"Año de la unidad, la paz y el desarrollo"

RESOLUCIÓN DE CONSEJO UNIVERSITARIO
N° 926 -2023-UNTRM/CU

Chachapoyas, 12 DIC 2023

VISTO:

El acuerdo de sesión extraordinaria N° LXX de Consejo Universitario, de fecha 12 de diciembre de 2023; y

CONSIDERANDO:

Que la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas, organiza su régimen de gobierno de acuerdo a la Ley Universitaria N° 30220, su Estatuto y reglamentos, atendiendo a sus necesidades y características;

Que con Resolución de Asamblea Universitaria N° 001-2023-UNTRM/AU, de fecha 02 de enero de 2023, se aprueba el Estatuto de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas, cuerpo normativo que consta de XXII Títulos, 178 Artículos, 04 Disposiciones Complementarias, 07 Disposiciones Transitorias, 01 Disposición Final, en 78 folios;

Que mediante Oficio N° 04535-2023-UNTRM-R/DGA, de fecha 19 de octubre de 2023, la Directora General de Administración, remite a la Oficina de Planeamiento y Presupuesto, el Oficio N° 210-2023-UNTRM-R-OTI, mediane el cual, el Director de la Oficina Tecnologías de la Información hace llegar la "POLÍTICA DE GESTIÓN DE BACKUPS EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS" y la "POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS", para su evaluación correspondiente;

Que mediante Informe N° 176-2023-UNTRM-R-OPP/UM, de fecha 20 de noviembre de 2023, el Jefe de la Unidad de Modernización, informa a la Jefa de la Oficina de Planeamiento y Presupuesto, que en virtud del principio de licitud y segregación de funciones, concluye que de la revisión de los proyectos de políticas presentados por la Oficina Tecnologías de la Información, se identifica que fueron formulados en el marco de las funciones asignadas en el ROF de la UNTRM; de modo que contando previamente con el visto bueno del área usuaria, es factible la aprobación de los proyectos de políticas denominados: "POLÍTICA DE GESTIÓN DE BACKUPS EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS" y la "POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS";

Que con Oficio N° 2269-2023-UNTRM-R/OPP, de fecha 01 de diciembre de 2023, la Jefa de la Oficina de Planeamiento y Presupuesto, remite a la Jefa de la Oficina de Asesoría Jurídica, los proyectos de las políticas denominadas: "POLÍTICA DE GESTIÓN DE BACKUPS EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS" y la "POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS", para el pronunciamiento en relación a la factibilidad de la aprobación de la Directiva, y posteriormente mediante su despacho sea derivado a la Dirección General de Administración para los trámites consiguientes para su aprobación;

Que mediante Informe Legal N° 237-2023-UNTRM-R/OAJ, de fecha 11 de diciembre de 2023, la Jefa de la Oficina de Asesoría Jurídica, concluye en lo siguiente: - Resulta factible la aprobación de la "POLÍTICA DE GESTIÓN DE BACKUPS EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS" y la "POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS". El presente cuerpo normativo, proyecto de Directiva, deberá ser sometida a Consejo Universitario, el cual, en el ejercicio de sus funciones, podrá aprobarla mediante resolución;

Consejo Universitario

"Año de la unidad, la paz y el desarrollo"

RESOLUCIÓN DE CONSEJO UNIVERSITARIO

N° 926 -2023-UNTRM/CU

Que mediante Oficio N° 05520-2023-UNTRM-R/DGA, de fecha 12 de diciembre de 2023, la Directora General de Administración, remite al señor Rector, el proyecto de "POLÍTICA DE GESTIÓN DE BACKUPS EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS" y la "POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS", que encontrándose acorde al marco normativo y con el visto bueno de las áreas competentes, recomienda poner a consideración del Consejo Universitario para su respectiva aprobación con acto resolutivo;

Que asimismo, el Estatuto Universitario señala en el "Artículo 30. Consejo Universitario. El Consejo Universitario es el máximo órgano de gestión, dirección y ejecución académica y administrativa de la UNTRM. (...)";

Que el Consejo Universitario en sesión extraordinaria, de fecha 12 de diciembre de 2023, acordó aprobar la "POLÍTICA DE GESTIÓN DE BACKUPS EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS", que consta de siete (07) folios, y la "POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS", que consta de diecinueve (19) folios;

Que estando a lo expuesto y en ejercicio de las atribuciones que la Ley Universitaria N° 30220, el Estatuto Universitario y el Reglamento de Organización y Funciones aprobado mediante Resolución Rectoral N° 022-2023-UNTRM/R y ratificado con Resolución de Consejo Universitario N° 012-2023-UNTRM/CU, le confieren al Rector en calidad de Presidente del Consejo Universitario de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas, y contando con los vistos buenos de la Dirección General de Administración, Oficina de Asesoría Jurídica y de la Unidad de Modernización;

SE RESUELVE:

ARTÍCULO PRIMERO.- APROBAR la *"POLÍTICA DE GESTIÓN DE BACKUPS EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS"*, que como anexo forma parte integrante de la presente resolución en siete (07) folios.

