

**Instituto Politécnico Nacional
Centro de Investigación en Computación
Laboratorio de Ciberseguridad**

Sesión 3: Ciberseguridad

Curso : Ciberseguridad
Febrero 14, 2017

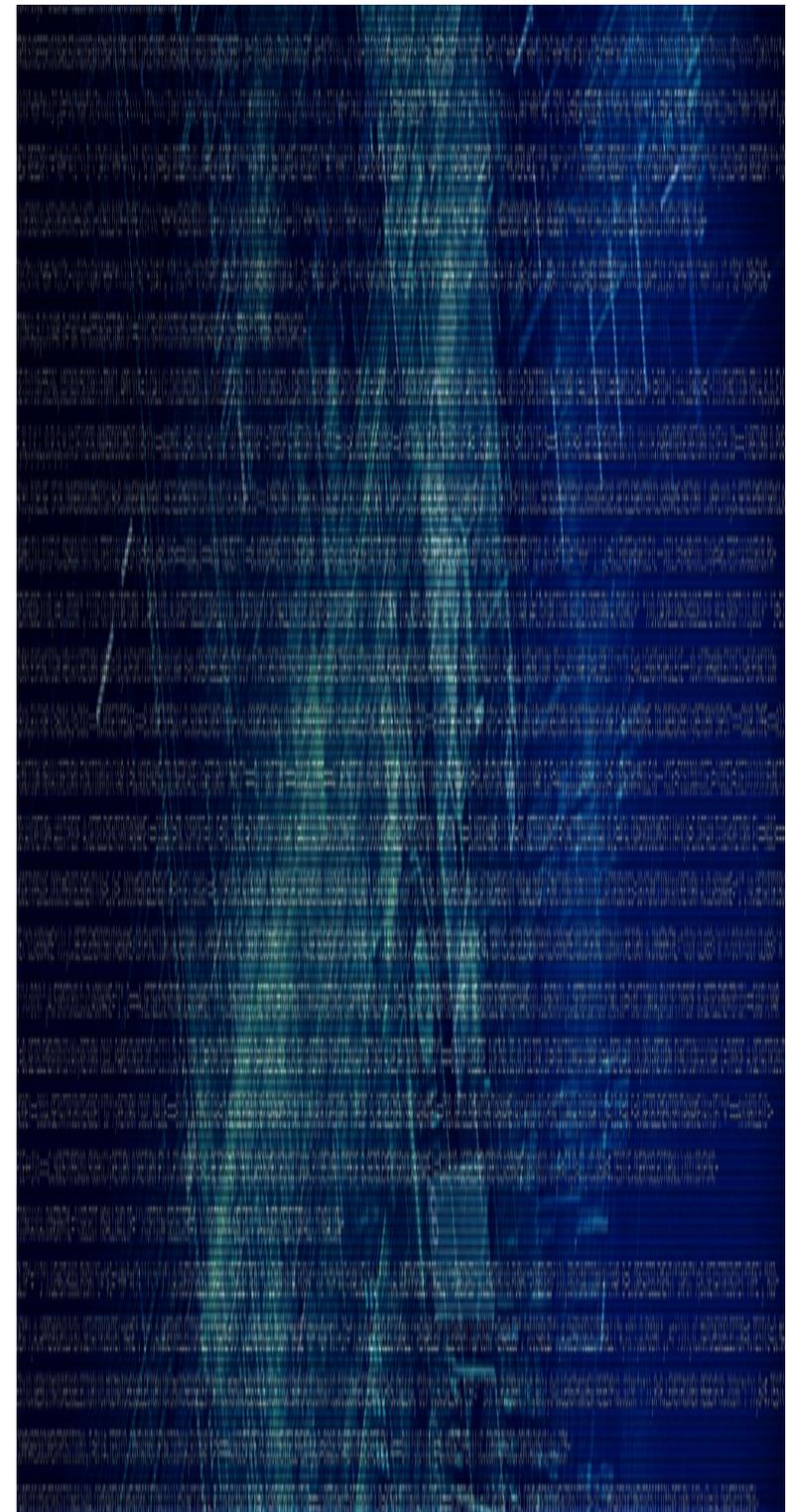
Dr. Moisés Salinas Rosales
msrosales@acm.org



INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Laboratorio de Ciberseguridad
Centro de Investigación en Computación
Instituto Politécnico Nacional
MÉXICO

