EVOLUCIÓN DE LA CIBERSEGURIDAD EN LAS IES DE MÉXICO

ANUIES
Asociación Nacional de Universidades e Instituciones de Educación Superior

ANUIES - TIC

metaredTIC Mx
by universia

Evolución de la Ciberseguridad en las IES de México

2025

ANUIES
ASOCIACIÓN NACIONAL DE UNIVERSIDADES
E INSTITUCIONES DE EDUCACIÓN SUPERIOR

Luis Armando González Placencia
Secretario General Ejecutivo

Gustavo Rodolfo Cruz Chávez
Coordinador General de Vinculación Estratégica

Luis Alberto Fierro Ramírez
Coordinador General de Fortalecimiento Académico
e Institucional

Irma Andrade Herrera
Coordinadora General de Planeación y Buena
Gestión

Evolución de la Ciberseguridad en las IES de México

2025

ANUIES

Coordinadores de obra
Héctor Bonola Virués

Coordinadores de contenido
Héctor Bonola Virués

Autores
Julia Bernuy Sánchez
Gloria Jokebed Vazquez Hernández
Rigo Daniel Salazar Falfán
Ricardo Gutierrez Alvarado
Eugenio Valle Landa
Juan José López Ávila
Héctor Bonola Virués

Diseño y formación editorial
Fabiola Herrera Neri

Diseño de gráficas y tablas
Fabiola Herrera Neri

Corrección de estilo:
Eugenio Valle Landa
Juan José López Ávila

Para citar la obra:

Bonola-Virués, H., (Coords.). (2025). Ciberseguridad en las Instituciones de Educación Superior. México: Asociación Nacional de Universidades e Instituciones de Educación Superior.

Para citar un capítulo de la obra:

Apellido 1 Apellido 2, A.A. y Apellido 1 Apellido 2, B.B.(2025). Título del capítulo o entrada. Bonola-Virués, H., (Coords.), Ciberseguridad en las Instituciones de Educación Superior. México: Asociación Nacional de Universidades e Instituciones de Educación Superior.

DIRECTORIO ANUIES

Luis Armando González Placencia
Secretario General Ejecutivo

Gustavo Rodolfo Cruz Chávez
Coordinador General de Vinculación Estratégica

Luis Alberto Fierro Ramírez
Coordinador General de Fortalecimiento Académico e Institucional

Irma Andrade Herrera

Coordinadora General de Planeación y Buena Gestión

DIRECTORIO COMITÉ ANUIES-TIC

Coordinador
Dr. Herik Germán Valles Baca
Director Ejecutivo de Innovación Académica, ANUIES

Secretarías Técnicas del Comité
Froylán López Valencia
Jefe de Departamento, DTI, ANUIES

Adrián Soto Girón
Jefe de Unidad, DTI, ANUIES

Grupo de Trabajo: Gobierno de TIC

Coordinadoras
Luz María Castañeda de León
Universidad Nacional Autónoma de México (DGTIC)

Alejandra Herrera Mendoza
Universidad Iberoamericana

Integrantes / Secretarías Técnicas
Carlos Alberto Franco Reboreda
Universidad de Guadalajara

Carmen H. de Jesús Díaz Novelo
Gobierno del Estado de Yucatán

Grupo de Trabajo: Seguridad de la Información

Coordinador
Héctor Bonola Virués
DGTI, Universidad Veracruzana

Secretarías Técnicas / Integrantes
Wilberth de Jesús Pérez Segura
Universidad Autónoma de Yucatán

Gloria Jokebed Vázquez Hernández
Universidad Autónoma del Estado de México

José Gabriel Aguilar Martínez
Universidad Autónoma Metropolitana

Ricardo Gutiérrez Alvarado
Universdidad Autónoma de Guadalajara

Israel Josué Novelo Zel
Universidad Autónoma de Yucatán

Rigo Daniel Salazar Falfán
Universidad Veracruzana

Grupo de Trabajo: Gestión Interinstitucional y Proveedores de TIC

Coordinador
Erick Yesser Rodríguez Arreola
Jefe del CERT, Universidad Autónoma de Chihuahua

Secretario Técnico
Noel Hortiales Corona
Subdirector de Cómputo y Software, Universidad Autónoma de Nuevo León

Grupo de Trabajo: Gestión de la Tecnología Educativa

Coordinadora
Claudia Marina Vicario Solórzano
Instituo Politécnico Nacional

Secretario Técnico
Víctor Álvarez Castorela
Universidad Pedagógica Nacional

Red de Mujeres en TIC

Coordinadora
Erika Sánchez Chablé
Universidad Autónoma de Campeche

Secretarías Técnicas
Beatriz Veliz Plascencia
Universidad de Guadalajara

María Guadalupe Cid Escobedo
Universidad de Guadalajara

Administración Electrónica

Coordinador
Jesús A. Nevárez Aceves
Universidad Autónoma de Coahuila

Secretaria Técnica
Erika Sánchez Chablé
Universidad Autónoma de Campeche

Colaboración para el Desarrollo de Internet en las IES

Coordinadora
María del Carmen Denis Polanco
IXY Internet Exchange Point Yucatán

Secretarías Técnicas
Eunice Alejandra Pérez Coello
Instituto Tecnológico de Mérida

José Manuel Ponce López
ANUIES

Inteligencia Artificial en la Educación Superior

Coordinadores

Carmen H. de Jesús Díaz Novelo
Gobierno del Estado de Yucatán

Francisco Hiram Calvo Castro
CIC, Instituto Politécnico Nacional

Secretario Técnico

Adrián Soto Girón
ANUIES

Vocales

Marcela Peñaloza Báez
Universidad Nacional Autónoma de México (DGTIC)

Ana Yuri Ramírez Molina
Universidad Nacional Autónoma de México (DGTIC)

María de Lourdes Velázquez Pastrana
Universidad Nacional Autónoma de México (DGTIC)

Gerardo Elías Navarrete Terán
Experto en TIC en ES

Carlos Alberto Castañeda González
Universidad de Guadalajara

Pablo Arturo Rentería Villaseñor
Universidad de Guadalajara

Elizabeth Velázquez Herrera
Universidad Autónoma de Nuevo León

Raúl Arturo Peralta
Universidad Autónoma de Campeche

Lizbeth Angélica Barreto Zúñiga
Universidad Nacional Autónoma de México (DGTIC)

Juan Manuel Arciniega Díaz
Especialista en proyectos educativos

Isabel García Ortiz
Universidad Juárez Autónoma de Tabasco

María Dacia González Cruz
Universidad Veracruzana

Raúl González López
Universidad de las Américas Puebla

Angélica Gómez Morales
Universidad Autónoma de Campeche

Emmanuel Serrano Piña
Universidad Autónoma de Yucatán

Edgar Liborio Morales
Tecnológico de Estudios Superiores de Ecatepec

Jesús Félix Martínez Mireles
Universidad Autónoma de Coahuila

Flavio Herrera Ramos
Universidad de Guanajuato

Julia Bernuy Sánchez
Universidad Nacional Autónoma de México

Jesús Cortés Hernández
Universidad Autónoma de Nuevo León

Rosalina Vázquez Tapia
Universidad Autónoma de San Luis Potosí

Antonio Felipe Razo Rodríguez
Universidad de las Américas Puebla

Rosario Lucero Cavazos Salazar
Universidad Autónoma de Nuevo León

María Luisa Zorrilla Abascal
Universidad Autónoma del Estado de Morelos

Colaboradores especiales

Héctor Benítez Pérez
Universidad Nacional Autónoma de México (DGTIC)

Mario Alberto González De León
Universidad Autónoma de Nuevo León

Mónico Payán Bustillos
Universidad Autónoma de Chihuahua

Max Ulises De Mendizábal Carrillo
Universidad Nacional Autónoma de México

Raúl Rivera Rodríguez
Centro de Investigación Científica y de Educación Superior de Ensenada, Baja California

Sergio Antonio Cervera Loeza
Universidad Autónoma de Yucatán

Carlos Luna Ortega
Universidad Autónoma Metropolitana

Iliana Flores Estrada
Universidad Autónoma Metropolitana

Lidia Elena Gómez Velasco
Centro de Investigación Científica y de Educación Superior de Ensenada, Baja California

PRÓLOGO

La ciberseguridad se ha consolidado como uno de los pilares fundamentales para asegurar la continuidad académica, la investigación y la gestión universitaria en las Instituciones de Educación Superior (IES). En un entorno donde los datos, el conocimiento y la innovación se han convertido en activos estratégicos, protegerlos no es únicamente una cuestión técnica, sino un compromiso colectivo que involucra a toda la comunidad universitaria.

En Iberoamérica, las universidades comparten desafíos comunes: presupuestos limitados, creciente exposición a amenazas digitales, déficit de personal especializado y la necesidad urgente de construir una cultura sólida de ciberseguridad. Sin embargo, también comparten una gran fortaleza: la colaboración. Es precisamente este espíritu colaborativo el que ha dado origen a MetaRed TIC, la mayor red de redes que articula a más de 1.600 instituciones en 15 países, y que ha permitido que los responsables de las áreas de tecnología trabajen de manera conjunta, compartiendo experiencias, buenas prácticas y soluciones para hacer frente a los riesgos del mundo digital.

México, con la diversidad y riqueza de sus IES, tiene un papel clave en esta construcción colectiva. La generación de conocimiento y la formación de talento en materia de ciberseguridad que se impulsa desde sus universidades no solo fortalece al país, sino que también enriquece la respuesta iberoamericana frente a un panorama global cada vez más complejo. Desde MetaRed, hemos comprobado que los ciberataques no entienden de fronteras, y por ello la cooperación internacional es la mejor herramienta para enfrentarlos.

Este informe refleja no solo un diagnóstico riguroso de la situación de la ciberseguridad en las IES de México, sino también una invitación a la acción: a seguir sumando esfuerzos, a fortalecer los equipos de respuesta, a innovar en la formación de profesionales y a consolidar espacios de confianza donde compartir lecciones aprendidas. La ciberseguridad universitaria no puede abordarse de manera aislada; requiere de la unión de voces, experiencias y compromisos que nos permitan construir un ecosistema más resiliente, inclusivo y sostenible.

Desde MetaRed TIC reiteramos nuestra convicción: la colaboración iberoamericana es el camino para garantizar que la educación superior avance con seguridad hacia la transformación digital. Invitamos a todas las instituciones a sumarse activamente a esta misión común, porque solo juntos podremos proteger lo más valioso que tenemos: el conocimiento.

Jesús Martínez Martínez
Coordinador GTI Ciberseguridad MetaRed

Índice

INTRODUCCIÓN

La información se ha convertido en uno de los recursos más valiosos para toda organización, y por consecuencia, los volúmenes de esta y la complejidad en su estructuración, han colocado a las Instituciones de Educación Superior (IES) ante un reto sumamente alto. La aceleración que ha tenido la transformación digital para los procesos docentes, de investigación y de gestión administrativa dependen de entornos digitales cada vez más interconectados y de gran capacidad. Esto ha provocado que la superficie de ataque de las amenazas como ransomware, denegación de servicio, malware, entre otros, haya crecido exponencialmente y hoy día, demos cuenta de afectaciones a las IES de todo el mundo, quienes han visto afectada su operación y su continuidad.

En este contexto, la seguridad de la información cobra un papel fundamental para el gobierno de las tecnologías de información y comunicación en las Instituciones de Educación Superior. Proteger la confidencialidad, integridad y disponibilidad de la información requiere de un compromiso institucional, un liderazgo consciente de estos riesgos y de la participación de todas las áreas. Para ello, marcos de referencia como la familia ISO 27000, NIST CSF y Controles CIS, son algunas de las metodologías que, con su implementación, podrían ayudar a generar un ecosistema más resiliente en las IES de México y del mundo.

La evolución de las amenazas y los retos que se enfrentan las IES genera un ambiente complejo y difícil de abordar; no obstante, las fortalezas de su vocación y la difusión del conocimiento, pueden ser las semillas para la generación de talento y recursos que permitan proteger las infraestructuras de las IES.

La presente publicación ofrece una visión de la evolución de la ciberseguridad en las IES de México en los últimos años, donde el Grupo de Seguridad de la Información de la ANUIES-TIC ha trabajado en la generación de una cultura de ciberseguridad y resiliencia, basada en la colaboración y vinculación entre los diferentes actores dentro de este ámbito. Por lo que este documento busca presentar los retos a los que se enfrentan las IES y propone aspectos relevantes a considerar para proteger sus entornos digitales.

Importancia de la Seguridad de la Información en las IES de México

01. Importancia de la Seguridad de la Información en las IES de México

Introducción

Los diversos cambios que se han presentado por el constante desarrollo tecnológico, el rápido crecimiento de la globalización y la evolución del cómputo, en particular en las tecnologías de la información y comunicación (TIC) durante la última década, han cambiado la forma en que los seres humanos interactuamos con nuestro entorno. Las computadoras y la conectividad en red no solo han modificado estás interacciones, sino que también han incrementado nuestra dependencia de dichas tecnologías e información, dando como resultado, el uso de dispositivos en nuestras actividades diarias, tanto en organizaciones, empresas, negocios e instituciones educativas, entre otros.

Sin embargo, está dependencia y uso de las tecnologías, directa o indirectamente, ha traído diversos retos. El generar datos sobre las actividades de diversos ámbitos, entre ellas, las laborables y las personales, ha implicado riesgos en relación a la protección de toda la información que se genera. Para ello, la seguridad de la información ha surgido como un elemento importante para resguardarla.

