https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 95 - 110

# Construcción de directrices para el cumplimiento normativo en infraestructuras críticas de tecnologías de la información para instancias educativas autónomas

**Información del reporte:**



Para citar este reporte técnico:

Cruz García, A. y Martínez López, A. Construcción de directrices para el cumplimiento normativo en infraestructuras críticas de tecnologías de la información para instancias educativas autónomas. *Cuadernos Técnicos Universitarios de la DGTIC, 3* (4) páginas (95 - 110). https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133

**Adriana Cruz García**
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
adriana.cruz@unam.mx
ORCID: 0009-0004-1857-7761

**Andrés Martínez López**
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
andres.martinez@unam.mx
ORCID: 0009-0002-9683-9697

## Resumen

El inminente incremento en el uso de la tecnología al interior de las instituciones educativas conlleva riesgos latentes que deben ser considerados dentro del marco legislativo y normativo institucional. Intentar llevar a cabo esta implementación de manera íntegra puede resultar excesivamente complejo y costoso, ya que estos marcos suelen ser extensos y puntualizan actividades que sobrepasan las capacidades, procesos y requerimientos de la institución. Además, estas funciones adicionales pueden generar desorganización al interior y repercutir en la productividad operativa, perdiendo de vista el objetivo central de la seguridad de la información. Por lo anterior, fue necesario el desarrollo inicial de un instrumento de cumplimiento para la gobernanza en tecnologías de la información y seguridad de la información que permitiera integrar la legislación vigente y emergente, contemplando la heterogeneidad tecnológica al interior de la Universidad

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 96 - 110

Nacional Autónoma de México. Este instrumento busca promover la coherencia institucional mediante la implementación de directrices que permitan converger a todas las entidades universitarias hacia objetivos comunes y cumplir con la función principal de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación: normar y supervisar la gobernanza institucional de las tecnologías de la información y la comunicación. Este esfuerzo sólo representa la base de un marco normativo más amplio para el manejo y supervisión de las tecnologías de la información y la comunicación, y debe ser perfeccionado acorde a su tiempo, así como acotado ante los procesos de digitalización y transformaciones inminentes al interior de la universidad.

**Palabras clave:**

Ciberseguridad, gestión tecnológica universitaria, normas de seguridad.

***Abstract***

*The imminent increase in the use of technology within educational institutions carries latent risks that must be considered within the institutional legislative and regulatory framework. Fully implementing this can be excessively complex and costly, as these frameworks are often extensive and specify activities that exceed the institution's capabilities, processes and requirements. Furthermore, these additional functions can generate internal disorganization and impact operational productivity, losing sight of the central objective of information security. Due to the above, it was necessary the initial development of a compliance instrument for information technology and information security governance that allowed to integrate current and emerging legislation, taking into account the technological heterogeneity within the Universidad Nacional Autónoma de México. This instrument seeks to promote coherence through the implementation of guidelines that allow all university entities to converge toward common objectives and fulfill the main function of the Dirección General de Cómputo y de Tecnologías de Información y Comunicación: to regulate and supervise the institutional governance of information and communication technologies. This effort only represents the basis of a broader regulatory framework for the management and supervision of information and communications technologies and it must be perfected in accordance with the times, as well as delimited in light of the digitalization processes and imminent transformations within the university.*

***Keywords:***

*Cybersecurity, university technological management, security norms.*

# 1. INTRODUCCIÓN

A partir del incremento en el uso de las Tecnologías de la Información y Comunicación (TIC) en las instituciones, ha sido fundamental contar con marcos de referencia para su gobernanza; sin embargo, la mayor parte de pautas establecidas por diferentes organizaciones, tanto nacionales como internacionales, se enfocan en industrias del sector financiero, industrial, comercial o de telecomunicaciones, dejando a un lado el sector educativo y obligando a entidades universitarias a crear modelos de gobernanza que respalden sus estrategias y marcos regulatorios (Cordero Guzmán & Bribiesca Correa, 2018).

Por lo anterior, las organizaciones, en general, se han visto envueltas en una transformación digital, sin embargo, es fundamental que tanto las herramientas como los instrumentos normativos y de control

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 97 - 110

también sean actualizados con este nuevo enfoque. Por ello, es importante que las instituciones de educación superior, que afirman ser líderes en su dominio y buscan mantenerse dentro de un escenario competitivo, desarrollen y evolucionen íntegramente sus modelos de operación y de normatividad (Benavides et al., 2020).

Como afirman Zhong, Vatanasakdakul y Aoun, los marcos de Gobernanza de TIC necesitan adaptarse a la cultura de cada región y país, en el que el conocimiento y experiencia dentro de cada organismo será influyente (Zhong et al., 2012). Es así como se plantea una problemática para la Universidad Nacional Autónoma de México (UNAM), una de las universidades más importantes a nivel nacional y latinoamericano, que, dada su extensa pluriculturalidad y una heterogeneidad tecnológica a través de sus diferentes campus, facultades y entidades, ha tenido la necesidad de normar y supervisar la gobernanza de las Tecnologías de Información y Comunicación, función de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC).

Para tal efecto, la DGTIC ha impulsado el desarrollo de documentos normativos que permitan comprobar el nivel de cumplimiento en las infraestructuras de Tecnologías de la Información dentro de cada entidad universitaria, con el propósito de robustecer la gobernanza en TIC dentro de la universidad. Este esfuerzo busca alinear instrumentos técnicos existentes e identificar cuáles carecían de atención.