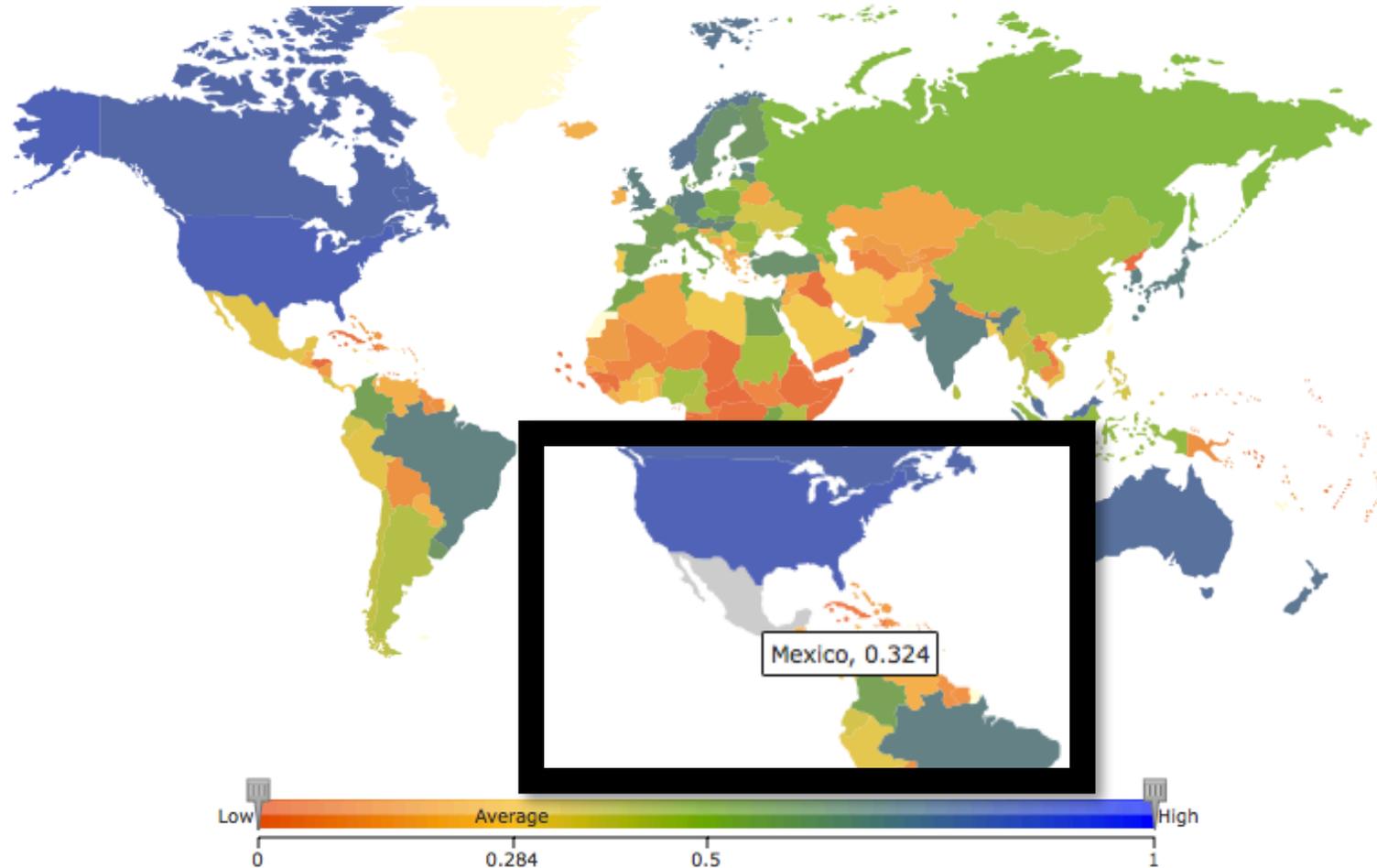


Instantáneas...

Cybersecurity Commitment 2014



CYBERWELLNESS PROFILE MEXICO



INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Laboratorio de Ciberseguridad
Centro de Investigación en Computación
Instituto Politécnico Nacional
MÉXICO