La seguridad de la información se refiere al conjunto de medidas, políticas y controles orientados a proteger la confidencialidad, integridad y disponibilidad de los datos, tanto en tránsito como en reposo, frente a accesos no autorizados, alteraciones o pérdidas . Su objetivo principal es garantizar que la información sea accesible solo por quienes están autorizados, se mantenga completa y esté disponible cuando se requiera.[1]

Según la Asociación Nacional de Instituciones de Educación Superior (ANUIES), la educación superior en México es diversa, está integrada por más de 216 universidades e instituciones públicas y privadas a nivel nacional e internacional, haciendo uso de las tecnologías en las Instituciones de Educación Superior (IES), en donde se realizan principalmente actividades de docencia y generación de conocimiento.[2]

Desde hace más de diez años, las IES han tenido que adaptarse a un entorno cada vez más digitalizado, que impacta directamente en sus funciones académicas y administrativas. Ante este panorama, ha sido necesario desarrollar e implementar estrategias sólidas para proteger la información, reconociendo la

[1] International Organization for Standardization (ISO). (s. f.). ISO/IEC 27001 – Sistemas de gestión de seguridad de la información.)
[2]Ponce-López, J.L., Castañeda-De León, L.M. y Valles-Baca, H. (Coords.). (2024). Estado actual de las tecnologías de la información y las comunicaciones en las instituciones de educación superior en México. Estudio 2024. México: Asociación Nacional de Universidades e Instituciones de Educación Superior.

importancia crítica que tiene la seguridad de los datos. Entre los aspectos que resultan fundamentales se encuentran el fortalecimiento de las capacidades en ciberseguridad, la promoción de programas de capacitación y concientización, así como la incorporación responsable de tecnologías emergentes. Resulta oportuno mencionar también sobre la brecha entre la normatividad y su aplicación, junto con la limitación de recursos, capacitación y personal especializado en el tema.

La educación superior no volverá a ser la misma después de la pandemia por COVID-19 (conseguir cita bibliográfica), está claro que hay un antes y después; la emergencia sanitaria fue un catalizador en la transformación digital hacia el uso de plataformas digitales orientadas a la comunicación institucional que indujo a que los procesos de enseñanza-aprendizaje aceleraran la implementación de sistemas automatizados para la gestión de escolar. Asimismo la consolidación de bases de datos académicas que reúnen información sobre las comunidades que se iban conformando para compartir información, incluyendo la de investigación, y dentro de este ambiente, las herramientas colaborativas en la nube ha sido un componente esencial en la infraestructura tecnológica de las instituciones educativas, y de forma paralela, el avance de la Inteligencia Artificial, particularmente la generativa, potenció la producción de contenidos y procesamiento de datos, que en conjunto, contribuyeron a la eficiencia operativa de los procesos y trajo un cambio de pensamiento en las Instituciones sobre lo que se necesita en el futuro. En consecuencia, las IES manejan volúmenes cada vez mayores de datos sensibles y estratégicos, cuya adecuada protección se ha vuelto prioritaria.

Por ello, es imperante que las IES cuenten con estrategias, mecanismos y se apoyen en marcos de referencia en materia de seguridad de la información, a fin de garantizar la integridad de los procesos y respaldar los objetivos institucionales de la educación superior.

Digitalización integral de las IES

Hoy en día, la seguridad de la información se ha convertido en un tema crucial que atraviesa todos los sectores de la sociedad, incluidas de manera destacada las instituciones de educación superior (IES). Estas instituciones, cuyo quehacer tradicional se ha enfocado en la docencia, la investigación y la vinculación con la sociedad, enfrentan ahora el desafío de incorporar tecnologías digitales en sus distintas áreas de trabajo. La digitalización no solo moderniza sus infraestructuras y simplifica procesos administrativos, sino que también transforma los métodos de enseñanza, amplía el acceso al conocimiento y fortalece los vínculos con su comunidad y otros actores externos.

El uso de herramientas tecnológicas como la inteligencia artificial, el análisis de datos, los servicios en la nube, la movilidad y las plataformas colaborativas ha comenzado a cambiar de fondo la manera en que se enseña, se aprende y se toman decisiones dentro de las IES. Estas tecnologías no son simplemente recursos de apoyo, sino factores que reconfiguran el funcionamiento integral de las instituciones.

La adopción de tecnologías digitales permite automatizar procesos administrativos (como la gestión escolar, la evaluación o la titulación), optimizar la trazabilidad de la información académica y financiera, mejorar la eficiencia operativa y fortalecer la transparencia institucional. Asimismo, facilita la implementación de

entornos virtuales de aprendizaje, sistemas de analítica institucional, gestión de datos de investigación y estrategias de internacionalización digital. Este proceso se alinea con tendencias globales que conciben la transformación digital como un medio para promover una educación más inclusiva, personalizada y basada en datos.

Algunos aspectos clave de la transformación digital en las IES son los siguientes:

Cambio cultural y enfoque en la experiencia de la comunidad universitaria:

La transformación digital no solo implica la adopción de herramientas, sino también un cambio en la forma en que la universidad gestiona la docencia, la investigación y la administración. El objetivo es mejorar la experiencia de los estudiantes, profesores y personal administrativo, adaptándose a las nuevas necesidades y expectativas de la sociedad digital.

Adopción de tecnologías:

Se han implementado plataformas de aprendizaje en línea (LMS), herramientas de realidad virtual y aumentada, así como sistemas de inteligencia artificial para personalizar el aprendizaje. También se han utilizado herramientas de análisis de datos y computación en la nube para mejorar la eficiencia y la administración de la institución.

Flexibilidad y accesibilidad:

La transformación digital permite ofrecer modalidades de aprendizaje más flexibles, como la educación a distancia, y facilita el acceso a la educación superior a personas que no pueden asistir a clases presenciales.

Desafíos y oportunidades:

Si bien la transformación digital ofrece grandes oportunidades para mejorar la calidad de la educación y la experiencia de la comunidad universitaria, también presenta desafíos como la capacitación del personal, la infraestructura tecnológica, y la adaptación a los cambios tecnológicos, así como también, la imperante necesidad de proteger la información que manejan las IES

Cambio en la forma de enseñar y aprender:

Se han implementado nuevos métodos de enseñanza y aprendizaje, como la creación de entornos virtuales de enseñanza y aprendizaje, y el uso de recursos educativos digitales, que facilitan la interacción entre estudiantes y profesores, promoviendo el aprendizaje activo.

Mayor uso de datos:

Las universidades están utilizando cada vez más los datos para tomar decisiones estratégicas, mejorar la calidad de la educación, y personalizar el aprendizaje.

Cambio en el modelo de negocio:

La transformación digital también está afectando el modelo de negocio de las IES, con el desarrollo de nuevos productos y servicios, como la oferta de cursos en línea y la creación de incubadoras de innovación.

Desarrollo de habilidades digitales:

Las universidades están dando mayor importancia al desarrollo de habilidades digitales en su comunidad universitaria, reconociendo que el dominio de la tecnología es fundamental en el mundo actual.

Importancia de la colaboración:

La transformación digital requiere la colaboración entre diferentes actores como la parte administrativa de la IES, el personal docente e investigadores, los estudiantes, y el sector tecnológico.

Otro elemento para considerar es la interconexión y, por consecuencia, la dependencia de la tecnología digital convirtiendo a las IES en depositarias de una gran cantidad de información sensible.

Sin embargo, esta transformación conlleva también consecuencias relevantes. Por un lado, plantea desafíos en materia de seguridad de la información, protección de datos personales y gobernanza de la información. Por otro, exige una reconfiguración del capital humano, tanto en lo técnico como en lo docente, lo que implica procesos de capacitación continua y cambios culturales dentro de las comunidades universitarias. Además, la dependencia tecnológica puede generar brechas internas entre quienes acceden plenamente a estos sistemas y quienes enfrentan limitaciones por motivos técnicos, económicos o formativos.

Tipos de datos sensibles manejados por las IES

Las IES manejan una variedad de datos sensibles que requieren protección especial para garantizar la privacidad y seguridad de estudiantes, docentes y personal administrativo.

Algunos de los principales tipos de datos sensibles incluyen:

- Datos de identificación personal de estudiantes, docentes y administrativos: nombre completo, fecha de nacimiento, dirección, fotografía, por mencionar algunos.
- Datos académicos y de desempeño: historial académico, calificaciones, certificados, materias, evaluaciones, titulaciones, planes de estudio.
- Datos de contacto: números de teléfonos personales, correos electrónicos.

- Datos de salud: expedientes médicos, información sobre alergias, discapacidades, medicamentos y condiciones médicas.
- Datos financieros: información sobre pagos de inscripciones, reinscripciones, cuentas bancarias, becas, subsidios.
- Datos laborales del personal: currículum vitae, contratos de trabajo, nóminas y evaluaciones de desempeño.
- Datos relacionados con actividades extracurriculares: información sobre participación en talleres, diplomados, congresos, deportes y eventos organizados por la IES.
- Proyectos de investigación y propiedad intelectual: participantes o colaboradores, documentos, licencias, patentes, resultados de investigaciones científicas, publicaciones

Amenazas y riesgos actuales

En los últimos diez años, las Instituciones de Educación Superior (IES) en México han enfrentado una creciente exposición a riesgos y amenazas cibernéticas, como resultado de su transformación digital y del uso intensivo de tecnologías de la información para la gestión académica, administrativa y científica. A continuación, se presenta un resumen de los principales riesgos y amenazas observados en este periodo:

Ataques de ransomware: Las IES son objeto de secuestros de datos mediante software malicioso que encripta o cifra, información crítica a cambio de un rescate.

Phishing: Este tipo amenaza ha evolucionado, los ataques van dirigidos a usuarios institucionales, mediante correos o plataformas falsas, que buscan sustraer información de acceso a sistemas como correo electrónico, aulas virtuales o servicios bibliográficos.

Deficiencias en la infraestructura de ciberseguridad: Muchas IES presentan desigualdad en sus capacidades técnicas para proteger sus redes, especialmente las instituciones más pequeñas o con menos recursos.

Ataques de denegación de servicio (DDoS): Algunas universidades han sufrido interrupciones en sus servicios digitales debido a ataques que saturan sus servidores y dificultan el acceso a plataformas académicas.

Falta de cultura institucional de ciberseguridad: Se ha identificado la ausencia de políticas claras, programas de capacitación o respuesta ante incidentes, lo cual incrementa la vulnerabilidad ante

amenazas externas, y aunque hay esfuerzos en algunas IES, esto no ha sido suficiente.

Uso no controlado de dispositivos y redes personales: El trabajo a distancia y la educación a distancia durante la pandemia expusieron a las IES a mayores riesgos debido al acceso remoto desde redes y equipos no protegidos.
Infraestructura tecnológica obsoleta: muchas IES operan con sistemas heredados y software sin soporte, lo que las hace vulnerables.

Presupuestos limitados: la falta de inversión en ciberseguridad dificulta la implementación de medidas de protección efectivas.

Uso de dispositivos personales (BYOD): la conexión de dispositivos personales (de alumnos, docentes y personal administrativo) a las redes institucionales aumenta la superficie de ataque.

Para mitigar estos riesgos, las IES deben fortalecer sus políticas de seguridad, capacitar a su comunidad y actualizar sus sistemas tecnológicos.

Algunas de las consecuencias de la materialización de los riesgos mencionados anteriormente son:

- ***Daño a la reputación:*** la confianza en la IES se ve afectada.
- ***Impacto financiero:*** costos asociados a la recuperación de datos y posibles sanciones legales.
- ***Riesgos para estudiantes y personal:*** exposición de información personal y financiera.

Importancia de la seguridad de la información:

La seguridad de la información es un pilar fundamental en la era digital para proteger los datos que se registran, procesan y almacenan en las IES, donde la información es un activo valioso, y para ello busca:

- ***Protección de la privacidad:*** para dar cumplimiento a las leyes como la Ley Federal de Protección de Datos Personales (en México) o el GDPR (en Europa).
- ***Garantía de continuidad operativa:*** Evitar que ciberataques interrumpan clases, investigaciones o trámites.
- ***Salvaguarda de la reputación institucional:*** Un incidente de seguridad puede afectar gravemente la confianza pública en una institución.

De lo anterior, las IES, en la medida de sus posibilidades, implementan diversas medidas de seguridad para proteger los datos sensibles de estudiantes, docentes y personal administrativo.

Algunas de las estrategias más comunes incluyen:

- ***Cifrado de datos:*** se utiliza para proteger la información almacenada y en tránsito, evitando su obtención.
- ***Autenticación y control de acceso:*** implementación de autenticación de dos factores y restricciones de acceso basadas en roles.
- ***Firewalls y sistemas de detección de intrusos:*** herramientas que previenen ataques cibernéticos y monitorean actividades sospechosas.
- ***Copias de seguridad periódicas:*** respaldo de datos para evitar pérdidas en caso de fallos o ataques.
- ***Políticas de privacidad y cumplimiento normativo:*** aplicación de regulaciones como la Ley Federal de Protección de Datos Personales en México.
- ***Capacitación y concienciación:*** programas de formación para estudiantes y personal sobre buenas prácticas de seguridad digital.

Conclusiones

El avance de la tecnología ha modificado profundamente las dinámicas cotidianas: la forma en que se trabaja, se aprende, se comunica e incluso, las relaciones con el entorno. En este escenario, la seguridad de la información ha dejado de ser una cuestión exclusiva de especialistas para convertirse en un componente esencial de la educación ciudadana, desde los primeros años escolares.

En la última década, el uso de las tecnologías ha transformado profundamente las IES, mejorando la enseñanza, la investigación y la gestión académica siendo una herramienta para la transformación de la educación, integrando contenidos de alfabetización digital y seguridad informática no solo contribuyendo a proteger la intimidad y los datos personales de sus comunidades universitarias, sino que también siembra las bases de una cultura responsable en el uso de las tecnologías. La seguridad de la información no sólo es hablar sobre la protección de datos y de dispositivos, se trata de formar ciudadanos digitales conscientes de sus derechos, responsabilidades y su impacto en su entorno virtual preparar a las generaciones con conocimiento, respeto, sentido ético y habilidades, frente a los riesgos ante un mundo digital.

