DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

ESTRATEGIA DE CIBERSEGURIDAD

DR. HÉCTOR BENÍTEZ PÉREZ

INTRODUCCIÓN

La ciberseguridad es una función esencial para la protección de los recursos digitales. En un contexto de amenazas cada vez más sofisticadas, la UNAM busca consolidar un modelo estratégico que le permita responder eficazmente a incidentes y, más aún, prevenirlos. Esta estrategia se fundamenta en un enfoque estructurado, colaborativo y escalable.

UNAM-CERT

Las actividades del **UNAM-CERT** en materia de ciberseguridad se estructuran en dos grandes categorías:

1

Las **actividades preventivas** están a cargo del Departamento de Seguridad en Sistemas, el cual ofrece servicios como las revisiones de seguridad. Estas revisiones se apoyan en marcos de referencia ampliamente reconocidos, como el **OWASP Top 10**, para identificar vulnerabilidades en activos tecnológicos.

2

Por otro lado, las **actividades correctivas** son responsabilidad del Departamento de Respuesta a Incidentes. Este área sigue estándares internacionales como el **NIST SP 800-61** para gestionar incidentes de ciberseguridad mediante la detección, análisis, contención y recomendaciones a las dependencias universitarias.

Esta estructura garantiza un enfoque integral que combina prevención, detección, respuesta y recuperación.

Estrategia:

¿HACIA DÓNDE VAMOS?

La estrategia de ciberseguridad debe evolucionar con base en:

Diversidad tecnológica:
Aunque lo ideal sería ofrecer servicios para todo tipo de tecnologías (lenguajes, sistemas operativos, arquitecturas, etc.), es necesario priorizar las tecnologías más adoptadas por la organización.

Enfoque práctico:
Esto exige un monitoreo constante de las tendencias tecnológicas y su impacto en el entorno institucional.

Limitantes reales:
Factores como el presupuesto y los recursos humanos disponibles obligan a delimitar los alcances, especializar funciones y optimizar los servicios con base en prioridades.

LIMITANTES

La implementación plena de una estrategia de ciberseguridad se ve limitada por factores como la disponibilidad de personal capacitado, los recursos presupuestales y las funciones delimitadas de cada área. Esto obliga a definir prioridades y ajustar el alcance de los servicios de manera racional y efectiva.

POLÍTICA, ALCANCES Y SISTEMA FEDERADO

Para garantizar un servicio eficiente y seguro es necesario establecer:

Políticas de uso aceptable:

Claras y específicas para cada tipo de servicio tecnológico, especialmente en el ámbito de la ciberseguridad.

Alcances definidos:

Por ejemplo, si el enfoque de los servicios es web, debe existir una política que limite la exposición a este tipo de tecnologías exclusivamente.

Modelo federado:

Algunas tecnologías específicas pueden requerir un esquema de responsabilidades compartidas con terceros especializados, particularmente cuando exceden la capacidad institucional.

APRENDIZAJE, RECURSOS Y CAPACITACIÓN

La rápida evolución tecnológica implica:

Una necesidad constante de **capacitación técnica** del personal en ciberseguridad.

Flexibilidad institucional para permitir la adquisición de habilidades nuevas relacionadas con amenazas emergentes.

Evaluaciones regulares del **software, hardware y talento humano** necesarios para operar con eficiencia.

PERÍMETROS DE SEGURIDAD Y SUPERFICIES DE EXPOSICIÓN

La definición de **perímetros de seguridad** debe basarse en el análisis de riesgos y no únicamente en criterios tecnológicos.

Ejemplos:

Aulas vs. áreas administrativas: distintas necesidades y riesgos.

Centros de investigación: protección reforzada por la sensibilidad de la información.

Una correcta **segmentación de redes y servicios** por tipo de actividad o sensibilidad de los datos es clave para reducir la superficie de ataque.