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

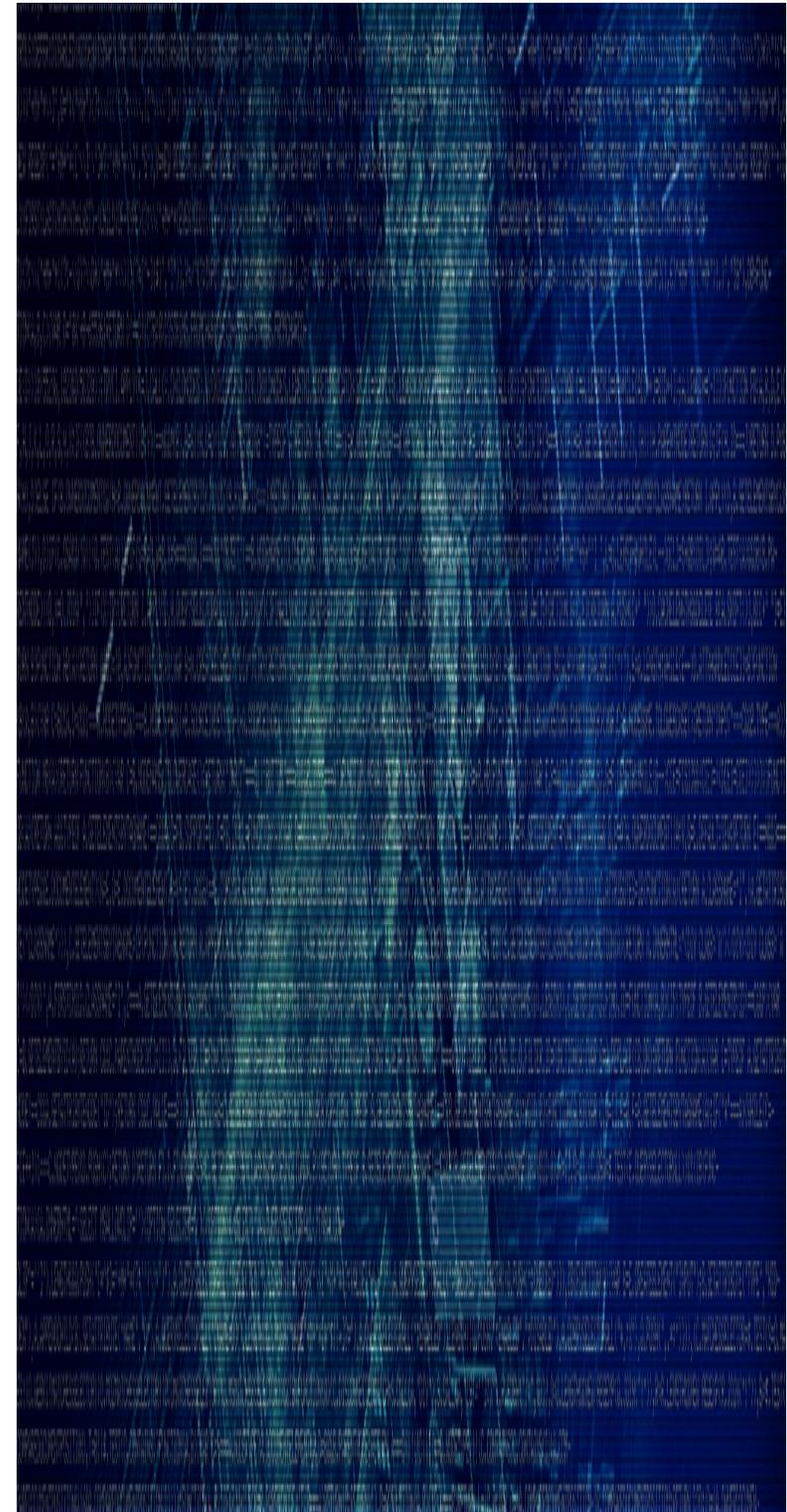
NIST



INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Laboratorio de Ciberseguridad
Centro de Investigación en Computación
Instituto Politécnico Nacional
MÉXICO



Motivación del Framework

- ❑ La sociedad actual depende en gran parte de:

Seguridad
Nacional

Seguridad
Económica

Seguridad
Pública

Las que a su vez dependen de un funcionamiento confiable de la infraestructura crítica.



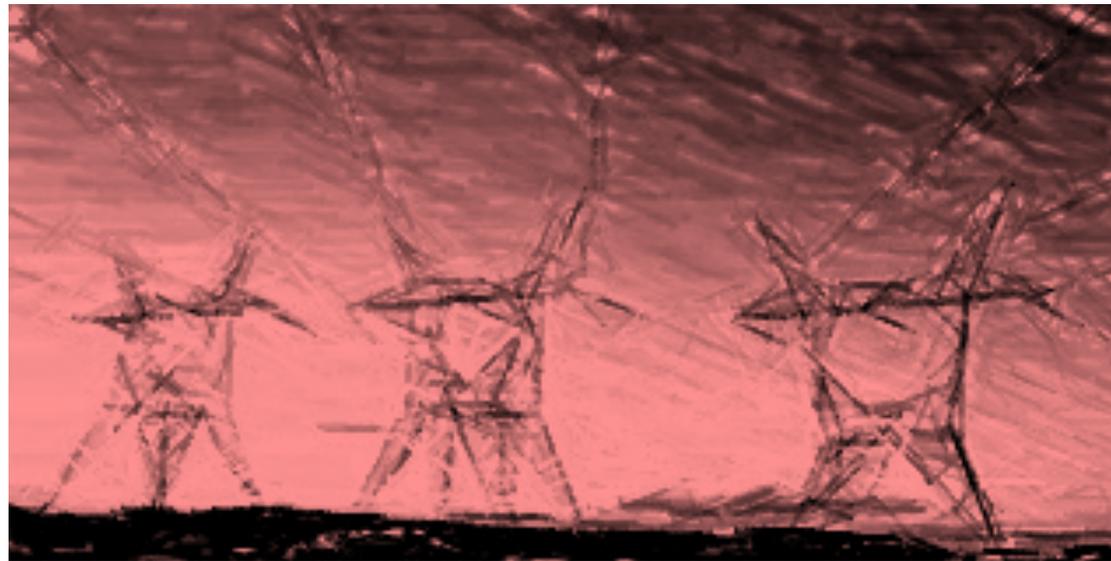
¿Que es la Infraestructura Crítica?

- ❑ Son aquellas infraestructuras que son necesarias para el funcionamiento normal de los servicios básicos y los sistemas de producción de cualquier sociedad.
 - ❖ Cualquier interrupción en su funcionamiento llega ser una fuente de perturbaciones graves en materia de seguridad: nacional, económica, pública.
 - ❖ Ejemplos:
 - sistema de transportes,
 - Sistema de distribución de agua
 - Red eléctrica
 - Telecomunicaciones
 - Nagevación, etc.



¿Que es la Infraestructura Crítica?

- Del Framework para Ciberseguridad se extrae:
 - ❖ “Son los sistemas y activos, ya sean físicos o virtuales, que son necesarios para la continuidad de la operación de la sociedad, de forma que su destrucción o inhabilitación pone en riesgo a la misma”



INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Laboratorio de Ciberseguridad
Centro de Investigación en Computación
Instituto Politécnico Nacional
MÉXICO

Enfoque

- ❑ El framework de Ciberseguridad del NIST se enfoca en la siguiente premisa:
 - ❖ Las amenazas a la ciberseguridad se enfocan en la explotación de la combinación de la:
 - **Alta complejidad**
 - **Alta conectividad**
 - ❖ Que hoy caracteriza a los sistemas de infraestructura crítica (crece día con día)
- ❑ El riesgo ante a dichas amenazas se asocia con impactos en:

Salud

Seguridad
Pública

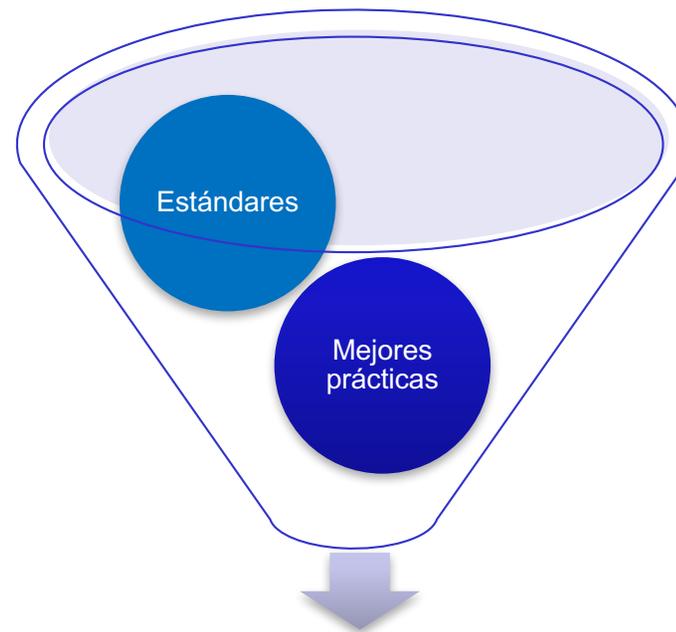
Economía

Seguridad
Nacional



Objetivo

- ❑ El framework de Ciberseguridad es la propuesta de US-gov para las organizaciones para ayudarlas a afrontar de mejor manera los riesgos en materia de ciberseguridad.



