DGTIC UNAM

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Política General de Seguridad de la Información en la DGTIC

Código	DGTIC- PolíticaGeneralSeguridadInformación			
Versión	1.1	**Fecha:**	31 de julio de 2023	
Vigencia	**Inicio**	16 de agosto de 2023	**Fin**	16 de agosto de 2025
Aprobación	Comité de Seguridad de la Información (Comité SI) de la DGTIC Dr. Héctor Benítez Pérez (HBP) Dra. Marina Kriscautzky Laxague (MKL) M. en C. Cristina Múzquiz Fragoso (CMF) Dra. Ana Yuri Ramírez Molina (AYRM) Ing. José Leopoldo Vega Correa (JLVC) M. en C. María de Lourdes Velázquez Pastrana (MLVP) Mtra. Elizabeth Rangel Gutiérrez (ERG) Mtro. Miguel Ángel Villanueva Vélez (MAVV) M. en C. Carlos Raúl Tlahuel Pérez (CRTP)			
Nivel de clasificación	Uso público			

Historial de versiones y revisiones

Fecha:	Autor:	Descripción
2023-06-16	M.I. Adriana Cruz García (ACG) M. en C. Carlos Raúl Tlahuel Pérez (CRTP)	Creación de la versión 1.0
2023-07-31	Lic. José Luis Chávez Sánchez (JLCS) M.A.T. Esteban R. Ramírez Fernández (ERRF) MTIA. Esther Lugo Rojas (ELR) Ing. Nidia Cendejas Cervantes (NCC)	Revisión y comentarios a la versión 1.1
2023-07-31	MATIE. Alberto González Guízar (AGG)	Revisión a la versión 1.1

Contenido

1. Definición de la Política 4
2. Objetivo de la Política 4
3. Alcance de la Política 4
4. Organización de la seguridad de la información 4
5. Seguridad relativa a los recursos humanos 5
6. Gestión de activos 5
7. Control de acceso a los activos asociados a los servicios institucionales 6
8. Criptografía 7
9. Seguridad física y del entorno 7
10. Seguridad en la operativa 8
11. Seguridad de las telecomunicaciones 8
12. Adquisición, desarrollo y mantenimiento de los sistemas informáticos 8
13. Relación con proveedores 9
14. Gestión de incidentes de seguridad de la información 9
15. Aspectos de seguridad de la información para la gestión de la continuidad del negocio 9
16. Cumplimiento 10
17. Documentos relacionados 10

Anexo. Relación Normativa Universitaria e ISO/IEC 27001 11

Política General de Seguridad de la Información en la DGTIC

1. Definición de la Política

Esta Política General de Seguridad de la Información define los principios y acciones de seguridad de la información a considerar para los activos universitarios pertenecientes a la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la UNAM.

2. Objetivo de la Política

Establecer un curso de acción que permita a la DGTIC realizar una adecuada gestión de la seguridad de sus activos de información y minimizar la manifestación de riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información.

3. Alcance de la Política

Esta Política General de Seguridad de la Información es aplicable a todo el personal que labore o preste servicios a la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la UNAM.

Este esfuerzo pretende coadyuvar a los trabajos relacionados con la seguridad de la información al interior de la DGTIC, sin embargo, no reemplaza las políticas, procedimientos y/o sistemas de gestión relacionados con la seguridad de la información, datos personales o calidad en los servicios.

4. Organización de la seguridad de la información

- El funcionamiento y coordinación de las acciones necesarias para la instalación y operación del comité SI (Comité de Seguridad de la Información) está plasmado en los "Lineamientos de Operación del Comité de Seguridad de la Información".
- Las direcciones de área deberán documentar los procesos asociados a servicios institucionales dirigidos a la comunidad universitaria. Preferentemente mediante diagramas de alto nivel, podrá usarse BPMN (Modelo y Notación de Procesos de Negocio) o cualquier otro considerado por la dirección de área. La documentación deberá considerar las funciones y roles de cada uno de los integrantes, reflejando una segregación de responsabilidades.
- Si el personal detecta actividad anómala en alguno de los sistemas de información pertenecientes a la DGTIC, deberá informar de inmediato a su director de área y/o a la Coordinación de Seguridad de la Información. A criterio de la dirección de área puede presentar casos en el seno del Comité SI de la DGTIC.
- La Coordinación de Seguridad de la Información podrá brindar apoyo para resolver un incidente que afecte la disponibilidad, integridad y confidencialidad en los activos a cargo de la DGTIC; los niveles y métodos de acceso serán acordados con la dirección de área procurando la continuidad de los servicios involucrados.