El objetivo del presente reporte técnico es abordar la metodología y los criterios discernidos para el desarrollo de las *Directrices generales en torno a la seguridad de la información que obra en los sistemas informáticos de la UNAM* (DGTIC-UNAM, 2023), con el propósito de apoyar a las entidades y dependencias de la universidad en el cumplimiento de medidas de seguridad en los sistemas informáticos, instrumento que favorece una gobernanza íntegra en TIC al interior de la UNAM.

## 2. DESARROLLO TÉCNICO

La información al interior de la UNAM es uno de los insumos para mantener las tres tareas sustanciales de esta institución: la docencia, la investigación y el desarrollo cultural; a través de las cuales se maneja información de carácter sensible y/o confidencial como son los trabajos de investigación orientados a la academia, así como los datos personales de la comunidad universitaria. Esto convierte a la institución en un objetivo codiciado para los ciberdelincuentes, quienes buscan la obtención de esta información para fines ilícitos, manchando la reputación y confianza de la universidad.

Es importante tener en claro que proteger un activo no se trata sólo de la computadora en la que se almacenan datos. De acuerdo con Computer Security Resource Center, un activo debe comprenderse como:

> Un elemento de valor para las partes interesadas. Un activo puede ser tangible (p. ej., un elemento físico como hardware, firmware, plataforma informática, dispositivo de red u otro componente tecnológico) o intangible (p. ej., personas, datos, información, software, capacidad, función, servicio, marca registrada, derechos de autor, patente, propiedad intelectual, imagen o reputación). El valor de un activo lo determinan las partes interesadas considerando las posibles pérdidas a lo largo de todo el ciclo de vida del sistema. Estas preocupaciones incluyen, entre otras, las relacionadas con el negocio o la misión. (NIST, s.f.)

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 98 - 110

El modelo más sencillo consistiría en implementar todos los sistemas e infraestructuras de TIC de forma idéntica, lo que permitiría mantener un cerco controlable de la información; sin embargo, la implementación de éste causaría un gran impacto en los recursos universitarios debido a que la universidad mantiene una diversidad de tecnologías, incluso algunas desarrolladas con adaptación a los recursos y requerimientos específicos de las entidades y dependencias, las cuales han evolucionado y fortalecido con el paso del tiempo.

Esta situación implica realizar un instrumento orientado a la gobernanza de TIC enfocado en la seguridad de la información al interior de la universidad; como lo indica Carlos Franco Reboreda (2024) en su artículo "Gobierno de las Tecnologías de Información":

> El propósito fundamental del Gobierno de TI es ofrecer principios rectores claros y precisos para los integrantes de la dirección de las organizaciones y las personas que los respaldan en su gestión. Estos principios están diseñados para garantizar que el uso de la tecnología de la información sea eficaz, eficiente y aceptable desde un punto de vista ético y operativo.

Actualmente, la universidad cuenta con una serie de documentos normativos que abordan la seguridad de la información y que obedecen a las buenas prácticas, sin embargo, son esfuerzos aislados que no se articulan entre sí, por lo que se requiere de un instrumento que realice una estructura integral que aborde aspectos digitales y físicos.

El instrumento, que en lo sucesivo se denominará *Directrices-Ciberseguridad-UNAM*, si bien debe adaptarse a los recursos y necesidades con los que cuenta la universidad, también debe mantener una trazabilidad y facilitar su implementación al interior de las entidades y dependencias, ocupando como referencia marcos normativos internacionales que impulsen la credibilidad y solidez en la implementación.

Con esto, no se pretende que las entidades y dependencias realicen un retrabajo de su infraestructura, sino que realicen un análisis crítico por medio de una estrategia metódica para identificar áreas de mejora y elementos que puedan optimizarse con base en sus necesidades. Posteriormente, podrán explorar las alternativas viables para la adaptación e implementación en sus respectivas áreas, dando paso a un gobierno de Tecnología de la Información.

## 2.1 METODOLOGÍA

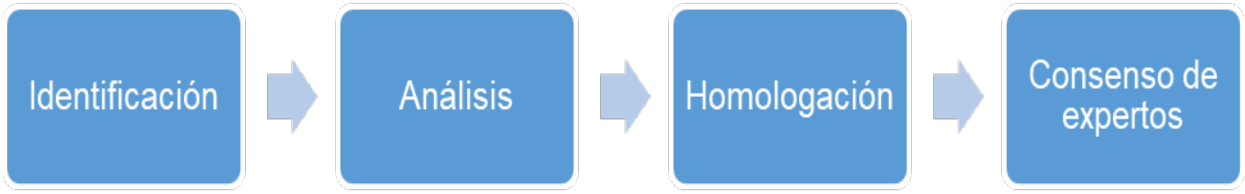
Para iniciar las primeras investigaciones e identificación preliminar de los tipos de activos que serían involucrados en una primera versión de las *Directrices-Ciberseguridad-UNAM*, se tuvo en claro que el documento debería ser elaborado tomando como referencia marcos internacionales. Esto permitió acercar a la universidad a puntos de comparación más allá del ámbito nacional, vislumbrando que, en un posible futuro, este tipo de documentos normativos puedan ser un punto de partida para la colaboración y retroalimentación entre instituciones educativas.