ARTÍCULO SEGUNDO.- APROBAR la *"POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS"*, que como anexo forma parte integrante de la presente resolución en diecinueve (19) folios.

ARTÍCULO TERCERO.- DEJAR SIN EFECTO las disposiciones internas que se opongan a la presente resolución.

ARTÍCULO CUARTO.- NOTIFICAR la presente resolución a los estamentos internos de la universidad, de forma y modo de Ley para conocimiento y fines.

REGÍSTRESE Y COMUNÍQUESE.

UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS
Jorge Luis Maicelo Quintana Ph.D.
Rector

UNIVERSIDAD NACIONAL TORIBIO RODRIGUEZ DE MENDOZA DE AMAZONAS
Abg. Mag. Roger Angeles Sánchez
Secretario General

JLMQ/R.
RAS/SG
Crhm/

POLÍTICA DE GESTIÓN DE BACKUPS EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS		
APROBADO MEDIANTE RESOLUCIÓN CONSEJO UNIVERSITARIO N° 926 -2023-UNTRM/CU		
ROL	**ÓRGANO**	**SELLO Y FIRMA**
ELABORADO POR	Oficina de Tecnologías de la Información	UNIVERSIDAD NACIONAL "TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS" Ing. ROISER CENTENO CACHAY Director (e) de la Oficina de Tecnologías de la Información
REVISADO Y VALIDADO	Oficina de Tecnologías de la Información	UNIVERSIDAD NACIONAL "TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS" Ing. ROISER CENTENO CACHAY Director (e) de la Oficina de Tecnologías de la Información
	Unidad de Modernización	UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS Abg. Carlos Francisco Grosso Vásquez JEFE DE LA UNIDAD DE MODERNIZACIÓN
	Oficina de Planeamiento y Presupuesto	UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS CPC. JESÚS E. REYNA TUESTA JEFA (e) DE LA OFICINA DE PLANEAMIENTO Y PRESUPUESTO
	Oficina de Asesoría Jurídica	UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS Abg. Karin del Rosario Burga Muñoz Jefa de la Oficina de Asesoría Jurídica
	Dirección General de Administración	UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS Milagritos del Carmen Zamora Vega Directora General de Administración

UNIVERSIDAD NACIONAL

TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS

POLÍTICA DE GESTIÓN DE BACKUPS EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS

ÍNDICE

POLÍTICA DE GESTIÓN DE BACKUPS EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS

I. OBJETIVO

Gestionar las actividades que permitan ejecutar copias de respaldo y resguardo de la información de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas.

II. ALCANCE

Comprende desde la revisión de la programación y ejecución del Backup de base de datos, firewall o de servicios, según la frecuencia establecida en el presente procedimiento hasta la recepción del informe correspondiente por parte del/la Director de la Oficina de Tecnologías de Información - OTI.

El presente procedimiento es de aplicación y cumplimiento obligatorio para los funcionarios y servidores públicos de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas.

III. BASE LEGAL

- Ley N° 27347. Ley de creación de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, y sus modificatorias.

IV. DEFINICIONES Y SIGLAS

- **Archivos:** documentos en formato digital de usuarios organizados en carpetas.
- **Backup o copia de respaldo:** Copia idéntica de información, copia de seguridad o copia respaldo de información almacenada en un lugar seguro con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Base de datos:** Colección de datos organizada de tal modo que sea fácilmente accesible, gestionada y actualizada.
- **Cinta de respaldo:** Medio magnético extraíble donde se almacena la información.
- **Data Center:** Ambiente donde se almacena y/o procesa información y/o datos de la entidad, es empleado para albergar los sistemas de información y/o componentes asociados, como telecomunicaciones y los sistemas de almacenamiento donde generalmente incluyen fuentes de alimentación redundante o de respaldo, para permitir que los equipos tengan el mejor nivel de rendimiento con la máxima disponibilidad de los sistemas.
- **Datos:** Los datos representan un fragmento de una cantidad, medida, descripción o palabra, los cuales son agrupados o clasificados de una determinada manera para generar información.
- **Repositorio:** Ambiente de respaldo donde se almacena, organiza, mantiene y difunde información como archivos informáticos, base de datos, entre otros. Los datos

almacenados en un repositorio pueden distribuirse a través de una red informática, como Internet, o de un medio físico, como un disco compacto.