Framework de
Ciberseguridad

Laboratorio de Ciberseguridad
Centro de Investigación en Computación
Instituto Politécnico Nacional
MÉXICO



INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Alcances

Ciberseguridad

Principios
Mejores
Prácticas



Infraestructura crítica

Para garantizar

A través de...

Principios Mejores
Prácticas

- Estándares
- Guías
- Procesos
- Procedimientos

Seguridad

Continuidad del
negocio

Libertades
civiles

Protección

Privacidad

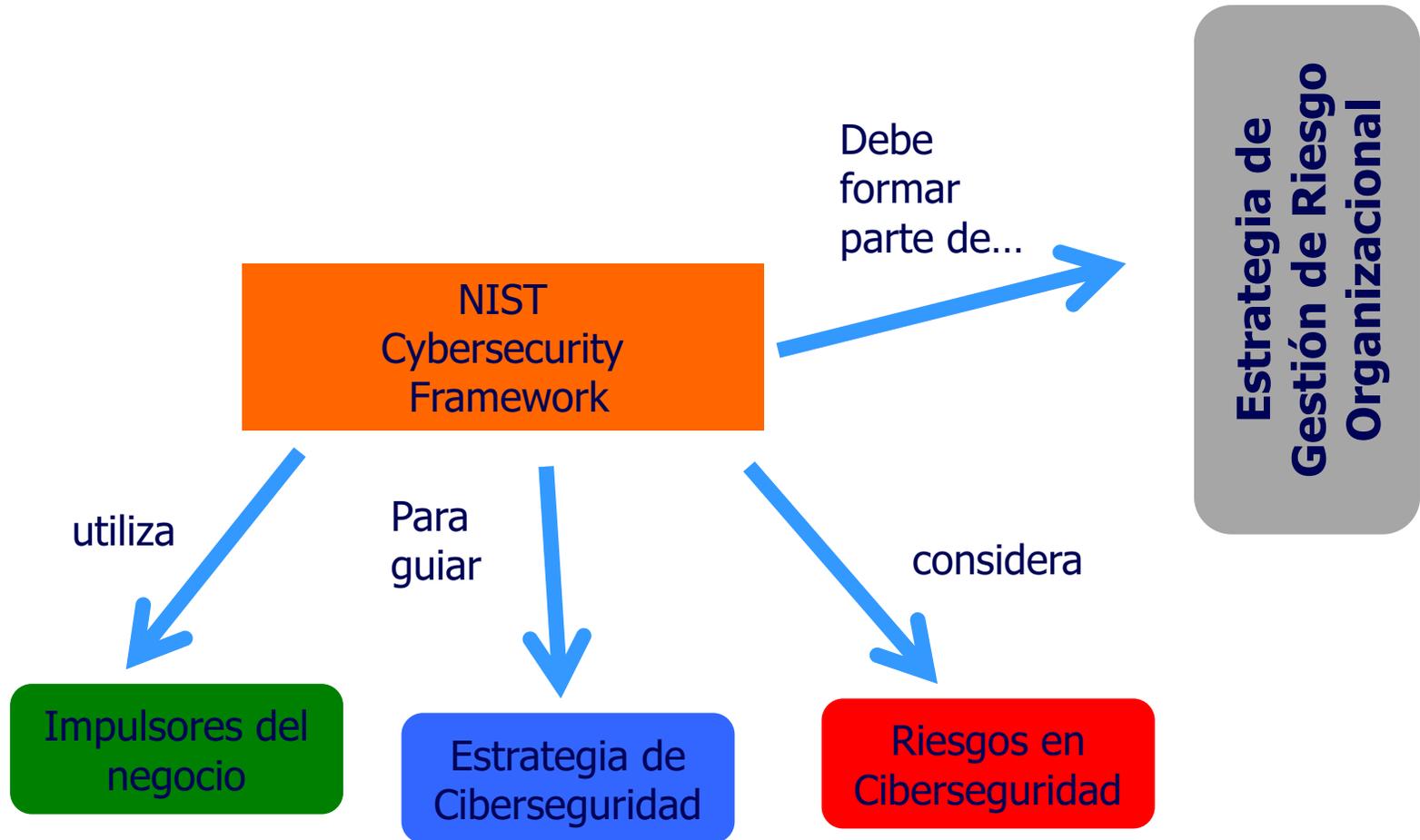


INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Centro de Investigación en Ciberseguridad
Centro de Investigación en Computación
Instituto Politécnico Nacional
MÉXICO