5. Seguridad relativa a los recursos humanos

- La dirección de área solicitará a todo personal de nuevo ingreso la subscripción de una carta compromiso en la cual se indique lo siguiente:
    - La dirección de área le informó de sus funciones basadas en los diagramas a alto nivel, descritos en la sección “Organización de la seguridad de la información”.
    - La dirección de área le notificó el nivel de confidencialidad de la información, expuesto en la sección “Gestión de activos”, así como el(los) método(s) de comunicación que deberán utilizarse.
    - Manifieste conocer el contenido del Código de ética de la UNAM y de la DGTIC.
    - Declare su compromiso para realizar las actividades asignadas con estricto apego al cumplimiento de cada uno de los puntos anteriores, así como lo que la dirección de área considere pertinente.
- Cuando algún miembro del personal sea relevado de su cargo, sea transferido a otra instancia o bien su contratación haya expirado y/o concluido, la dirección de área deberá asegurarse de revocar todo acceso a activos de los procesos internos de la DGTIC. Para los sistemas de información involucrados en servicios institucionales para la comunidad universitaria, se debe evaluar la pertinencia de métodos para comprobar la vigencia de usuarios.
- Al culminar sus labores en la DGTIC por cualquier motivo, la dirección de área deberá asegurar que el personal devuelva todos los activos de los procesos internos de la DGTIC y cualquier documentación para su operación que tenía en resguardo.

6. Gestión de activos

- Las direcciones de área deberán identificar los activos asociados a los servicios institucionales a su cargo que son ofrecidos a la comunidad universitaria, a través de un inventario donde además se identifique el personal a cargo del resguardo, ubicación, la actividad relacionada con las funciones del área descritas en el Manual de la Organización, fechas de revisiones y/o auditorías, así como medidas preventivas y correctivas implementadas. Los directores deberán asegurar la realización de revisiones periódicas verificando la existencia y correcta funcionalidad de los activos asociados.
- Las direcciones de área deberán comunicar al personal adscrito que los activos relacionados con los servicios institucionales para la comunidad universitaria, como los equipos, el acceso a Internet, las aplicaciones y los servicios de mensajería electrónica serán utilizados exclusivamente para fines laborales. El personal deberá conocer las pautas y gestionar los recaudos necesarios para proteger los activos de información al interior de la DGTIC.
- El personal deberá evitar el uso de dispositivos de almacenamiento extraíbles en activos informáticos asociados a los servicios institucionales proporcionados por la DGTIC, en caso de ser necesario, se debe realizar una minuta firmada por los responsables, en donde se incluirá los mecanismos de cifrado utilizados y/o el procedimiento utilizado para la destrucción del medio.
- En caso de que un activo asociado a servicios institucionales para la comunidad universitaria sea dado de baja o reutilizado para otro servicio, deberá implementar una medida de seguridad mediante la cual se establezcan los métodos y técnicas para la eliminación

definitiva de los datos, de modo que la probabilidad de recuperarlos sea mínima o nula. Puede consultar la Guía de Borrado Seguro de información (https://www.cert.unam.mx/borrado-seguro-de-informacion).

- Independiente al tipo de soporte de los activos, la información deberá atender la clasificación estipulada en la Normativa universitaria y adicionalmente deberá clasificarse en caso de exposición de la información, las clases mínimas recomendadas son:
    - Público: sin nivel de confidencialidad.
    - Interno: nivel más bajo de confidencialidad.
    - Restringido: nivel medio de confidencialidad.
    - Confidencial: nivel más alto de confidencialidad.