Principales amenazas en el sector

02. Principales amenazas en el sector

La información, un activo valioso para las universidades.

Las Universidades han adoptado las tecnologías de la información y Comunicación (TIC) para apoyar en el cumplimiento de sus funciones sustantivas, es así que las TIC cumplen un papel muy importante, pues es través de estas, que se facilitan los accesos a los recursos educativos, se mejora la colaboración entre estudiantes y profesores y se apoya en la gestión eficiente de la información y los procesos universitarios, las TIC tienen un impacto transformador en la educación superior.

En el Estudio 2024 “Estado actual de las Tecnologías de la Información y Comunicación en las Instituciones de Educación Superior en México: Estudio 2024” (cita bibliográfica) se reflexiona como las TIC a lo largo de este tiempo han evolucionado para convertirse en un pilar estratégico en las Instituciones de Educación Superior, lo que nos motiva a potenciar el uso de las TIC, pero también a gestionarlas de manera segura y responsable.

Mantenerse en un mundo hiperconectado, si bien como sociedad nos ha aportado grandes beneficios, también ha abierto la puerta a grandes riesgos y amenazas que, de no gestionarse eficientemente, pueden traer consecuencias con grandes impactos a las organizaciones que han adoptado a la tecnología como la base y apoyo de sus funciones.

El ciberespacio, entendido como ese dominio no tangible interconectado por servicios y protocolos de red donde los usuarios desarrollan sus actividades cotidianas, no es ajeno a la presencia de riesgos. Al igual que en el mundo físico, en este entorno digital acechan amenazas constantes contra la confidencialidad, la integridad y la disponibilidad de la información que las personas y organizaciones gestionan a través de sus sistemas y redes interconectadas.

Precisamente, uno de los activos más importantes dentro de las IES es la información, la cual emerge como resultado directo de sus procesos y operaciones; su gestión requiere gran responsabilidad, ya que, si esta se ve comprometida, puede tener impactos negativos a la IES. Actividades como la investigación, docencia y la administración generan información sensible y estratégica que, debido a su alto valor e impacto, requieren de la implementación de controles de seguridad en la infraestructura tecnológica que soporta los servicios generadores de esta información.

Desde el contexto de la ciberseguridad (definición y cita bibliográfica), esta información puede verse comprometida por varias amenazas (situaciones adversas conocidas, pero aún no materializadas definición y cita bibliográfica), las cuales, de llegar a materializar podrían desencadenar efectos perjudiciales.

Por lo anterior, las universidades se han convertido en un objetivo específico y atractivo para las cibercriminales, quienes, a través de diversos mecanismos, estrategias y artilugios, pueden llegar a comprometer este importante activo digital.

El hecho de la información valiosa pueda verse comprendida en una IES, puede tener impactos negativos como los siguientes:

- Compromiso de datos y consecuencias legales: La pérdida o el compromiso de datos de investigación pueden frenar avances científicos y tecnológicos, la pérdida o el compromiso de datos personales puede generar disputas legales por incumplimiento de regulaciones.
- Interrupción de operaciones: La indisponibilidad de sistemas informáticos puede interrumpir procesos críticos como la gestión de matrículas, la administración de recursos humanos y la operación financiera, causando impactos significativos.
- Daño a la Reputación: Construir y mantener una reputación positiva puede tardar años, sin embargo, un ciberataque de gran impacto puede disminuir esta confianza de la comunidad universitaria y del público en general hacia la IES.
- Pérdidas Económicas: El impacto de un ciberataque puede conllevar grandes costos de recuperación y posibles costos por sanciones legales.

El sector educativo, uno de los más ciber atacados

Las organizaciones se enfrentan constantemente a un número creciente de ataques cibernéticos, cada vez más focalizados y con mayor complejidad, y en las Instituciones de Educación Superior no ha sido la excepción; los cibercriminales, motivados principalmente por un interés económico, emplean técnicas y herramientas cada vez más sofisticadas para intentar vulnerar la infraestructura tecnológica de las IES y obtener beneficios económicos rápidamente.

El sector de la educación superior es uno de los sectores más afectados a nivel global por los ciberataques en los últimos años (poner referencia), y entre los ciber ataques con mayor impacto en estos últimos años en las IES se pueden mencionar los siguientes:

– En el 2020, la Universidad de Utah en Estados Unidos n 2020 tuvo que pagar más de 457,000 dólares a fin de evitar una filtración de datos.

–En el 2021 la Universidad Autónoma de Barcelona sufrió un ciberataque de ransomware que dejó inoperativa toda su red interna, la conexión a internet, su página web, y los servicios en la nube de Microsoft que utilizaban los estudiantes, dejando sin servicio 1,200 servidores, 10,000 equipos personales y más de 50 mil usuarios afectados.

– En Latinoamérica un ataque muy mencionado fue el que tuvo la Universidad del Bosque en Colombia en el 2021 en el que se dejó sin servicio el correo electrónico, su campus virtual, así como sus sistemas informáticos, hackeando también su red social de twitter.

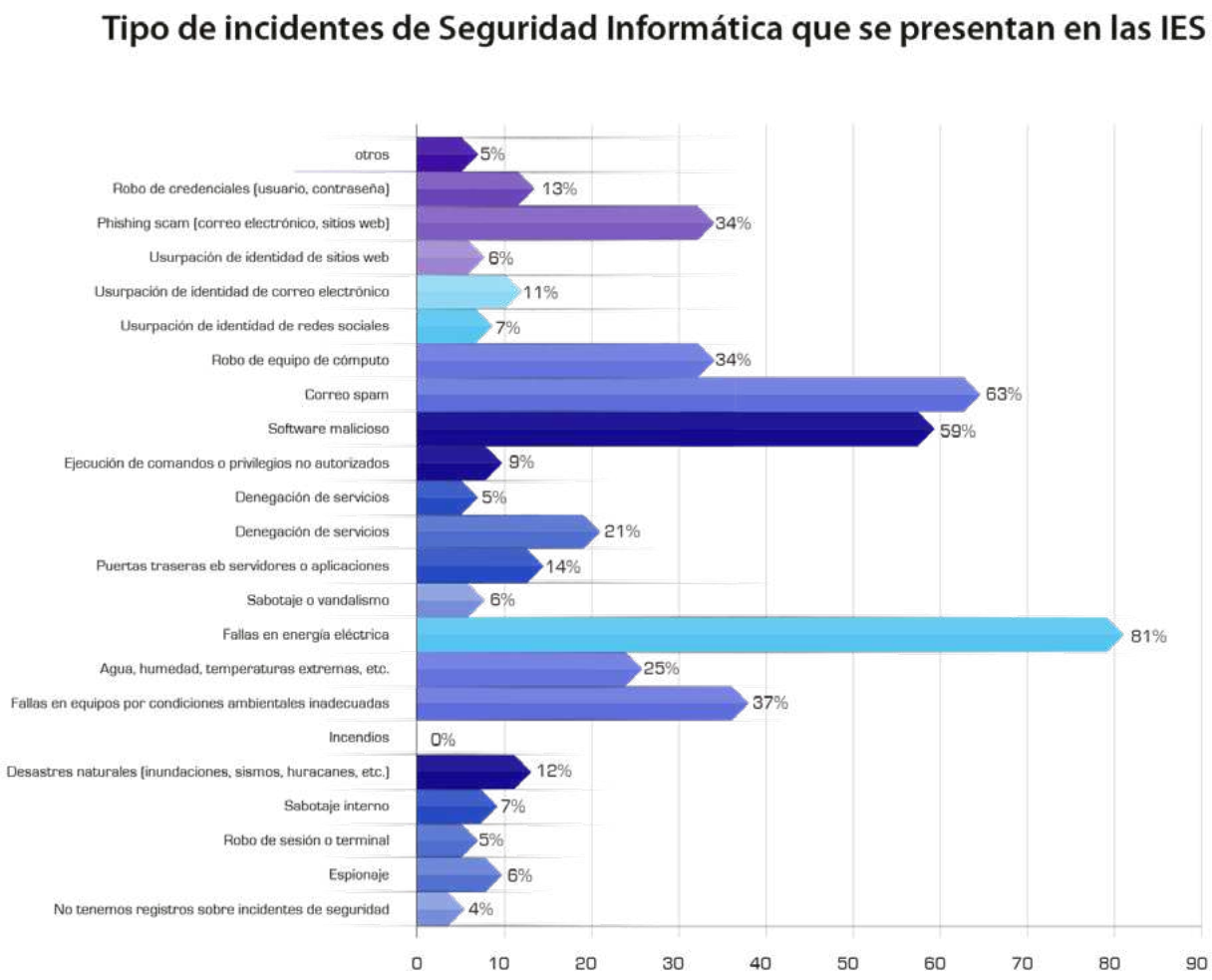
– En el 2021, la Universidad Javeriana de Colombia también, fue víctima de un ataque cibernético que obligó a deshabilitar algunos servicios.

De acuerdo al primer ***"Índice de Madurez en Ciberseguridad (IMC) de las instituciones de educación superior"***, elaborado por Banco Santander, a través de MetaRed, y la Secretaría General Iberoamericana (SEGIB), en donde participaron 14 países, entre ellos México y con más de 240 universidades, resalta que en el 2023, 6 de cada 10 universidades iberoamericanas fueron objeto de algún tipo de incidente de ciberseguridad que derivó en la afectación total o parcial de los principales servicios y aplicaciones corporativas.

Aunque en nuestro país no existen datos oficiales específicos sobre ciberataques a Instituciones de Educación de Superior, desde ANUIES existe un esfuerzo que mediante una encuesta anual que se viene aplicando desde el 2016, se busca recabar información sobre diversos aspectos del cómo las IES miembros de ANUIES gestionan la tecnología educativa, el cual nos permite obtener datos para conocer las amenazas que se han materializado a través de incidentes de seguridad de la información.

En este estudio, desde el contexto de la seguridad de la información podemos visualizar como en la primera versión de este estudio en 2016," se identificó que los incidentes de seguridad que más reportaron las IES fueron el correo spam, el software malicioso y las fallas de energía eléctrica, es decir fueron amenazas que se materializaron.

Ilustración 1 Tipos de incidentes



FUENTE: Estado actual de la Tecnologías de la Información y Comunicación, ANUIES, 2016

Ya para el estudio del 2024 “Estado actual de las Tecnologías de la Información y Comunicación en las Instituciones de Educación Superior en México. Estudio 2024” elaborado por el Grupo de Gestión de la Tecnología Educativa del Comité ANUIES TIC, se concluyó que los incidentes más comunes en las IES fueron ocasionados por amenazas como el malware y correo SPAM, esto permitió identificar que resultaba necesario robustecer la sensibilización y el autocuidado al utilizar las plataformas digitales.

Ilustración 2 Número de incidentes de segurida de la Informacion presentacdos en las IES

Atributo	Valor
Malware	989,939.20
Correo Spam	892,043.00
Phishing scam	351,254.00
Fallas en energía eléctrica	734.00
Ejecución de comandos con privilegios no autorizados	474.00
Uso de software sin licenciamiento para fines institucionales	438.00
Robo de credenciales de acceso a correo electrónico institucional	266.00
Temperaturas extremas	266.00
Ransoware	259.00
Descarga de contenido no autorizado para fines institucionales	238.00
Total	**2,236,043.20**

FUENTE: Estado actual de las Tecnologías de la Información y Comunicación en las Instituciones de Educación Superior en México. Estudio 2024

Este análisis nos permite reconocer que, en México, las Instituciones de Educación Superior (IES) se han enfrentado a una creciente exposición a riesgos y amenazas cibernéticas, algunas que persisten como el malware, el correo no deseado y el phishing, pero hemos visto como otras como el ransomware han emergido y tomado gran relevancia por el impacto mediático, económico y operacional que han ocasionado a las IES.

En este complejo panorama de la ciberseguridad que enfrentan las instituciones de educación superior, las amenazas pueden categorizarse de diversas maneras para facilitar su comprensión y gestión; por un lado, se pueden identificar amenazas externas que se originan fuera del perímetro de la IES y que buscan explotar vulnerabilidades en sistemas, redes o usuarios; y por otro lado, amenazas internas que surgen desde el interior mediante personas que cuentan con accesos legítimos a los activos de TI de la institución.

Adicionalmente, podemos considerar una clasificación basada en la afectación de algún pilar de la seguridad de la información, distinguiendo entre amenazas orientadas a la afectación de la confidencialidad (como el robo de datos), a la integridad (como la manipulación de información) y a la disponibilidad (como los ataques de denegación de servicio).

Amenazas emergentes

En el ámbito de la ciberseguridad, las Instituciones de Educación Superior (IES) enfrentan un panorama de amenazas emergentes cada vez más sofisticado. Estas amenazas van más allá de los ataques tradicionales, evolucionando constantemente para explotar nuevas vulnerabilidades, y entre las principales se encuentran las siguientes:

Infostealers: Las universidades se enfrentan al robo de datos de sus usuarios, y una de las formas como los cibercriminales lo están haciendo es mediante los infostealers, un tipo de malware en auge y que permite robar datos sin dejar rastros, usando la ejecución sin archivos y técnicas de ofuscación para evitar ser detectados por los sistemas de protección; sin duda este malware es una amenaza que debe preocupar a las IES ya que pueden comprometer información en cuestión de segundos y compartirla en los mercados o foros de cibercriminales.