Interacción del framework



Motivación del Framework

Salud

Seguridad
Pública

Economía

Seguridad
Nacional

SOPORTE

Infraestructura
crítica

Virtual

Física

Riesgos

Identifica



Evalúa



Gestiona



Estrategia
de
mitigación
de riesgos

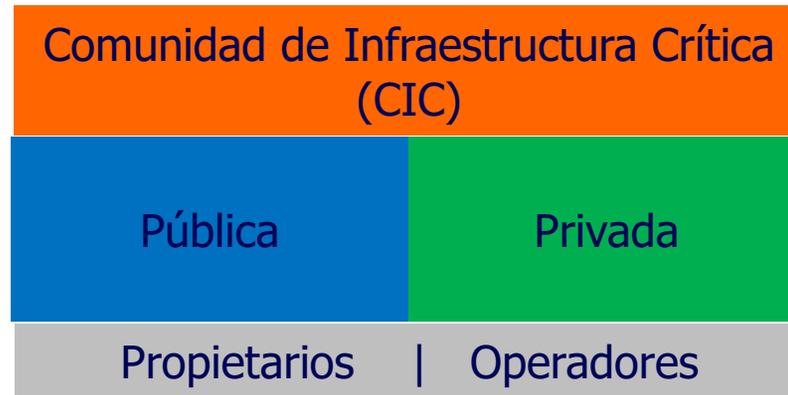


INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Laboratorio de Ciberseguridad
Centro de Investigación en Computación
Instituto Politécnico Nacional
MÉXICO

Motivación del Framework



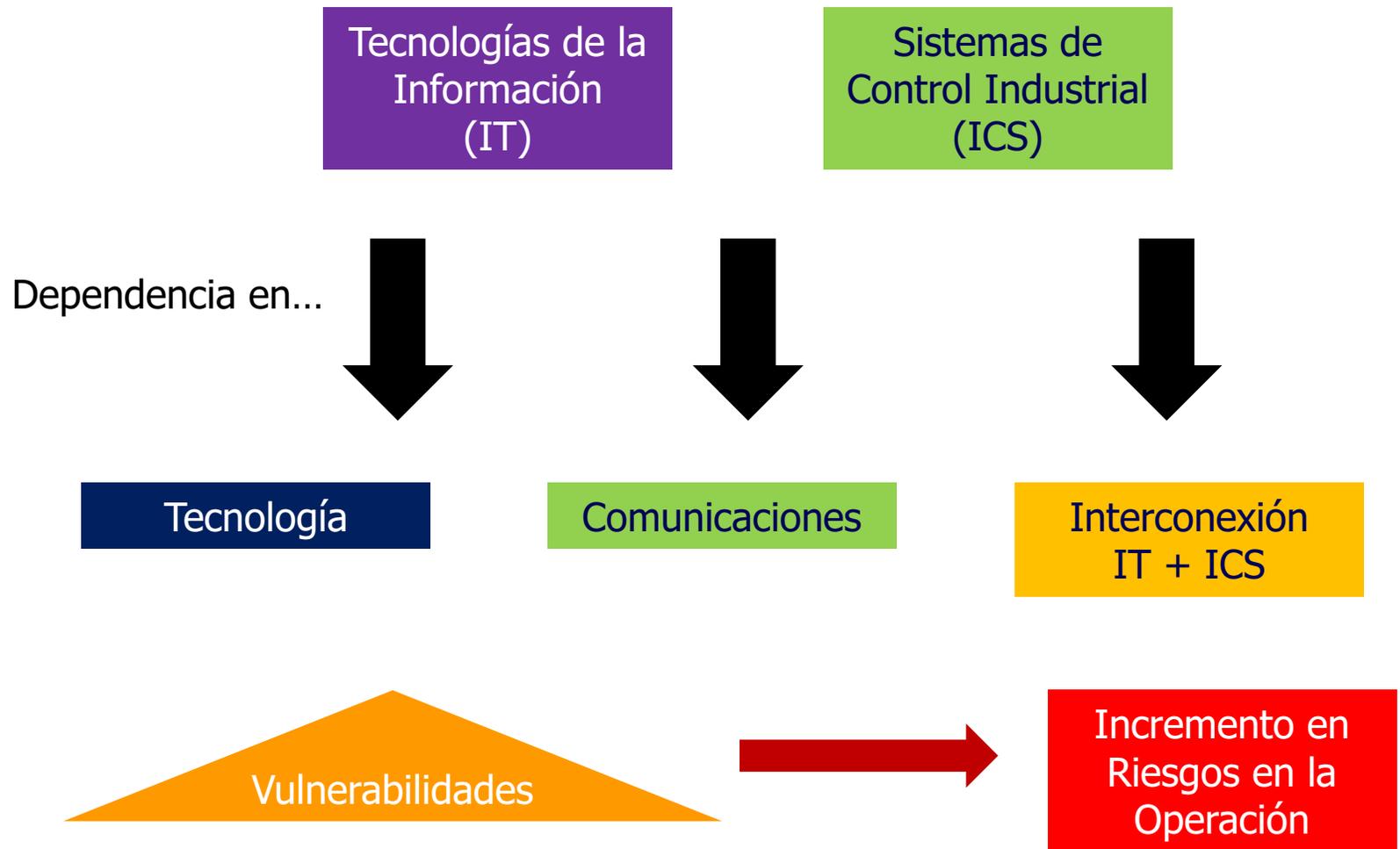
Tecnologías de la
Información
(IT)



Sistemas de
Control Industrial
(ICS)