7. Control de acceso a los activos asociados a los servicios institucionales

- Las direcciones de área son responsables de autorizar el acceso a los activos, definiendo un protocolo de asignación de credenciales (usuario y contraseña) para desempeñar los roles y funciones alineadas a la sección “Organización de la seguridad de la información” contenida en la presente política. Deberá reflejarse la segregación de responsabilidades y limitar las acciones del personal de amplia visibilidad. Se favorecerán los mecanismos de doble factor de autenticación.
- Queda estrictamente prohibido el uso de credenciales genéricas o de uso múltiple, las credenciales deberán ser únicas e intransferibles.
- Se deberá implementar y almacenar un registro no menor a seis meses de antigüedad, o el tiempo que requieran cada una de las direcciones de área, donde se registren fecha, hora, usuario y las actividades realizadas, tales como inicio de sesión, cierre de sesión, alta, baja y edición de usuarios, así como aquellas que la dirección de área considere necesarias.
- Deberán limitar a tres intentos de inicio de sesión o lo que considere la dirección de área en los activos, después de los intentos fallidos, la sesión se bloqueará, y el personal deberá ponerse en contacto con la dirección de área, o quien sea designado, para solicitar una reposición de contraseña, a través de un formato o cualquier medio que evidencie el evento.
- Las sesiones a los activos deberán establecer un rango de inactividad de 15 minutos, o el tiempo que la dirección de área considere, para volver a solicitar contraseña y/o cerrar sesión.
- El acceso remoto a los activos será únicamente a través de una red privada virtual.
- Si por algún motivo se requiere que una persona ajena a la dirección de área y/o a la DGTIC tenga acceso a alguno de los activos, deberá ser autorizado previamente por el director de área.
- Todas las áreas sin excepción deberán contar con un procedimiento de alta, modificación y baja de usuarios para cada uno de los activos.
- Toda contraseña utilizada en activos informáticos deberá cumplir con al menos:
    - Una longitud de ocho caracteres o más.
    - Combinaciones de caracteres numéricos, letras minúsculas y mayúsculas, y símbolos especiales.

  - Evitar el uso de palabras que se encuentren en un diccionario.
  - Evitar la relación con información de carácter personal.
- Las credenciales a los activos del personal deberán contar con una clasificación de usuario. La clasificación mínima recomendada es:
  - Usuario: acceso restringido en la aplicación.
  - Administrador: gestiona el sistema y los permisos de usuarios.
  - Sistema: automatización de tareas.

Adicionalmente, las credenciales podrán tener los siguientes permisos:

  - Lectura: acceso de únicamente visualización de información.
  - Escritura: permite la creación o modificación de información en el sistema.
  - Eliminación: puede borrar información contenida dentro del sistema.
  - Ejecución: permite la realización de tareas dentro del sistema.

El personal puede contar con dos o más clasificaciones, dependiendo su rol, función y nivel de responsabilidad. Es decisión de cada dirección de área si agrega o modifica su clasificación acorde al servicio institucional a su cargo y que se ofrece a la comunidad universitaria.

8. Criptografía

- Todos los activos que consten en el inventario descrito en el apartado “Gestión de Activos” de este documento deberán implementar un algoritmo criptográfico, de acuerdo con lo establecido en la sección “Directrices Generales en Torno a la Seguridad de la Información que obra en los Sistemas Informáticos” de este documento, para el almacenamiento y tránsito de los datos.
- El intercambio de información deberá documentar el proceso de gestión de llaves criptográficas.
- Se deberá evaluar la gestión de las llaves criptográficas utilizadas por los medios criptográficos que incluya su generación, su uso y protección, la distribución que se realiza de estas y su renovación o destrucción.

9. Seguridad física y del entorno

- Se deberá restringir el acceso físico a los Centros de Datos de la DGTIC, sitios donde se alojen los activos y oficinas de todas las direcciones de área; únicamente se permitirá el acceso al personal autorizado en dichas ubicaciones, acorde a sus roles, funciones y responsabilidades en la DGTIC. En el caso de dar acceso a personal adicional o proveedores externos, será bajo responsabilidad del personal que haya proporcionado el acceso y deberá documentar los accesos y actividades realizadas, o lo que la dirección de área considere.
- El acceso deberá estar monitoreado 24/7 a través de cámaras, biométricos o las medidas que la dirección de área determine en las áreas descritas anteriormente, así como las medidas adicionales que la dependencia considere pertinentes.

