

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

Sesión 3: Introducción a la Ciberseguridad

Curso : Ciberseguridad
Agosto 23 2016

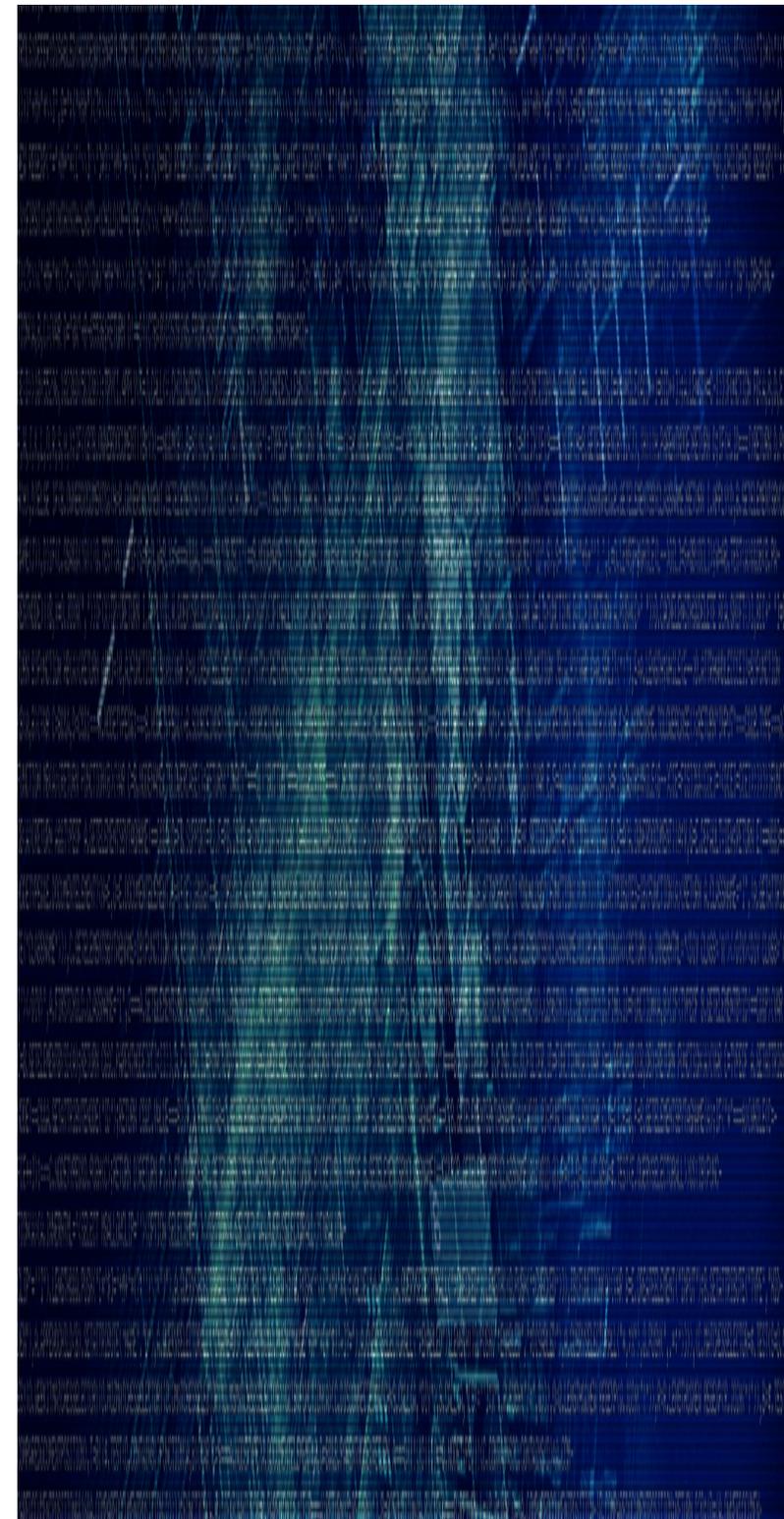
Dr. Moisés Salinas Rosales
msrosales@acm.org



INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



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



Instituto Politécnico Nacional
Centro de Investigación en Computación
Laboratorio de Ciberseguridad

Lectura de

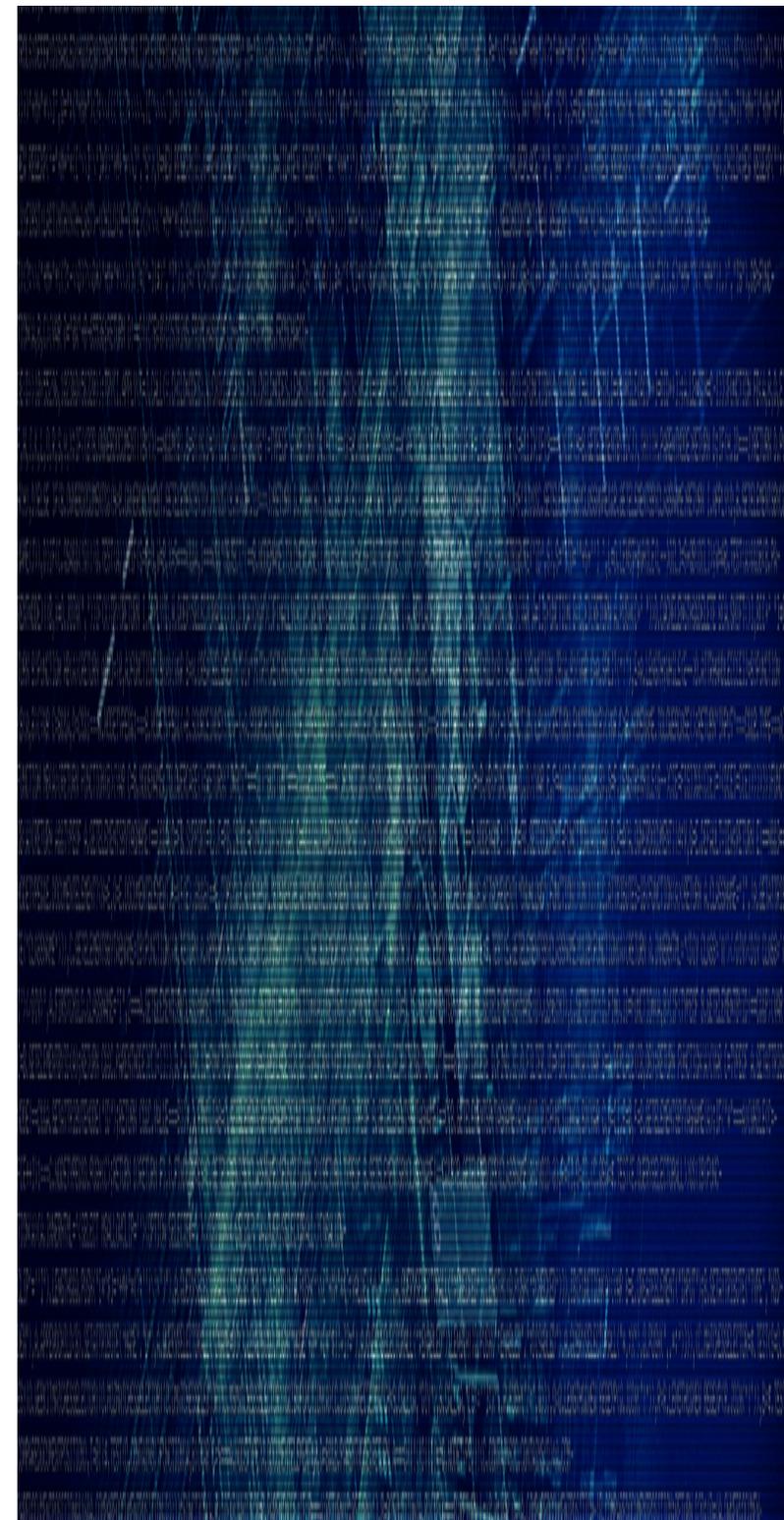
**Framework for Improving Critical
Infrastructure Cybersecurity**
Version 1.0
NIST



INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Laboratorio de Ciberseguridad
Centro de Investigación en Computación
Instituto Politécnico Nacional
MÉXICO
Dr. Moisés Salinas Rosales
msrosales@acm.org



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
 - Navegación, 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

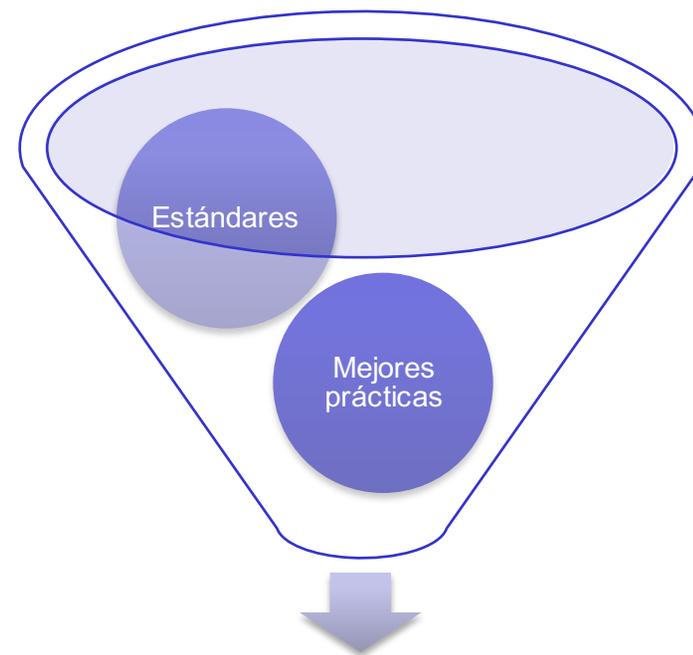
Economía

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

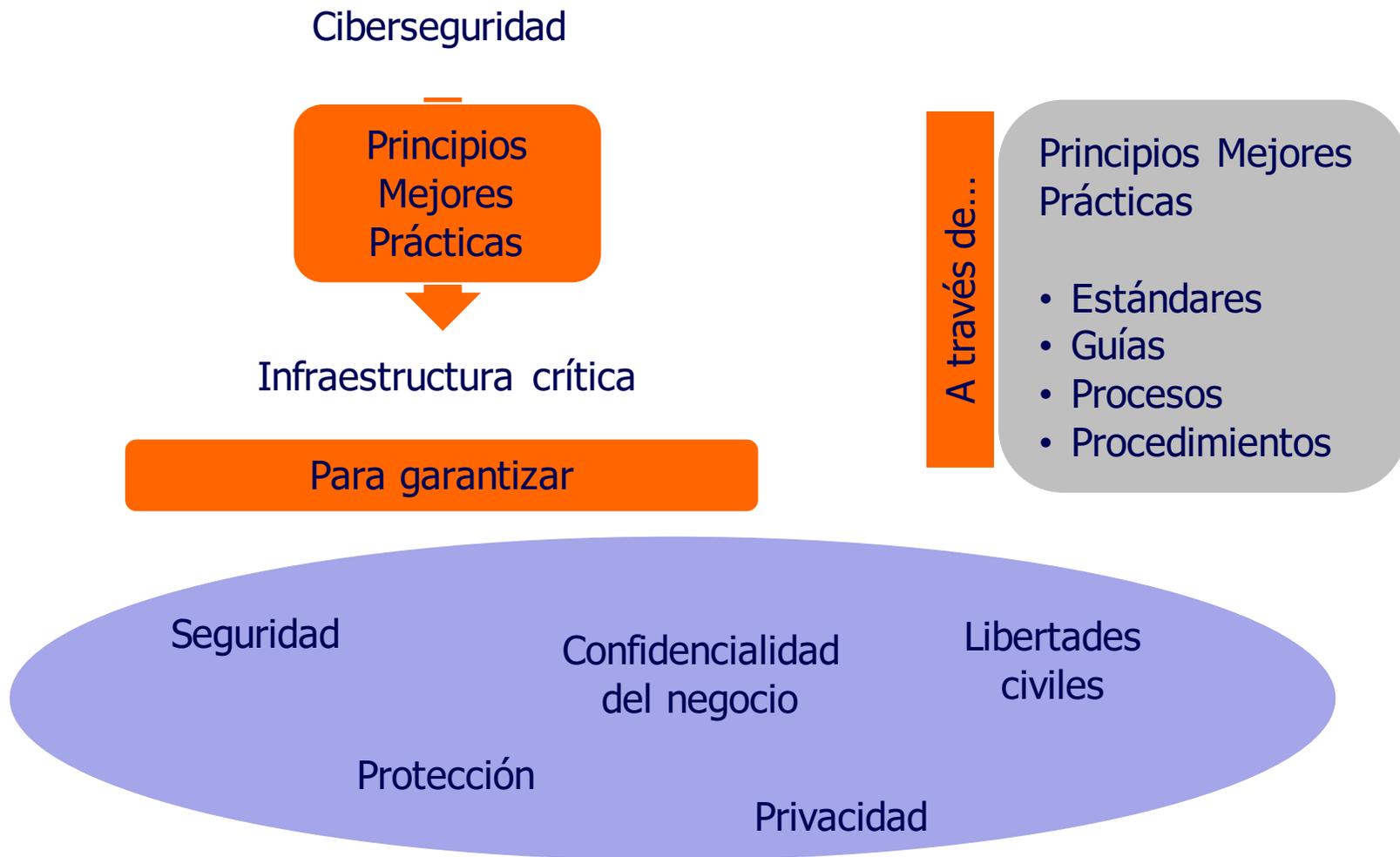
Laboratorio de Ciberseguridad
Centro de Investigación en Computación
Instituto Politécnico Nacional
MÉXICO



