (Deep, Darknet)
 - Multitud de objetivos (gobierno, individuos, entidades públicas, entidades privadas)
 - Actividades remotas



MOTIVOS, MEDIOS Y ACTIVIDADES

Motivos	Medios de actuación	Actividades
Creencias	Sitios web	Difusión de propaganda
Ideología	Redes sociales y aplicaciones de mensajería instantánea	Captación, reclutamiento o radicalización
Gobernabilidad	Foros y chats	Preparación de atentados (esteganografía)
Captación	Videojuegos	Financiación
Reclutamiento	Revistas en línea	Formación
Radicalización	Género musical (Nasheed musulmán, narraciones bélicas)	Ciberataques
Afectación en el mundo real		Delitos
Posicionamiento del mensaje		



IDENTIFICACIÓN DE AMENAZAS



Proveedores y cadena de suministro TIC

- Debilidad de conocimiento y habilidades
- Sistemas o servicios vulnerables



Personas

- Intenciones maliciosas
- Utilización de software y otras herramientas
- Falta de conocimiento y habilidades
- Errores



Infraestructuras

- Dependencia de sistemas de energía.
- Dependencia de redes de servicio



Configuración y entornos

- Sistemas o servicios públicamente accesibles
- Dispositivos ubicados sin la debida protección física



EL PASADO

Previo al año 2017





Secretaría Nacional de la
Administración Pública

Secretaría nacional de la
Administración pública

El 19-Ago-011, crea la Comisión para la
Seguridad Informática y de las Tecnologías de la
Información



Secretaría Nacional de la
Administración Pública

Ministerio de
Telecomunicaciones y de la
Sociedad de la Información

3

EGSI V.1
19-sep-2013

2

Secretaría Nacional de
Inteligencia



alphalaw

Legaltech and cybersecurity

Eliminación de la Secretaría Nacional de Administración

Pública

Decreto
Ejecutivo N° 5 -
24May2017

Decreto
Ejecutivo N° 5 -
24May2017

Decreto
Ejecutivo N° 526
- 21Sep2018

A.M 025-2019
10Ene2020

A.M 06-2021
17May2021

1 Se **elimina** la Secretaría Nacional de Administración Pública.

2 **MINTEL**, 1. Gestionar la política, y directrices emitidas para la gestión de la implementación del **gobierno electrónico**. 2. Desarrollar y coordinar planes, programas o proyectos sobre **gobierno electrónico** que sean necesarios para su implementación.

3 **Elimina** la Secretaría Nacional de Inteligencia, y se crea el Centro de inteligencia Estratégica.

4 **MINTEL**, expide el Esquema Gubernamental de Seguridad de la Información **EGSI v2**, el cual es de implementación obligatoria en las instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

5 **MINTEL**, emite la Política Nacional de Ciberseguridad; Gabinete Sectorial de Seguridad tuvo lugar en la ciudad de El Coca el 1 de abril de 2021. En ella se aprobó la Política Nacional de Ciberseguridad y se designó al Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) como el encargado de publicarla mediante Acuerdo Ministerial.



Legaltech and cybersecurity

LEY ORGÁNICA DE TELECOMUNICACIONES

Art. 140.- Rectoría del sector

El Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información es el órgano rector de las telecomunicaciones y de la sociedad de la información, informática, tecnologías de la información y las comunicaciones y de la **seguridad de la información**. A dicho órgano le corresponde el establecimiento de políticas, directrices y planes aplicables en tales áreas para el desarrollo de la sociedad de la información, de conformidad con lo dispuesto en la presente Ley, su Reglamento General y los planes de desarrollo que se establezcan a nivel nacional.

Los planes y políticas que dicte dicho Ministerio deberán enmarcarse dentro de los objetivos del Plan Nacional de Desarrollo y serán de cumplimiento obligatorio tanto para el sector público como privado.



LEY ORGÁNICA DE TELECOMUNICACIONES

Telecomunicaciones

Sistema de transmisión y recepción a distancia de señales de diversa naturaleza por medios electromagnéticos.