Motivación del Framework



Estructura

Framework de Ciberseguridad

Core

Capas de
Implementación

Perfiles

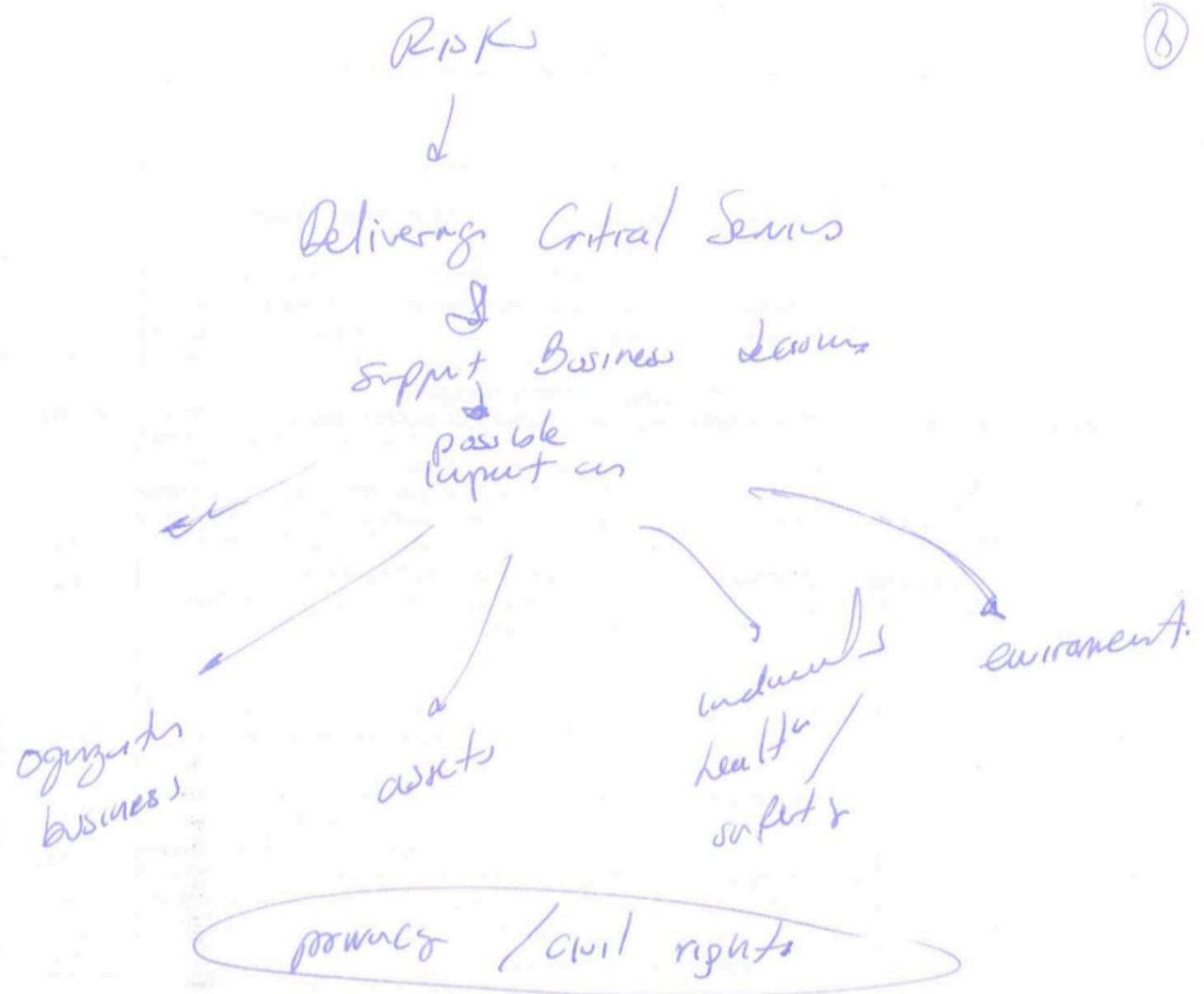


INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA

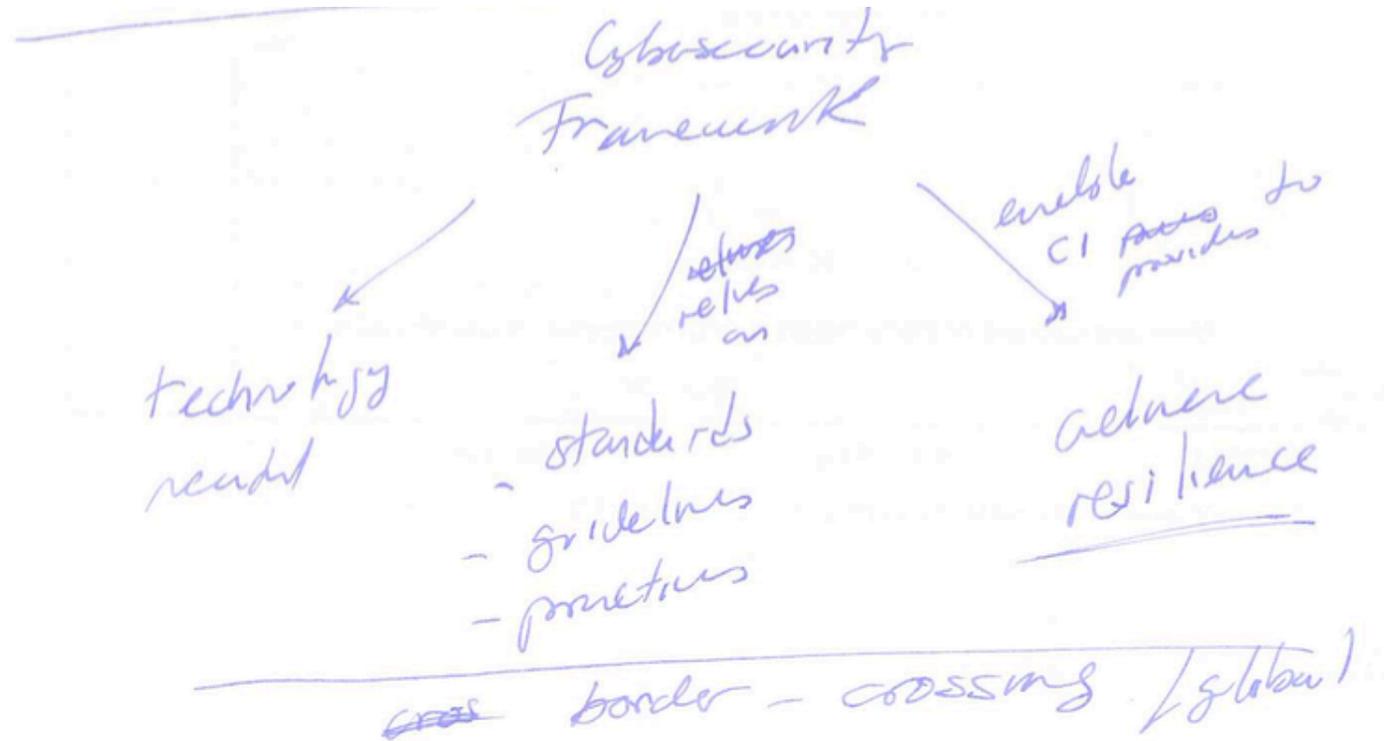


Laboratorio de Ciberseguridad
Centro de Investigación en Computación
Instituto Politécnico Nacional
MÉXICO