- **Resguardo externo:** Resguardo realizado por un proveedor contratado por la institución, para brindar el servicio de custodia y almacenamiento externo de las cintas magnéticas de backup, bajo estándares recomendados por el fabricante.
- **Resguardo interno:** Ambiente de custodia de los medios de almacenamiento, ubicado dentro del Data Center o en un ambiente cercano a este.
- **Servidor:** Equipo informático que forma parte de una red y provee servicios a otros equipos cliente, es decir, es el equipo que provee servicios utilizados por los usuarios de la red del SENAMHI, estos servicios pueden ser de almacenamiento de datos centralizados, provisión de programas, autenticación de usuarios, etc.

V. RESPONSABILIDADES

5.1 Oficina de Tecnologías de la Información – OTI

a) Actualizar y formular propuestas de optimización y mejora del presente procedimiento, en el marco de las normas legales correspondientes y las medidas de racionalidad y austeridad en el uso de recursos públicos.
b) El Director de la OTI es el responsable de velar por el cumplimiento de lo dispuesto en el presente procedimiento.

5.2 Encargado y/o especialista de seguridad y respaldo

a) Identificar el tipo de backup y realizar las actividades correspondientes al mismo.
b) Validar los backups ejecutados y realizar copias de backups en cintas

VI. GENERALIDADES

6.1 Reglas generales

a) Realiza pruebas trimestrales de recuperación y calidad de la información respaldada, estas pruebas se deben de seleccionar de manera aleatoria y están a cargo del Director de la OTI.
b) Mensualmente se debe de remitir un informe al Director de la OTI conteniendo la información de los backup realizados, la elaboración de dicho informe es responsabilidad del encargado y/o especialista de seguridad y respaldo.

6.2 Tipos de backup

a) Backup de base de datos

Identificar la base de datos (administrativa y/o técnica) a respaldar y ejecutar. Posteriormente se debe validar el respaldo efectuado para su almacenamiento en el repositorio. Una vez almacenado este debe ser grabado en cintas de respaldo.

El backup de base de datos es realizado por el/la Especialista de la OTI. Existen dos tipos de respaldo de base de datos: Respaldo en caliente y respaldo en frio.

Respaldo en caliente. Es el respaldo que se realiza cuando el motor de la base de datos se encuentra en funcionamiento, es decir se realiza una copia de seguridad cuando los usuarios acceden a la base de datos.
Respaldo en frio. El respaldo que se realiza cuando el motor de la base de datos no se encentra en funcionamiento, se respalda las estructuras, configuraciones y datos de la base de datos.

b) Backup de Firewall

En este tipo de backup se realiza una copia de las configuraciones y políticas del firewall.

c) Backup de Servicios

En este tipo de backup se realiza una copia de seguridad de la información de los usuarios (documentos, archivos o carpetas digitales), de los aplicativos y/o sistemas de información desarrollados o adquiridos por la institución de los servicios de correo institucional, normas emitidas, entre otros.

6.3 Frecuencia de ejecución de backup

La frecuencia dependerá del tipo de backup a ejecutar, conforme se detalla a continuación:

a) Para Backup de base de datos

La frecuencia de respaldo de la base de datos institucional es ejecutada de manera diaria, semanal y mensual.

b) Para backups de firewall

La frecuencia de backup de firewall se ejecuta mensualmente.

c) Para backups de servicios

La frecuencia de backup de servicios alojados en los en los servicios, se ejecuta por una programación automática de manera diaria, semanal y mensual, siempre que estos actualicen su versión.

d) Ubicación de backup

El backups se validan, para luego ser almacenado en un repositorio y posteriormente en cintas de respaldo, las cuales son custodiadas por el jefe de la OTI.