Para abordar las problemáticas inherentes en el desarrollo de un documento normativo que permita alinear instrumentos de cumplimiento técnico, dada la heterogeneidad tecnológica al interior de la universidad como principal desafío, se implementó una metodología que permitiera seguirse en futuras revisiones, descrita en 4 fases:

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 99 - 110

**Figura 1**

*Diagrama de la metodología seguida*



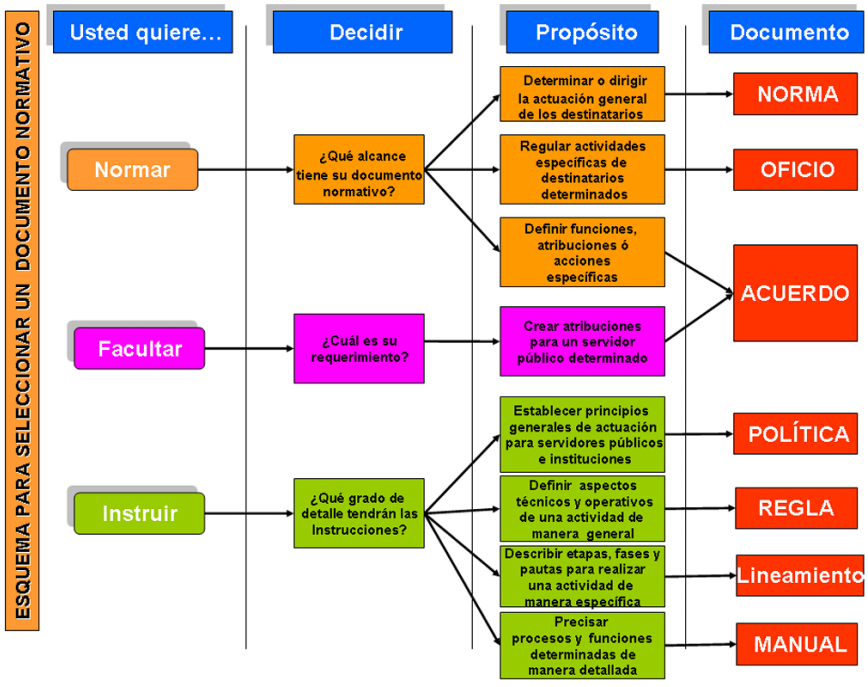

## Identificación del tipo de instrumento a desarrollar

De acuerdo con la *Guía para emitir documentos normativos* en su tercera edición, expedida por el Gobierno Federal, se busca "un instrumento que facilite el desarrollo y estandarización de su marco normativo, haciéndolo, simple, ágil y de fácil aplicación" (Subsecretaría de la Función Pública [SFP], 2011).

De esta forma, para determinar qué tipo de instrumento se requería, se tomó como base su esquema propuesto (Figura 2), identificando que, para este estudio, se buscaba la creación de un documento normativo que permitiese instruir a titulares y responsables TIC de las diferentes entidades y dependencias, a fin de evaluar y robustecer la gobernanza y seguridad de la información de su propia infraestructura TIC.

**Figura 2**

*Esquema para la selección de documentos normativos*




*Nota.* De la *Guía para emitir documentos normativos*, por la Subsecretaría de la Función Pública, 2011.

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 100 - 110

## 2.1.1 ANÁLISIS NORMATIVO ESTRUCTURADO

La implementación efectiva de estándares o documentos normativos en materia de seguridad de la información y gobernanza de TIC no puede llevarse a cabo sin el empleo de marcos de ciberseguridad que proporcionen procesos de alcance, implementación y evaluación, ofreciendo lineamientos aplicables dentro de una organización. Estos marcos otorgan una estructura y metodología general para proteger activos informáticos críticos (Taherdoost, 2022). Una vez adaptado este proceso al contexto de la universidad e identificado el tipo de instrumento a desarrollar, con un contexto internacional en mente, se procedió a realizar un análisis de cinco marcos normativos establecidos por diversas organizaciones en materia de seguridad de la información:

- NIST SP 800-53 Rev.5 Controles de seguridad y privacidad para sistemas de información y organizaciones (NIST, 2020): Este marco normativo enlista una serie de controles de seguridad y privacidad dirigidos a organizaciones que buscan proteger sus operaciones y activos a través de un proceso a nivel organizacional, es decir, que están muy relacionados con la filosofía y operación de la organización desde una visión de capacidad y salvaguarda de la información. Este estándar cuenta con 20 familias de controles, teniendo en cada familia controles base y, en algunos casos, controles de reforzamiento, sumando más de 1000 controles según el caso; en este trabajo, se utilizó la versión con 1189 controles. Así mismo, se encuentran clasificados como controles comunes, controles específicos del sistema y controles híbridos.
- NIST SP 800-171 Protección de información controlada y no clasificada en sistemas y organizaciones no federales (NIST, 2024): Existe información que puede impactar en procesos críticos que afecten otras instancias de carácter gubernamental. Este marco normativo proporciona controles para preservar la confidencialidad de información cuando ésta reside en sistemas y organizaciones no federales, como es el caso de la universidad en su calidad de autónoma. Los controles buscan salvaguardar la información que se procesa, transmite y almacena en los sistemas y activos, evaluando los requisitos de seguridad. Este estándar cuenta con 17 familias de controles. Cada familia cuenta con sus requisitos de seguridad. En este caso, al hablar de requisitos, nos referimos a un contexto específico de un control de seguridad.
- Marco de Ciberseguridad del NIST (NIST, 2024): Este marco normativo es una guía para identificar el nivel de madurez de la organización independientemente del tamaño que tenga. Esto permite identificar las oportunidades de mejora y orientar sobre sus iniciativas de ciberseguridad que podrían complementar sus controles actuales para lograr resultados exitosos. Este marco no contiene controles a implementar, en su caso, se dividen en 106 subcategorías, las cuales, para este trabajo, se utilizaron como referencia; estas subcategorías se encuentran agrupadas en 6 funciones principales: gobernar, identificar, proteger, detectar, responder y recuperar.
- Controles de Seguridad Críticos de CIS (CIS, 2023): Este conjunto de controles se vislumbran desde una perspectiva de estrategia técnica. Estos controles se centran en medidas de seguridad simplificadas para atender una acción específica. Se dividen en 18 familias técnicas, de las cuales derivan 153 acciones específicas tanto de carácter técnico como administrativo. Estas acciones, a su vez, se encuentran clasificadas en grupos para implementar: básicos, intermedios y avanzado; esto según el nivel de madurez de la organización.
- ISO/IEC 27001 Seguridad de la Información (ISO/IEC, 2013): Es una norma orientada a sistemas de