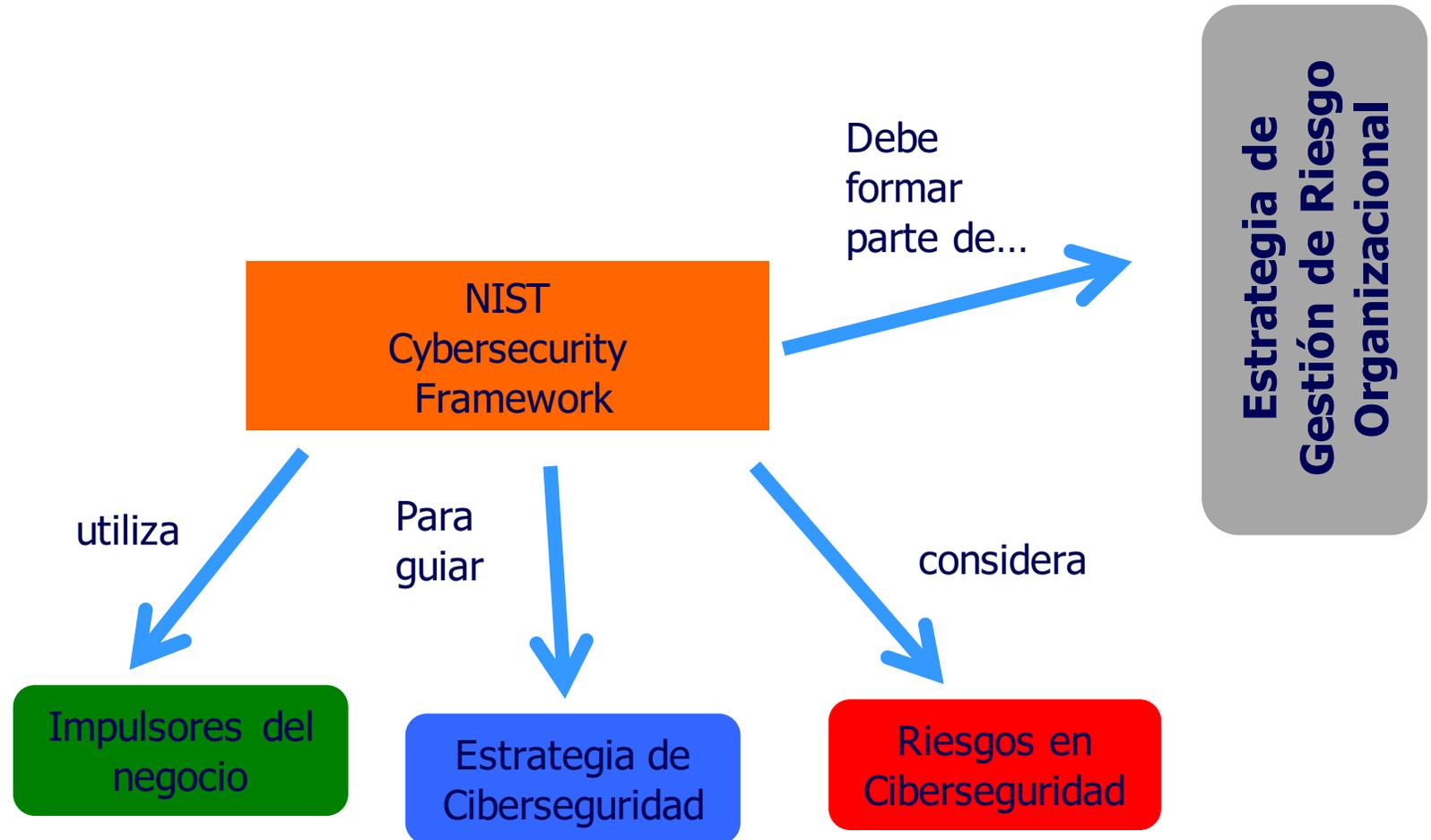
INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Alcances