LEY ORGÁNICA DE TELECOMUNICACIONES

Sociedad de la Información

La sociedad de la información es aquella en la cual las tecnologías que facilitan la creación, distribución y manipulación de la información juegan un papel importante en las actividades sociales, culturales y económicas debe estar centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida.



MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

Misión:

Ser el órgano rector del desarrollo de las tecnologías de la información y comunicación en el Ecuador, que incluyen las telecomunicaciones, el espectro radioeléctrico, gobierno electrónico, simplificación de trámites y sociedad de la información, que emite normativa, políticas, planes y realiza el seguimiento y evaluación de su implementación, que regula y controla el sector postal, coordinando acciones con los actores de los sectores estratégicos para garantizar el acceso igualitario a los servicios y promover su uso efectivo, eficiente y eficaz, que asegure el avance hacia la sociedad de la información para el desarrollo de la población

Visión:

Constituirse en la entidad, referente de la gestión pública, que lidere y gobierne todos los procesos necesarios para que los ciudadanos accedan y generen información y conocimiento, mediante el uso efectivo de las Tecnologías de la Información y Comunicación; además de fortalecer el gobierno electrónico, la simplificación de trámites, el sector postal y sociedad de la información, en beneficio de los ciudadanos y del desarrollo socio económico del país.

<https://www.telecomunicaciones.gob.ec/valores-mision-vision/>



Legaltech and cybersecurity

PRESENTE

2017 - 2022



- Plan Nacional de Seguridad Integral 2019-2030 *
- Plan Específico de Defensa 2019-2030 *
- Plan Específico de Seguridad Pública y Ciudadana 2019-2030

- Política Específica de Defensa 2019-2023
- Política Nacional de Ciberseguridad, del 23 de junio de 2021 mediante Acuerdo Ministerial No. 006-2021, emitido en la Edición Especial del Registro Oficial 479.

- Estrategia Nacional de Ciberseguridad del Ecuador 2023-2025
- Estrategia de Ciberdefensa 2021

- Plan Estratégico Institucional PEI de la Defensa 2021-2025, del de junio de 2023 mediante Cuarto Suplemento del Registro Oficial 331, 14-VI-2023

- Ley Orgánica para la Transformación Digital y Audiovisual, del 7 de febrero de 2023, publicada en el Registro Oficial - Tercer Suplemento N° 245
 - Reglamento a la Ley Orgánica para la Transformación Digital y Audiovisual del 11 de julio de 2023, publicada en el Registro Oficial - Segundo Suplemento N° 350



- Ley Orgánica de Telecomunicaciones. (varias actualizaciones)
 - Reglamento a la Ley Orgánica de Telecomunicaciones.
- Esquema Gubernamental de Seguridad de la Información V2, 10 de enero del 2020 expedido en el Registro Oficial mediante Acuerdo Ministerial 025-2019 MINTEL.
- *Proyecto de Ley de Seguridad Digital y Verdad de los Hechos*

Decreto Ejecutivo 262 R.O. Sup 592 de 07-dic.-2021
Art.8.- Gabinete Sectorial de Seguridad

El Ministerio del Interior (preside)

El Ministerio de Defensa Nacional

Centro de Inteligencia Estratégica

El Servicio Nacional de Gestión de Riesgos y Emergencias

Servicio Nacional de Atención Integral a Personas Privadas de la Libertad y a Adolescentes

Infraestructores



Ley de Seguridad Pública y del Estado

Art. 6.- Órganos Del Consejo de Seguridad Pública y del Estado (COSEPE)

- Presidente o Presidenta Constitucional de la República (dirige)
- Vicepresidente o Vicepresidenta Constitucional de la República
- Presidente o Presidenta de la Asamblea Nacional
- Presidente o Presidenta de la Corte Nacional de Justicia
- Ministro o Ministra de Coordinación de Seguridad
- Ministro o Ministra de Defensa Nacional
- Ministro o Ministra de Gobierno, Policía y Cultos
- Ministro o Ministra de Relaciones Exteriores
- Jefe del Comando Conjunto de las Fuerzas Armadas
- Comandante General de la Policía

