Universidad Nacional Autónoma de México

Secretaría de Desarrollo Institucional

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Directrices generales en torno a la seguridad de la información que obra en los sistemas informáticos de la UNAM

Junio de 2023

DIRECTRICES GENERALES EN TORNO A LA SEGURIDAD DE LA INFORMACIÓN QUE OBRA EN LOS SISTEMAS INFORMÁTICOS DE LA UNAM

Contenido

DIRECTRICES GENERALES EN TORNO A LA SEGURIDAD DE LA INFORMACIÓN QUE OBRA EN LOS SISTEMAS INFORMÁTICOS DE LA UNAM

Objetivo

Este documento tiene como propósito apoyar a las entidades y dependencias de la Universidad Nacional Autónoma de México (UNAM) en el cumplimiento técnico de sus obligaciones para implementar medidas de seguridad en los sistemas informáticos a su cargo, a través de un conjunto de directrices generales.

Alcance

Generar un documento integrador y/o referenciado hacia las normas, lineamientos, políticas y reglamentos existentes, tanto dentro como fuera de esta universidad, con la finalidad de crear una lista de comprobación para instrumentar el nivel de cumplimiento y la brecha existente con respecto a la seguridad implementada en la entidad o dependencia.

Usuarios (Público objetivo)

Las directrices generales contenidas en este documento deben ser aplicables por los responsables de los sistemas informáticos de la UNAM y las áreas vinculadas de manera directa o indirecta con los servicios, activos de información, aplicaciones e infraestructura que los soportan.

Consideraciones generales

A los responsables TIC de la UNAM se les recomienda revisar la implementación de estas directrices de forma semestral, al menos, y cada vez que haya cambios significativos en los sistemas informáticos de las entidades y dependencias universitarias.

El documento apoya al cumplimiento técnico de las disposiciones legales aplicables a la UNAM, así como aquellas normas, políticas y reglamentos expedidos y publicados por la Oficina de la Abogacía General y en la Normateca de TIC de la UNAM.

El contenido de las directrices generales no es extensivo y representa un extracto mínimo e indispensable de las intersecciones de los siguientes estándares internacionales:

- NIST SP 800-53 Rev.5 Controles de seguridad y privacidad para sistemas de información y organizaciones
- NIST SP 800-171 Protección de información controlada y no clasificada en sistemas y organizaciones no federales
- Marco de Ciberseguridad del NIST
- Controles de Seguridad Críticos de CIS
- ISO/IEC 27001 Seguridad de la Información

DIRECTRICES GENERALES EN TORNO A LA SEGURIDAD DE LA INFORMACIÓN QUE OBRA EN LOS SISTEMAS INFORMÁTICOS DE LA UNAM

Este documento no reemplaza los esfuerzos realizados en los sistemas de gestión relacionados con la seguridad de la información, datos personales o calidad en los servicios. Las directrices generales se pueden considerar como un primer acercamiento si las entidades o dependencias de la UNAM desean implementar una certificación en alguno de los estándares mencionados previamente.

Ilustración 1. Representación gráfica de la realización del compendio

DIRECTRICES GENERALES EN TORNO A LA SEGURIDAD DE LA INFORMACIÓN QUE OBRA EN LOS SISTEMAS INFORMÁTICOS DE LA UNAM

1. Control de acceso

1.1 Gestión de acceso físico y digital controlado en activos universitarios

Restringir a los usuarios el acceso a los activos informáticos, procesos u otros activos autorizados, a través de una identificación única, y limitando a los procesos, funciones, roles y/o responsabilidades alineadas a la entidad o dependencia. Se recomienda definir privilegios de acceso y tipos de cuenta, además de mantener bitácoras de acceso con información como la hora del día, el día de la semana, las restricciones por tipo de cuenta, así como los datos que el responsable TIC considere pertinentes con base en la criticidad de su activo.

1.2 Inicio, bloqueo y término de una sesión

Limitar la cantidad de intentos de inicio de sesión no válidos, definir bloqueos temporales y/o definitivos según sea el caso.