Fuga de información o exfiltración de datos: Es la transferencia de datos no autorizada desde equipos de cómputo o redes hacia otros equipos externos. Las organizaciones que poseen información de gran valor tienen un riesgo mayor de sufrir de este tipo de ataques; en este sentido la información de las IES, por su alto valor crítico, se ha convertido en un atractivo para los cibercriminales, quienes han encontrado la oportunidad de lucrar con la información que es sustraída de manera ilegal.

Por mencionar un ejemplo, en México una gran filtración global revelada en 2024, expuso más de 177.000 cuentas de correo institucional comprometidas. Este hallazgo incluyó miles de credenciales pertenecientes a varias universidades del país.

Ingeniería social avanzada: El impulso de la IA no solo ha traído beneficios a las organizaciones, también se convertido en una oportunidad de mejora para los cibercriminales quienes han hecho uso de estas herramientas para sofisticar sus ataques, en este sentido las IES ahora se enfrentan a nuevas amenazas impulsadas con IA como el diseño de Phishing y los deepfakes

Ataques basados en inteligencia artificial (IA): La IA no solo permite automatizar y escalar ataques existentes, sino que también posibilita la creación de amenazas completamente nuevas y más difíciles de detectar. La IA permite automatizar la búsqueda y explotación de vulnerabilidades en sistemas, y desarrollar malware que evada las defensas tradicionales. Estos avances hacen que los ataques sean más rápidos, adaptables y persistentes, exigiendo que las IES adopten defensas también con IA para protegerse eficazmente.

Conclusión

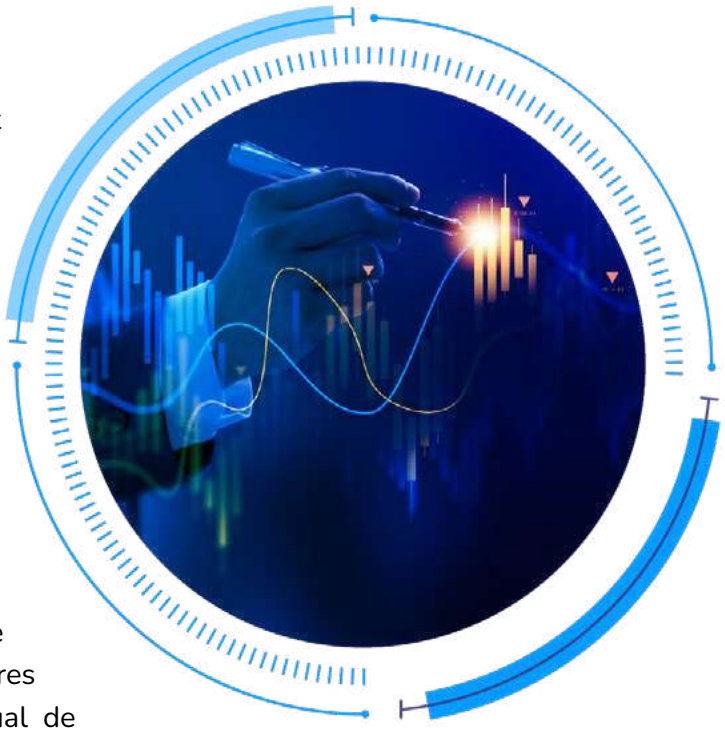
Ante este panorama, es necesario que las IES adopten un enfoque proactivo en la gestión de riesgos cibernéticos. No basta con reaccionar; es esencial anticiparse y fortalecer las defensas en todos los frentes. Esto implica no solo invertir en tecnología de vanguardia, sino también fomentar una cultura de ciberseguridad que permee a todos los niveles de la institución y que sea constante, desde la alta dirección hasta cada usuario final. La capacitación continua, la implementación de políticas claras, la modernización de infraestructuras y la concientización sobre las nuevas amenazas impulsadas por la IA, son pasos fundamentales para salvaguardar el conocimiento, la información y la confianza que definen a nuestras universidades en la era digital.

Retos de ciberseguridad que enfrentan las IES

03. Retos de ciberseguridad que enfrentan las IES

Como se ha mencionado anteriormente, las Instituciones de Educación Superior (IES), como todas las industrias y sectores, enfrentan retos asociados al desarrollo y crecimiento de sus capacitades con relación a la ciberseguridad. Existen diversos estudios a nivel mundial, principalmente enfocados en la industria, que sin embargo, para as IES en México, se reflejan los mismos retos que son expresados por el sector privado, aunque con algunas variantes o particularidades.

Recursos limitados

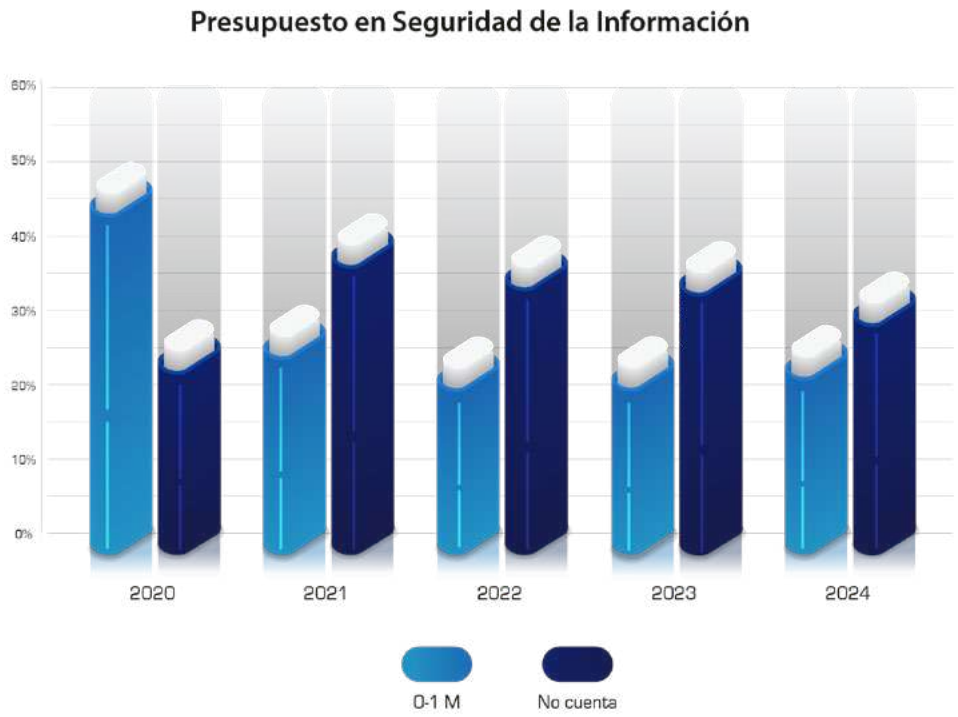


De acuerdo con el informe de PWC “Digital Trust Insights 2025 Edición México”[3] se espera que los presupuestos en ciberseguridad aumenten no más del 10% el siguiente año, lo cual, si bien pareciera un dato esperanzador, al reconocer a la ciberseguridad como una prioridad en las organizaciones y un diferenciador en la entrega de servicios y un área clave para asegurar no solo el crecimiento sino la propia permanencia, los presupuestos que han venido destinándose a estas áreas, aún no cubre lo necesario para atender el volumen y sofisticación de las amenazas que se enfrentan. Situación que, para el caso particular de las IES en México, se puede identificar en los indicadores que se encuentran en los estudios del Estado actual de las Tecnologías de la Información y las Comunicaciones de la ANUIES, donde podemos observar que los presupuestos asignados a seguridad de la información se han mantenido a lo largo de los años principalmente en menos de 1 millón de pesos y aún existen más de un tercio de las instituciones sin un presupuesto asignado para ello. (cita bibliográfica)

Esta situación no solo limita la protección de las IES ante las amenazas digitales, sino que además, limita el desarrollo de un ecosistema que permita elevar la ciber resiliencia, poniéndolas en un alto riesgo, ya que, cada vez más, la gestión académica y administrativa dependen del uso de sistemas informáticos y telecomunicaciones para lograr el cumplimiento de las funciones sustantivas.

[3] https://download.pwc.com/mx/archivo/2025/2025-digital-trust-insights-mex.pdf

Ilustración 3 Presupuesto en seguridad de la información en las IES de México



FUENTE: Estado actual de las Tecnologías de la Información y Comunicación en las Instituciones de Educación Superior en México 2020, 2021, 2022, 2023 y 2024

Déficit de personal calificado

Por otro lado, de acuerdo con un estudio de la empresa Linked-in[4], México es uno de los países con mayor número de vacantes en el ámbito de la ciberseguridad, siendo que para 2024, se presenta un crecimiento en la demanda del 6.8% respecto del año anterior. Así mismo, las personas que laboran en ciberseguridad en el país apenas alcanzan el 0.68% del total de empleados, una cifra muy baja para alcanzar un desarrollo adecuado y sostenible.

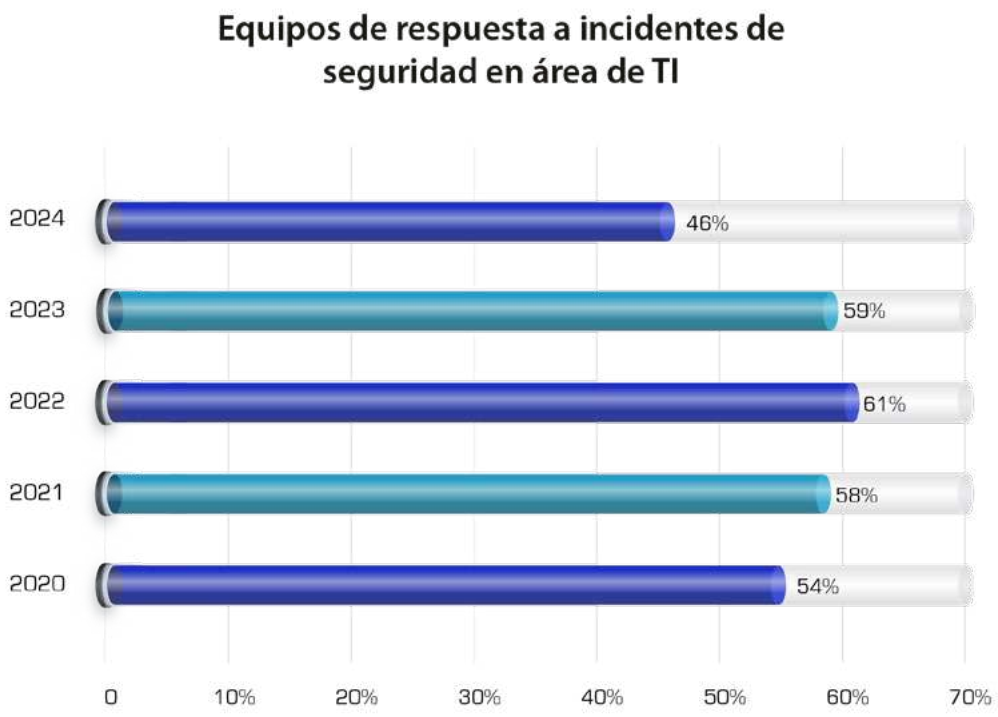
En este sentido, otro de los retos importantes con los que las IES se enfrentan y que por su naturaleza y vocación están obligadas a atender, es la escaza oferta de formación en la materia, el desarrollo de profesionales competentes y éticos, han generado una brecha importante en las empresas. Otro dato del estudio que resulta revelador de esta brecha son los requisitos que establecen los ofertantes en sus vacantes, donde en su mayoría exigen un profesional formado al menos en una licenciatura.

Al analizar estos datos con mayor detenimiento, se pueden identificar dos vertientes que afectan a las IES del país; por un lado, no se cuenta con profesionales calificados para su contratación, lo cual implica que los responsables de las áreas encargadas del aseguramiento de la infraestructura tecnológica, han tenido que formarse de manera empírica o autogestionada, provocando largas curvas de aprendizaje,

[4] https://economicgraph.linkedin.com/content/dam/me/economicgraph/en-us/PDF/global-cybersecurity-talent-trends.pdf

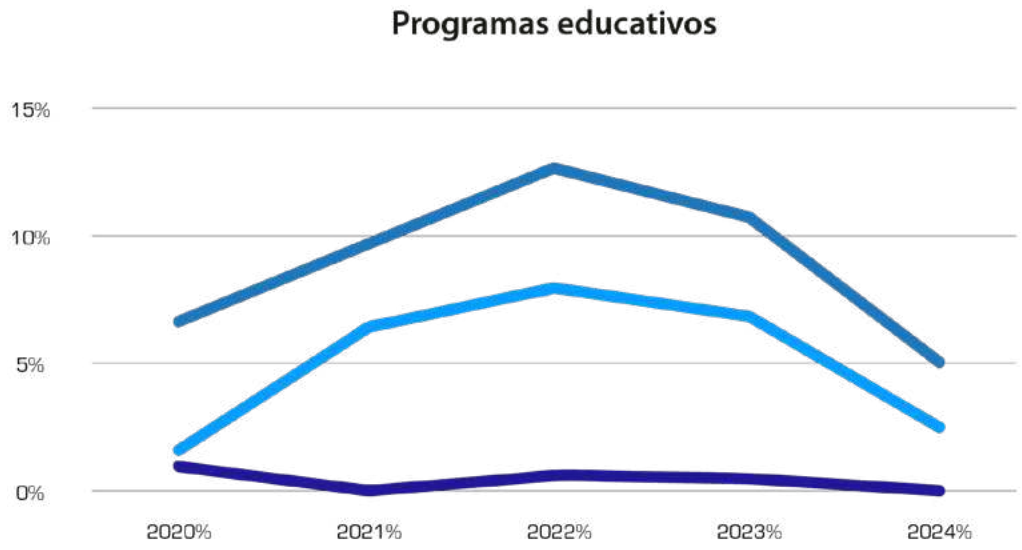
deficiencias en la toma de decisiones y una falta importante de metodologías aplicadas, limitando la visión y una estrategia de madurez a largo plazo, y es por ello que los equipos de respuesta a incidentes de ciberseguridad continúan siendo un área que para las autoridades siguen incrustada dentro de las actividades de las áreas de TI y solo responde a los incidentes que al interior de dichas áreas se generan; por otro lado, los docentes requeridos para el diseño de planes de estudio y la impartición de experiencias educativas de calidad, se ve limitado dado que, de igual forma, no existen suficientes docentes formados íntegramente en ciberseguridad. Dado lo anterior, los planes de estudio reflejan solo una concepción parcial de la ciberseguridad y se encuentran sesgados por el propio conocimiento auto adquirido de los docentes. Estas situaciones se convierten en un círculo vicioso que limitan el crecimiento y el desarrollo adecuado de los niveles de seguridad para los entornos universitarios.

