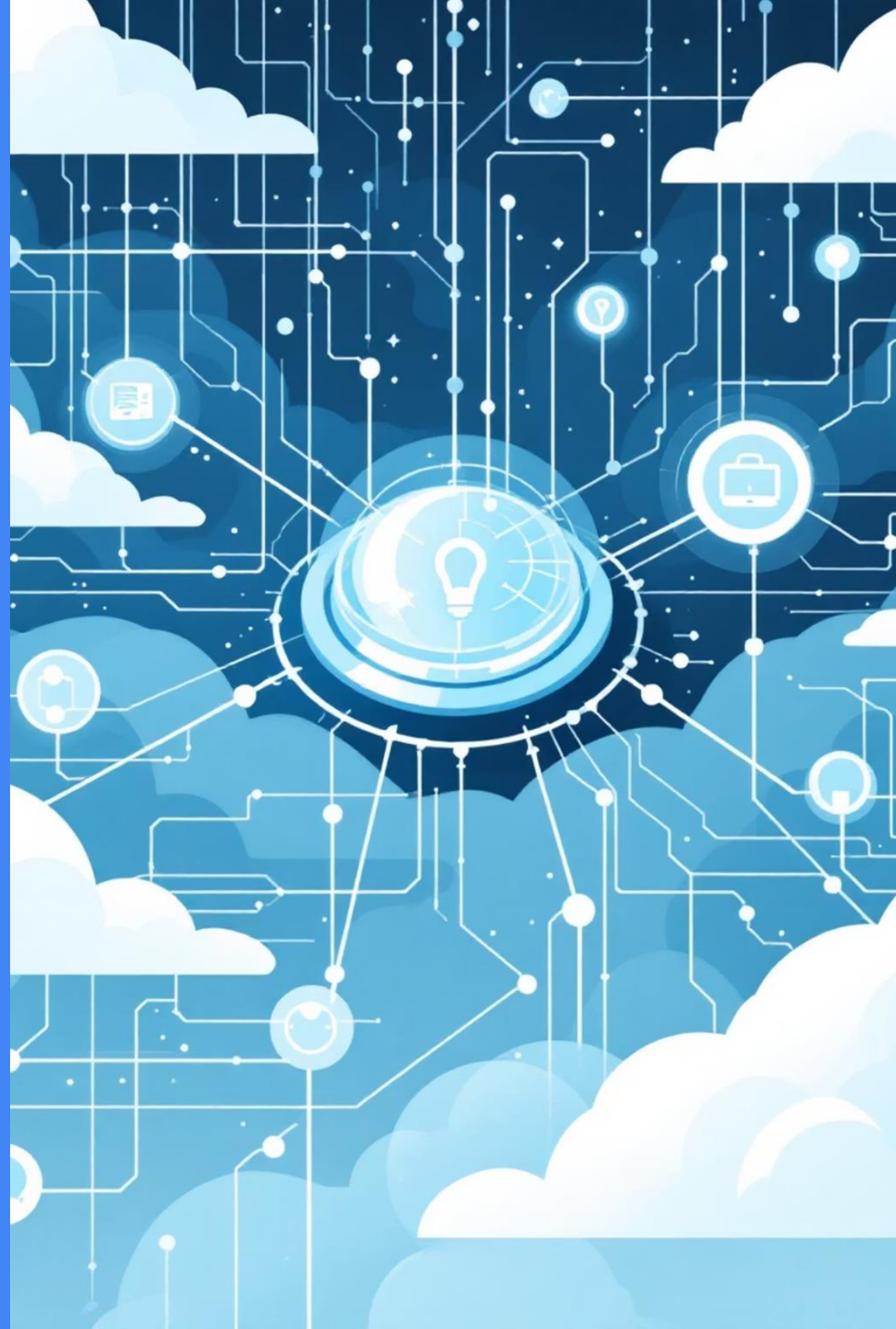
CiN Subcomisión de Ciberseguridad
Comisión de Conectividad y Sistemas de Información