Por la naturaleza de algunos sistemas y sus actividades es indispensable bloquear y/o inhabilitar automáticamente la sesión para evitar transacciones no deseadas, sin sustituir el cierre de sesión.

Finalizar la sesión consiste en concluir todos los procesos asociados al autenticarse en un sistema, ya sea por decisión del usuario o por un tiempo de inactividad determinado.

1.3 Controlar las sesiones de acceso remoto

Controlar a través de un proceso automatizado las sesiones provenientes de redes externas, con la intención de detectar incidentes de seguridad.

2. Sensibilización y formación

2.1 Información y capacitación del personal

Establecer y mantener un programa de capacitación y concientización sobre seguridad y privacidad del sistema informático. Debe contemplar mejores prácticas de autenticación, manejo de datos, reconocimiento y notificación de incidentes de seguridad, identificación de actualizaciones de seguridad y los peligros que implica conectarse y transmitir datos en redes inseguras. La periodicidad del programa estará sujeta a las capacidades y necesidades de la entidad y/o dependencia y deberá incluir las lecciones aprendidas en incidentes o violaciones de seguridad ocurridas.

2.2 Capacitación basada en roles, funciones y responsabilidades

Ofrecer capacitación en seguridad y privacidad con base en los roles, funciones y responsabilidades de los responsables involucrados en el sistema, antes de autorizar el acceso a este, a la información o a realizar alguna de las actividades asignadas. El contenido de la capacitación se actualizará de acuerdo con la periodicidad definida por la entidad y/o dependencia.

2.3 Capacitación sobre respuesta a incidentes

Desarrollar un programa de capacitación en respuesta a incidentes para que los involucrados conozcan su rol y responsabilidad ante un evento de seguridad de la información. El contenido de este programa de capacitación se actualizará de acuerdo con la periodicidad definida por la entidad y/o dependencia o cuando algún evento de seguridad lo amerite.

3. Revisión y rendición de cuentas

3.1 Verificación de reglamentos, lineamientos y legislación universitaria vigente

Identificar los reglamentos, lineamientos y la legislación universitaria aplicable y vigente, publicados en la Oficina de la Abogacía General y en la Normateca de TIC de la UNAM; deberá estar definida de forma explícita, documentada y actualizada para cada sistema informático. También se deben establecer revisiones periódicas para determinar si el sistema informático cuenta con los requisitos propios de la entidad y/o dependencia, se mantiene actualizado y con un funcionamiento eficaz. Esto se debe informar a los usuarios a través de una notificación al inicio de cada sesión.

3.2 Implementar mecanismos para el registro de actividades del sistema informático

Crear y conservar el registro de las actividades realizadas en el sistema y su entorno para supervisar, monitorear y auditar actividades inusuales consideradas ilegales o no autorizadas conforme a los criterios establecidos por la entidad y/o dependencia.

Los niveles de abstracción, detalle, cantidad de registros, así como la periodicidad con la que se generarán deberán ser analizados por la entidad y/o dependencia, acorde con sus posibilidades. Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados, de acuerdo con los reglamentos, lineamientos y la legislación universitaria vigente.

3.3 Rastreo de información por usuario.

Registrar las actividades realizadas por los usuarios en los sistemas informáticos.

4. Gestión de la configuración

4.1 Inventarios de activos y su documentación

Implementar inventarios de componentes de hardware y software, con sus respectivas configuraciones documentadas, revisadas formalmente y acordadas por los responsables TIC, para sistemas o elementos de configuración dentro de los sistemas, será una base ante futuras complicaciones, versiones y cambios en los sistemas. El mantenimiento, actualización y/o cambio deberán realizarse periódicamente y/o cuando el sistema lo requiera o las actualizaciones estén disponibles.