Ilustración 4 Número de equipos de respuesta a incidentes de seguridad en las IES de México



FUENTE: Estado actual de las Tecnologías de la Información y Comunicación en las Instituciones de Educación Superior en México 2020, 2021, 2022, 2023 y 2024

Ilustración 5 Número de programas educativos en seguridad de las IES en México



FUENTE: Estado actual de las Tecnologías de la Información y Comunicación en las Instituciones de Educación Superior en México 2020, 2021, 2022, 2023 y 2024

Ambientes heterogéneos y complejos

En este ámbito, una de las mayores premisas para la implementación de servicios tecnológicos, es lograr un equilibrio entre la eficiencia operativa y la seguridad, siendo esto algo sumamente complejo cuando nos enfrentamos a los entornos que caracterizan a las IES, la diversidad de cátedras, la dispersión geográfica, la particularidad de herramientas tecnológicas empleadas para la impartición de experiencias educativas y los diferentes grados de apropiación de las tecnologías de la información y comunicación por parte de las comunidades académicas y administrativas, resulta en un ambiente altamente complejo para el establecimiento de controles efectivos para cada caso.

Particularmente, este reto es el de mayor impacto para la seguridad en las IES, pensando en los requerimientos tecnológicos que cada facultad tiene o incluso, lo que cada experiencia educativa demanda.

Legislación

Por otro lado, aunque México ha desarrollado leyes y estrategias nacionales de ciberseguridad, existe una falta de normatividad específica, clara y vinculante para el sector educativo superior. Algunas IES carecen de políticas internas robustas de protección de datos, protocolos de respuesta a incidentes, y directrices sobre uso y resguardo de información sensible en base a buenas prácticas de seguridad de la información y ciberseguridad. Por esto, la ausencia de exigencias legales claras reduce la urgencia

institucional para invertir en ciberseguridad y genera un entorno desprotegido ante posibles sanciones o responsabilidades legales.

Este vacío en la legislación ha llevado a las IES a tomar acciones reactivas y descoordinadas, lo que dificulta la implementación de controles adecuados para las amenazas digitales a las que se enfrentan, poniendo en riesgo a todos los activos de las instituciones. Si no se definen requerimientos mínimos a cumplir y se estandarizan, la colaboración es más difícil de realizarla de una manera efectiva, colocando al sector a la disposición de los atacantes quien en muchas de las ocasiones se encuentran perfectamente coordinados y estandarizados.

Así mismo, la falta de legislación en la materia deja un espacio para la determinación de responsabilidades antes ciberataques, y dado que no se cuenta con una definición clara del tratamiento ante estos, la preservación de evidencia, su tratamiento y la investigación, carecen de marcos de actuación, limitando la denuncia y exponiendo a las instituciones y a los propios responsables de estos temas ante juicios carentes de toda orden.

Otros retos relevantes tales como:

- Resistencia al cambio: La adopción de nuevas tecnologías, como por ejemplo la IA, suele encontrar resistencia por parte de la comunidad universitaria, ya sea por desconocimiento, falta de interés o temor a la complejidad o riesgos.
- Fragmentación institucional: Las políticas y procedimientos de ciberseguridad suelen estar dispersos o ser inconsistentes entre diferentes áreas o campus de una misma institución, lo que dificulta una protección homogénea.
- Falta de colaboración interinstitucional: La ausencia de redes de colaboración entre IES limita el intercambio de buenas prácticas, desarrollo de capacidades colectivas y respuesta coordinada ante incidentes de gran escala.

El desarrollo de la ciberseguridad en las IES mexicanas entre 2015 y 2025 ha enfrentado numerosos retos que aún requieren atención prioritaria. La solución implica no solo la inversión en tecnología, sino también la formación continua de toda la comunidad universitaria, la creación de políticas claras y específicas, y el fortalecimiento de la colaboración interinstitucional. Solo así será posible construir

ambientes digitales seguros, capaces de proteger la información y los procesos que sustentan la vida académica y administrativa de las IES.

Conclusiones

Los retos en la materia son muy diversos ya que no solo tienen que ver con la implementación de soluciones tecnológicas; existen retos importantes en las propias estructuras y su operación, así como en el impulso de normativas que además de proteger a sus propias comunidades, generen un entorno estandarizado para la identificación, atención y remediación de incidentes de seguridad, así como la compartición de indicadores con otros entes.

De igual forma, es necesario generar una cultura en ciberseguridad, que abarque a todos los estratos de las IES, iniciando con la alta dirección y el compromiso con un liderazgo que ponga como elemento estratégico a la ciberseguridad.

Marcos de referencia y buenas prácticas

04. Marcos de referencia y buenas prácticas

Introducción.

La seguridad de la información y la ciberseguridad, que, en estricto sentido, forma parte integral de la seguridad de la información de todas las organizaciones, han sido constantemente sobrepasados por la enorme problemática que este tópico genera en la comunidad en general. Desde los múltiples y variantes eventos e incidentes que los ciberdelincuentes llevan a cabo con la intención de vulnerar cualquier activo de información, hasta los intentos constantemente exitosos en lo que se ha denominado ingeniería social, pasando por campañas de comunicación maliciosamente orquestadas por extraños, y a veces, por propios, buscando la afectación reputacional de las instituciones, en nuestro entorno, de la educación superior del país, y aunque esto no es una situación particular de México, puesto que se ha visto que a nivel mundial los atacantes están poniendo foco en las IES del mundo, debido a la información valiosa que resguardan y a los mínimos ,y a veces inadecuados, mecanismos de gestión de la seguridad de la información con que cuentan.

Para los encargados de la seguridad de la información y ciberseguridad de las IES, el resguardo de la información, en su forma inicial denominada la triada de confidencialidad, integridad y disponibilidad, resulta una labor de permanencia, constancia y resistencia, pero también de inteligencia, visión y atención oportuna, pues mientras más rápido se identifiquen y resuelvan las vulnerabilidades que se exploten, menos tiempo tendrán los atacantes de obtener mayores resultados. Esto es una carrera sin fin, realmente. Bajo esta situación, resulta fundamental que las IES, desde su máxima autoridad en lo individual y en lo grupal, estén conscientes de las situaciones que se generan en torno a la seguridad de la información y de la ciberseguridad de sus organizaciones, y ser corresponsables del “riesgo aceptable” que este ámbito genera, pues se requiere de contar con muchos recursos, tanto humanos como materiales, de preparación, de aceptación y de operación permanente, que en muchas ocasiones sale de toda rutina transaccional normal; el equipo encargado del entorno de la seguridad de la información y ciberseguridad, siempre deberá estar atento y disponible para intervenir ante cualquier evento o incidente que se presente en la IES, y esto puede suceder las 24 horas del día de cualquier día.

En seguimiento con todo lo mencionado, la protección de los activos de información de las IES desde el entorno de la triada indicada anteriormente (confidencialidad, integridad y disponibilidad), ha tenido un aspecto crítico para su entendimiento y aplicación, ya que ahora tenemos que integrar una variable adicional con todo lo que se relaciona a la llamada inteligencia artificial, puesto que desde el lado de los atacantes, los artefactos de ataque generados por esa inteligencia artificial, con la búsqueda implacable por encontrar la vulnerabilidad de los activos de información, agrega un aspecto importante a considerar para mantener el riesgo aceptable en términos de la definición de la propia IES; en este mismo sentido, es importante contar con elementos tecnológicos, normativos, aplicables y adecuados, para contrarrestar

los continuos y permanentes ataques desde el exterior o desde el interior. Por lo tanto, presentamos ahora una serie de recomendaciones y prácticas que pueden, si no eliminar por completo, si contar con mecanismos sobre la gestión de seguridad de la información y ciberseguridad de las IES, considerando que esto es una carrera sin fin, como ya lo hemos mencionado también.

Buenas prácticas en las IES.

Las buenas prácticas de ciberseguridad son un conjunto de mecanismos y recursos para proteger la información personal, financiera y profesional contra amenazas y accesos no autorizados, abarcando la confidencialidad, integridad y disponibilidad de los datos. Se centra en la implementación de medidas preventivas y de respuesta ante incidentes, con el objetivo de salvaguardar los activos de información.

Se mencionan algunas de las mejores prácticas de ciberseguridad

- Contraseñas fuertes
- Activar la autenticación de dos factores (2FA)
- Mantener actualizado el software
- Tener cuidado con el correo electrónico y los enlaces
- Navegación segura
- Utilizar WIFI pública con seguridad
- Realizar copias de seguridad de sus datos
- Protección de sus dispositivos
- Conocer sobre el phishing,
- Supervisar cuentas con regularidad
- Tener cuidado con las redes sociales
- Mantenerse informado y precavido

Para todos los usuarios de las IES, es importante tener unos estándares mínimos de ciberseguridad, para evitar que se afecte la información por amenazas cibernéticas, entre las cuales se puede mencionar la filtración de datos confidenciales.

En el año 2023 de acuerdo con AMECI en México, 10 escuelas fueron víctimas de ciberataques; esto se dio principalmente en los estados de Sinaloa, Chiapas, Nuevo León, Jalisco y Ciudad de México, y alrededor del 80% de las IES de todo el mundo fueron atacadas mediante ransomware (https://www.ameci.org/blog/en-mexico-10-escuelas-fueron-victimas-de-ciberataques).

La principal amenaza de las escuelas es el secuestro de información, que reporta incluso, un incremento de más del 20% en los ciberataques del 2022 al 2023, siendo el robo de credenciales y la explotación de vulnerabilidades de sistemas informáticos, los principales puntos de intrusión.
Checklist de buenas prácticas en el área de informática (INCIBE)

1. Establecer e implementar una política de copias de seguridad periódicas
2. Implementar medidas de protección física de las copias de seguridad.
3. Realizar pruebas periódicas de restauración de las copias de seguridad
4. Establecer una política de contraseñas que incluya uso de mayúsculas y minúsculas, números y caracteres especiales.
5. Implementar controles técnicos para el cambio periódico de las contraseñas de todos los usuarios
6. Mantener los sistemas y equipos de usuarios actualizados y comprobarlo periódicamente.
7. Realizar auditorías periódicas de seguridad de los servidores
8. Subscribirse a servicios de noticias de seguridad.
9. Implementar controles de acceso físico a áreas restringidas
10. Desarrollar e implantar un procedimiento de gestión de las incidencias de seguridad.
11. Llevar a cabo programas de formación y concienciación a los usuarios
12. Desarrollar procedimientos de las principales tareas técnicas
13. Utilizar herramientas de protección como antivirus, IDS, etc.
14. Desarrollar un plan de recuperación ante desastres.

Marcos de referencia NIST, ISO 27000, CIS

Con el fin de estructurar un esquema ordenado de atención para cubrir todas las aristas estratégicas y operacionales de las IES, puede ser consultado, y de alguna manera elegido, lo que conocemos como marco de referencia, norma o “framework”, sobre el cual se establecen controles y pautas bien estructurados, buscando fortalecer la seguridad de la información de las IES.

Existen entonces varios marcos de seguridad de la información y ciberseguridad a nivel internacional que pueden ser adoptados por las IES, en el entendido que se refieren a los lineamientos probados, que aunque no completamente infalibles, que existen. Esto se indica ahora para quitar desde ya, la idea simplista que ronda sobre la inconsciencia que, al contar con un marco o normativa, la IES esta “completamente segura”; este es quizás el mito más generalizado dentro del entorno de la seguridad de la información. Se puede considerar que solamente las instituciones que no cuenten con acceso a información, que no tengan múltiples actores y que estén aisladas del entorno mundial, posiblemente, podrían estar “seguras”. Obviamente esto es, quizás, la mayor utopía de nuestro ámbito.

Esto existe, más aún en un mundo digitalizado, interconectado, con una amplia variedad de sistemas de información, plataformas interconectadas que pretenden funcionar de manera armónica, y que desde las sencillas relaciones de información, como lo podría ser el simple correo electrónico, hasta los sistemas complejos de control escolar, académico y financiero (SIS, ERP, CRM, etc.), o de los sistemas de gestión del conocimiento (LMS), o cualquier otro sistema de información, se requieren establecer estrategias, tácticas y normativas sobre la confidencialidad de la información, que esta se pueda mantener confiable

e íntegra y siempre disponible, para su utilización en cualquier momento y desde cualquier lugar.
Quizás, y a manera de conclusión preliminar, podemos mencionar que no hay ningún estándar, protocolo, normativa o esquema que por sí solo tenga todos los vectores gestionados. Por lo tanto, el entendimiento de cada uno de estos lineamientos, de la adopción para la IES y la complementación de varias de estas alineaciones, sería la mejor recomendación ahora.