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 101 - 110

gestión de seguridad de la información y se basa en un sistema de controles que permita gestionar los riesgos asociados a la seguridad de datos al interior de una organización. Esta norma se alinea con otras normas ISO, lo que permite una implementación conjunta basada en la mejora continua. Para este caso, se utilizó la norma que se divide en 14 temas centrales, de los cuales se derivan 114 controles orientados a la seguridad de la información tanto física y tecnológica como de los usuarios. Aunque esta norma fue actualizada en 2022, se establece un período de transición de tres años durante el cual su vigencia sigue siendo válida.

El estudio de los marcos normativos proporcionó una serie de ideas que fueron integradas y articuladas con el fin de desarrollar una propuesta orientada a las particularidades y demandas de la universidad.

## 2.1.2 HOMOLOGACIÓN DE LOS ELEMENTOS APLICABLES

Como se menciona en el marco de Gestión Integrada de Riesgos de Ciberseguridad (i-CSRM) (Kure et al., 2022): "Identificar los objetivos de seguridad de los activos es vital para que una organización determine qué aspectos críticos de la seguridad debe garantizar cada activo durante su procesamiento, almacenamiento o transmisión por parte de sistemas, aplicaciones o personas autorizadas", por lo que se abordó un análisis comparativo de los cinco marcos de trabajo estudiados, identificando áreas de convergencia que resultan pertinentes y aplicables al contexto universitario, así como tomando en cuenta los aspectos técnicos fundamentales para la seguridad de la información.

En total, se obtuvo una matriz de 1138 elementos, homologando aquellos puntos que aportaban valor a las tareas esenciales de la universidad. Para incluir o descartar los elementos, se tomaron dos consideraciones importantes:

1. Que los elementos se alinearan a las actividades esenciales de la universidad: docencia, investigación y cultura.
2. Que los elementos repetitivos y consistentes en los marcos normativos fueran unificados.

**Figura 3**

*Método para la homologación de aspectos técnicos*


*Nota.* De *Directrices generales en torno a la seguridad de la información que obra en los sistemas informáticos de la UNAM* de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, 2023.

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 102 - 110

El análisis realizado permitió identificar y seleccionar un conjunto mínimo de controles considerados estrictamente indispensables para una infraestructura informática con enfoque en seguridad de la información. El objetivo principal fue alinear controles con la normativa vigente e identificar posibles brechas de seguridad existentes, tomando en cuenta los distintos contextos que enfrenta cada entidad universitaria.

### 2.1.3 CONSENSO DE EXPERTOS

Como parte final del desarrollo, se entregó un manuscrito de las *Directrices-Ciberseguridad-UNAM* a varios especialistas en tecnologías de información y comunicación pertenecientes a distintas entidades y dependencias de la UNAM, con el propósito de obtener una revisión crítica con base en su conocimiento y experiencia.

Este consenso de expertos debe ser visto como una fuente de conocimiento que sustenta acuerdos construidos colectivamente para la toma de decisiones informadas a través de sus funciones principales, tales como la definición y estandarización de conceptos, terminologías y mediciones. De igual forma, se evalúa la calidad de los resultados y se emiten juicios de valor (Jorm, 2025) tanto técnicos como normativos que permitan aproximar las *Directrices-Ciberseguridad-UNAM*, como instrumento de cumplimiento técnico, a una versión completa que abarque, en lo general, las necesidades de la universidad y, en lo particular, las características fundamentales para la seguridad dentro de infraestructuras informáticas.

La metodología aquí sugerida es adaptable y permite su aplicación en cada actualización o mejora que se plantee realizar al instrumento normativo, con la finalidad de asegurar su mejora continua e innovación ante el inminente progreso de la entidad y de la propia universidad.

## 3. RESULTADOS

Como fruto de este análisis, se desarrolló el documento normativo *Directrices generales en torno a la seguridad de la información que obra en los sistemas informáticos de la UNAM* (DGTIC-UNAM, 2023) para apoyar a las entidades y dependencias de la universidad. Éste es el primer esfuerzo en consolidar criterios técnicos referidos en marcos normativos internacionales mediante un análisis que sea personalizable a las necesidades específicas de cada entidad.