- Las direcciones de área deberán diseñar zonas que puedan ser utilizadas para mantenimiento y/o pruebas que no pongan en riesgo la operación de los activos en ambientes de producción.
- Los directores de área deberán llevar un registro de las acciones preventivas y correctivas para el óptimo funcionamiento de los activos relacionados con el suministro de energía eléctrica, climatización y telecomunicaciones.
- Si alguno de los activos debe salir de las instalaciones, la dirección de área debe establecer un procedimiento interno donde se justifique:
    - Motivo de retiro.
    - Fecha de retiro.
    - Fecha de devolución.
    - Responsable del activo.
    - Área a la que pertenece.
- Deberán de revisar la viabilidad de contratar un seguro ante robo y/o extravío.

10. Seguridad en la operativa

- Las direcciones de área deberán verificar la viabilidad para el cumplimiento de los lineamientos técnicos descritos en la normatividad universitaria:
    - Lineamientos de seguridad de la información en sitios web de la UNAM.
    - Lineamientos y recomendaciones para el resguardo de información electrónica.
- Las direcciones de área deberán asegurarse de que el uso de dispositivos propios debe ser autorizado y restringido a funciones específicas; el dispositivo deberá contar con una protección contra malware. La DGTIC no asumirá ninguna responsabilidad sobre el dispositivo.

11. Seguridad de las telecomunicaciones

- Las direcciones de área deberán asegurar la implementación de mecanismos de seguridad asociados a la red de datos y además de contar con medidas como mecanismo de autenticación usuario y contraseña, filtrado en distintos niveles del modelo OSI o cualquier otro mecanismo que la dirección de área determine.
- Las direcciones de área deberán elaborar diagramas que documenten el entorno de red de los activos a su cargo.
- Las direcciones de área deberán segregar los entornos de red, de acuerdo con los procesos internos de la DGTIC, tomando en cuenta las funciones y roles del personal que acceda a cada uno de los entornos.
- Las consolas de administración de los activos deberán estar en una red exclusiva y únicamente accesible por VPN.

12. Adquisición, desarrollo y mantenimiento de los sistemas informáticos

- Las direcciones de área deberán asegurarse de implementar métricas sobre herramientas, técnicas y mecanismos para realizar el mantenimiento de los activos. Las herramientas de mantenimiento pueden incluir medios físicos y/o digitales.

- Para la creación y/o reestructuración de procesos al interior de la DGTIC, las direcciones de área deberán contar con un plan de trabajo que incluirá hitos y responsables. Adicionalmente, se documentará con diagramas la integración, consolidación, modificación, y/o segregación de activos.

13. Relación con proveedores

- Cuando un proveedor ingrese a las instalaciones, el personal que dé acceso al activo será el responsable de las acciones realizadas por dicho proveedor.
- En caso de que el proveedor del servicio deba procesar, almacenar o transmitir datos relacionados a los servicios institucionales para la comunidad universitaria, con el propósito de realizar acciones diagnósticas dentro de los activos y su entorno, la dirección de área deberá implementar mecanismos para monitorear dichas acciones.
- La dirección de área deberá verificar que el proveedor cumple con las especificaciones estipuladas en el contrato de servicio, y deberá proveer una carta de confidencialidad al proveedor donde garantice la no transferencia de información, la cual será firmada de manera autógrafa por el personal de éste.
- Al finalizar el contrato con el proveedor, la dirección de área debe asegurar la devolución de los activos de información, la eliminación o destrucción de datos, y la cancelación y revocación de accesos.

14. Gestión de incidentes de seguridad de la información

- Todos los servicios institucionales para la comunidad universitaria deberán documentar un protocolo de atención ante posibles incidentes relacionados con la disponibilidad, integridad y/o confidencialidad de la información.
- Las direcciones de área proveerán los medios de comunicación para que cualquier miembro del personal pueda reportar el incumplimiento de esta Política General de Seguridad de la Información.
- Las direcciones de área deberán atender oportunamente las vulnerabilidades o amenazas detectadas, y generar un plan para la mitigación y/o erradicación de éstas.
- Cuando las direcciones de área consideren pertinente documentar un incidente de seguridad deberán guardar evidencia con al menos los siguientes datos:
    - Fecha del evento suscitado.
    - Fecha de resolución.
    - Descripción de los hechos.
    - Solución implementada.

