Resolución de Presidencia

No. 014-2024-UNM

Lima, 31 de enero de 2024

Visto el Oficio No. 041-2024-DGA-UNM de la Dirección General de Administración, el Oficio No. 02-2024-UTIC-UNM y el Informe No. 04-2024-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 18º de la Constitución Política del Perú de 1993 y el Artículo 8º 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 1º de la Ley No. 30597 se denomina Universidad Nacional de Música al Conservatorio Nacional de Música, asimismo el Artículo 2º establece que deberá adecuar su estatuto y órganos de gobierno conforme a lo dispuesto en la Ley No. 30220 Ley Universitaria;

Que el Artículo 4º 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 29º 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 reconforma 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. 02-2024-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. 04-2024-UTIC-UNM y recomienda la aprobación de la Política de Seguridad de la Información - Directiva de Control de Usuarios a los sistemas de la Universidad Nacional de Música según lo establecido en el Decreto Legislativo No. 1412-2018 Cap. IV Art. 33 que 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 No. 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. 041-2024-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. 02-2024-UTIC-UNM y el Informe No. 04-2024-UTIC-UNM que contiene la propuesta de Política de Seguridad de la Información - Directiva de Control de Usuarios y Acceso a los sistemas de la Universidad Nacional de Música, elaborado 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

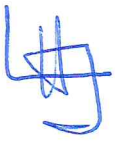
APROBAR la Directiva de Control de Usuarios y Acceso a los Sistemas de la Universidad Nacional de Música.

Regístrese y comuníquese.

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

PCO-UNM
PCO/LHW
SG/MIDR
DGA/SSG
UTIC/JPCHC
Cecilia Q.

DIRECTIVA DE CONTROL DE USUARIOS Y ACCESO A LOS SISTEMAS DE LA UNIVERSIDAD NACIONAL DE MÚSICA

DESCRIPCIÓN	CARGO	NOMBRE	FIRMA
ELABORADO:	Unidad de Tecnología de la Información y la Comunicación	Jean Pierre Chalán Castro de Cavalcanti	
REVISADO:	Dirección General de Administración	Samuel Enrique Sánchez Gómez	
APROBADO:	Presidencia de la Comisión Organizadora	Lydia Fátima Hung Wong	

Acceso y Control de Usuarios

1. Procedimientos para la gestión de cuentas de usuario:

A. **Creación de cuentas:** Las cuentas de usuario solo serán creadas por el personal autorizado de TI, siguiendo un procedimiento estándar que incluya la validación de la necesidad de la cuenta y la aprobación correspondiente.

- Solicitud de cuenta: Los usuarios deben completar un formulario de solicitud de cuenta, especificando la necesidad de acceso y el nivel de privilegios requeridos.
- Aprobación y validación: Un supervisor o un responsable designado debe aprobar la solicitud antes de que el equipo de TI proceda a crear la cuenta.
- Notificación al usuario: Una vez creada la cuenta, se notificará al usuario con instrucciones para configurar su contraseña inicial y cualquier otro detalle relevante.

Procedimiento de Creación de cuentas de usuario:

1. Solicitud de cuenta:

- Un empleado que requiere acceso a sistemas o datos específicos completa un formulario de solicitud de cuenta, indicando la justificación para el acceso y los privilegios necesarios.

2. Validación y aprobación:

- La solicitud es revisada por el supervisor o responsable del departamento para confirmar la necesidad y el nivel de acceso solicitado.
- El supervisor aprueba o deniega la solicitud, basándose en las políticas de acceso y necesidades laborales del empleado.

3. Procesamiento por el equipo de TI:

- Una vez aprobada, la solicitud se envía al equipo de TI, quienes crearán la cuenta del usuario según los criterios establecidos en la política de contraseñas seguras y niveles de acceso.
- Se genera un correo electrónico automático al solicitante, indicando que su cuenta ha sido creada y proporcionando instrucciones para la configuración inicial de la contraseña.

4. Configuración inicial de la cuenta:

- El usuario sigue las instrucciones proporcionadas para establecer su contraseña inicial.
- La contraseña debe cumplir con los estándares de seguridad definidos en la política de contraseñas seguras.

5. Entrega de credenciales y acceso:

- Una vez que la contraseña ha sido establecida, el usuario recibe sus credenciales de acceso y puede iniciar sesión en los sistemas autorizados según los privilegios otorgados.