4.2 Control de cambios

Supervisar, revisar, validar y documentar los cambios en el sistema controlados por la configuración, así como aprobar o desaprobar los cambios necesarios y/o propuestos, teniendo en cuenta un análisis de impacto en la seguridad y la privacidad. Deberá conservar los registros de cambios controlados por la configuración en el sistema por un periodo determinado, acorde con sus necesidades y recursos.

4.3 Funcionalidad mínima

Establecer mecanismos que permitan la prohibición y restricción en el uso de funciones, puertos, protocolos, software y/o servicios, dejando las capacidades esenciales definidas por las necesidades de la entidad y/o dependencia.

5. Identificación y autenticación

5.1 Identificar usuarios, procesos y dispositivos involucrados en las actividades dentro del sistema

Implementar mecanismos que permitan identificar aquello que realice modificaciones y/o ejecuciones dentro del sistema, haciendo énfasis en el caso de los dispositivos a las direcciones físicas de la tarjeta de red, las direcciones de protocolo de Internet o tokens únicos del dispositivo; en el caso de los usuarios, asociar las cuentas del sistema asignadas.

5.2 Verificar la legitimidad de la identidad

Desarrollar mecanismos para acreditar que el usuario, proceso y/o dispositivo cuenta con los permisos necesarios para acceder al sistema de manera legítima.

6. Respuesta a incidentes

6.1 Manejo de incidentes

Desarrollar un plan de emergencia ante incidentes para sistemas informáticos, que, en medida de lo posible, incluya la preparación, detección, análisis, contención, recuperación y respuesta al usuario.

6.2 Notificación y seguimiento de incidentes

Notificar incidentes de seguridad a los funcionarios y/o autoridades designadas dentro de su entidad y/o dependencia. También deberá enviar al CERT-UNAM una descripción de los hechos, del activo involucrado y su dirección IP real asociada, a través del correo electrónico csi.incidentes@unam.mx. Si el responsable TIC requiere apoyo de especialistas, deberá especificarlo en el correo y posteriormente formalizar la petición con un oficio ingresado a la Oficialía de Partes de la DGTIC.

De acuerdo con la criticidad del activo, deberá documentar sus incidentes de seguridad para mantener registros con información pertinente y necesaria que permitan su manejo. Esta documentación será fundamental en caso de requerir un análisis forense.

7. Mantenimiento

7.1 Mantenimiento al sistema y sus componentes

Programar, documentar, revisar, aprobar y monitorear los registros y actividades de mantenimiento preventivo y mantenimiento correctivo; reparar y reemplazar los componentes del sistema de acuerdo con las especificaciones del fabricante, proveedor y/o los requisitos de la entidad y/o dependencia. Prever las acciones de eliminación segura de datos, en caso de que el mantenimiento, reparación y/o reemplazo se realicen fuera del sitio.

7.2 Implementar métricas al mantenimiento realizado por agentes externos

Implementar métricas sobre herramientas, técnicas, mecanismos y personal autorizado para realizar el mantenimiento del sistema cuando externos a la entidad y/o dependencia lo realicen y sea necesario procesar, almacenar o transmitir datos para acciones diagnósticas. Las herramientas de mantenimiento pueden incluir software, hardware y firmware.

8. Control de medios digitales

8.1 Control de medios digitales y no digitales

Implementar medidas para limitar el acceso a las especificaciones de diseño en medios digitales, así como controles que consideren la realización de inventarios, el mantenimiento de la responsabilidad por los medios almacenados y la garantía de que existan procedimientos para permitir a las personas retirar y devolver los medios a donde corresponde, así como su almacenamiento seguro.

8.2 Eliminación segura de datos

Implementar mecanismos para la limpieza de medios ante baja de activos y/o su reutilización.

8.3 Limitar el acceso a los medios digitales y no digitales a usuarios autorizados

Controlar el acceso físico a los medios del sistema y las áreas de almacenamiento seguras.

8.4 Control criptográfico

Establecer y gestionar mecanismos criptográficos en el sistema y sus medios digitales, es recomendable utilizar estándares vigentes. Si requiere más información, consulte la sección Documentos de interés.

