



Resolución de Presidencia

No. 015-2024-UNM

Lima, 31 de enero de 2024

Visto el Oficio No. 042-2024-DGA-UNM de la Dirección General de Administración, el Oficio No. 03-2024-UTIC-UNM y el Informe No. 05-2024-UTIC-UNM del jefe de la Unidad de Tecnología de la Información y la Comunicación de la Universidad Nacional de Música.

CONSIDERANDO:

Que de conformidad con el Artículo 18° de la Constitución Política del Perú de 1993 y el Artículo 8° de la Ley No. 30220 Ley Universitaria, cada universidad es autónoma en su régimen normativo, de gobierno, académico, administrativo y económico y las universidades se rigen por sus propios estatutos en el marco de la Constitución y de las leyes;

Que mediante el Artículo 1° de la Ley No. 30597 se denomina Universidad Nacional de Música al Conservatorio Nacional de Música, asimismo el Artículo 2° establece que deberá adecuar su estatuto y órganos de gobierno conforme a lo dispuesto en la Ley No. 30220 Ley Universitaria;

Que el Artículo 4° de la Ley No. 30851, sobre la conformación de la Comisión Organizadora señala que, el Ministerio de Educación designa a los integrantes de la Comisión Organizadora de la Universidad Nacional de Música, previo procedimiento previsto en la norma; asimismo, el Artículo 29° de la Ley No. 30220 Ley Universitaria, dispone que la Comisión Organizadora tiene a su cargo la aprobación del estatuto, reglamentos y documentos de gestión académica y administrativa de la universidad, así como su condición y dirección hasta que se constituyan los órganos de gobierno que de acuerdo a la ley le corresponda;

Que mediante la Resolución Viceministerial No. 002-2019-MINEDU, la Resolución Viceministerial No. 068-2019-MINEDU y la Resolución Viceministerial No. 121-2021-MINEDU, se constituye y reconfirma la Comisión Organizadora de la Universidad Nacional de Música; asimismo mediante la Resolución Viceministerial No. 054-2023-MINEDU se designa a la maestra Lydia Fátima Hung Wong en el cargo de Presidenta de la Comisión Organizadora, quien ejerce funciones junto al maestro Claudio German Panta Salazar, Vicepresidente Académico y al maestro Jack Diego Puestas Castro, Vicepresidente de Investigación;

Que de conformidad con el inc. d) del numeral 6.1, sub numeral 6.1.5. del Artículo VI DISPOSICIONES ESPECÍFICAS de la Resolución Viceministerial No. 244-2021-MINEDU, documento normativo que aprueba las "Disposiciones para la constitución y funcionamiento de las comisiones organizadoras de las universidades públicas", es función de la Presidenta de la Comisión Organizadora emitir resoluciones en el ámbito de su competencia; asimismo el inc. k) establece la función de velar por el cumplimiento estricto de las exigencias de los sistemas administrativos y funcionales, de acuerdo a la normatividad vigente;

Que mediante el Oficio No. 03-2024-UTIC-UNM de fecha 16 de enero de 2024 el jefe de la Unidad de Tecnología de la Información y la Comunicación remite el Informe No. 05-2024-UTIC-UNM y recomienda la aprobación de la Política de Seguridad de la Información - Política de Seguridad de Datos de TI según lo establecido en el Decreto Legislativo No. 1412-2018 Cap. IV Art. 33 que se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información, Decreto Supremo N° 004-2013-PCM que aprueba la Política Nacional de Modernización de la Gestión Pública, la Resolución Ministerial No. 119-2018-PCM, que dispone que cada entidad de la administración pública constituya un Comité de Gobierno Digital, la Norma NTP-ISO/IEC 17799:2004 que ofrece recomendaciones para realizar la gestión de la seguridad de la información y la Norma NTP-ISO/IEC 27001:2014 que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización;

Que mediante el Oficio No. 042-2024-DGA-UNM de fecha 29 de enero de 2024, el Director General de Administración, Magíster Samuel Enrique Sánchez Gómez, remite a la Presidencia de la Comisión Organizadora, el Oficio No. 03-2024-UTIC-UNM y el Informe No. 05-2024-UTIC-UNM que contiene la propuesta de la Política de Seguridad de la Información - Política de Seguridad de Datos de TI, elaborada por el jefe de la Unidad de Tecnología de la Información y la Comunicación, Ing. Jean Pierre Chalán Castro de Cavalcanti, el cual cuenta con su visto bueno;