Motivación del Framework



Motivación del Framework

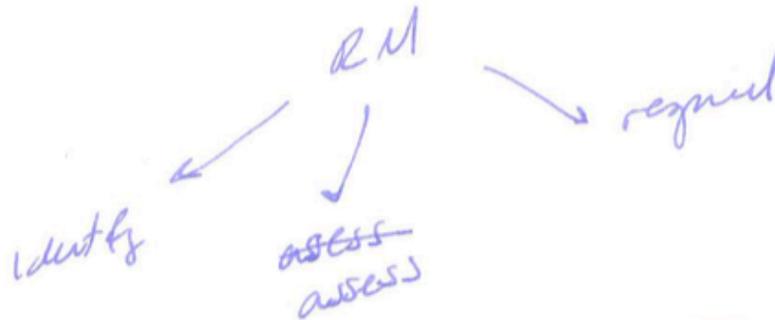


Motivación del Framework

Cybersecurity

Uso del Plan de seguridad por la
Gestión del Rys

21/03/15

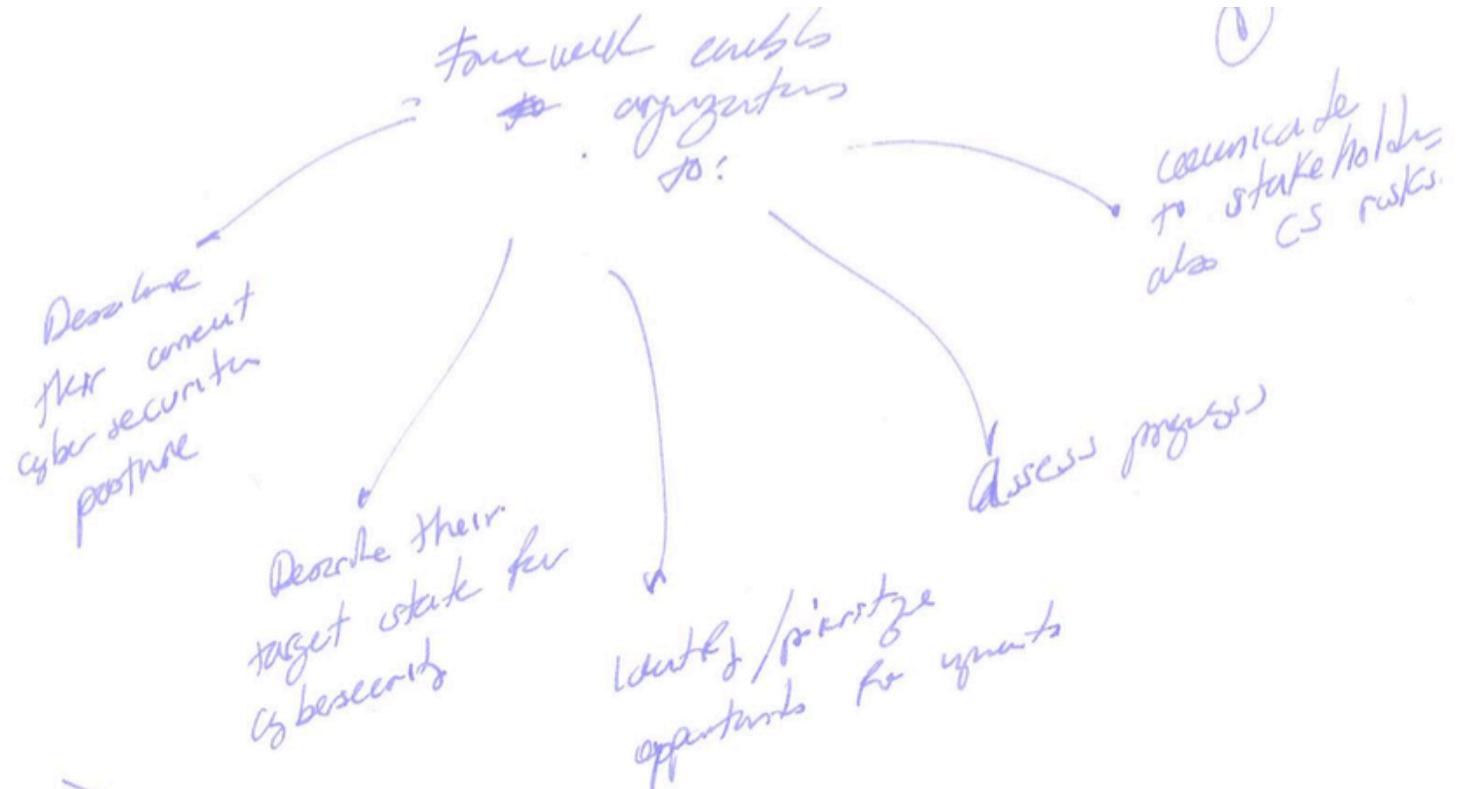


Motivación del Framework

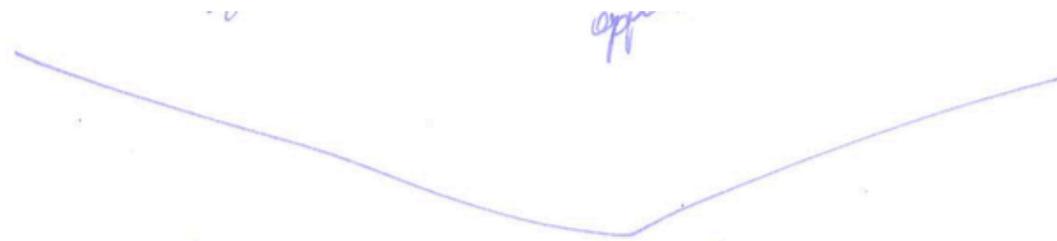
ambigüedad (likelihood) monitoreo del ambiente
 (the likelihood) para detectar eventos que pueden
 hacer un impacto en la organización



Motivación del Framework



Motivación del Framework



It captures Org's Risk management process / cybersecurity program

It can be used to derive a cybersecurity program when it doesn't exist yet