9. Seguridad del personal

9.1 Evaluación para selección del personal involucrado en el sistema

Evaluar y/o valorar la conducta, integridad, juicio, lealtad, confiabilidad y estabilidad del individuo antes de autorizar el acceso a los sistemas informáticos de carácter crítico. Así como, determinar el nivel de acceso de acuerdo con los puestos asignados.

9.2 Proteger los sistemas de carácter crítico durante y después de las acciones del personal

Implementar mecanismos oportunos para la devolución de la(s) propiedad(es) relacionada(s) con el sistema informático cuando el personal sea eximido de toda responsabilidad respecto al sistema, ya sea por transferencia, despido y/o renuncia.

10. Protección física

10.1 Permitir el acceso físico a los activos y sus entornos únicamente a personas autorizadas

Dar acceso a aquellas áreas críticas de carácter no público a través de los mecanismos que le permitan sus recursos.

10.2 Supervisar el acceso físico

Crear controles para proteger y monitorear las áreas. Esto ayudará a prevenir daños accidentales, interrupciones y manipulaciones físicas.

11. Evaluación de la seguridad

11.1 Evaluación y monitoreo de controles de seguridad

Determinar un rango de tiempo para revisar los controles de seguridad de los sistemas informáticos y sus entornos, tanto físicos como digitales, con la intención de evitar la pérdida de efectividad. El resultado de la revisión deberá ser plasmado en un informe con el detalle que la entidad y/o dependencia considere necesario. Esto facilitará el conocimiento continuo de las amenazas, las vulnerabilidades y la seguridad de la información para respaldar las decisiones relacionadas con la gestión de riesgos de la entidad y/o dependencia.

11.2 Planes de acción para sistemas informáticos

Desarrollar, documentar, analizar e implementar planes de acción diseñados para corregir deficiencias y reducir o eliminar vulnerabilidades en los sistemas informáticos. Los planes de acción deberán ser actualizados periódicamente.

11.3 Planes de seguridad

Desarrollar, documentar, actualizar e implementar planes de seguridad de los sistemas informáticos que describen a alto nivel los límites del sistema, sus entornos de operación, la implementación de los requisitos de seguridad y sus relaciones con otros sistemas. Los planes de seguridad efectivos hacen uso extensivo de referencias a políticas, procedimientos y documentos adicionales, como los

"Lineamientos y recomendaciones para el resguardo de información electrónica", en los que se puede obtener información detallada. Consulte la sección Documentos de interés.

12. Protección del sistema y las comunicaciones

12.1 Supervisar, controlar y mantener protegidas las comunicaciones de los sistemas informáticos

Supervisar, controlar y proteger las comunicaciones transmitiendo de forma segura, tanto en redes externas como internas, de acuerdo con la arquitectura de seguridad y privacidad que la entidad y/o dependencia determine para sus sistemas informáticos.

12.2 Arquitectura de seguridad y privacidad

Desarrollar arquitecturas de seguridad y privacidad para el sistema informático, empleando técnicas de desarrollo de software e ingeniería de sistemas que promuevan la seguridad de la información efectiva dentro de los sistemas informáticos. Los "Lineamientos de seguridad de la información en sitios web de la UNAM" le otorgan información aplicable al desarrollo, operación y/o actualización de sitios web institucionales y que están a cargo de las entidades o dependencias de la Universidad Nacional Autónoma de México. Consulte la sección Documentos de interés.

13. Integridad del sistema y de la información

13.1 Manejo oportuno de fallas en sistemas

Identificar y corregir los sistemas afectados por fallas de software y firmware, incluidas las vulnerabilidades anunciadas por el fabricante e informar al personal designado con responsabilidades de seguridad de la información.

13.2 Métodos de prevención y protección ante agentes maliciosos

Implementar métodos de prevención y protección en los elementos de entrada y salida designados de los sistemas informáticos, tales como definiciones de firmas, antivirus y tecnologías basadas en la reputación.

Glosario

Los términos y definiciones pueden ser consultados en los documentos de referencia.