Órgano permanente de coordinación, apoyo técnico y asesoría

Art. 13.- Secretaría Nacional de Inteligencia (CIES)



LEY DE SEGURIDAD PÚBLICA Y DEL ESTADO

El artículo 10. en referencia a las Funciones del Ministerio de Coordinación de Seguridad o quien haga sus veces señala que, El Ministerio de Coordinación de Seguridad o quien haga sus veces cumplirá las siguientes funciones:

f) Coordinar con la Secretaría Nacional de Inteligencia, en función de disponer de una oportuna y fluida información estratégica, para la toma de decisiones en políticas de seguridad del Estado, y ponerla oportunamente en conocimiento del Presidente o Presidenta de la República.



LEY DE SEGURIDAD PÚBLICA Y DEL ESTADO

El artículo 14. En referencia a inteligencia y contrainteligencia, para efectos de esta ley se entenderá por:

a) Inteligencia, la actividad consistente en la obtención, sistematización y análisis de la información específica referida a las amenazas, riesgos y conflictos que afecten a la **seguridad integral**. **La información de inteligencia es sustancial para la toma de decisiones en materia de seguridad.**

b) Contrainteligencia, la actividad de inteligencia que se realiza con el propósito de evitar o contrarrestar la efectividad de las operaciones de inteligencia que representan amenazas o riesgos **para la seguridad.**



LEY DE SEGURIDAD PÚBLICA Y DEL ESTADO

El artículo 15. el artículo 15 señala las funciones de la Secretaría Nacional de Inteligencia, siendo la responsable de:

b) Coordinar y ejecutar las actividades de obtención y análisis de la información para la producción de conocimientos e inteligencia pertinentes, **a fin de garantizar la seguridad** pública y del Estado y el buen vivir.

e) **Contribuir al mantenimiento de la integridad e independencia del Estado**, el estado de derechos y justicia; sus instituciones y la prevención del crimen organizado. No podrá contar entre sus miembros con personal extranjero.



REG. LEY DE SEGURIDAD PÚBLICA Y DEL ESTADO

Artículo 6. Del Sistema Nacional de Inteligencia.- Es el conjunto de organismos de inteligencia independientes entre sí, funcionalmente coordinados y articulados por la Secretaría Nacional de Inteligencia, que ejecutan actividades específicas de inteligencia y contrainteligencia, para asesorar y proporcionar inteligencia estratégica a los niveles de conducción política del Estado, con el fin de garantizar la soberanía nacional, la seguridad pública y del Estado, el buen vivir y defender los intereses del Estado.



Artículo 8. De la Secretaría Nacional de Inteligencia.- La Secretaría Nacional de Inteligencia es el órgano rector del Sistema Nacional de Inteligencia, con rango de Ministerio de Estado, responsable de producir inteligencia, inteligencia estratégica y contrainteligencia.



REG. LEY DE SEGURIDAD PÚBLICA Y DEL ESTADO

Artículo 9. De la competencia de la Secretaría Nacional de Inteligencia.- Dentro del ámbito de su competencia, y sin perjuicio de aquellas establecidas por ley a la Secretaría Nacional de Inteligencia le corresponde:

c) Identificar las amenazas, riesgos y vulnerabilidades internas y externas, con el apoyo de las entidades que conforman el sector público, dentro del ámbito de sus competencias, para lo cual se establecerán mecanismos de enlace y entrega de información relacionada con la Seguridad Pública y del Estado, de conformidad con el Plan Nacional de Seguridad Integral;

d) Realizar la adquisición de equipos y tecnología, y contratar la prestación de servicios de acuerdo con la normativa especial establecida para la ejecución de operaciones encubiertas de inteligencia y seguridad;

e) Proporcionar, los análisis e inteligencia estratégica producida al Presidente o Presidenta de la República, Ministerio de Defensa Nacional o quien haga sus veces y a los organismos que tienen la responsabilidad de formular respuestas para evitar afectaciones a los intereses del Estado.

g) Identificar las estructuras, la dimensión y los impactos a la seguridad pública y del Estado del crimen organizado nacional y transnacional, y su colaboración con los fines del sistema nacional de justicia criminal y cuando corresponda con operaciones internacionales en contra del crimen transnacional.