6. Registro y documentación:

- Se registra la creación de la cuenta en un registro interno, indicando quién solicitó la cuenta, quién aprobó la solicitud, la fecha de creación y los privilegios asociados a la cuenta.

7. Auditoría y seguimiento:

- Se llevará a cabo una auditoría periódica para verificar que todas las cuentas creadas estén justificadas y en cumplimiento con las políticas de seguridad.
- En caso de cuentas inactivas o que ya no se necesiten, se seguirá el procedimiento para desactivar o eliminar dichas cuentas según lo establecido en la política.

B. **Modificación y eliminación de cuentas:** Cualquier cambio en los privilegios o la información de la cuenta debe ser solicitado y aprobado a través de un canal designado. Las cuentas de usuarios que ya no sean necesarias deben ser desactivadas o eliminadas inmediatamente.

- Solicitud de cuenta: Los usuarios deben completar un formulario de solicitud de cuenta, especificando la necesidad de acceso y el nivel de privilegios requeridos.
- Aprobación y validación: Un supervisor o un responsable designado debe aprobar la solicitud antes de que el equipo de TI proceda a crear la cuenta.
- Notificación al usuario: Una vez creada la cuenta, se notificará al usuario con instrucciones para configurar su contraseña inicial y cualquier otro detalle relevante.

Procedimiento de Modificación y eliminación de cuentas de usuario:

1. Solicitud de modificación o eliminación:

- Un usuario o su supervisor directo solicita cambios en los privilegios de una cuenta o la eliminación de una cuenta, proporcionando detalles sobre la razón del cambio.

2. Validación y aprobación:

- La solicitud es revisada por el departamento de TI, asegurándose de que la solicitud esté debidamente justificada y cumpla con las políticas de acceso y seguridad establecidas.
- La aprobación se realiza por el supervisor directo del usuario o por un responsable designado, dependiendo del nivel de acceso y la sensibilidad de los datos asociados a la cuenta.

3. Proceso de modificación o eliminación:

a) **Modificación de cuentas:**

- Si se aprueba una modificación, el equipo de TI realiza los cambios en los privilegios de la cuenta según la solicitud validada.

b) **Eliminación de cuentas:**

- En caso de aprobación para eliminar una cuenta, el equipo de TI procede a desactivar o eliminar la cuenta según lo establecido en las políticas de retención de datos.

4. Comunicación al usuario:

- Se notifica al usuario sobre cualquier cambio realizado en su cuenta, ya sea una modificación en los privilegios o la eliminación de la cuenta, según corresponda.
- En caso de eliminación de la cuenta, se proporciona orientación sobre los pasos a seguir y cualquier respaldo de datos o información necesaria antes de la eliminación.

5. Registro y documentación:

- Se registra y documenta cada modificación o eliminación de cuenta, incluyendo quién solicitó el cambio, quién lo aprobó, la fecha y la razón de la modificación o eliminación.

6. Auditoría y seguimiento:

- Se realizarán auditorías periódicas para verificar que los cambios en las cuentas estén debidamente documentados y justificados, además de asegurarse de que se sigan los procedimientos establecidos.
- En caso de que se identifiquen cuentas inactivas o desactualizadas, se procederá a tomar las medidas correspondientes según las políticas internas para mantener la seguridad de los sistemas y datos.

2. Políticas de contraseñas seguras y su rotación periódica:

- **Requisitos de contraseña:** Todas las contraseñas deben cumplir con estándares de seguridad, incluyendo una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. Se deben evitar contraseñas fáciles de adivinar.
  - Longitud y complejidad: Las contraseñas deben tener al menos 12 caracteres, incluyendo letras mayúsculas, minúsculas, números y caracteres especiales. Se evitarán palabras comunes o información personal.
  - Prohibiciones: Se prohibirá el uso de contraseñas reutilizadas, secuenciales o que hayan sido comprometidas en filtraciones de datos.
- **Rotación de contraseñas:** Las contraseñas deben rotarse periódicamente, con una frecuencia establecida según la sensibilidad de los datos y los sistemas a los que se accede.

- **Frecuencia de rotación:** La rotación de contraseñas se realizará cada 90 días para cuentas estándar y con mayor frecuencia (por ejemplo, cada 30 días) para cuentas con acceso a datos altamente sensibles o sistemas críticos.

3. Proceso de autorización de acceso a sistemas y datos sensibles:

- **Proceso de autorización:** El acceso a sistemas y datos sensibles requiere una autorización explícita por parte de un supervisor o administrador designado. Esta autorización debe ser documentada y mantenerse actualizada.