Documentos de referencia

- Joint Task Force. (2020). *Security and privacy controls for information systems and organizations. Rev.5*. National Institute of Standards and Technology.
- Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020). *Protecting controlled unclassified information in nonfederal systems and organizations.* National Institute of Standards and Technology.
- Stocchetti, V. (s.f.). *CIS Critical Security Controls v8*. Center for Internet Security.
- National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1*. National Institute of Standards and Technology.
- International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology - Security techniques – Information security management systems - Requirements.* https://www.iso.org/standard/27001

Documentos de interés

- National Institute of Standards and Technology. (2019). *Cryptographic Algorithm Validation Program.* https://csrc.nist.gov/projects/cavp
- National Institute of Standards and Technology. (2019). *Cryptographic Module Validation Program*. https://csrc.nist.gov/projects/cmvp
- National Institute of Standards and Technology. (2019). Cryptographic Standards and Guidelines. https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines
- Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (2022). *Lineamientos de seguridad de la información en sitios web de la UNAM*. https://www.red-tic.unam.mx/content/lineamientos-seguridad-sitios-web-unam
- Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (2023). *Lineamientos y recomendaciones para el resguardo de información electrónica*.

DIRECTRICES GENERALES EN TORNO A LA SEGURIDAD DE LA INFORMACIÓN QUE OBRA EN LOS SISTEMAS INFORMÁTICOS DE LA UNAM

Anexo 1

NIST SP 171	ISO/IEC 27001
1. Control de acceso	9. Control de acceso
2. Sensibilización y formación	7. Seguridad ligada a los recursos humanos
3. Revisión y rendición de cuentas	18. Cumplimiento
4. Gestión de la configuración	8. Gestión de activos 12. Seguridad operativa
5. Identificación y autenticación	9. Control de acceso
6. Respuesta a incidentes	6. Aspectos organizativos de la seguridad de la información 16. Gestión de incidentes de la seguridad de la información
7. Mantenimiento	14. Adquisición, desarrollo y mantenimiento de sistemas de información 15. Relaciones con suministradores
8. Control de medios digitales	8. Gestión de activos 10. Cifrado
9. Seguridad del personal	7. Seguridad ligada a los recursos humanos
10. Protección física	11. Seguridad física y ambiental
12. Evaluación de la seguridad	17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio
13. Protección del sistema y las comunicaciones	13. Seguridad de las telecomunicaciones
14. Integridad del sistema	12. Seguridad operativa

DIRECTRICES GENERALES EN TORNO A LA SEGURIDAD DE LA INFORMACIÓN QUE OBRA EN LOS SISTEMAS INFORMÁTICOS DE LA UNAM

Créditos

Rector
Dr. Enrique Luis Graue Wiechers

Secretaria de Desarrollo Institucional
Dra. Patricia Dolores Dávila Aranda

Director General de Cómputo y de Tecnologías de Información y Comunicación
Dr. Héctor Benítez Pérez

Coordinación DGTIC, UNAM
Dra. Ana Yuri Ramírez Molina
M. en C. María de Lourdes Velázquez Pastrana
Mtro. Juan Manuel Castillejos Reyes

Elaboración DGTIC, UNAM
M.I. Adriana Cruz García
M. en C. Carlos Raúl Tlahuel Pérez

Revisión técnica
Ing. Arturo Bahena Armas – DGAPA, UNAM
M.T.I.A Esther Lugo Rojas – DGTIC, UNAM
Mtro. Jesús Ojeda Arévalo – DGCP. UNAM
Ing. Luis Armando Sánchez Ruiz – SG, UNAM

Revisión jurídica
Mtra. Elizabeth Rangel Gutiérrez – DGTIC, UNAM
Lic. José Luis Chávez Sánchez – DGTIC, UNAM

Revisión estructural y publicación en NormaTIC
Mtra. Ma. Teresa Ventura Miranda – DGTIC, UNAM
L.A. Heidi Alejandra Pérez Vera – DGTIC, UNAM