Familia ISO 27000 (27001, 27002:2022)

Para iniciar este breve recorrido, podemos empezar con la familia de la norma ISO 27000 (ISO 27001, 27002, 27005, 27032), generados por la Organización Internacional de Estandarización que desde 1947 y en atención a más de 160 países, genera estándares funcionales prácticamente para todo el mundo. La familia 27000 se refiere a la estandarización que, sobre un sistema de gestión de seguridad de la información, pretende organizar los esfuerzos estratégicos y operativos para la gestión integral de la información y todo su contexto dentro de las organizaciones, y tiene fundamental aportación sobre que la máxima autoridad es corresponsal de la gestión del sistema de seguridad de la información avalando políticas y lineamientos aplicables a toda la organización, y que con la implementación de los 93 controles que se integran en la versión 2022, opera la gestión de la seguridad de la información, generando las evidencias básicas para entrar en un modelo de mejora continua, con el cual se pueda lograr la actualización correspondiente y mantener en funcionamiento óptimo todo ese sistema de gestión de seguridad de la información (conocido como SGSI).

El SGSI sobre la ISO 27000 es un marco de referencia muy robusto y completo, que, para algunas organizaciones, incluyendo las IES, les resulta complicada su implementación. Sin embargo, instituciones de calidad mundial, han logrado su incorporación dentro de la cultura básica de su comunidad, y esta incorporación ha representado beneficios tácitos, tanto en la propia gestión de la seguridad de la información, como de competitividad y reconocimiento en sus mercados.

Tanto el SGSI en sus fundamentos (ISO 27001), como en sus controles operacionales (ISO 27002), generan un sistema completo para fomentar el seguimiento de la protección de la información, del resguardo y disponibilidad de esta, así como la adecuada integración de varias áreas específicas de la organización, quienes colaboran de manera estructurada y corresponsablemente para asegurar, siguiendo el riesgo institucional aceptable, el manejo de la información y de la operación que se hace en toda la institución.

Siendo una normativa completa, se necesita también contar con los elementos humanos y materiales para que la definición y la implementación de la norma se logre en un tiempo adecuado, generalmente de 1 a 2 años, y que en ese mismo sentido, se inicie el ciclo de mejora continua que se mencionó anteriormente.

Para la implementación de esta norma, se puede definir la estrategia de operacionalización sobre los 4 dominios en que se agrupa la aplicación de los 93 controles (ISO 27002) y que son los siguientes:

1. Controles tecnológicos (34 controles)
2. Controles organizacionales (37 controles)
3. Controles físicos (14 controles)
4. Controles de personas (8 controles)

Aunque también se puede realizar la implementación a partir de las 15 capacidades operativas que se estructuran y que se agrupan sobre activos de información y/o actividades más específicas; estas capacidades operativas son:

1. Gestión de eventos e incidentes de seguridad.
2. Aseguramiento de la seguridad de la información.
3. Seguridad en la relación con proveedores.
4. Gestión de la continuidad.
5. Gestión de amenazas y vulnerabilidades.
6. Gestión de identidades y accesos.
7. Seguridad de aplicaciones.
8. Configuración segura.
9. Seguridad de sistemas y redes.
10. Seguridad física.
11. Seguridad de los recursos humanos.
12. Gobernanza y ecosistema.
13. Gestión de activos de información.
14. Legal y cumplimiento.
15. Protección de la información.

Como recomendación final, es importante realizar un proceso de entendimiento y/o capacitación sobre la propia norma ISO 27000 previamente a la creación de un proyecto de implementación en las IES, porque esto aterriza los conceptos generales en elementos concretos con los que se ubique la organización, y al mismo tiempo, es recomendable acercarse a personal profesional (asesoramiento) con quien se pueda realizar un proyecto de implementación.

NIST (NIST SP 800-53 / NIST CSF 2.0, 2024)

El NIST es un marco de ciberseguridad específica de Estados Unidos, creado por el National Institute of Standards and Technology, y, de la misma forma como está estructurada la ISO 27000, el NIST consta de dos partes generales. Por un lado, lo que se conoce como el NIST SP 800-53 rev 5.0, que es la revisión

más reciente, y es un conjunto o catálogo de controles, políticas, lineamientos, protocolos, que se aplican a los activos de información de las organizaciones, y están clasificados de la siguiente manera:

1. Control de acceso.
2. Concienciación y capacitación.
3. Auditoria y responsabilidad.
4. Evaluación, autorización y monitoreo.
5. Gestión de la configuración.
6. Planificación y evaluación de contingencias (continuidad).
7. Identificación y autenticación (control de accesos).
8. Respuesta a incidentes.
9. Mantenimiento de sistemas de información.
10. Protección de medios de información.
11. Protección física y ambiental.
12. Planificación de la implementación de los controles.
13. Gestión general del plan de seguridad de la información.
14. Seguridad del personal.
15. Gestión de la privacidad de la información.
16. Evaluación de riesgos.
17. Gestión en la adquisición de sistemas y servicios de información.
18. Protección de sistemas y comunicaciones.
19. Integridad de sistemas e información.
20. Gestión del riesgo en la cadena de suministro.

Dentro de cada una de estas 20 familias de controles se desglosan específicamente más de 1,000 controles y subcontroles, lo que hace de este marco un mecanismo muy completo, pero también complicado en la selección e implementación del marco operacional para las organizaciones, y aunque se puede elegir dentro de una primera categorización que se identifica como tipo de impacto del control (bajo, moderado o alto), se necesita de un entendimiento amplio de esta normativa para poder llevar a su implementación. El otro componente del NIST se conoce como el Cyber Security Frame o CSF, que en su versión 2.0 explica desde un nivel alto y más estratégico, la gestión que, sobre el riesgo de ciberseguridad, se quiere mover la institución. Las 6 funciones que integran este marco son:

- Gobernar (donde se define la estrategia de ciberseguridad desde la alta dirección).
- Identificar (para definir la gestión de todos los activos de información que operan en la organización).
- Proteger (que desarrolla e implementa las acciones correspondientes a la protección que sobre los activos de información se tiene que hacer).

- Detectar (desarrolla acciones para identificar posibles eventos de ciberseguridad).

- Responder (sirve para crear los protocolos de acción en caso de la ocurrencia de un evento de ciberseguridad).

- Recuperar (en esta fase se definen los planes y acciones para recuperarse de un evento de ciberseguridad y mantener la operación de las organizaciones).

La incorporación de elementos de varios marcos o normas de seguridad de la información y ciberseguridad es una práctica común que siguen los equipos de seguridad de la información y ciberseguridad, con lo que se genera un marco ad hoc para la organización. Aun cuando alcanzar una certificación específica en alguno de los marcos o normas no sea un objetivo estratégico de la organización, obtener una certificación resulta muy valioso para la gestión de los riesgos aceptables en cuestión de la seguridad de la información, recordando que resulta prácticamente imposible, o considerablemente caro e inoperante, pensar en tener una organización absoluta y completamente segura e infalible, que como se dijo anteriormente, es una completa utopía.

CIS versión 8.1

Este framework o marco de referencia surge a partir de una comunidad creada en Estados Unidos desde un grupo llamado Cosmos y que ha evolucionado en 25 años hasta convertirse en el Centre for Internet Security o CIS. Consta de 18 categorías de atención en términos de la seguridad de la información y ciberseguridad en las que se incluyen 153 controles que la norma identifica como salvaguardas, que un sentido práctico, buscan ofrecer recursos, políticas, prácticas u objetivos específicos para atender lo relacionado con los activos de la información de las organizaciones.

Para establecer una modelo de madurez, CIS define tres niveles que se identifican según el grado de profundización que cada organización pretende obtener con la aplicación de la normatividad, de tal manera que dentro del primer nivel se especifican las practicas con un nivel básico, siendo también el inicio reconocido al momento de implementar este marco de referencia de la seguridad de la información; para cumplir con este primer nivel se especifican 56 salvaguardas o controles. Para el segundo nivel de madurez, se deberá cumplir con otros 74 salvaguardas o controles y se aplica para organizaciones que requieran de un nivel mayor de protección y gestión del riesgo de seguridad de la información por el tipo de activo de información que manejan. Ya para el tercer nivel, el de mayor alcance, se aplican otros 23 controles, sumando los 153 que en total se consideran para este marco de referencia. A continuación, se mencionan las 18 practicas categorías que integran al CIS en su versión 8.1:

1. Inventario y control de activos empresariales.
2. Inventario y control de activos de software.
3. Protección de datos.
4. Configuración segura de activos y software empresariales.
5. Gestión de cuentas.

6. Gestión de control de acceso.
7. Gestión continua de vulnerabilidades.
8. Gestión de registros de auditoria (logs).
9. Protección de correo electrónico y navegadores web
10. Defensas contra malware.
11. Recuperación de datos.
12. Gestión de la infraestructura de red.
13. Monitoreo y defensa de la red.
14. Concienciación y capacitación en seguridad.
15. Gestión de proveedores de servicios.
16. Seguridad del software de aplicación.
17. Gestión de respuesta a incidentes.
18. Pruebas de penetración.

Como se podrá observar en la lista anterior, los controles se relacionan de manera análoga en varios marcos de referencia, por lo que una combinación entre los marcos resulta en una práctica justamente complementaria y perfectamente adecuada.

CYBER KILL CHAIN

Aunque este marco no es exactamente un conjunto de procesos y controles para aplicar en la operación de las organizaciones, si es un mecanismo complementario para la identificación y contención de amenazas de seguridad de la información y ciberseguridad, describiendo a través de 7 fases, los pasos que se siguen en un ataque. Las 7 fases son:

1. Reconocimiento (reconnaissance, por el termino en inglés). Durante esta primera fase, se ha identificado que los atacantes buscan y recopilan cualquier clase de información que les permita definir su estrategia para el ata.
2. Armamento (weaponization). Aquí se pretende diseñar un protocolo completo de cómo, con qué y cuando aplicar elementos maliciosos que potencialmente puedan afectar a la organización en cualquiera de sus activos de información.
3. Entrega (delivery). Se refiere al proceso de entrega de ese artefacto potencialmente dañino que puede ser ingresado en la organización, en un proceso o en un activo de información.
4. Explotación (exploitation). Ya para esta fase, el artefacto o mecanismo de afectación se ejecuta buscando aprovechar una vulnerabilidad expuesta en el entorno de la organización.
5. Instalación (installation). Una vez que el mecanismo malicioso ha logrado colocarse dentro de las líneas de la organización, esta se puede instalar abriendo “huecos” en la infraestructura que

es aprovechada para realizar futuras intervenciones y afectar reiteradamente los activos de información.

6. Comando y control (command and control). Cuando esta fase se logra aplicar, el atacante hace un puente de control desde su sitio para realizar las intervenciones dentro de la infraestructura de la organización. Para entonces, el problema se ha complicado porque, de manera difícilmente perceptible, se obtiene el control hacia dentro de la organización.
7. Acciones y objetivos (actions on objetives). Se refiere a la aplicación tácita del objetivo del atacante, que puede ser extraer información, penetrar activos críticos de la organización o encriptar archivos, por mencionar algunas acciones maliciosas.

Aplicar este marco específico de ataques complementando con algún otro marco de los aquí mencionados, ayudan a los especialistas y encargados de la seguridad de la información y ciberseguridad de las IES para reforzar la estrategia institucional al respecto y considerar la integración de herramientas tecnológicas para hacer frente a las amenazas que constantemente salen en el ámbito nacional e internacional.

MITRE ATT&CK

Este es otro marco de referencia específico para identificar como se realizan las intervenciones maliciosas hacia las organizaciones por parte de los maleantes cibernéticos, que algunas veces pueden estar desde adentro de las organizaciones. Se basa en la identificación de tácticas (son objetivos estratégicos del atacante), técnicas (explican la forma como de pretenden realizar la táctica específica), y procedimientos (en donde se explican los pasos a seguir para la realización del objetivo buscado por parte del atacante). Como encuadre practico de este marco, se han definido alrededor de 14 tácticas, más de 300 técnicas y un mayor número de procedimientos, estructura que sirve para identificar ataques y la forma como contrarrestarlos.

De manera similar al marco del Cyber kill chain, el marco de Mitre ATT&ck sirve para complementar una estrategia robusta de seguridad de la información y ciberseguridad con lo cual las IES puedan hacer frente al entorno de la ciberdelincuencia que cada vez más creciente y que se ha vuelto, más complicada y compleja.

Políticas, Leyes y reglamentaciones específicas.

Aun cuando las incursiones de la ciberdelincuencia han ido creciendo de manera descomunal, tanto nacional como internacionalmente, y a pesar de la importancia que le dan al tema organismos como el Foro Económico de Davos (WEF, World Forum Economics) y considerando que en otros países o regiones, como Estados Unidos o la Unión Europea, si existe una legislación fuerte confrontar de manera legal estos asuntos, en México existe poca o nula reglamentación al respecto; apenas se han hecho sonar las voces jurídicas en ciertas intervenciones para crear, abogar y avalar, una ley de ciberseguridad que de certeza jurídica a las organizaciones fundamentadas en territorio nacional, lo que deja un vacío amplio todavía para aplicar la ley a los ciberdelitos.

Por tal razón, resulta muy importante y valioso, que las IES desarrollen sus estrategias de seguridad de la información y ciberseguridad, siguiendo uno o algunos de los marcos expresados anteriormente, para que, al menos, puedan crear controles adecuados y por sí mismas, las IES, den confianza y certeza hacia sus comunidades sobre aspectos de protección de la información, para mantener la continuidad de las operaciones universitarias, y poder subsistir en este entorno agresivo que en términos digitales se vive ahora.