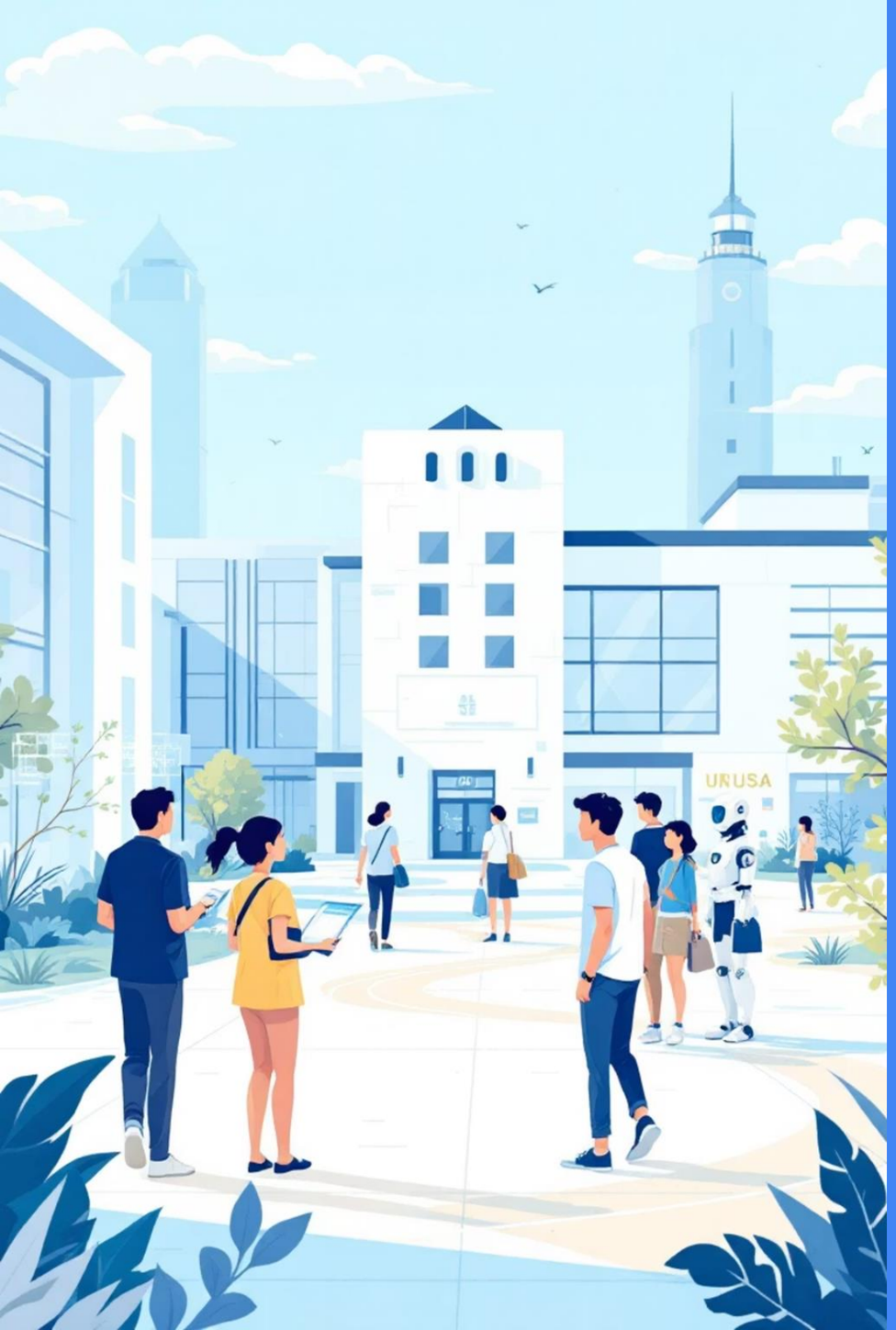
Gobernanza de la Gestión de la Ciberseguridad.Desafíos 2025



El Contexto Crítico de 2025

Las amenazas alcanzan una sofisticación sin precedentes: **uso malicioso de IA, agentes autónomos, ataques estatales dirigidos y vulnerabilidades en cadenas de suministro**.

La gobernanza de ciberseguridad trasciende las herramientas técnicas: exige **coordinación estratégica de responsabilidades, cultura y resiliencia institucional.**



Entornos Institucionales en Transformación

Modelos Híbridos

Migración hacia arquitecturas on-premise + nube + servicios colaborativos que multiplican superficies de ataque

Interconectividad

Redes académicas, colaboraciones internacionales y plataformas compartidas crean ecosistemas complejos

Asunto Estratégico

La seguridad no es solo técnica: requiere alineamiento, incentivos, cultura organizacional y capacidad de respuesta

¿Qué es la Gobernanza de Ciberseguridad?

> El conjunto de estructuras, procesos, reglas, roles, métricas y cultura que permiten gestionar estratégicamente los riesgos y capacidades de ciberseguridad, alineados con la misión institucional y marcos regulatorios externos.