REG. LEY DE SEGURIDAD PÚBLICA Y DEL ESTADO

Artículo 11. Del Comité Nacional de Inteligencia.- Es la instancia en la que los subsistemas y agencias, proveen obligatoriamente información e inteligencia y contrainteligencia en forma oportuna y permanente a la Secretaría Nacional, desde cada uno de sus ámbitos de acción, y coordinan e intercambian estos productos entre sí en salvaguarda de los intereses y seguridad integral del Estado. El Comité Nacional de Inteligencia estará presidido por el Secretario Nacional de Inteligencia.

Artículo 14. Del mecanismo de control interno del Sistema Nacional de Inteligencia.- Es obligación de los organismos que conforman el Sistema Nacional de Inteligencia establecer procedimientos idóneos de control previo y concurrente destinados a precaver el adecuado uso de la información a través de acciones de inteligencia y contrainteligencia, detección y erradicación de fugas de información, protección de garantías y derechos constitucionales activación de medidas y procedimientos de asuntos internos.



EL FUTURO

2023



SECTOR ESTRATÉGICO

- CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR
- Capítulo quinto
- Sectores estratégicos, servicios y empresas públicas
- **Art. 313.-** El **Estado** se reserva el derecho de **administrar, regular, controlar y gestionar** los sectores estratégicos, de conformidad con los principios de sostenibilidad ambiental, precaución, prevención y eficiencia.

Los sectores estratégicos, de decisión y control exclusivo del Estado, son aquellos que por su **trascendencia y magnitud tienen** decisiva **influencia económica, social, política o ambiental**, y deberán orientarse al pleno desarrollo de los derechos y al interés social.

Se consideran sectores estratégicos la **energía en todas sus formas, las telecomunicaciones, los recursos naturales no renovables, el transporte y la refinación de hidrocarburos, la biodiversidad y el patrimonio genético, el espectro radioeléctrico, el agua**, y los demás que determine la ley.

Nota: Por Resolución No. 1 de la Corte Constitucional, publicada en el Registro Oficial Suplemento 629 de 30 de Enero del 2012 (ver...), se interpreta estos artículos distinguiendo la gestión de la administración, regulación y control por el Estado y determina el rol de las empresas públicas delegatarias de servicios públicos.

- **Art. 314.-** El Estado será responsable de la provisión de los **servicios públicos de agua potable y de riego, saneamiento, energía eléctrica, telecomunicaciones, vialidad, infraestructuras portuarias y aeroportuarias**, y los demás que determine la ley.

El Estado garantizará que los servicios públicos y su provisión respondan a los principios de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad. El Estado dispondrá que los precios y tarifas de los servicios públicos sean equitativos, y establecerá su control y regulación.



AMENAZAS A LAS INFRAESTRUCTURAS CRÍTICAS

- Falta de definición de responsabilidades
 - GOBIERNO (Principal Parte Interesada)
 - Designación de **Ministerio** que lidere/coordine
 - COMPETENCIAS SECTORIALES
 - Público (Ministerios, Corporaciones Nacionales, GAD Provincial, GAD Municipal)
 - Privado
 - Integrado Público-Privado
 - EMPRESAS LOCALES (operadores locales)
 - Establecer **estrategia** y **análisis** de situación.
 - Diseño de **políticas** de seguridad y un **marco de gobierno** alineado a la **seguridad integral**.
 - Definir **estructuras organizativas** para la protección de la seguridad integral.
 - Gestionar temas de **relación e interés** con la **seguridad** de manera **transversal**.
 - Analizar **riesgos** y las **amenazas** para mejorar la seguridad integral.
 - Concienciar al personal interno sobre la **importancia** del **cumplimiento** de la normativa nacional, sectorial y propia.
 - TERCERAS PARTES