DEFINICIÓN DE ALCANCES EN SEGURIDAD

Para definir alcances concretos se debe:

01

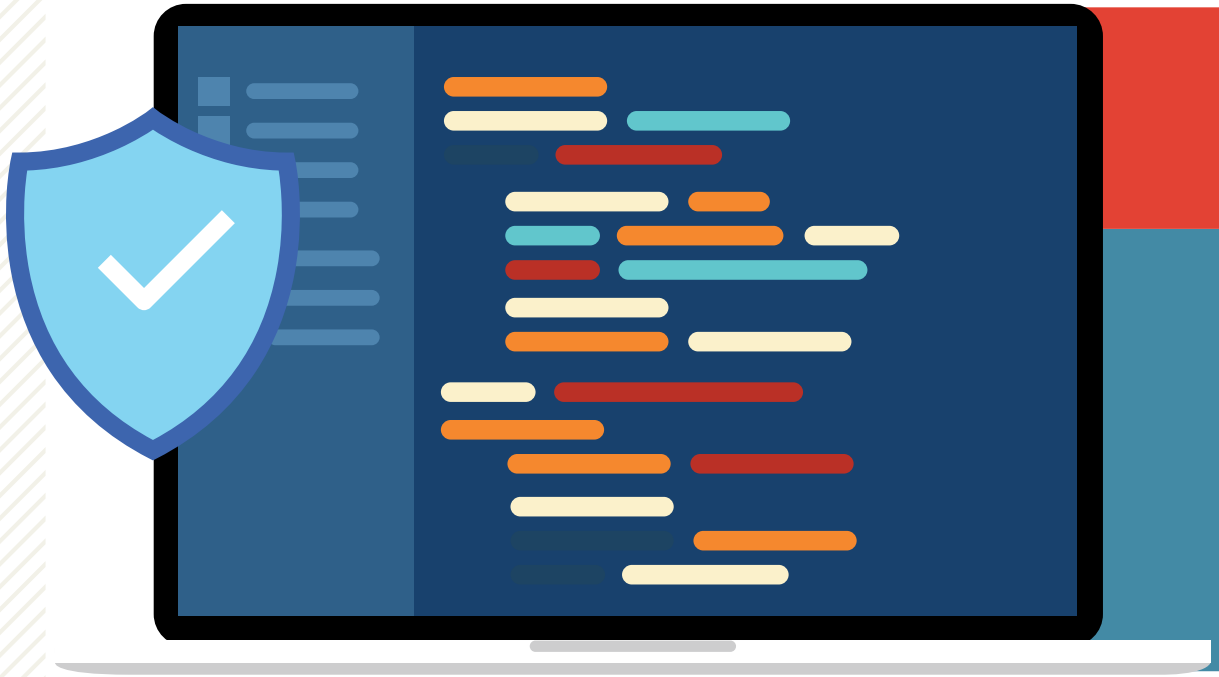
Priorizar los servicios según el **riesgo asociado**.

02

Establecer criterios de escalamiento y colaboración con terceros.

03

Identificar qué áreas deben estar bajo vigilancia directa de ciberseguridad.



CASOS ESPECIALES

Cuando se presenten tecnologías poco comunes o necesidades fuera del ámbito de especialización del CERT, se debe considerar la transferencia de riesgo o la colaboración con terceros especializados. Esta práctica permite garantizar calidad sin comprometer los recursos internos.

SEGURIDAD DISTRIBUIDA

La ciberseguridad no puede centralizarse por completo:

- **Ataques laterales** son comunes; un activo aparentemente no crítico puede servir como puerta de entrada.
- Las personas fuera del área de TI suelen ser el eslabón más débil (ingeniería social, phishing, etc.).
- Es necesario fomentar una **cultura organizacional de seguridad** compartida.

GARANTIZAR LA SEGURIDAD: POLÍTICAS Y LINEAMIENTOS

La implementación de políticas debe basarse en marcos reconocidos internacionalmente como:

- **ISO/IEC 27001**
- **NIST Cybersecurity Framework**
- **CIS Controls**
- Aunque ninguna política garantiza inmunidad frente a incidentes, su implementación fortalece la **resiliencia institucional** mediante la mejora continua.

ESCALA DE SEGURIDAD EN REDES Y SOFTWARE

La ciberseguridad debe escalar según:

El tamaño y criticidad de los sistemas.

La exposición a internet o redes abiertas.

El volumen de información manejada.

Se debe promover una infraestructura adaptable que permita reforzar controles conforme crecen las amenazas o los activos.

DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

GRACIAS