Estructuras

Quién decide qué y cómo se rinde cuentas

Procesos

Priorización de riesgos y evaluación continua

Coordinación

Articulación entre TI, seguridad, gobierno y cumplimiento

Desafíos

01

Gestión Integrada de Identidades

La difuminación entre identidades humanas y no humanas

02

Riesgo en Cadenas de Valor

Gobernanza de proveedores y ecosistemas digitales

03

Inteligencia Artificial y Agentes

Tecnologías emergentes y sus implicaciones de seguridad

04

Adaptación Normativa

Velocidad de respuesta y coordinación interinstitucional

01. Identidades Humanas y No Humanas

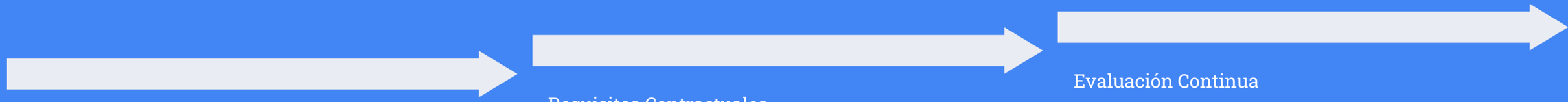
El Reto de la Difuminación

En 2025, la identidad trasciende las personas. Los sistemas operan con agentes autónomos, microservicios, dispositivos IoT, APIs automatizadas y contenedores que actúan "en nombre de" la institución.

Esta **convergencia humano-máquina** crea vectores de ataque inéditos y exige marcos unificados de control. Las investigaciones recientes proponen modelos de gobernanza que no segmentan rígidamente, sino que evalúan el riesgo a lo largo de todo el ciclo de vida.

Muchas instituciones tratan los accesos máquina como "delegaciones libres" sin supervisión sistemática ni auditoría periódica

02. Riesgo en Cadenas de Proveedores



Clasificación de Riesgo

Categorizar proveedores según criticidad e impacto potencial (alto/medio/bajo)

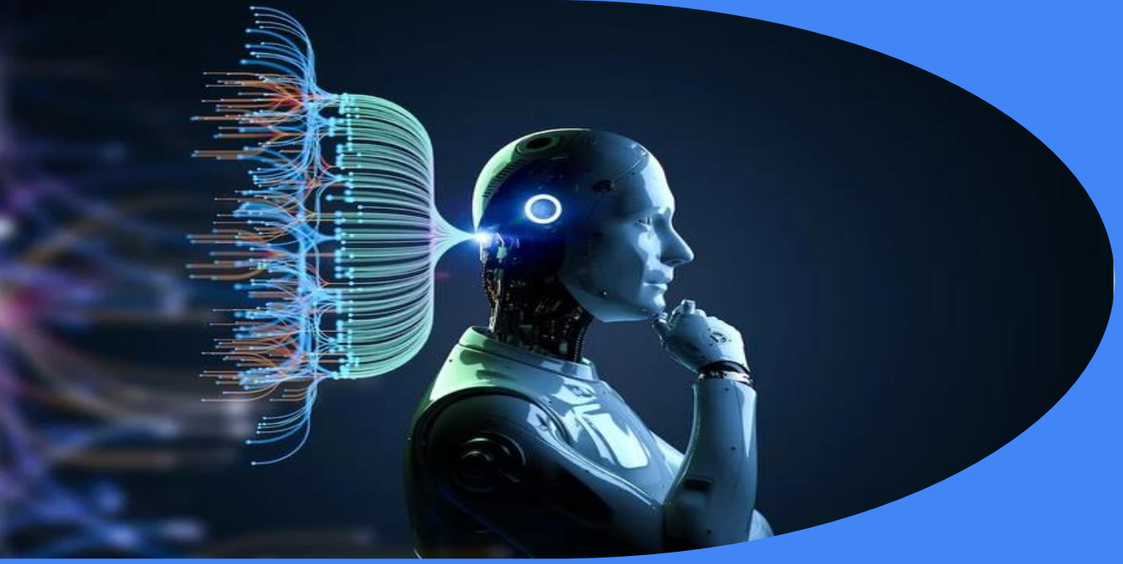
Requisitos Contractuales

Cláusulas de seguridad, derecho de auditoría y planes de continuidad obligatorios

Evaluación Continua

Certificaciones, auditorías periódicas y monitoreo de incidentes en terceros

En 2025, los ataques a terceros y proveedores se consolidan como uno de los vectores más explotados. Un eslabón débil en la cadena puede comprometer a toda la institución.



03. IA y Tecnologías Emergentes

La Nueva Frontera del Riesgo

Política Institucional

Definir usos permitidos, controles obligatorios y niveles de supervisión para sistemas de IA

Comité Interdisciplinario

Integrar TI, seguridad, ética y legal para revisar proyectos antes de su adopción

Monitoreo y Control

Definir alertas, trazabilidad de decisiones y mecanismos de "kill switch" para agentes

Capacitación Específica

Formar al personal en riesgos particulares de IA y estrategias de mitigación

Pregunta crítica: ¿Quién responde cuando un agente autónomo genera comportamiento indebido o toma decisiones erróneas con impacto institucional?