La información deberá resguardarse por la dirección de área o el área que determine, de conformidad con los términos señalados en la normatividad universitaria.

15. Aspectos de seguridad de la información para la gestión de la continuidad del negocio

- Las direcciones de área deberán llevar a cabo un análisis de riesgos a partir de los servicios institucionales a su cargo.

- Cada seis meses, o el tiempo que la dirección de área defina, las políticas y los controles de seguridad serán revisados evitando perder su efectividad en el tiempo, el resultado de la revisión deberá ser plasmado en un informe con el detalle suficiente según lo consideren necesario, el cual contendrá el conocimiento continuo de amenazas y vulnerabilidades con el propósito de respaldar las decisiones relacionadas con la gestión de riesgos de la DGTIC.
- Las direcciones de área deberán desarrollar, documentar, analizar e implementar planes de acción diseñados para corregir deficiencias y reducir o eliminar vulnerabilidades en los activos.
- La dirección de área debe evaluar la viabilidad de un plan de continuidad de la operación sobre los servicios institucionales a su cargo.

16. Cumplimiento

- Las direcciones de área deberán:
    - Crear y conservar un registro de las actividades realizadas en los activos y su entorno, que permita la supervisión, monitoreo y auditoría de actividades inusuales consideradas ilegales o no autorizadas de acuerdo con lo establecido en la normatividad universitaria.
    - Deberán revisar y asegurarse que los sistemas de información cumplen con la normativa universitaria vigente, así como los lineamientos técnicos respectivamente.
- En caso de incumplimiento de la presente Política, el Comité de Seguridad de la Información actuará de acuerdo con el procedimiento establecido en la normatividad universitaria vigente.

17. Documentos relacionados

- Lineamientos de seguridad de la información en sitios web de la UNAM.
- Lineamientos y recomendaciones para el resguardo de información electrónica.
- Lineamientos de Operación del Comité de Seguridad de la Información.
- Estándar ISO/IEC 27001:2013.
- NIST SP 800-53 Controles de seguridad y privacidad para sistemas de información y organizaciones.

Anexo. Relación Normativa Universitaria e ISO/IEC 27001

Directrices Generales en entorno a la Seguridad de la Información que obra en los Sistemas Informáticos	ISO/IEC 27001	PGSI
1. Control de Acceso	9. Control de Acceso	7. Control de acceso a sistemas de información
2. Sensibilización y formación	7. Seguridad ligada a los recursos humanos	5. Seguridad relativa a los recursos humanos
3. Revisión y rendición de cuentas	18. Cumplimiento	16. Cumplimiento
4. Gestión de la configuración	8. Gestión de activos 12. Seguridad Operativa	6. Gestión de activos 10. Seguridad en la operativa
5. Identificación y Autenticación	9. Control de acceso	7. Control de acceso a sistemas de información
6. Respuesta a Incidentes	6. Aspectos Organizativos de la Seguridad de la Información 16. Gestión de incidentes de la seguridad de la Información	4.Organización de la seguridad de la información 14. Gestión de incidentes de seguridad de la información
7. Mantenimiento	14. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información 15. Relaciones con suministradores	12. Adquisición, desarrollo y mantenimiento de los sistemas informáticos 13. Relación con proveedores
8. Control de Medios Digitales	8. Gestión de activos 10. Cifrado	6. Gestión de activos 8. Criptografía
9. Seguridad del Personal	7. Seguridad ligada a los recursos humanos	5. Seguridad relativa a los recursos humanos
10. Protección física	11. Seguridad Física y Ambiental	9. Seguridad física y del entorno
11. Evaluación de la seguridad	17. Aspectos de seguridad de la información en la gestión de la continuidad del Negocio	15. Aspectos de seguridad de la información para la gestión de la continuidad del negocio
12. Protección del sistema y las comunicaciones	13. Seguridad de las Telecomunicaciones	11. Seguridad de las telecomunicaciones