  - Solicitud de Acceso:

    - Cuando un empleado o usuario requiere acceso a sistemas o datos sensibles, debe presentar una solicitud formal. Esta solicitud puede realizarse a través de un formulario estandarizado o sistema de tickets que detalla la necesidad de acceso y la justificación para ello.

  - Revisión y Aprobación:

    - La solicitud de acceso es revisada por un supervisor, gerente o administrador designado. Esta persona evalúa la pertinencia del acceso solicitado en función de las responsabilidades laborales del solicitante y la necesidad de acceder a datos sensibles para cumplir con sus funciones.

  - Autorización Explícita:

    - Una vez revisada, la solicitud debe recibir una autorización explícita por parte del supervisor o administrador designado. Esta autorización debe ser documentada de manera adecuada, incluyendo detalles como la fecha de aprobación, el motivo del acceso y la duración (si aplica).

  - Segregación de Privilegios:

    - Los privilegios de acceso se asignan de acuerdo con los roles y responsabilidades específicos de cada usuario. Se asegura que cada usuario tenga acceso únicamente a los recursos y datos necesarios para llevar a cabo sus tareas laborales.

  - Mantenimiento y Actualización:

    - Se establece un protocolo para mantener actualizada la información sobre autorizaciones de acceso. Esto implica revisar regularmente los privilegios de los usuarios para asegurarse de que estén alineados con sus funciones actuales. Si hay cambios en las responsabilidades laborales, se ajustan los permisos de acceso en consecuencia.

  - Registro y Auditoría:

    - Se lleva un registro detallado de todas las autorizaciones de acceso concedidas, incluyendo quién otorgó la autorización, a quién se le

otorgó, el tipo de acceso concedido y la razón para ello. Estos registros son fundamentales para auditorías internas y externas, así como para mantener la trazabilidad de acceso a datos sensibles.

- Protección contra Abusos:
    - Se establecen medidas para prevenir el abuso de privilegios de acceso, como la monitorización de actividades sospechosas o inusuales, la implementación de límites de acceso en función del tiempo y la ubicación, y la capacitación continua para los usuarios sobre la importancia de la seguridad de la información.

- **Segregación de privilegios:** Los privilegios de acceso se asignarán de acuerdo con los roles y responsabilidades específicos de cada usuario. El acceso se limitará a lo estrictamente necesario para realizar las funciones laborales.
    - Identificación de Roles y Responsabilidades:
        - Se identifican y definen los distintos roles dentro de la organización, determinando las responsabilidades asociadas a cada uno. Por ejemplo, un administrador de sistemas, un profesor, un estudiante, etc., tendrán diferentes niveles de acceso y responsabilidades.

    - Asignación Basada en Roles:
        - Los privilegios de acceso se asignan en función de los roles y responsabilidades definidos. Cada rol tendrá un conjunto específico de permisos que reflejen las tareas que se espera que ese rol realice. Por ejemplo, un administrador de sistemas tendrá acceso completo a la infraestructura, mientras que un estudiante puede tener acceso limitado a los recursos del aula virtual.
    - Principio de Menor Privilegio:
        - Se aplica el principio de "menor privilegio", lo que significa que se otorgan los permisos mínimos necesarios para que un usuario realice su trabajo. No se otorgan permisos adicionales o privilegios administrativos a menos que sea estrictamente necesario.
    - Control de Acceso Granular:

Se implementa un control de acceso granular para limitar el acceso a datos sensibles o recursos críticos. Esto puede incluir la segmentación de redes, la encriptación de datos y la configuración de permisos específicos a nivel de archivos o carpetas.

- Revisión Periódica de Privilegios:

Se establece un proceso de revisión periódica de los privilegios de acceso para asegurarse de que sigan siendo adecuados y estén alineados con las funciones actuales

de los usuarios. Esto implica ajustar los permisos en caso de cambios en los roles o responsabilidades de los usuarios.

- Monitorización y Auditoría:

Se lleva a cabo un monitoreo continuo de los accesos y actividades de los usuarios con privilegios, registrando y auditando estas acciones para identificar posibles anomalías o usos indebidos de los privilegios.

- Capacitación y Concientización:

Se ofrece formación a los usuarios sobre la importancia de la segregación de privilegios, concienciándolos sobre los riesgos de un acceso excesivo y fomentando prácticas seguras en el uso de los recursos informáticos.