### 3.1 CRITERIOS CONSIDERADOS PARA EL DESARROLLO DE LAS DIRECTRICES-CIBERSEGURIDAD-UNAM

La elección de los tópicos se originó considerando los siguientes factores:

- Ser un documento corto, de fácil entendimiento e implementación sencilla, con la intención de que sea adaptado por todas las áreas de cómputo o afines, en donde exista incluso una sola persona a cargo de los sistemas de información.
- Ser diseñado tomando en consideración los marcos de referencia para que el instrumento tenga un sustento teórico, evitando cualquier tipo de arbitrariedad en el contenido.
- Ser lo suficientemente flexible para la aplicación en la heterogeneidad de las tecnologías y de los sistemas existentes en la UNAM.

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 103 - 110

- Ser lo suficientemente acotado a los sistemas de información y no abarcar otros servicios que provoquen la ambigüedad o confusión por parte de los responsables.

Como se mencionó en la sección "2.1.2 Homologación de los elementos aplicables", al realizar la revisión de estándares, se identificaron puntos de coincidencia entre los diferentes controles y requisitos analizados, relevantes en el ámbito universitario, lo que dio como resultado las directrices existentes

## 3.2 CONTENIDO DEL DOCUMENTO

El instrumento culminó con 13 directrices:

1. Control de acceso
2. Sensibilización y formación
3. Revisión y rendición de cuentas
4. Gestión de la Configuración
5. Identificación y autentificación
6. Respuesta a incidentes
7. Mantenimiento
8. Control de medios digitales
9. Seguridad del personal
10. Protección física
11. Evaluación de la seguridad
12. Protección del sistema y las comunicaciones
13. Integridad del sistema y de la información

Estas directrices permiten a las entidades universitarias evaluar y robustecer la gobernanza y seguridad de la información de su propia infraestructura TIC, así como su grado de cumplimiento con respecto a la legislación. Adoptar las *Directrices-Ciberseguridad-UNAM*, como marco de referencia, ayuda a la identificación de brechas y a priorizar acciones tanto preventivas como correctivas, alcanzando a ser la base para el desarrollo de planes de mejora continua y de recuperación ante desastres.

Se aborda una ontología relacional en la que los diferentes elementos heterogéneos de la infraestructura de TIC (incluidos desde los recursos humanos hasta resultados algorítmicos) son definidos a través de sus redes relacionales (Sullivan, 2022) y no sólo vistos como entes individuales que deben de ser abordados de forma separada. Este enfoque incorpora conceptos como la seguridad en profundidad, como lo define el NIST (NIST, s.f.), entendida como una estrategia de la seguridad de la información que integra a las personas, la tecnología y las capacidades operativas. De esta manera, se establecen controles variables en múltiples capas, logrando con ello una integración de los diferentes activos involucrados directa e indirectamente a la infraestructura informática de las entidades universitarias.

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 104 - 110

Dentro de los juicios de valor de los expertos, es consensuado que las *Directrices-Ciberseguridad-UNAM* sirven como respaldo normativo para los responsables en tecnologías de la información que constantemente emiten propuestas innovadoras y, de la misma forma, son minimizadas o postergadas hasta que un incidente de seguridad sucede, entorpeciendo parte de la transformación digital a la que debe someterse una institución competitiva.

## 3.3 DOCUMENTOS TÉCNICOS Y NORMATIVOS RESULTANTES

Como lo mencionamos anteriormente, la universidad mantiene una diversidad de tecnologías implementadas que ofrecen, a su vez, diferentes servicios a la comunidad universitaria; para éstos, las *Directrices-Ciberseguridad-UNAM* son un apoyo para identificar las áreas de mejora en la seguridad de la información. Con base en este instrumento, la DGTIC ha logrado gestionar de manera significativa la política de seguridad de la entidad, documento que se ha vuelto regidor y obligatorio para las áreas al interior.

Así mismo, y a manera de ejemplo, en la Coordinación de Seguridad de la Información dentro de la DGTIC, se tienen desarrolladas guías técnicas de instalación o configuración de diversas herramientas que se comparten con responsables TIC como recomendaciones para ayudarlos a robustecer su infraestructura informática. A partir de la creación de las *Directrices-Ciberseguridad-UNAM*, abordadas en este documento, ha sido posible alinear las guías técnicas con los puntos referenciados en las directrices, considerando este instrumento como referente para la evaluación del cumplimiento en materia de seguridad de la información dentro de su infraestructura; de esta manera, se deja en los responsables TIC el análisis e implementación de dichas guías teniendo en cuenta el contexto de su entidad universitaria y partiendo de que las recomendaciones proporcionadas responden al cumplimiento de la legislación en materia de gobernanza de TIC y seguridad de la información.

Como se describe en la Tabla 1, el impacto de las *Directrices-Ciberseguridad-UNAM* es significativo al interior de la universidad, ya que, al constituirse como instrumento normativo y de orientación, brinda un marco de referencia para las diversas entidades y dependencias universitarias, permitiendo alinear la documentación vigente y establecer lineamientos fundamentales en la creación de nuevas políticas o documentos normativos. Esto conlleva de manera inherente la actualización e innovación en los procesos y controles en los activos informáticos universitarios.