It is not industry-specific.



Motivación del Framework

Framework → helps to
support
recovery
risk assessments
downstreamly
select &
direct
implement in
controls in
IT/ICS.

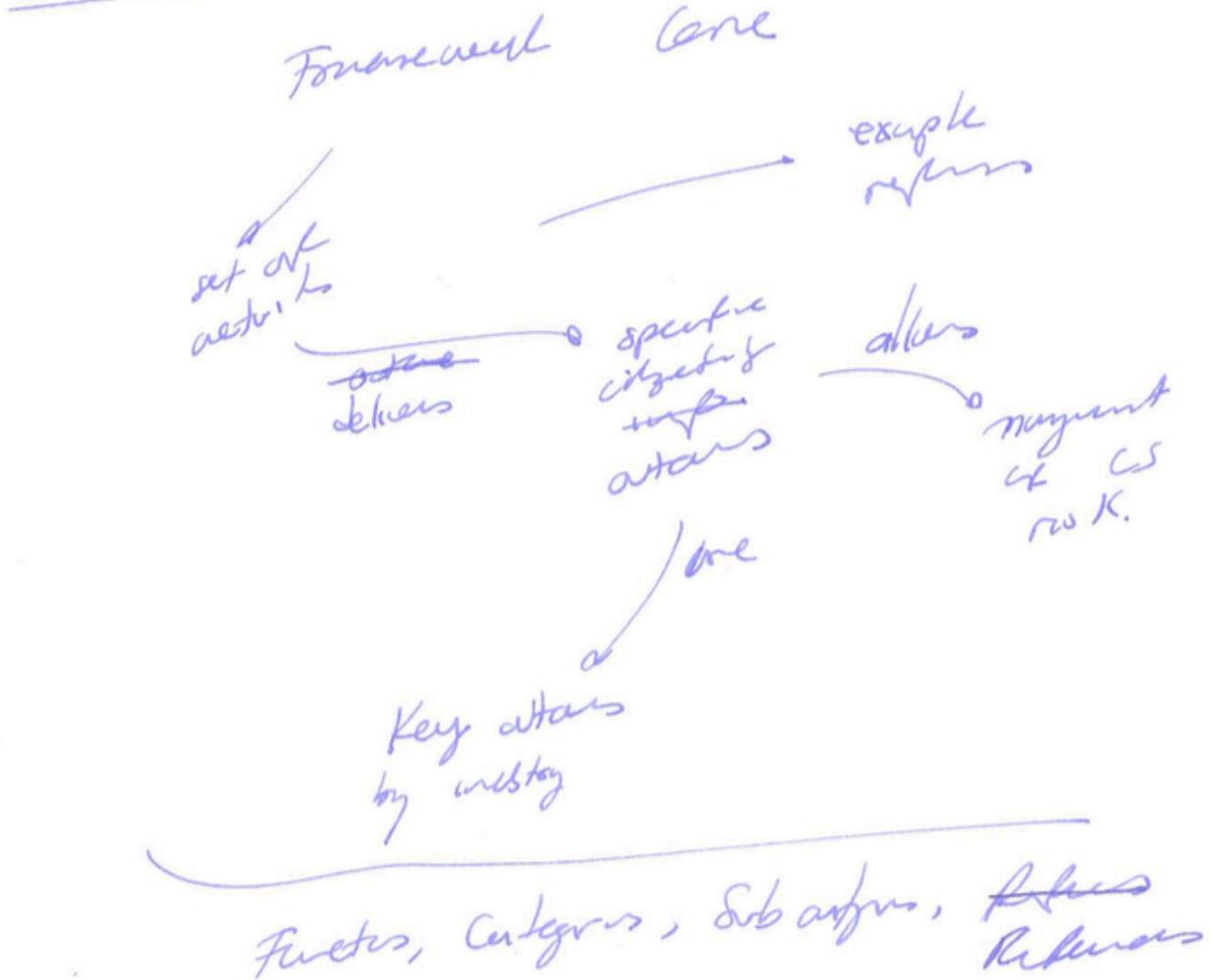


INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Laboratorio de Ciberseguridad
Centro de Investigación en Computación
Instituto Politécnico Nacional
MÉXICO

Motivación del Framework



Motivación del Framework

Factos → high level CS activities

Identify

Protect

Detect

Respond

~~Recover~~ Recover

ongoing inherent
enables RM devices
address threats
improves by being
learning

aligned with methodology for
incident response