4. Restricciones de acceso a recursos específicos según roles:

- **Asignación de roles y permisos:** Los roles serán claramente definidos y se asignarán a los usuarios de acuerdo con sus responsabilidades. Los permisos se configurarán de manera que cada usuario solo pueda acceder a los recursos necesarios para realizar sus tareas.

Definición de Roles y Responsabilidades:

Se identifican y definen los distintos roles dentro de la organización o sistema. Esto puede incluir roles como administrador de sistemas, administrador de base de datos, usuario estándar, etc. Cada rol tiene responsabilidades específicas.

Asignación de Roles a Usuarios:

Cada usuario o miembro del sistema se asigna a un rol específico basado en sus responsabilidades y funciones dentro de la organización. Por ejemplo, un empleado de contabilidad puede tener un rol de "usuario de contabilidad" con permisos específicos relacionados con esa función.

Configuración de Permisos por Rol:

Se establecen los permisos y accesos asociados con cada rol. Esto implica definir qué recursos, archivos, carpetas, bases de datos o aplicaciones tienen acceso permitido para cada rol específico. Por ejemplo, el rol de "administrador de sistemas" tendría acceso a configuraciones críticas de red y servidores, mientras que un usuario estándar tendría acceso limitado a sus propios archivos y recursos compartidos necesarios para su trabajo.

Principio de Menor Privilegio:

Se sigue el principio de "menor privilegio" al configurar los permisos. Es decir, se otorgan los permisos mínimos necesarios para que un usuario realice sus tareas específicas. No se conceden permisos adicionales o privilegios que no sean estrictamente requeridos para su función.

Implementación de Control de Acceso:

Se utiliza un sistema de gestión de acceso que permita asignar y controlar estos permisos de manera efectiva. Esto puede incluir herramientas de gestión de identidad y acceso (IAM) o sistemas de control de acceso basados en roles (RBAC).

Revisión y Actualización Periódica:

Se lleva a cabo una revisión periódica de los roles, responsabilidades y permisos asignados a cada usuario. Esto garantiza que los accesos estén alineados con las funciones actuales de los usuarios y se ajusten en caso de cambios en las responsabilidades laborales.

Registro y Auditoría de Accesos:

Se registra y audita el acceso a recursos sensibles o críticos. Estos registros son fundamentales para identificar posibles brechas de seguridad, actividades sospechosas o accesos no autorizados.

- **Monitoreo y revisión:** Se realizarán auditorías periódicas para asegurar que los privilegios de acceso sean apropiados y estén actualizados. Cualquier cambio inusual o no autorizado en los accesos será investigado y corregido de inmediato.

Programación de Auditorías Regulares:

Se establece un calendario regular para realizar auditorías de los privilegios de acceso. Esto puede ser mensual, trimestral o anual, dependiendo de la criticidad de los datos y la frecuencia de cambios en las responsabilidades laborales.

Revisión de Permisos y Roles:

Durante estas auditorías, se examinan detalladamente los roles y los permisos asociados a cada usuario o grupo de usuarios. Se verifican las asignaciones de roles para asegurarse de que estén alineadas con las funciones actuales de los empleados.

Identificación de Cambios Inusuales o No Autorizados:

Durante la auditoría, se buscan cambios inusuales en los privilegios de acceso. Esto puede incluir accesos recientemente otorgados a recursos críticos, cambios en los permisos sin justificación o accesos a áreas que no corresponden al rol del usuario.

Investigación de Anomalías:

Cualquier cambio sospechoso o no autorizado se investiga de inmediato. Se busca la causa y se rectifica el acceso no autorizado o los permisos incorrectos. Esto puede implicar la revocación inmediata de los privilegios o la revisión de los registros de acceso para identificar posibles brechas de seguridad.

Actualización y Corrección:

Se realizan los cambios necesarios para corregir los problemas identificados durante la auditoría. Esto puede implicar la actualización de roles, la revocación de permisos indebidos o la corrección de errores en la asignación de accesos.

Registro y Documentación:

Se documentan todas las auditorías realizadas, los cambios efectuados y las acciones tomadas como resultado de la revisión. Estos registros son valiosos para futuras investigaciones y para demostrar el cumplimiento normativo.

Esta política será revisada periódicamente para asegurar su efectividad y ajustarse a los cambios en las tecnologías y riesgos de seguridad. El incumplimiento de estas políticas puede resultar en medidas disciplinarias, incluyendo la revocación de accesos.