**Tabla 1**

*Impacto de las directrices*

| Elemento clave | Descripción | Impacto de las directrices |
|---|---|---|
| Diversidad tecnológica | La universidad tiene múltiples tecnologías y servicios implementados. | Instrumento de cumplimiento técnico adaptable a cualquier tecnología o servicio. |
| Análisis de cumplimiento | Proceso sistemático para evaluar el cumplimiento de una entidad en materia de Gobernanza de TIC y Seguridad de la Información. | Permite identificar puntos de cumplimiento y de mejora al interior de la institución |

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 105 - 110

| Elemento clave | Descripción | Impacto de las directrices |
|---|---|---|
| Desarrollo de políticas | Instrumento normativo que la institución debe seguir para proteger su información, sistemas y activos informáticos. | Funge como pauta para el desarrollo de documentos normativos para la gobernanza en las infraestructuras de TI y resguardo de la información que debe ser ajustada al contexto y necesidades específicas de las entidades y dependencias. |
| Guías técnicas | Guías técnicas desarrolladas al interior de una dependencia o entidad universitaria como parte de su documentación. | Las guías técnicas se ajustan y alinean a las directrices, respondiendo conforme a la legislación universitaria |

Uno de los beneficios más relevantes de contar con las *Directrices-Ciberseguridad-UNAM* es promover la coherencia institucional en la aplicación de controles de cumplimiento técnicos y normativos en materia de Gobernanza de TIC y de Seguridad de la Información, sin importar el nivel de avance tecnológico o particularidades de cada infraestructura informática al interior de la universidad. Al tratarse de un instrumento integrador, permite que todas las áreas converjan hacia objetivos comunes, permitiendo una transformación digital mediante la innovación pertinente de los lineamientos y legislación que rigen en cada una de las entidades y dependencias universitarias.

## 3.4 TRABAJO CONSTANTE

El estudio y metodología planteada en este reporte técnico es sólo la base de un marco de referencia normativo cuyo desarrollo deberá continuar en fases posteriores. El verdadero valor en el esfuerzo aquí constituido radica en la capacidad de evolución, adaptación y perfeccionamiento a medida que se afrontan nuevos desafíos tecnológicos, incluyendo las amenazas constantes que enfrenta la universidad.

## 3.5 PRESERVACIÓN DEL INSTRUMENTO

Los marcos normativos, como el resultado de este trabajo, no deben entenderse como productos finales o estáticos, sino como procedimientos que deben mantenerse constantemente actualizados, considerando los cambios en las circunstancias, el entorno, las necesidades del contexto institucional y los riesgos identificados (Angraini et al., 2019); así mismo, es necesario acompañar el desarrollo y procurar mantener la calidad, pero, sobre todo, preservar el objetivo.

De esta manera, como parte de la preservación del instrumento, es necesario incorporar en un futuro a corto o mediano plazo un instrumento de medición que establezca indicadores e intervalos de referencia para determinar de manera cuantitativa su nivel de cumplimiento. Uno de los mecanismos que podrían adoptarse sería el estipulado en la ISO 27004 que establece:

> Este documento proporciona directrices para ayudar a las organizaciones a evaluar el rendimiento de la seguridad de la información y la eficacia de un sistema de gestión de la seguridad de la información. (International Organization for Standardization & International Electrotechnical Commission [ISO/IEC], 2016)

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 106 - 110

A través de ciclos de mejora continua que aborden las siguientes etapas:

1. Identificar las necesidades de la información.
2. Crear y mantener medidas.
3. Establecer procedimientos.
4. Monitorear y medir.
5. Analizar resultados.
6. Evaluar el desempeño de la seguridad de la información y su efectividad.

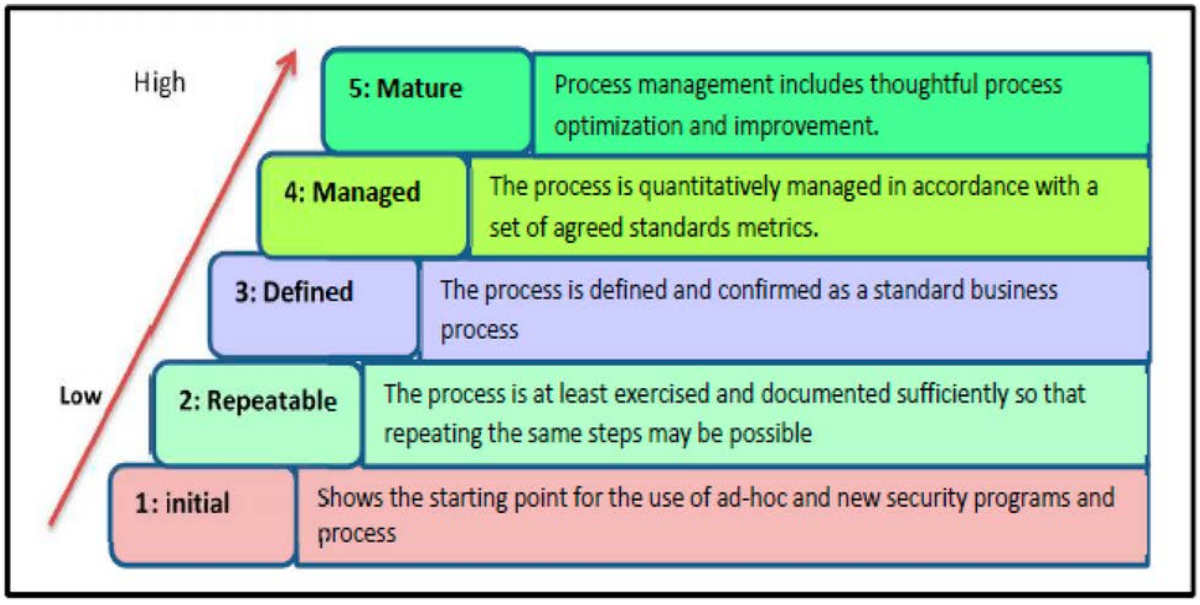
El procedimiento es estructurado y puede modificarse a las necesidades de cada entidad y dependencia universitaria. Es de vital importancia construir un instrumento de estas características, pero con tiempos y recursos de implementación mínimas, ya que un instrumento muy extenso impactaría negativamente la continuidad operativa, sobre todo en aquellas entidades donde los responsables de tecnología de la información y comunicación se reducen a una sola persona; este instrumento se plantea para investigaciones futuras.