Con el visado de la Dirección General de Administración y la Unidad de Tecnología de la Información y la Comunicación; y

De conformidad con la Constitución Política del Perú de 1993 y sus modificatorias, la Ley No. 30220 y sus modificatorias, Ley Universitaria, la Ley No. 30597, la Ley No. 30851, el Decreto Legislativo No. 1412-2018, el Decreto Supremo No. 004-2013-PCM, la Resolución Ministerial No. 119-2018-PCM, la Resolución Viceministerial No. 068-2019-MINEDU, la Resolución Viceministerial No. 121-2021-MINEDU, la Resolución Viceministerial No. 244-2021-MINEDU, la Resolución Viceministerial No. 055-2022-MINEDU, la Resolución Viceministerial No. 054-2023-MINEDU, la Norma NTP-ISO/IEC 17799:2004 y la Norma NTP-ISO/IEC 27001:2014.

SE RESUELVE

APROBAR la Política de Seguridad de Datos de TI de la Universidad Nacional de Música.

Regístrese y comuníquese.


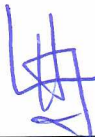


LYDIA F. HUNG WONG
Presidenta de la Comisión Organizadora
Universidad Nacional de Música



 Universidad Nacional de Música	Política de Seguridad de Datos de TI	Código:	UTIC-ADM-01
		Versión:	V.01

POLÍTICA DE SEGURIDAD DE DATOS DE TI DE LA UNIVERSIDAD NACIONAL DE MÚSICA

DESCRIPCIÓN	CARGO	NOMBRE	FIRMA
ELABORADO:	JEFE DE UTIC	Ing. Jean Pierre Chalán Castro de Cavalcanti	
REVISADO:	Dirección General de Administración	Mg. Samuel Enrique Sánchez Gómez	
APROBADO:	Presidencia de la Comisión Organizadora	Mtra. Lydia Fátima Hung Wong	

 Universidad Nacional de Música	Política de Seguridad de Datos de TI	Código:	UTIC-ADM-01
		Versión:	V.01

Política de Seguridad de Datos de TI

1. Propósito

El propósito de esta política es establecer los estándares y procedimientos para proteger la confidencialidad, integridad y disponibilidad de los datos sensibles manejados por los sistemas de tecnología de la información (TI) de la Universidad Nacional de Música.

2. Manejo de Datos Sensibles y Confidenciales

1. Clasificación de Datos:

- Se establecerá un sistema de clasificación que identifique y categorice los datos según su nivel de sensibilidad. Por ejemplo:
- Datos Públicos: Información no confidencial y de acceso público.
- Datos Internos: Información para uso interno, no confidencial pero restringida al personal autorizado.
- Datos Confidenciales: Información sensible que requiere protección especial, como datos financieros, información de clientes o datos personales.

2. Control de Acceso:

- Se implementarán medidas de control de acceso basadas en roles y privilegios para restringir el acceso a los datos confidenciales. Esto incluirá:
- Autenticación de dos factores para el personal autorizado.
- Limitación de acceso según la necesidad de conocer (principio de mínimo privilegio).
- Registro y monitoreo de accesos para detectar actividades inusuales.

3. Políticas de Retención y Eliminación:

- Se establecerán políticas claras de retención de datos sensibles, determinando el tiempo durante el cual estos datos deben ser mantenidos activos y útiles.
- Se establecerán procedimientos seguros y permanentes para la eliminación de datos sensibles cuando ya no sean necesarios, evitando la posibilidad de recuperación por parte de terceros.

4. Auditorías y Revisiones:

- Se realizarán auditorías periódicas para evaluar el cumplimiento de las políticas de manejo de datos sensibles y para identificar posibles mejoras o actualizaciones necesarias.

3. Procedimientos de Cifrado

a. Datos en Reposo: Los datos en reposo se refieren a la información almacenada en dispositivos de almacenamiento, servidores o bases de datos cuando no están en movimiento o



 Universidad Nacional de Música	Política de Seguridad de Datos de TI	Código:	UTIC-ADM-01
		Versión:	V.01

siendo transferidos. Para garantizar su seguridad, se emplea el cifrado, que consiste en transformar estos datos en un formato ilegible a menos que se posea la clave de descifrado correspondiente.