Dentro de la legislación que si está aplicándose en México, existe la ley de protección de datos personales en posesión de particulares, que, aunque se creó originalmente desde el 2012, da cierta certeza a los usuarios y lineamientos de atención para las organizaciones, en términos de la protección de los activos de información y de la información en particular. A partir de marzo de 2025, se renovó y publicó en el Diario Oficial de la Federación, La Ley Federal de Protección de Datos Personales en Posesión de Particulares, dando algunas actualizaciones a la ley anterior (DOF, 20 de marzo de 2025)

También es del dominio público la promoción, mas no publicación oficial, de la ley de ciberseguridad, reglamentación que todavía no está en el ámbito aplicativo porque aún sigue en debate entre los legisladores

Ahora bien, se ha creado toda una ideología sobre otro concepto subyacente a lo generado con la legislación, refiriéndome a los “derechos digitales”, que están siendo expresados por todos los usuarios de medios digitales para quienes tienen sus entornos, cuentas, servicios y responsabilidades en el mundo digital, y que también se deben de proteger. Aspectos como la reputación, el acoso cibernético o la trata de personas desde este ámbito precisamente digital, se han ido creando y desarrollando fuera de un marco jurídico completo que marque las pautas legales y dé certeza jurídica precisamente.

Recomendaciones para gestión de incidentes de ciberseguridad en las IES (guía de incidentes).

Uno de los conceptos que se manejan prácticamente en todos los marcos de referencias, se refiere a las acciones, protocolos, procesos y controles que cuando los incidentes de ciberseguridad se presentan, dan sentido, orden y gestión de estos, toda vez que, en la práctica, los incidentes de ciberseguridad son muchos y muy variados. Desde un ataque de phishing, hasta la encriptación masivas de archivos y los ataques a la infraestructura de la operación, la gestión adecuada de los incidentes de ciberseguridad genera que la continuidad de las operaciones de las organizaciones se mantenga o se reestablezcan en plazos y formas adecuadas.

Ante esta realidad, lo mejor es tener un mecanismo eficiente de atención a todos esos incidentes que seguirán llegando, y que sirvan para proteger los ecosistemas digitales de las IES.

Siguiendo el marco del NIST, las fases en las que se debe atender un incidente de ciberseguridad son:

1. Identificar. Se refiere a la identificación de los activos de información y la relación que existe entre ellos y todo el ecosistema institucional, así como entender los riesgos y amenazas en que se se incurre por la operación y el manejo de la información.
2. Proteger. Desde esta fase se desarrollan e implementan protocolos de acción ante los incidentes de seguridad de la información y ciberseguridad; tiene que ver con la clasificación de los datos, procesos de respaldos y recuperación, gestión de vulnerabilidades de los dispositivos, capacitación y concienciación de usuarios
3. Detección. Establece las acciones para monitorear los activos registrados del ecosistema institucional, buscando identificar comportamientos fuera de parámetros previamiente definidos, que potencialmente tienen un impacto en la operación de los propios activos de información.
4. Responder. Establecer protocolo de acción cuando estos comportamientos se detecten y se defina la intervención oportuna de los mismos. Incluye los mecanismo de comunicación interna y externa.
5. Recuperar. Bajo esta fase se operan los mecanismos para recuperar la operatividad de los activos en caso un incidente de seguridad de la información.

Dentro de la norma ISO 27002, hay una capacidad operativa que atiende la respuesta de incidentes y que cuenta con una gestión similar al NIST, ya que opera la capacidad de Eventos e incidentes de seguridad siguiendo una lógica de los siguientes pasos:

1. Detectar y reportar, desde un monitoreo activo y permanente o a través de los usuarios quienes reciben una amenaza.
2. Evaluar y decidir. Una vez recibida la alerta de amenaza a la seguridad de la información de la organización, se procede a evaluar desde el grado de impacto y riesgo, hasta la valides de la alarma.
3. Intervención. En esta etapa se realiza la investigación profunda sobre el incidente, a nivel lógico y tecnológico, para identificar las vulnerabilidades y la remediación correspondiente, mediante técnicas de contención, erradicación, recuperación y resolución.
4. Una vez aplicados los procesos y protocolos correspondientes al paso anterior, se realiza el seguimiento adecuado para poder cerrar el registro del incidente.

5. Finaliza con el registro de las lecciones aprendidas y la acción proactiva para evitar o gestionar de mejor manera un futuro incidente, procurando disminuir al máximo el riesgo e impacto.

Con el CIS, se aplica el Control 17, en donde simplifican aún más la gestión de incidentes de seguridad de la información y ciberseguridad en tres fases generales:

1. Gobierno. Con la definición del proceso de atención a los incidentes y la generación de roles y funciones de cada miembro participante, así como acciones de comunicación.
2. Respuesta. Considera los mecanismos de atención sobre que hacer, como y a quien comunicarlo.
3. Recuperación. En esta fase se definen procesos y protocolos de actuación para el antes, durante y después del incidente.

Una buena recomendación es conocer los tres marcos generales de gestión de la seguridad de la información mencionados en esta sección y establecer las estrategias, procesos y acciones locales que den funcionalidad al mecanismo de gestión de incidentes de seguridad de la información y ciberseguridad de la institución. También es adecuado adoptar un marco por completo y normalizar su funcionamiento interno, inclusive a nivel de aspirar a una certificación internacional por el uso de dicho marco.

Conclusiones.

La ciberseguridad es un aspecto fundamental en todas las organizaciones, afectando directamente la operatividad, la continuidad del negocio, la reputación, la privacidad y confidencialidad de los usuarios. Al implementar las mejores prácticas de seguridad de la información, cualquier organización puede fortalecer su defensa cibernética y proteger sus activos más valiosos. Es crucial que todos estén comprometidos con estas prácticas y marcos de ciberseguridad para crear un entorno digital seguro.

Tecnologías emergentes y el futuro de la ciberseguridad

05. Tecnologías emergentes y el futuro de la ciberseguridad

Introducción

Los ciberataques realizados a través de Internet han aumentado significativamente en los últimos años, y se anticipa que nuevas tácticas puedan surgir en el futuro. Los ciberataques abarcan muchas técnicas empleadas por delincuentes informáticos para explotar vulnerabilidades en sistemas y redes electrónicas, con el objetivo de causar daño u obtener acceso no autorizado a datos sensibles.

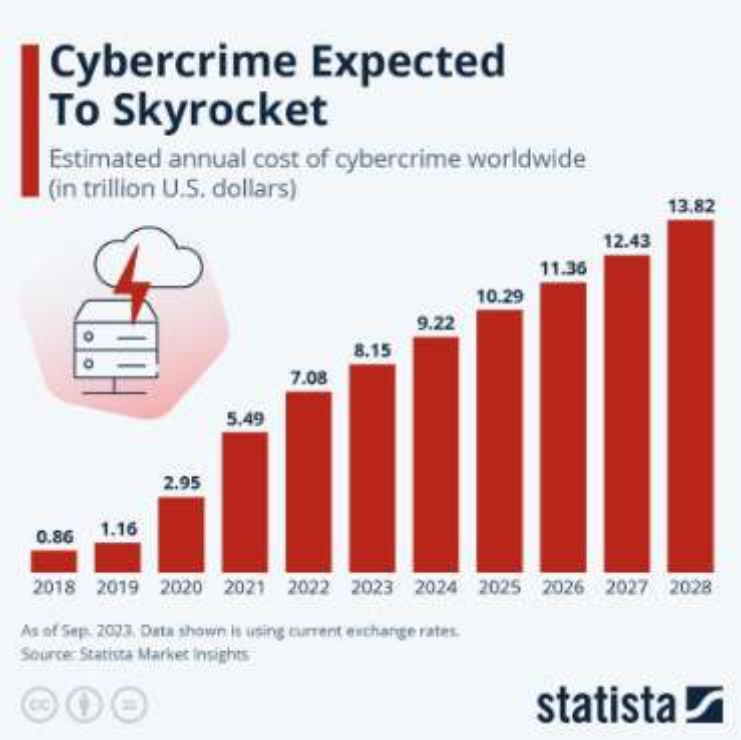
El desarrollo de la ciberseguridad enfatiza el uso de nuevas tecnologías y técnicas diseñadas para combatir las amenazas cibernéticas. Las áreas clave en los avances son la inteligencia artificial (IA) y el aprendizaje automático para la detección de amenazas, el potencial de la criptografía cuántica para asegurar canales de comunicación, la integración de la tecnología blockchain para una gestión de datos descentralizada e inviolable y la adopción de una arquitectura de confianza cero para mejorar la seguridad de la red.

Estos ataques podrían originarse de varios sitios web, incluidos aquellos que contienen enlaces engañosos, contenido falso o código dañino. Se ha demostrado que impactan a una amplia gama de organizaciones. Cualquier ciberataque representa una amenaza sustancial para la seguridad de empresas, instituciones educativas, organizaciones e individuos, ya que puede llevar a la recopilación no autorizada de datos e información de sus dispositivos. Además, se conoce que estos ataques tienen la capacidad de interrumpir servicios, operaciones comerciales y otros elementos dentro del ámbito digital. Las empresas y organizaciones deben implementar soluciones prácticas para mitigar este problema y minimizar sus efectos perjudiciales en sus operaciones digitales.

Actualmente, las organizaciones e instituciones dependen de medidas de monitoreo, detección, prevención y respuesta como los principales medios para prevenir ciberataques. Hay que estar mejorando constantemente estas tácticas y ampliando su capacidad para reconocer y comprender amenazas electrónicas.

Estos ataques pueden ser realizados por personas o grupos con fines como lucro financiero, objetivos políticos o agendas personales. La Figura 1 muestra como se proyecta que los gastos asociados con el cibercrimen superen los $23 billones para 2027. Los ciberataques emplean una variedad de métodos, incluidos virus, malware, phishing y ataques de denegación de servicio (DoS). Los virus y el malware tienen la capacidad de penetrar profundamente en los sistemas informáticos, obstaculizar su funcionamiento, robar datos valiosos y destruir archivos vitales. Estas tácticas se difunden comúnmente a través de correos electrónicos, chats instantáneos o sitios web ilícitos.

Ilustración 6 Gastos asociados al cibercrimen 2018 – 2028



Fuente: Anna Fleck. (2024, 22 de febrero). Cybercrime Expected To Skyrocket in Coming Years. Statista.

Las Instituciones de Educación Superior (IES) de México no han sido la excepción de los ataques cibernéticos, y han tenido que ir integrando nuevas tecnologías emergentes de acuerdo con sus recursos económicos y humanos, lo que se ha convertido en un componente crítico de su estrategia institucional.

Tecnologías emergentes y las IES

En un entorno educativo cada vez más influido por la tecnología, resulta fundamental comprender cómo las instituciones de educación superior en México están adoptando herramientas emergentes.

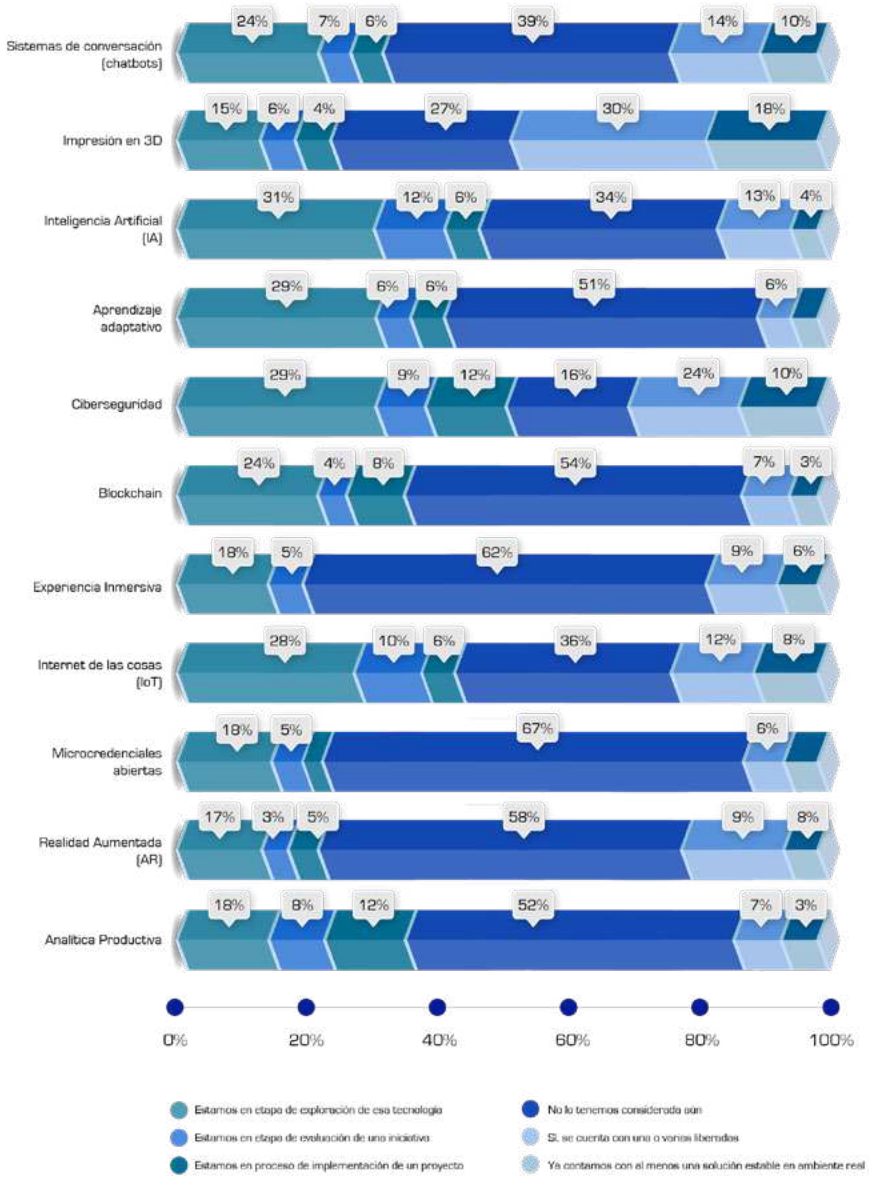
Como parte de un ejercicio de diagnóstico sobre innovación en la educación superior, se aplicó un cuestionario a 112 instituciones mexicanas con el propósito de conocer el nivel de adopción de tecnologías emergentes en sus entornos académicos y administrativos. Esta indagación se alinea con los hallazgos más recientes del Estudio de Tecnologías de la Información en Instituciones de Educación Superior 2024, elaborado por ANUIES–TIC, el cual destaca la necesidad de avanzar hacia una transformación digital estratégica, sostenible y centrada en el estudiante.