AMENAZAS A LAS INFRAESTRUCTURAS CRÍTICAS

Eventos Naturales



Terrorismo



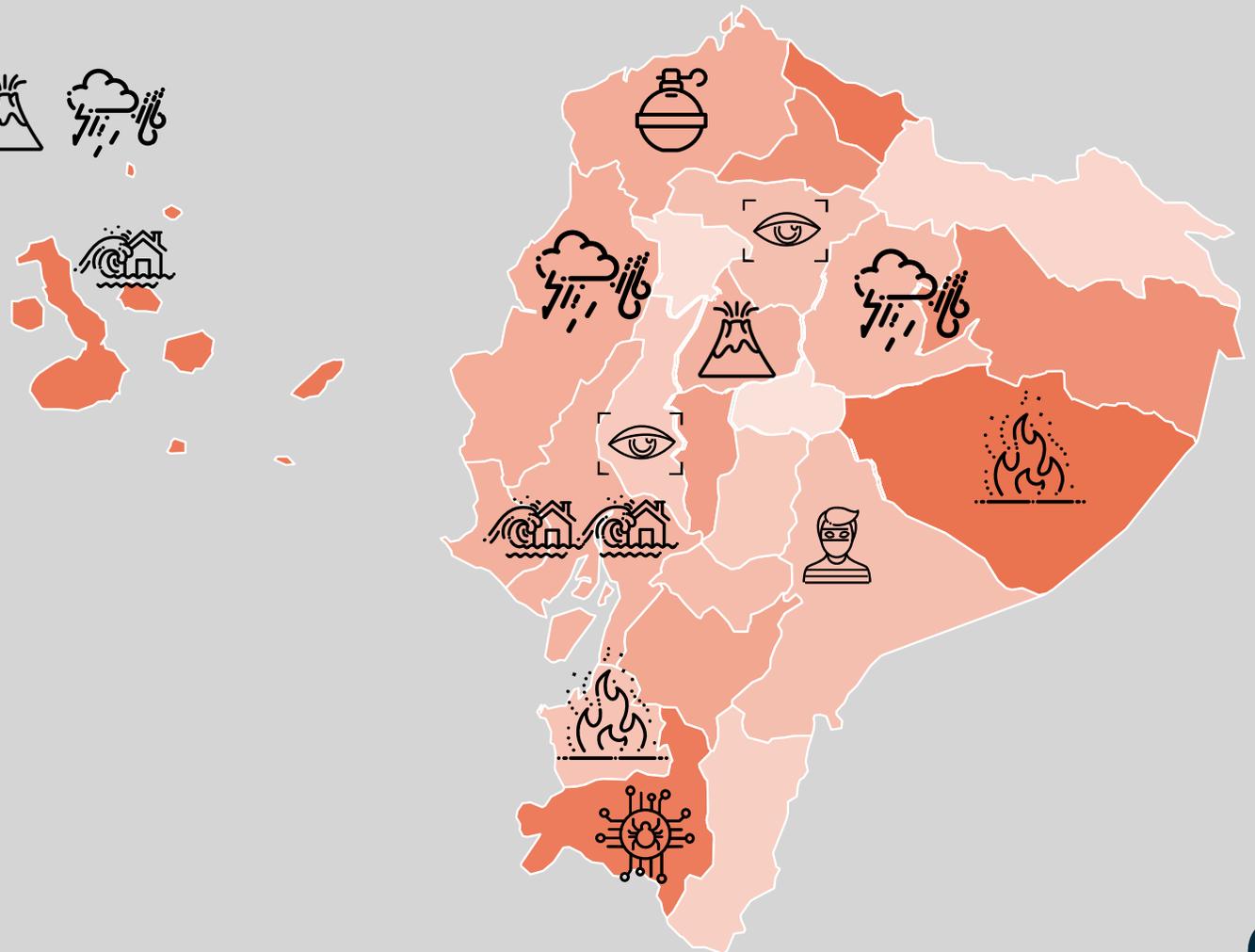
Crimen organizado



Espionaje



Ciberataques



GRACIAS