Interacción del framework



Estructura

Framework de Ciberseguridad

Core

Capas de
Implementación

Perfiles

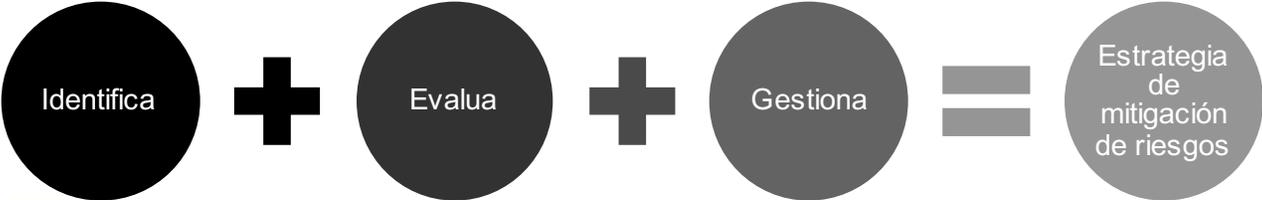
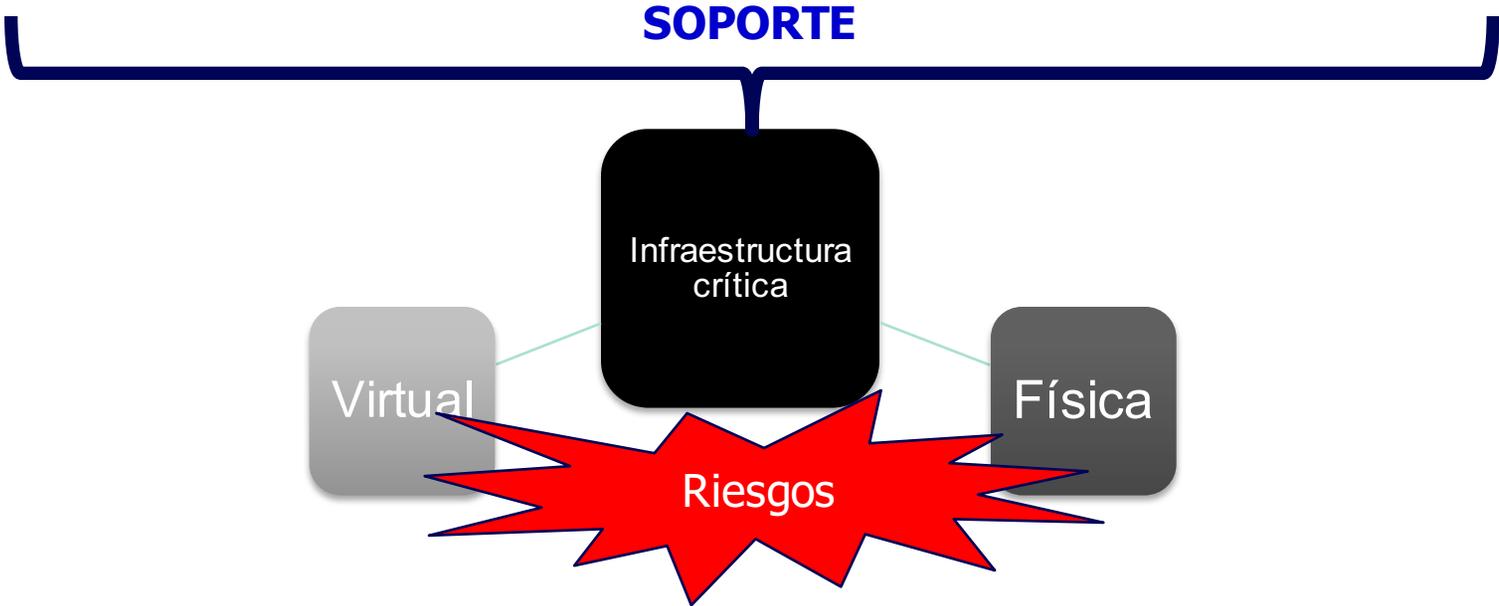


INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



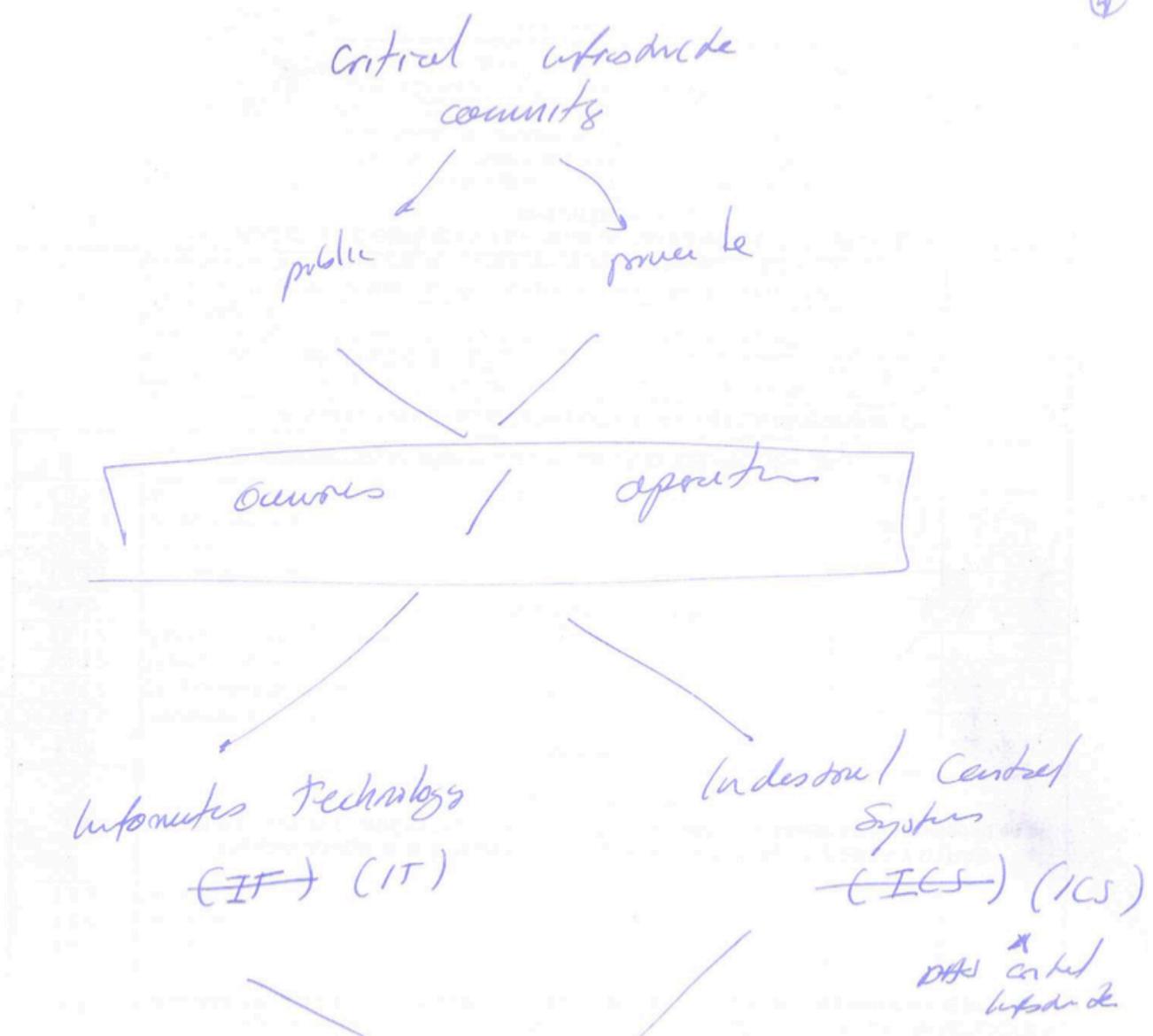
Laboratorio de Ciberseguridad
Centro de Investigación en Computación
Instituto Politécnico Nacional
MÉXICO