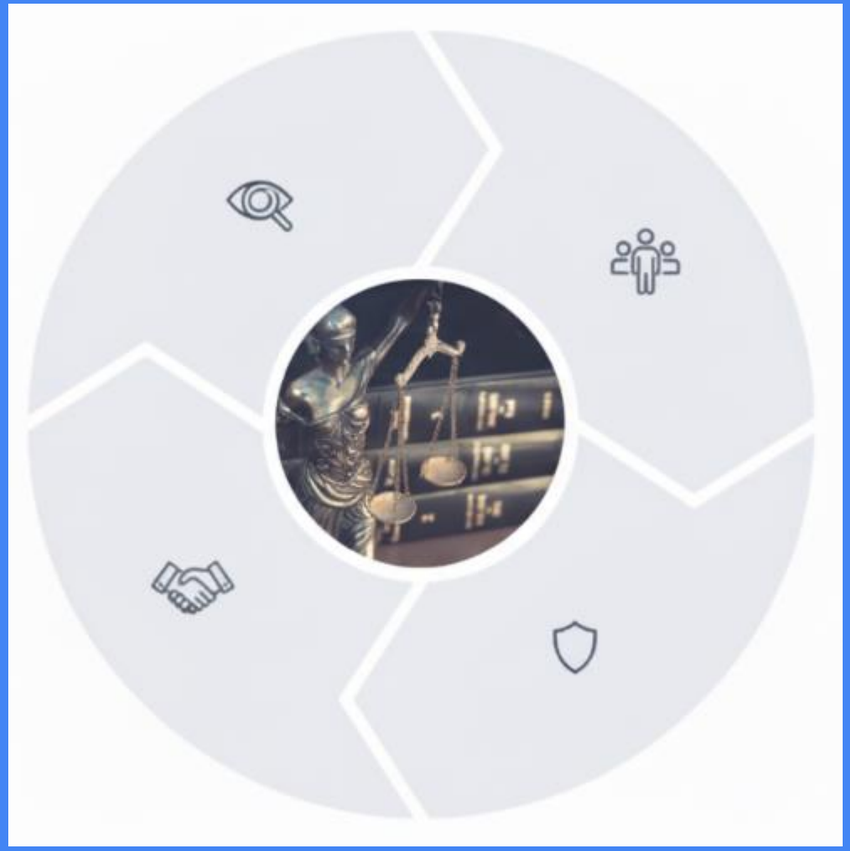
04.Adaptación Normativa y Coordinación

Vigilancia Normativa

Monitoreo continuo de nuevas leyes, estándares y marcos emergentes

Alianzas Estratégicas

Compartir políticas modelo y experiencias entre instituciones



Participación Activa

Foros nacionales e internacionales de armonización normativa

Resiliencia Normativa

Anticipación de escenarios de cambio legal y preparación institucional

Métricas y Transparencia Institucional

El Déficit de Medición

Definición de KPIs

Establecer indicadores clave alineados con riesgo institucional

1

Monitoreo Continuo

Dashboards en tiempo real y seguimiento sistemático

2

Auditoría Externa

Evaluaciones independientes y certificaciones sectoriales

3

Reporte Anual

Informe de ciberseguridad para stakeholders institucionales

4

Indicadores Esenciales

- Cantidad y severidad de incidentes
- Tiempo medio de detección (MTTD)
- Tiempo medio de respuesta (MTTR)
- Porcentaje de sistemas actualizados
- Vulnerabilidades críticas sin remediar

Recomendaciones:

- Comité estratégico
- Desarrollar una estrategia de ciberseguridad institutional
- Adoptar marcos reconocidos
- Métricas e indicadores
- Promover la cultura de la seguridad y la corresponsabilidad
- Auditorías y ejercicios de prueba continuos
- Colaboración institucional y compartición de inteligencia
- Procesos de mejora continua

En síntesis:

La gobernanza de ciberseguridad en 2025 exige visión estratégica, compromiso institucional y colaboración sostenida. Estos cinco desafíos no son problemas técnicos aislados: representan transformaciones sistémicas que definirán la resiliencia de nuestras instituciones.

Desde la Subcomisión de Ciberseguridad, los invitamos a **profundizar el trabajo colaborativo**, compartir experiencias y construir juntos un ecosistema más seguro, transparente y preparado para el futuro.

Muchas Gracias

Nestor Gareis
Analía Barberio

Subcociberseg@campus.ungs.edu.ar

CiN
Subcomisión de Ciberseguridad
Comisión de Conectividad
y Sistemas de Información