## 3.6 EVALUACIÓN DE MADUREZ

Finalmente, debe plantearse una evaluación del nivel de madurez, como lo menciona Henock Mulugeta Melaku (2023), que describe de forma concisa y estandarizada la postura de seguridad de una organización teniendo como referencia una escala de cinco procesos, como se muestra en la Figura 4:

**Figura 4**

*Procesos para la evaluación del nivel de madurez*




*Nota.* De "A dynamic and adaptive cybersecurity governance framework.", por Melaku, H. M., 2023.

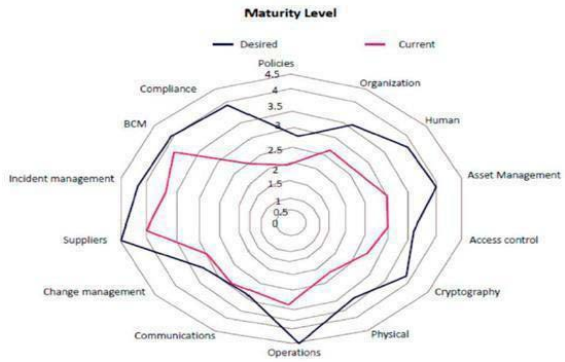
https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 107 - 110

1. Inicial: Muestra que la institución comienza a implementar controles de seguridad, pero bajo ningún estándar, proceso definido o buena práctica. Los procesos de seguridad no se evalúan o auditan.
2. Repetible: Las prácticas y procesos de seguridad se documentan para su repetición, sin embargo, no existen métricas de evaluación.
3. Definido: Los procesos están definidos como un estándar. La organización puede analizar riesgos y proponer contramedidas.
4. Gestionado: Los procesos se gestionan cuantitativamente bajo métricas consensuadas.
5. Madurez: En este punto, la institución cuenta con los procesos de seguridad implementados y comienza su optimización bajo un esquema de mejora continua, rigiéndose por políticas y directivas bien definidas. Su efectividad se evalúa periódicamente mediante indicadores de rendimiento.

Esto permitirá contrastar el nivel de madurez actual de la entidad o dependencia universitaria contra el deseado, destacando brechas o puntos de mejora en cada uno de los procesos o controles implementados como se observa en el ejemplo de la Figura 5.

**Figura 5**

*Ejemplo - Gráfico comparativo del nivel de madurez deseado contra el actual*




*Nota.* La línea de color rojo representa el nivel de madurez alcanzado, que contrasta con la línea de color negro que es el nivel de madurez deseado en los diferentes procesos. De "A dynamic and adaptive cybersecurity governance framework.", por Melaku, H. M., 2023.

## 4. CONCLUSIONES

Uno de los principales objetivos de implementar una gobernanza de tecnologías de la información y comunicación es integrar los recursos tecnológicos con las tareas sustanciales de una organización. Al realizar una correcta implementación, contribuye a mantener un marco de control estructurado, beneficia la eficiencia operativa y se mantiene como prevención para la seguridad de la información; así mismo, busca asegurar la continuidad, eficacia y evolución a futuro.

Derivado de lo anterior, se ha expuesto el estudio y análisis de marcos referenciados en materia de seguridad de la información como parte de una transformación digital que busca la innovación en la

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 108 - 110

normatividad existente y la legislación emergente al interior de entidades universitarias. Los marcos analizados pueden verse acotados debido a sus limitaciones específicas en los componentes tecnológicos, así como la interoperabilidad de estos mismos (Dunsin, 2024), sin dejar de lado las limitantes *per se* de los recursos humanos. Por tal motivo y como se ha mencionado, el desarrollo de este tipo de normativa siempre debe de tomar en cuenta la heterogeneidad y la diversidad tecnológica presentes en el contexto específico de cada entidad.

Cada entidad o dependencia puede definir e implementar las medidas que mejor se adapten a sus recursos y necesidades; las *Directrices-Ciberseguridad-UNAM* ofrecen un primer acercamiento no vinculante, ni limitativo, mismo que busca evolucionar en una fase posterior.

La implementación del instrumento no debe dar por sentado que exista una certeza absoluta de que no se presentarán incidentes de seguridad, como lo menciona Bejarano y Martín en la Revista Management & Innovation:

> **Los ciberataques no se pueden evitar, pero su impacto en el negocio sí se puede controlar.** La resiliencia de la empresa (no de la tecnología) es el objetivo último de cualquier estrategia de ciberseguridad. Los pilares de la mejor estrategia son la sinceridad y la responsabilidad. Las empresas deben actuar ya: la ciberseguridad dejó de ser un problema de TI; ahora ya es evidente para todos que es un reto clave del negocio que debe ocupar una posición destacada en las agendas de la Alta Dirección y los Consejos de Administración. (Bejarano & Martín, 2021)

Hoy en día, nos encontramos en un mundo cada vez más interconectado digitalmente, por lo que salvaguardar la integridad, confidencialidad y disponibilidad de la información se considera una necesidad para mantener las actividades sustanciales de la universidad. Implementar controles permite la prevención de incidentes y pérdidas de información, posibilitando una organización estructurada que aporta valor a la universidad; sin embargo, se debe establecer un ciclo de revisión, ya que el continuo avance tecnológico impide que la seguridad se refleje en un 100%.