Motivación del Framework



Motivación del Framework

(4)

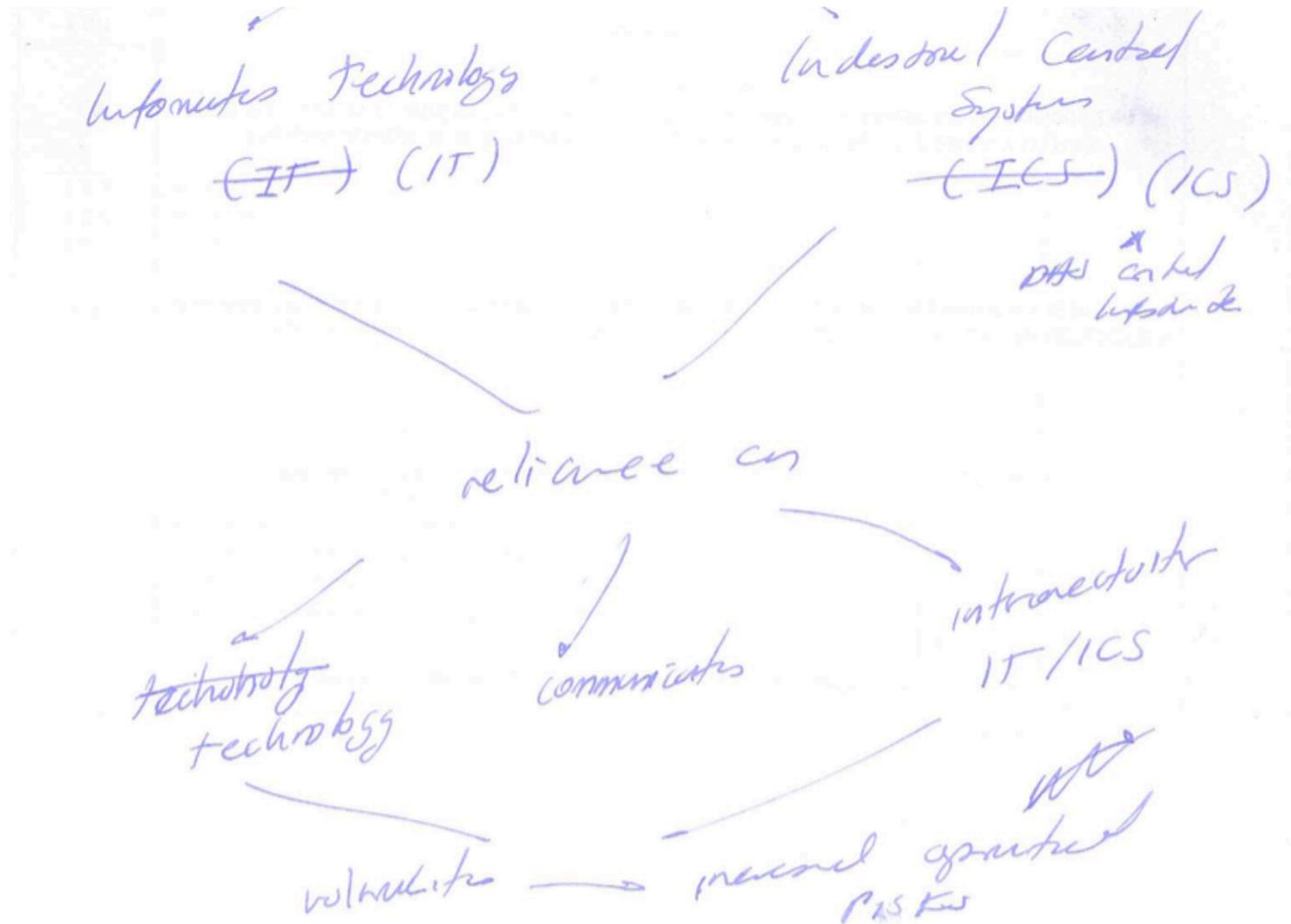


INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA

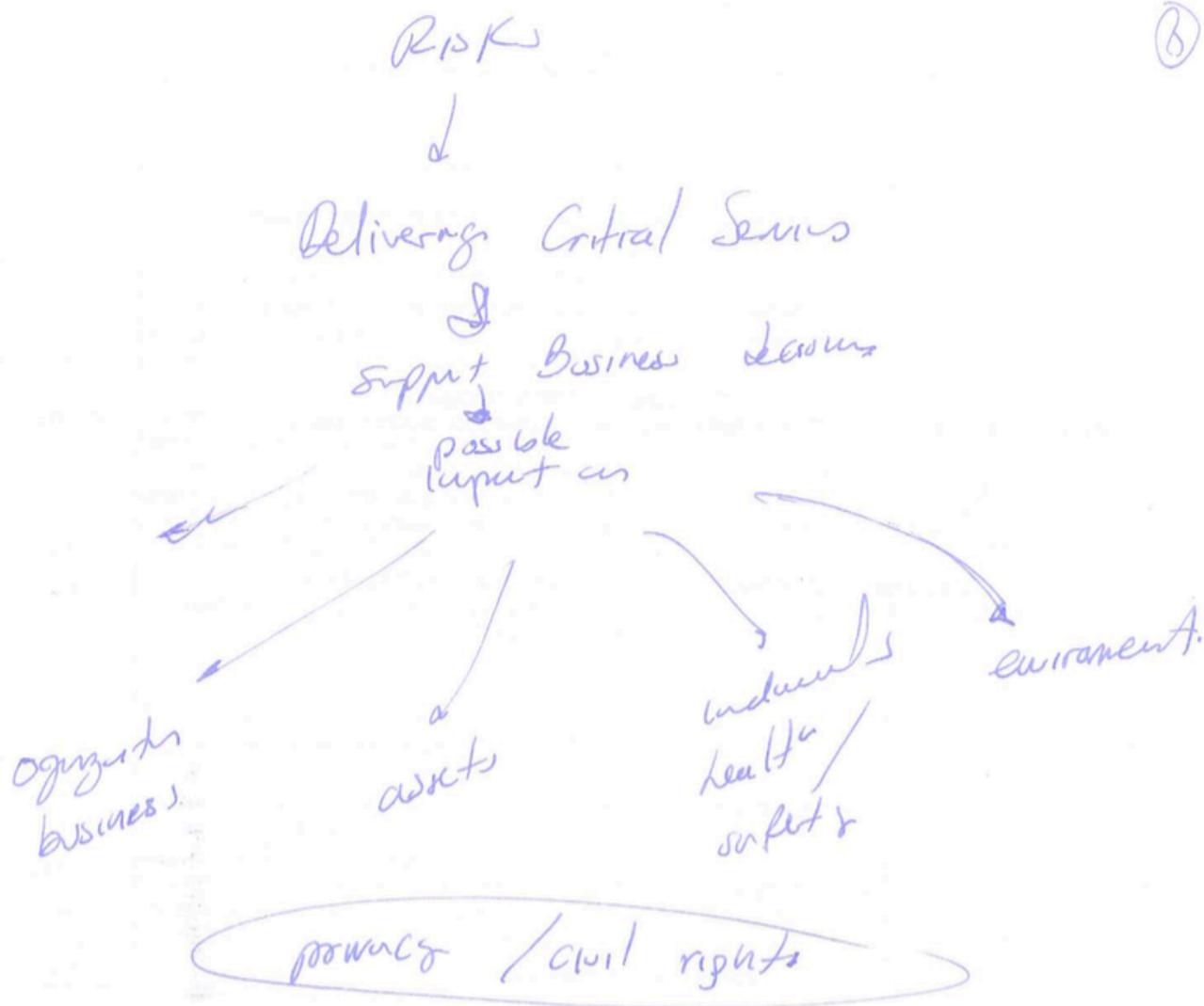


Laboratorio de Ciberseguridad
Centro de Investigación en Computación
Instituto Politécnico Nacional
MÉXICO

