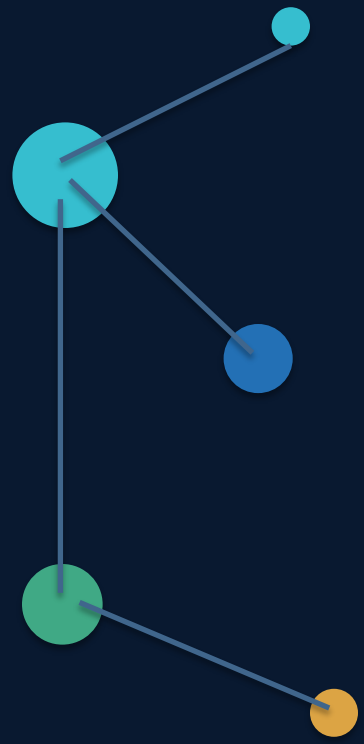
ENCUENTRO DE CISOs UNIVERSITARIOS

De la estrategia a la colaboración



Construyendo ciberseguridad universitaria desde la experiencia UCN

GOBIERNO | CAPACIDADES | QUICK WINS | REUNA | HOJA DE RUTA

Francisco Javier Gutiérrez
Especialista en Seguridad de la Información y Ciberseguridad
UCN
Noviembre 2026 | Experiencia institucional

CC BY

Complejidad del ecosistema universitario

Cuatro condiciones que hacen particular la gestión de ciberseguridad en educación superior.

Ecosistema abierto

Docencia, investigación, estudiantes, académicos y proveedores externos.

Diversidad tecnológica

Plataformas heterogéneas, sistemas heredados y nuevas soluciones en la nube.

Información valiosa

Datos personales, propiedad intelectual de I+D y servicios críticos institucionales.

Exposición creciente

Servicios web públicos, identidades digitales federadas y trabajo remoto.

Principio guía: la ciberseguridad debe habilitar la misión universitaria, no convertirse en un obstáculo.

Sostenibilidad con recursos limitados

La pregunta central trasciende la compra de tecnología aislada: exige un modelo de madurez progresivo.

Gobierno

Políticas, gestión de riesgos y decisiones institucionales.

Capacidades

Personas, procesos, tecnología y respuesta a incidentes.

Colaboración

Herramientas compartidas y coordinación interuniversitaria.

¿Cómo construimos capacidades sostenibles cuando los recursos son limitados?

De la operación a la función institucional

Desafíos estratégicos priorizados y una filosofía de ejecución gradual.

- Gobierno claro: fortalecer responsabilidades e institucionalidad.
- Visibilidad activa: monitorear la exposición externa real.
- Consolidación de controles: cobertura en endpoints, redes y web.
- Formalización operativa: ordenar políticas y respuesta a incidentes.
- Priorización fuerte: ejecutar según riesgo y capacidad real.

Principio de madurez gradual

No intentar resolver todo al mismo tiempo: establecer una línea base sólida, priorizar riesgos relevantes y avanzar por etapas medibles.

La madurez se construye progresivamente.

Evolución estratégica del rol del CISO

El CISO no debe limitarse a la administración de herramientas: debe impulsar gobierno, coordinación y mejora continua.

ESTADO INICIAL

Operación reactiva

Atender alertas puntuales y responder a requerimientos técnicos inmediatos.

Enfoque en herramienta

TRANSICIÓN UCN

Gestión de riesgo

Priorizar riesgos, formalizar responsabilidades y medir efectividad de controles.

Enfoque en proceso

META ESTRATÉGICA

Gobierno integrado

Integrar la ciberseguridad directamente en las decisiones y procesos institucionales.

Enfoque en estrategia

Quick wins: avances institucionales de alto impacto

Reglas claras, responsabilidades y trazabilidad sin depender exclusivamente de nuevas inversiones.

APROBADO

Reglamento RIOHS

Incorporación de materias de ciberseguridad en el Reglamento Interno de Orden, Higiene y Seguridad.

Responsabilidades claras

PRÓXIMO COMITÉ

Política PUA

Revisión integral de la Política de Uso Aceptable. Actualiza reglas sobre recursos tecnológicos y compromisos de usuarios.

Marco normativo al día

IMPLEMENTADO

Política de correo

Protección del correo institucional: suplantación, phishing, tratamiento de datos y protocolos de reporte.

Mitigación de phishing

Estrategia organizada por capacidades

Conectar iniciativas técnicas y operativas con objetivos de gobierno e infraestructura resiliente.

Gobierno

SGSI, políticas, análisis de riesgos y cumplimiento.

Personas

Cultura, concientización y programa KnowBe4.

Visibilidad

Evaluación continua mediante EduScan y EduScore.

Protección

EDR/MDR, WAF, hardening de servidores y nube.

Respuesta

Gestión de incidentes, coordinación y recuperación.

Mejora

Indicadores, pruebas técnicas y revisión continua.

El plan conecta iniciativas técnicas operativas con objetivos de gobierno y resiliencia.