El análisis consideró once herramientas clave que están redefiniendo el panorama educativo a nivel global: chatbots (sistemas conversacionales), impresión 3D, inteligencia artificial (IA), aprendizaje adaptativo, ciberseguridad, tecnología blockchain, experiencias inmersivas, internet de las cosas (IoT),

microcredenciales abiertas, realidad aumentada (AR) y analítica predictiva.[5]

Más allá de identificar su presencia, el estudio exploró en qué áreas se están utilizando y con qué propósito. Se analizaron entornos como la docencia, el aprendizaje personalizado, el control escolar, la investigación, la innovación educativa y diversas funciones operativas.
Este tipo de diagnóstico resulta fundamental para reconocer tendencias, brechas y oportunidades en la integración tecnológica del sistema de educación superior mexicano.

Ilustración 6 Gastos asociados al cibercrimen 2018 – 2028



FUENTE: Estado Actual de las Tecnologías de la Información y Comunicaciones en las Instituciones de Educación Superior en México 2024

[5] Díaz Novelo C.H, Soto Girón A. (2024) Tecnologías emergentes: Un nuevo futuro . En J.L. Ponce López, L.M. Castañeda de León y F. López Valencia (Coords.), Estado actual de las tecnologías de la información y las comunicaciones en las instituciones de educación superior en México. Estudio 2024. México: Asociación Nacional de Universidades e Instituciones de Educación Superior.

Nuevas tecnologías

Las IES en México han comenzado a incorporar de manera progresiva diversas tecnologías emergentes como la impresión en 3D, el internet de las cosas (IoT), realidad aumentada (RA), entre otros, como puede observarse en la imagen anterior.Estas herramientas han ampliado significativamente las capacidades institucionales, permitiendo nuevas formas de enseñanza, investigación y gestión.

Sin embargo, este tipo de tecnologías conlleva nuevos desafíos, principalmente en el ámbito de la ciberseguridad, a medida que se incrementan la interconexión entre dispositivos y sistemas, también se incrementan los riesgos de ataques cibernéticos. Las principales amenazas incluyen accesos no autorizados, robo de datos personales y académicos, ataques a la infraestructura tecnológica y explotación de vulnerabilidades en dispositivos conectados, entre otros.

En este contexto, la ciberseguridad debe considerarse de forma integral, no solo como un aspecto técnico, sino como un elemento estratégico que resguarda la integridad institucional y la confianza de la comunidad académica. Implementar políticas de seguridad robustas, capacitar al personal y adoptar una cultura de prevención institucional son el punto de partida para consolidar entornos digitales seguros en el ámbito universitario.

IA Generativa y Ciberseguridad

La inteligencia artificial generativa (IA generativa) es una de las tecnologías emergentes más disruptivas. Permite crear contenido automatizado, como textos, imágenes, videos y código, lo que ofrece grandes oportunidades, pero también desafíos significativos en materia de ciberseguridad.
Riesgos de la IA Generativa

Las IES deben enfrentar posibles amenazas derivadas de un mal uso de la IA generativa, como:

- Generación de correos de phishing altamente personalizados.
- Creación de deepfakes para suplantar autoridades o manipular información.
- Automatización de malware o scripts maliciosos.
- Difusión masiva de desinformación o contenido engañoso.

Oportunidades de la IA Generativa para la Ciberseguridad

La IA generativa también puede ser una aliada, por ejemplo:

- Generación automatizada de código seguro.
- Simulación de ataques cibernéticos para pruebas de resiliencia.
- Creación de entornos de entrenamiento realistas.
- Detección temprana de incidentes mediante análisis masivo de datos.

Las universidades deben establecer lineamientos éticos y de ciberseguridad para el uso responsable de

la IA generativa, promoviendo su aprovechamiento y minimizando los riesgos.

Ciberseguridad e internet de las cosas (IoT)

El Internet de las Cosas es una red de dispositivos físicos que intercambian datos a través de Internet. Estos dispositivos contienen sensores y crean un ecosistema interconectado. Aunque han transformado varios sectores, el IoT plantea preocupaciones sobre seguridad y privacidad, ya que las medidas no son suficientes para los desafíos actuales de seguridad.

Entre las amenazas se encuentran:

- Accesos no autorizados, como insertar dispositivos USB con código malicioso.
- Problemas de cifrados si es que el dispositivo está configurado para que los datos almacenados

no se puedan visualizar.

- Denegación de Servicio (DDoS): El acceso al dispositivo es inaccesible debido a la saturación de solicitudes.,
- Comprometer el firmware: Falta de actualizaciones en el software de fabricación.
- Botnets: Dispositivos que se utilizan como bots para propagar malware.
- Ataques Man-in-the-Middle (MiTM): Intercepción de las comunicaciones entre los sistemas.
- Ransomware: Cifrar archivos del sistema.

Computación cuántica

El poder de procesamiento que permitirá la computación cuántica es otra de las tecnologías que en un futuro se espera revolucione las capacidades de la ciberseguridad. La computación cuántica es un campo multidisciplinario que une aspectos de ciencias de la computación, física y matemáticas y utiliza mecánicas cuánticas para resolver problemas complejos más rápido que las computadoras clásicas[6]. Estos equipos permitirán resolver problemas complejos mucho más rápido que los equipos de hoy, siendo una de las aplicaciones más esperadas la incorporación de estos equipos para el uso de aprendizaje máquina (machine learning), lo cual permitiría acelerar los procesos de predicción y toma de decisiones.

En el campo de la ciberseguridad, el uso de computadoras cuánticas permitirá desarrollar algoritmos de encriptación sumamente robustos, apoyando en el incremento de los niveles de protección de la información. Sin embargo, este poder de cómputo también pudiera ser utilizado de manera malintencionada por los ciberdelincuentes para vulnerar y “romper” los algoritmos que hoy día se encuentran en operación, es por ello que organismos como el NIST desarrolló en 2024 su primer grupo de algoritmos

[6] https://aws.amazon.com/what-is/quantum-computing/#:~:text=Quantum%20computing%20is%20a%20multidisciplinary,faster%20than%20on%20classical%20computers.

de encriptación para resistir ataques con computadoras cuánticas (https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based), situación que más allá del logro e importancia del trabajo realizado por los investigadores involucrados en el proyecto, nos hace reflexionar lo cerca que está la liberación de los equipos cuánticos en el mundo.

Conclusiones

Las IES mexicanas se encuentran en un punto crítico: la transformación digital es irreversible, pero su sostenibilidad depende de una gestión efectiva de los riesgos de ciberseguridad. Tecnologías como la IA generativa y la computación cuántica redefinirán los entornos digitales. Aquellas universidades que se anticipen, inviertan en conocimiento y adopten un enfoque integral de la ciberseguridad estarán mejor preparadas para proteger su misión académica, su reputación y su contribución a la sociedad.
Explorar las tendencias futuras en ciberseguridad muestra un entorno caracterizado por el rápido progreso tecnológico y los vectores de amenaza cambiantes. Tecnologías de vanguardia como la Inteligencia Artificial (IA), Blockchain, Computación Cuántica y soluciones de seguridad IoT ofrecen un potencial sustancial para mejorar la ciberseguridad y mitigar riesgos. Estas tecnologías facilitan la detección sofisticada de amenazas, el almacenamiento de datos distribuido y el cifrado que es inmune a ataques cuánticos, permitiendo a las empresas superar a los atacantes cibernéticos avanzados. Tácticas innovadoras como la automatización de ciberseguridad, marcos de confianza cero y el intercambio de inteligencia sobre amenazas trabajan junto con mejoras técnicas para crear un enfoque integral hacia la ciberseguridad. Las organizaciones deben mantenerse atentas, ágiles y colaborativas para combatir las amenazas cibernéticas en evolución. Las organizaciones pueden proteger sus activos, datos e infraestructura contra nuevas amenazas cibernéticas utilizando nuevas tecnologías e implementando medidas de seguridad proactivas en la era digital.

Reflexiones finales

- Conciencia institucional sobre la ciberseguridad, conocimiento de toda la comunidad de una institución, medidas preventivas y reactivas con el objetivo de mantener la confidencialidad, integridad y disponibilidad de la información.
- Políticas, contar con lineamientos normativos, reglamentos, guías, etc.
- Procesos: Conocimiento de estos, documentación,
- Incidentes de seguridad: conocimientos, medidas preventivas, aprendizajes, documentación.
- Apoyo de la alta dirección: Madurez, participación.
- Presupuesto: Infraestructura, herramientas, capacitación y formación
- Gestión de riesgos
- Resiliencia

Referencias

- Diaz, J., Alcántara Machado, D.S., Regalado Menchaca, J.L., Fuentes Maldonado, A., Bonola, H., Giraldo Agudelo, M., Balarezo, S., Córdova Erreis, C. G., Bartra Gardini, G., Pineda Arévalo, J. A., Santos, C. A., Sampalo Lainz, F. J. y Pedrosa, T. (Coords.). (2024). Índice de madurez en ciberseguridad de las IES iberoamericanas 2024. Iberoamérica: Metared by Universia.
- Ponce López, J.L., Vicario Solórzano, C.M. y López Valencia, F. (Coords.). (2020). Estado actual de las tecnologías educativas en las IES en México. Estudio 2020. México: Asociación Nacional de Universidades e Instituciones de Educación Superior.
- Ponce López, J.L., Vicario Solórzano, C.M. y López Valencia, F. (Coords.). (2021). Estado actual de las tecnologías educativas en las IES en México. Estudio 2021. México: Asociación Nacional de Universidades e Instituciones de Educación Superior.
- Ponce López, J.L., Vicario Solórzano, C.M. y López Valencia, F. (Coords.). (2022). Estado actual de las tecnologías educativas en las IES en México. Estudio 2022. México: Asociación Nacional de Universidades e Instituciones de Educación Superior.
- Ponce López, J.L., Castañeda de León, L.M. y López Valencia, F. (Coords.). (2023). Estado actual de las tecnologías de la información y las comunicaciones en las instituciones de educación superior en México. Estudio 2023. México: Asociación Nacional de Universidades e Instituciones de Educación Superior.
- Ponce López, J.L., Vicario Solórzano, C.M. y López Valencia, F. (Coords.). (2024). Estado actual de las tecnologías educativas en las IES en México. Estudio 2024. México: Asociación Nacional de Universidades e Instituciones de Educación Superior.

https://attack.mitre.org/
https://www.cisecurity.org/controls/v8-1
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
https://www.nist.gov/cyberframework

Ciberseguridad en las Instituciones de Educación Superior se terminó de revisar en noviembre de 2025 por la Asociación Nacional de Universidades e Instituciones de Educación Superior, en la Av. Tenayuca 200, Col. Santa Cruz Atoyac, C.P. 03310, CDMX.

Esta obra tuvo un tiraje de 1 ejemplar en su versión digital.

Evolución de la ciberseguridad en las IES de México

La transformación digital ha generado cambios sustanciales en el funcionamiento de las Instituciones de Educación Superior (IES) en México y en cómo estás dan cumplimiento a su labor en la sociedad. Si bien la tecnología ha optimizado la docencia, la investigación y la gestión administrativa, también ha expandido exponencialmente la superficie de ataque, convirtiendo a la información en el activo más valioso de las universidades y codiciado por los ciber atacantes.

Esta publicación se realiza en el marco del décimo aniversario del Comité ANUIES-TIC, quien desde su formación a colocado como un eje esencial para la transformación digital de las IES, a la seguridad de la información y en este contexto, a la ciberseguridad. La publicación ofrece un diagnóstico sobre la evolución de la seguridad de la información en el sector educativo en México. A través de un análisis detallado, se exponen los riesgos críticos actuales - como el ransomware, el phishing y la exfiltración de datos- que amenazan la continuidad operativa y la reputación de las instituciones.

Más allá del diagnóstico, este documento pretende ser una guía estratégica para la toma de decisiones y generar acciones de transformación y madurez. Aborda los retos estructurales que enfrentan las IES, desde la limitación presupuestal y la escasez de talento especializado, hasta la falta de normatividad vinculante. Para contrarrestar estos desafíos, se presentan:

- Marcos de Referencia y Buenas Prácticas: Una revisión de estándares internacionales como ISO 27000, NIST y Controles CIS para estructurar defensas sólidas.
- Gestión de Incidentes: Protocolos clave para identificar, proteger, detectar, responder y recuperar la normalidad ante ciberataques.
- Tecnologías Emergentes: Un análisis sobre el doble papel de la Inteligencia Artificial Generativa y la Computación Cuántica, tanto como herramientas de defensa como vectores de nuevas amenazas.

La publicación no solo se centra en el lado técnico de la seguridad de la información, sino que busca incentivar en la alta dirección para colocarla como un pilar estratégico en la gobernanza institucional, transitar de una postura reactiva a la creación de entornos seguros en el ámbito digital y establecer una cultura de la seguridad de la información que permee a todos los niveles y permita construir un ecosistema resiliente que permita la continuidad de la educación superior en la era digital.

Asociación Nacional de Universidades e Instituciones de Educación Superior
ANUIES
ANUIES - TIC
meta@redTIC Mx
by universia