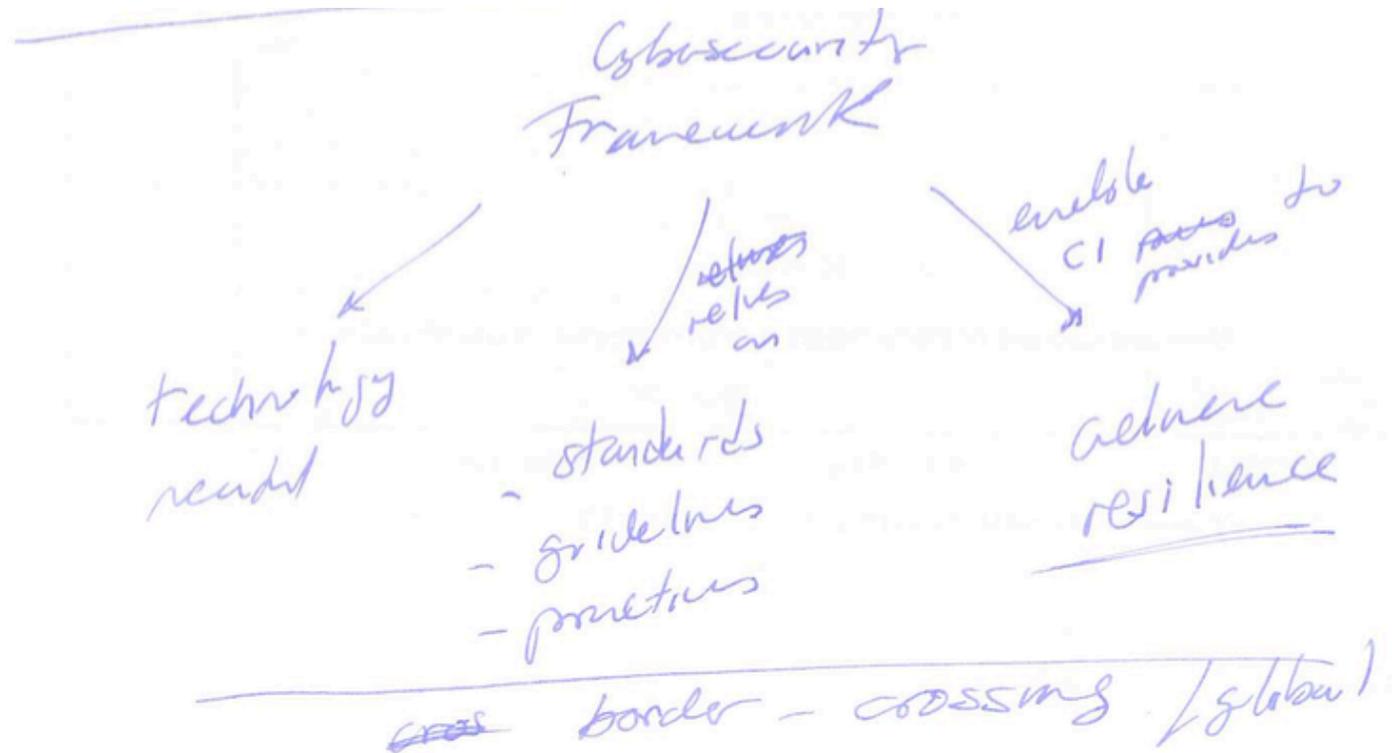
Motivación del Framework



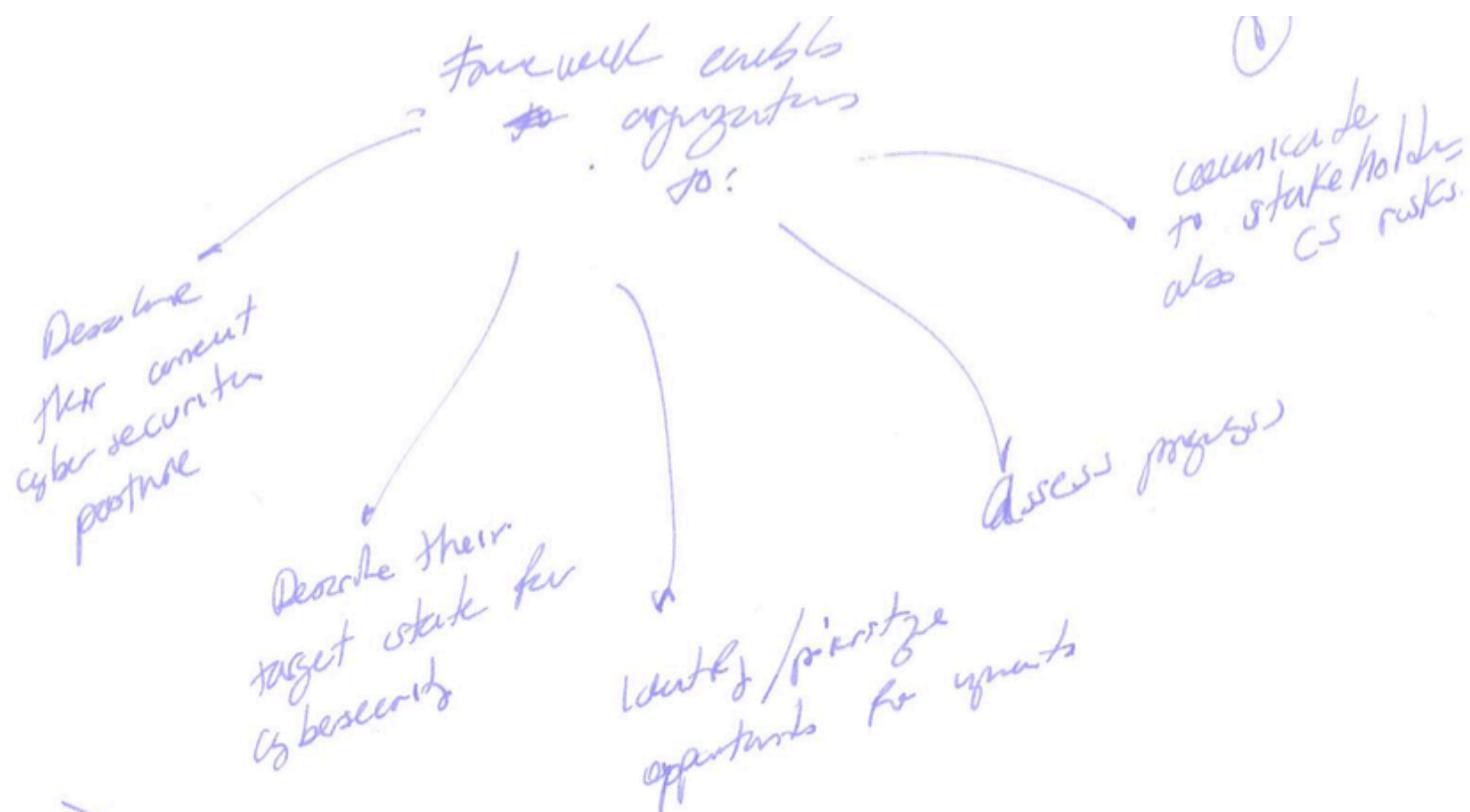
Motivación del Framework



Motivación del Framework



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.