13. Integridad del sistema	12. Seguridad Operativa	10. Seguridad en la operativa

Archivo	20230816-DGTIC_PGSI_Aprobado.pdf		
Identificador único (hash)	7a18e008b79460aed084aedc48dcd6f6a8fbd25508a6a8373e93863be630579b		
Fecha y hora de cierre	23/08/2023 18:43:07	**Fecha y hora de emisión**	23/08/2023 18:43:32
Número de páginas	11	**Firmantes**	12

Firmantes

Nombre	Dr. Héctor Benítez Pérez	**Fecha y hora de firma**	21/08/2023 08:43:21
Presidente			
Hash Firma	47a157700738ca86500c5ee833ed779f53e9fb432ef521009211325fe6fe7b37e1e9105622eea225a0f98c618c6490c2		

Nombre	Mtra. María de Lourdes Velázquez Pastrana	**Fecha y hora de firma**	21/08/2023 18:08:56
Integrante			
Hash Firma	16e227d05bdcdf17d8bac700632a7b32646e6e3d29c199779fe328f14a8be5cbe471bc694ce99171e0a526541d9f4f91		

Nombre	Ing. José Leopoldo Vega Correa	**Fecha y hora de firma**	23/08/2023 17:53:31
Integrante			
Hash Firma	37d55d928b47d6ba5914d4700dffe04fca05cd2b2dbb9f489e01d79662a5475c2073634066344b505e3177157873e318		

Nombre	Dra. Ana Yuri Ramírez Molina	**Fecha y hora de firma**	22/08/2023 18:05:48
Integrante			
Hash Firma	550c412f56f08435504614b528cf27296608b8811fb8f885452775058f616db844c943bda42bec8921c39a2faf3382db		

Nombre	Dra. Marina Kriscautzky Laxague	**Fecha y hora de firma**	23/08/2023 17:54:02
Integrante			
Hash Firma	13a3b68d9f539a0aaf96fc93d23df5eae028f4c807f35d9ff4c89beb0bb3940cf0dc60877f1c22f894fd9405a1e3345e		

Nombre	Mtra. Maria Cristina Múzquiz Fragoso	**Fecha y hora de firma**	22/08/2023 13:52:42
Integrante			
Hash Firma	635b9fbe1ba2bc93b593baa062ba2875fbaff202f12ee36fb172788f129fd109389c2b9951bd6cd337dc937e34646feb		

Nombre	Mtra. Elizabeth Rangel Gutiérrez	**Fecha y hora de firma**	18/08/2023 13:26:05
Integrante			
Hash Firma	e3162e52c2924ea53fae49db6f49db6e1bbc9c594ae076cac25e69c15bf19746d8c3e7baf63c3d38ef32393ed9620d53		

Nombre	Mtro. Miguel Ángel Villanueva Vélez	**Fecha y hora de firma**	23/08/2023 12:22:46
Integrante			
Hash Firma	b5307b71d3edc6a8d04ed1505c0cd08301578174e216959422f7ab7573a3e9ee4baee6185e9c8b8a77dc41ce608d47bf		

Nombre	Mtro. Carlos Raúl Tlahuel Pérez	**Fecha y hora de firma**	18/08/2023 12:47:33
Secretario Técnico			
Hash Firma	16d4b68cb649f6599d7daf5fbe3bace1d1d63b498af10d2a1e44d38110227aefae6952b7d992a3efc17e799f58a6ac19		

Nombre	Ing. Nidia Cendejas Cervantes	**Fecha y hora de firma**	23/08/2023 18:27:22
Integrante			
Hash Firma	c1982974d1f361b7a6213843f119f15f687c92fc88c43ed353fcb81381f23c34fa95c6eaea5c9ef8028bf8b72f4ed925		

Nombre	Mtro. Alberto Gonzalez Guizar	**Fecha y hora de firma**	23/08/2023 18:43:07
Integrante			
Hash Firma	ea6d588f1711af8acfb7532deb6048de6bd60959e618ff04e359b15b1676d4e94360bb91829cfce47dc3ba8622f2af4b		

Nombre	Esteban Roberto Ramirez Fernandez	**Fecha y hora de firma**	23/08/2023 17:51:45
Integrante			
Hash Firma	7c8815033e21c961663f705ffb7e7ec5e35df48519f8eb53c75525dca625188df9b5d4b043ffcd407329d5ec32df647f		