- **Algoritmos Robustos y Actualizados:** Se utilizarán algoritmos de cifrado sólidos y actualizados, como AES (Advanced Encryption Standard), para garantizar la protección de los datos almacenados. Estos algoritmos tienen la capacidad de dificultar enormemente cualquier intento de acceso no autorizado a la información.

b. Datos en Tránsito: Los datos en tránsito se refieren a la información que se está transmitiendo a través de redes, ya sea internas o externas. Durante esta transmisión, es fundamental proteger la confidencialidad de los datos.

- **Protocolos de Cifrado (TLS/SSL):** Para proteger la información confidencial durante la transmisión, se aplicarán protocolos de cifrado como TLS (Transport Layer Security) o su predecesor SSL (Secure Sockets Layer). Estos protocolos utilizan técnicas criptográficas para codificar los datos, asegurando que solo el emisor y el receptor autorizados puedan acceder a la información.

4. Respaldo y Recuperación de Datos

Procedimientos de Respaldo y Recuperación de Datos

a. Política de Respaldo:

- **Programa de Respaldo Regular y Automático:** Se establecerá un programa que realice copias de seguridad automáticamente y de manera regular de los datos sensibles. Esto asegurará que la información crítica esté respaldada con frecuencia, minimizando la pérdida de datos en caso de incidentes.
- **Almacenamiento en Ubicaciones Externas Seguras:** Los respaldos se almacenarán en ubicaciones externas seguras, fuera de las instalaciones principales. Esto puede incluir servicios de almacenamiento en la nube con altos estándares de seguridad o centros de respaldo remotos con medidas de protección física y lógica robustas.
- **Pruebas Periódicas de Integridad y Disponibilidad:** Se realizarán pruebas periódicas para verificar la integridad de los respaldos y asegurar su disponibilidad en caso de necesidad. Estos ejercicios garantizan que los datos respaldados sean recuperables y estén libres de errores o corrupción.

b. Plan de Recuperación de Incidentes:

- **Plan Detallado de Recuperación de Datos:** Se mantendrá un plan exhaustivo que describa los procedimientos específicos para restaurar la información en situaciones como fallos del sistema, violaciones de seguridad u otros eventos adversos. Este plan detallará pasos concretos a seguir, roles y responsabilidades, y un cronograma de recuperación.
- **Procedimientos para Restaurar Datos:** El plan incluirá métodos claros para restaurar los datos desde los respaldos, ya sea a nivel de sistema completo o de datos específicos, dependiendo de la naturaleza del incidente.



 Universidad Nacional de Música	Política de Seguridad de Datos de TI	Código:	UTIC-ADM-01
		Versión:	V.01

- **Pruebas y Actualizaciones del Plan:** El plan de recuperación se probará regularmente para evaluar su efectividad y se actualizará según sea necesario para adaptarse a cambios en la infraestructura, tecnologías de respaldo o nuevos riesgos identificados.

5. Monitoreo y Auditoría

Monitoreo:

- **Supervisión Continua:** Se implementará un sistema de monitoreo continuo que registre y evalúe las actividades relacionadas con los datos sensibles y los sistemas de TI. Esto implica la observación constante de accesos, transacciones y comportamientos que puedan representar un riesgo para la seguridad de la información.
- **Detección de Anomalías:** El monitoreo se centrará en identificar patrones o comportamientos inusuales que puedan indicar posibles amenazas o brechas de seguridad. Herramientas como sistemas de detección de intrusiones o análisis de comportamiento pueden ser empleadas para esta finalidad.
- **Alertas y Respuesta a Incidentes:** Ante la detección de actividades sospechosas, se establecerán mecanismos de generación de alertas para que el equipo de seguridad de TI pueda responder rápidamente a posibles amenazas. Esto incluirá procedimientos claros para investigar y mitigar incidentes.

Auditoría:

- **Revisiones Periódicas:** Se llevarán a cabo auditorías periódicas de los sistemas, procesos y controles de seguridad de datos para evaluar su efectividad y verificar el cumplimiento de las políticas establecidas.
- **Evaluación de Cumplimiento:** Las auditorías analizarán si los procedimientos de seguridad de datos se ajustan a las normativas internas de la empresa, así como a las regulaciones externas y mejores prácticas de la industria.
- **Generación de Informes y Recomendaciones:** Se elaborarán informes detallados a partir de las auditorías, incluyendo hallazgos, áreas de mejora y recomendaciones para fortalecer la seguridad de los datos y el cumplimiento normativo.
- **Seguimiento y Acciones Correctivas:** Cualquier hallazgo derivado de las auditorías se abordará con acciones correctivas y preventivas, con un seguimiento para garantizar su implementación efectiva.