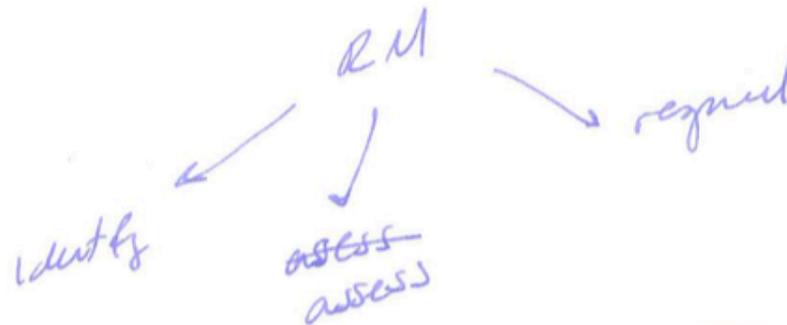


Motivación del Framework

Cybersecurity

Uso del Plan de seguridad por la
Gestión del Rys

21/03/15



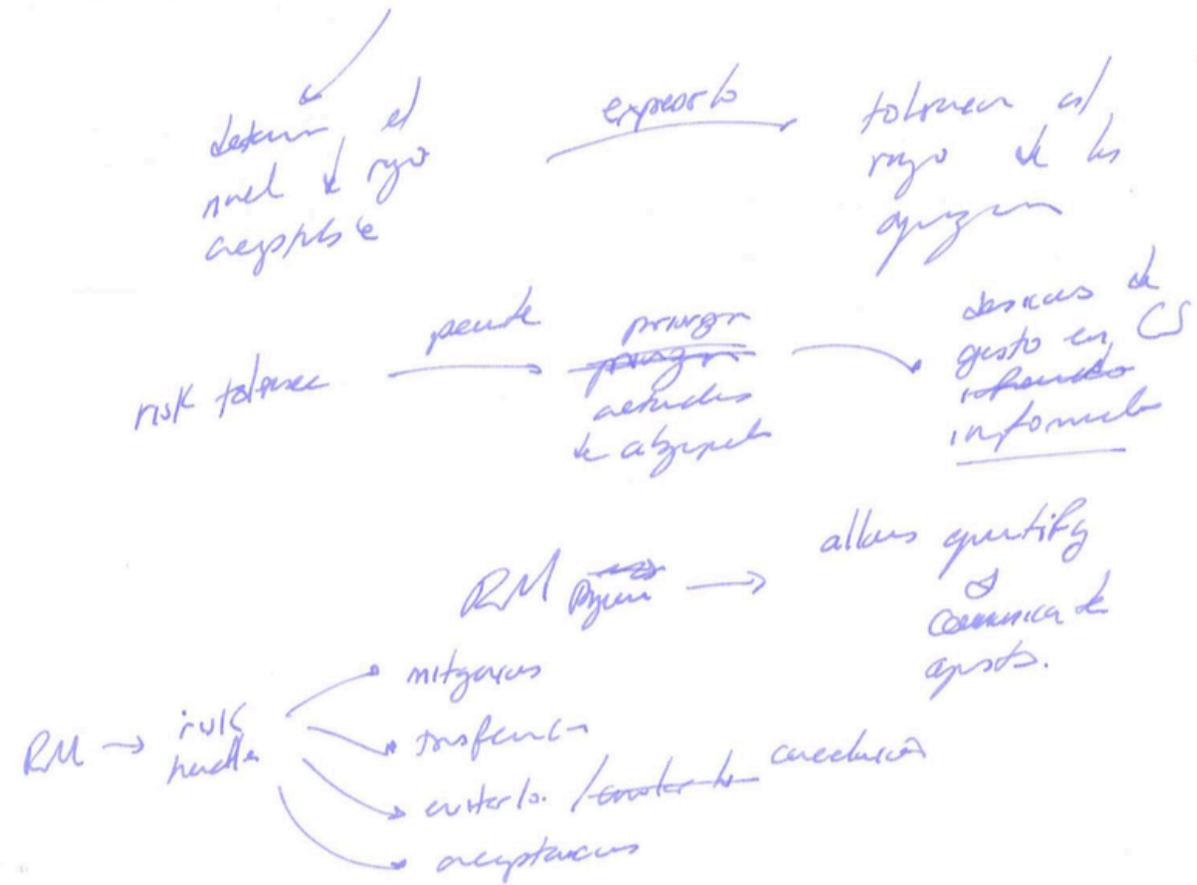
INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