En términos generales, las *Directrices-Ciberseguridad-UNAM* cumplen con el objetivo principal de normar y supervisar la gobernanza institucional de las tecnologías de información y comunicación al interior de la universidad. Asimismo, sientan las bases para futuros desarrollos y actualizaciones de los instrumentos de cumplimiento normativo en materia de gobernanza de TIC, con un enfoque en seguridad de la información. Además, promueven una perspectiva flexible, progresiva y adaptable al cambio tecnológico constante, siendo un medio de prevención para minimizar el impacto ante situaciones que comprometan la seguridad de la información.

## REFERENCIAS

Angraini, R., Alias, R. A., & Okfalisa. (2019). Information security policy compliance: Systematic literature review. *Procedia Computer Science*, 161, 1216–1224. https://doi.org/10.1016/j.procs.2019.11.235

Bejarano, F., & Martín, J. L. (2021). La ciberseguridad no es un problema de TI, nunca lo fue. *Harvard Deusto Management & Innovation*, (39). https://www.harvard-deusto.com/la-ciberseguridad-no-es-un-problema-de-ti-nunca-lo-fue

Benavides, L. M. C., Tamayo Arias, J. A., Arango Serna, M. D., Branch Bedoya, J. W., & Burgos, D. (2020). Digital transformation in higher education institutions: A systematic literature review. *Sensors*,

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 109 - 110

20(11), 3291. https://doi.org/10.3390/s20113291

Center for Internet Security. (2023). CIS *Critical Security Controls Version 8.1*. https://www.cisecurity.org/controls/v8-1csf.tools+2

Cordero Guzmán, D., & Bribiesca Correa, G. (2018). Model for information technology governance (GTI) in a university environment. *Computación y Sistemas*, 22(4), 1503–1518. https://doi.org/10.13053/cys-22-4-2797

CSRC Content Editor. (n.d.-c). *Asset – Glossary*. National Institute of Standards and Technology. https://csrc.nist.gov/glossary/term/asset

CSRC Content Editor. (n.d.-c). *Defense-in-depth – Glossary*. National Institute of Standards and Technology. https://csrc.nist.gov/glossary/term/defense_in_depth

Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (2023). *Directrices generales en torno a la seguridad de la información que obra en los sistemas informáticos de la UNAM*. Universidad Nacional Autónoma de México. https://www.red-tic.unam.mx/directrices-seguridad-informacion

Dunsin, D. (2024). Evaluating cybersecurity frameworks for protecting consumer IoT devices from emerging phishing and ransomware threats. *Journal of Cybersecurity and Privacy, 3*(4), 327–350. https://doi.org/10.3390/jcp3040017

Franco Reboreda, C. (2024). Gobierno de las Tecnologías de Información. En J.L. Ponce-López, L.M. Castañeda-De León y H. Valles-Baca (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.

International Organization for Standardization & International Electrotechnical Commission. (2013). *ISO/IEC 27001:2013 – Information security, cybersecurity and privacy protection – Information security management systems* – Requirements.

International Organization for Standardization & International Electrotechnical Commission. (2016). *ISO/IEC 27004:2016 – Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluations*. https://www.iso.org/standard/64120.html

Jorm, A. (2025). Specifying "Experts" and "Consensus". In: *Expert Consensus in Science*. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-97-9222-1_7

Kure, H.I., Islam, S. & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for critical infrastructure protection. *Neural Comput & Applic. 34* (15241). https://doi.org/10.1007/s00521-022-06959-2

Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy, 3*(3), 327–350. https://doi.org/10.3390/jcp3030017

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations* (NIST Special Publication 800-53 Revision 5). https://doi.org/10.6028/NIST.SP.800-53r5

https://doi.org/10.22201/dgtic.30618096e.2025.3.4.133 **Vol. 3, Núm. 4.** octubre-diciembre 2025, págs. 110 - 110

National Institute of Standards and Technology. (2024). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (NIST Special Publication 800-171 Revision 3). https://csrc.nist.gov/pubs/sp/800/171/r3/final

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper No. 29). https://doi.org/10.6028/NIST.CSWP.29

Subsecretaría de la Función Pública. (2011). *Guía para emitir documentos normativos*. Secretaría de la Función Pública. https://www.gob.mx/cms/uploads/attachment/file/914320/guia-emitir-documentos-normativos-sfp-07052024.pdf

Sullivan, G. (2022). Law, technology and data-driven security: Infra-legalities as method assemblage. *Journal of Law and Society*, 49(S1), 31–50. https://doi.org/10.1111/jols.12352

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. *Electronics, 11*(14), 2181. https://doi.org/10.3390/electronics11142181

Zhong, X., Vatanasakdakul, S., & Aoun, C. (2012). It Governance In China: Cultral Fit And It Governance Capabilities. *PACIS 2012 Proceedings*. (55). https://aisel.aisnet.org/pacis2012/55