Conocer nuestra exposición digital real

EduScan y EduScore han permitido visibilizar aspectos que antes permanecían fuera del radar operativo.

Desafío histórico

Falta de visibilidad sobre qué activos estaban expuestos a Internet y cuál era su postura de seguridad.

- Identificar activos e IP visibles desde Internet.
- Obtener señales para priorizar vulnerabilidades.
- Asignar hallazgos a responsables directos.
- Medir la evolución temporal de la postura.

EduScan

Diagnóstico continuo y evaluación objetiva de la exposición digital pública.

EduScore

Métricas para seguir la madurez y postura de riesgo global.

REUNA: socio estratégico de capacidades

Reducir brechas operativas y acelerar el desarrollo de capacidades institucionales.

Herramientas compartidas

Acceso estructurado a servicios especializados como EduScan, EduScore y plataformas de concientización como KnowBe4.

Conocimiento técnico

Intercambio de buenas prácticas, criterios normativos, lecciones aprendidas y arquitecturas de referencia.

Red de apoyo mutuo

Articulación comunitaria para afrontar amenazas comunes mediante aprendizaje colectivo y coordinación continua.

REUNA permite reducir brechas y acelerar el desarrollo de capacidades institucionales.

Integración de REUNA en la estrategia UCN

Vincular los servicios y la colaboración con capacidades concretas.

PERSONAS	Capacitación continua y cultura de seguridad mediante KnowBe4.	CULTURA
VISIBILIDAD	Diagnóstico externo y monitoreo constante con EduScan y EduScore.	DIAGNÓSTICO
PREVENCIÓN	Priorización efectiva de vulnerabilidades y buenas prácticas de hardening.	MITIGACIÓN
RESPUESTA	Intercambio oportuno de información y coordinación ante incidentes.	COORDINACIÓN
RESILIENCIA	Ejercicios conjuntos, aprendizaje continuo y fortalecimiento interuniversitario.	COMUNIDAD

El desafío de los recursos: competir vs. colaborar

La colaboración no reemplaza la responsabilidad institucional; permite ejercerla con mejores capacidades y eficiencia.

Brecha de inversión

USD 3,1M en empresa relacionada con el litio
USD 10M en banco asociado a la teletón

Frente a capacidades presupuestarias acotadas en la mayoría de las universidades, se nos hace imposible competir

Respuesta estratégica institucional

Priorizar con criterio de riesgo
No intentar replicar individualmente todas las arquitecturas del mercado.

Compartir servicios y economías de escala
Maximizar el valor de convenios marco y plataformas colaborativas.

Roadmap WAF: de la visibilidad a la protección

Secuencia progresiva para pasar del inventario a una operación continua.

01 Inventariar

Dominios, apps, IP, responsables y criticidad.

02 Diseñar

Arquitectura, DNS, SSL y continuidad.

03 Pilotear

Aplicación prioritaria en modo observación.

04 Afinar

Reglas, falsos positivos y excepciones.

05 Proteger

Bloqueo activo y despliegue masivo.

06 Operar

Monitoreo, reportes y tuning continuo.

Éxito WAF = cobertura crítica + reglas afinadas + operación continua

Hoja de ruta institucional | Horizonte de 18 meses

Plan adaptable a disponibilidad presupuestaria, evaluación continua de riesgos y capacidad operativa real.

Meses 01–04

Gobierno y diagnóstico

RIOHS, PUA, política de correo, inventario de activos, análisis de riesgos y visibilidad EduScan.

ETAPA 1

Meses 05–09

Protección operativa

Despliegue de WAF, consolidación EDR/MDR, hardening de servidores y remediación de vulnerabilidades.

ETAPA 2

Meses 10–14

Detección y respuesta

Protocolos formales de incidentes, monitoreo continuo y ejercicios de simulación con REUNA.

ETAPA 3

Meses 15–18

Madurez e indicadores

Métricas SGSI, pentesting continuo, retest técnico y consolidación de la cultura de seguridad.

ETAPA 4

Aprendizajes desde la experiencia UCN

Cinco principios para que la estrategia se convierta en práctica institucional.

PRIORIZAR

No todo puede abordarse simultáneamente.

FORMALIZAR

Las políticas habilitan la adopción tecnológica.

MEDIR

La visibilidad debe traducirse en acciones concretas.

COLABORAR

Las capacidades compartidas reducen brechas.

SOSTENER

Cada iniciativa requiere responsables y operación.

La estrategia no es un documento estático: es una práctica institucional viva en constante revisión.

REFLEXIÓN FINAL

La ciberseguridad universitaria se construye en comunidad.

Gobierno, personas, procesos y tecnología deben avanzar juntos. La colaboración permite que las instituciones fortalezcan sus capacidades sin tener que construirlo todo desde cero.

De la estrategia a la colaboración: una responsabilidad compartida.

Experiencia UCN · REUNA · Encuentro de CISOs Universitarios 2026

Descarga la presentación desde aquí
https://repositorio.ucn.cl/handle/20.500.14729/10338