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

Motivación del Framework

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



Motivación del Framework

Framework → helps to dynamically select & direct implementation of abstract req. IS/ICS.

support
recovery
risk assessments

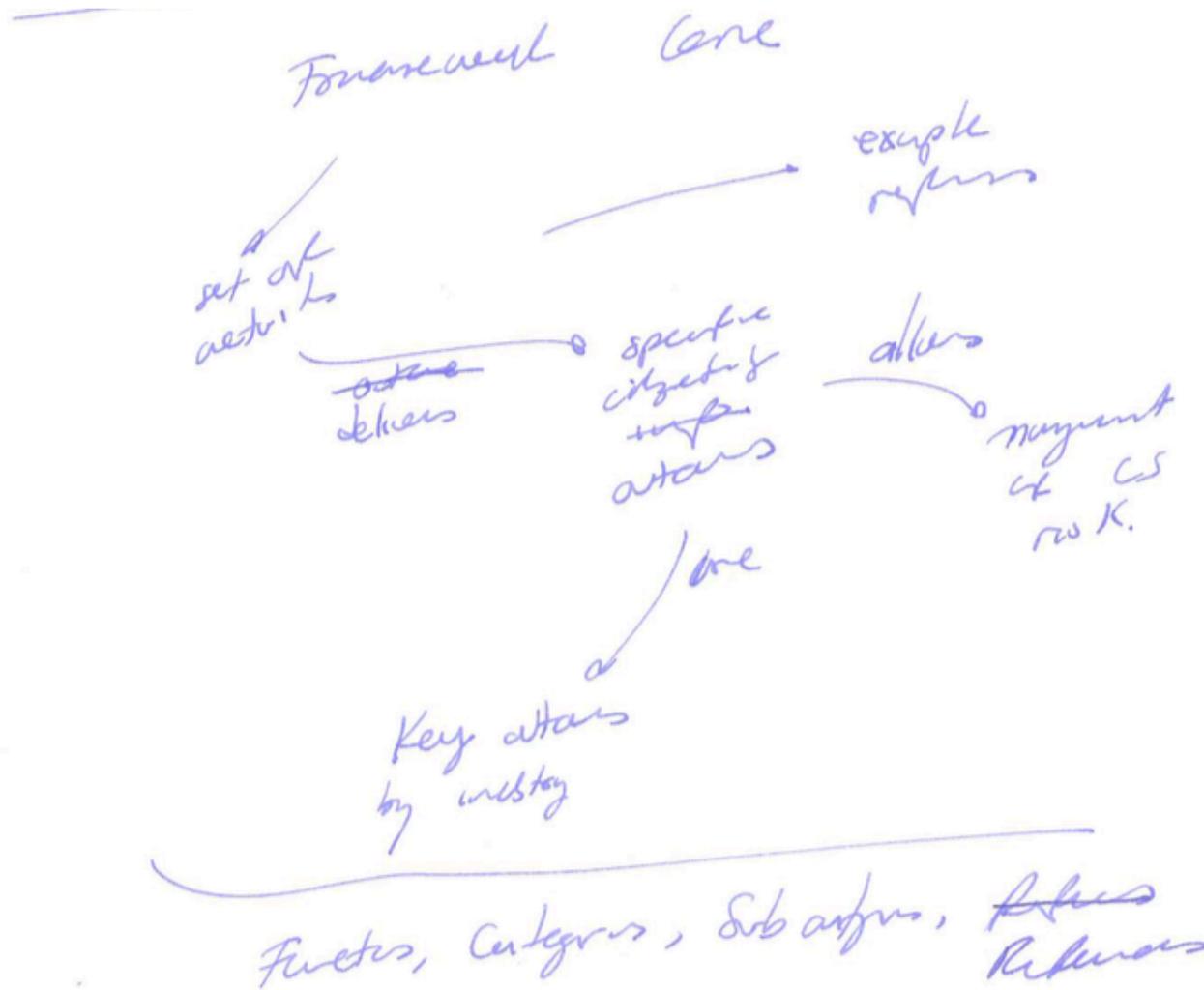


INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



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

Visión del Framework



Actividades de alto nivel del Framework

Funciones → high level activities

Identify

Protect

Detect

Respond

~~Recover~~ Recover

ongoing inherent
enables RM domains
address threats
improves by being
learning

aligned with methodologies for
incident response



Organización del Framework

Categories → Subdivisions of actors according to
actors closely tied
ie. Asset Management
Access Control
Network Protocols

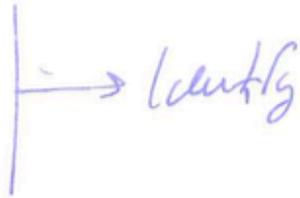
Subdivisions → subdivisions of actors
as ~~an~~ into specific actors
technical / management actors
ie - "Data at rest is protected"
"Notifications per detected
spots are assigned"

Rules → standards, guidelines, protocols CI



Función de Identificación

Funciones



→ describe org understanding to manage
~~risk~~ CS risks to

- systems
- assets
- data
- capabilities

CI: Context Information

Context

- business context
- resources that support context factors
- CS risks

re-outputs ie. Asset Mgmt, Org Env, Gov, Risk Assessment, Risk Mgmt Strategy.



Función de Protección

→ Protect → develop / implement appropriate safeguards
to ensure delivery of ~~critical~~ CI
services
i.e. access control, access / tracking,
data security, inputs protection
process / procedures, maintenance



Detección y Respuesta

→ Detect

→ develop/audit scripts to identify the occurrence of cybersecurity events

ie. - Anomalous/Events
Scripts
Alerts
Centers monitoring

→ Respond

→ develop/audit scripts to take actions
ie. - Alerts ...

ie. - Response Planning,
Communications
Analysis
Mitigation
Log management



Recuperación

→ Recover → develop/implement activities to
maintain plans for resilience
and to restore any components / services
as before CS event
ie Recovery Planning
Incidents
Continuity