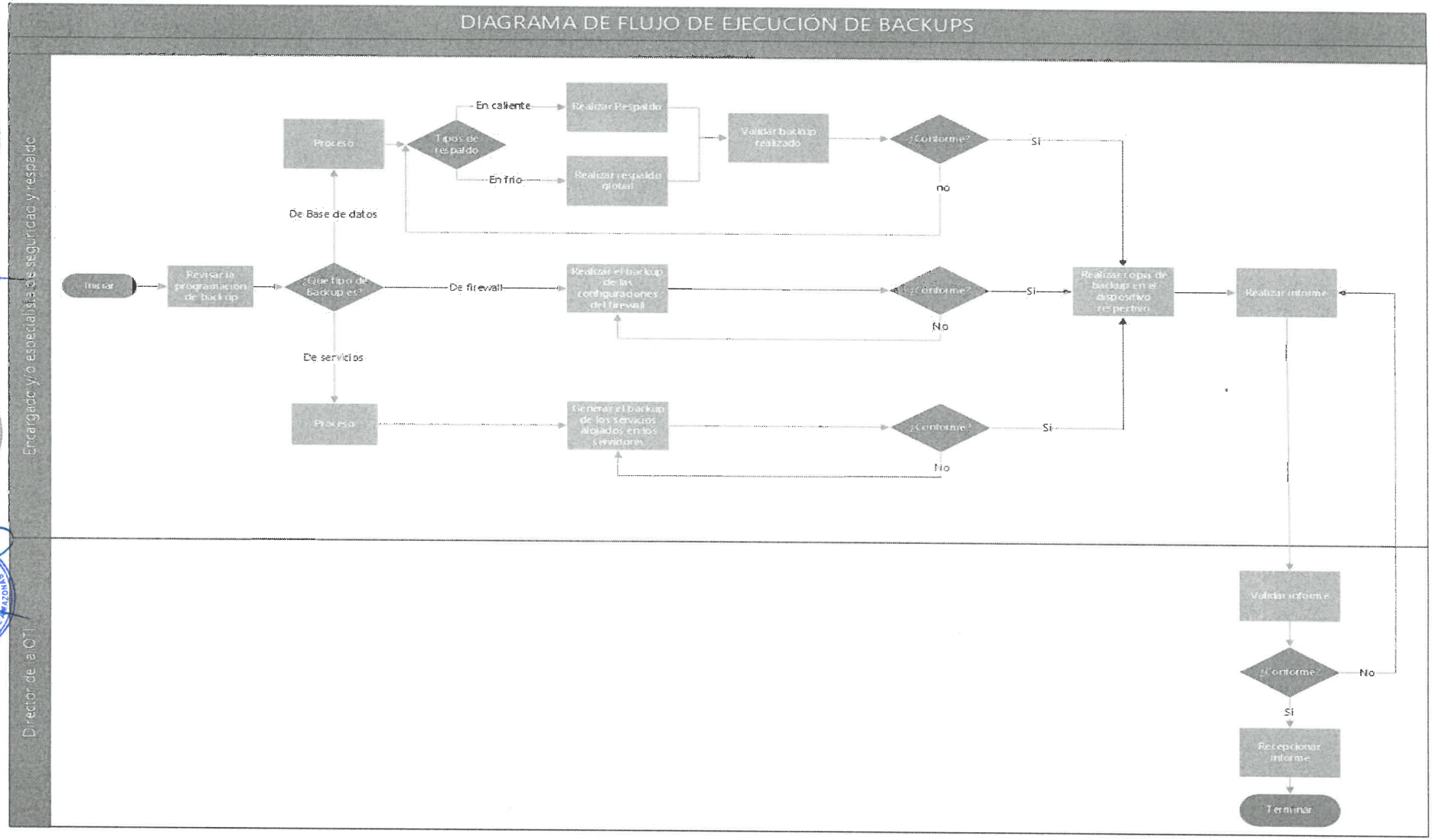
VII. DESARROLLO

Se detalla el proceso de ejecución de backup mediante diagrama de flujo.

VIII. ANEXO

Anexo N° 01: Diagrama de flujo.

Anexo N° 01: Diagrama de flujo



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS

APROBADO MEDIANTE
RESOLUCIÓN CONSEJO UNIVERSITARIO N° 926 -2023-UNTRM/CU

ROL	ÓRGANO	SELLO Y FIRMA
ELABORADO POR	Oficina de Tecnologías de la Información	UNIVERSIDAD NACIONAL "TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS" Ing. ROISER CENTENO CACHAY Director (e) de la Oficina de Tecnologías de la Información
REVISADO Y VALIDADO	Oficina de Tecnologías de la Información	UNIVERSIDAD NACIONAL "TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS" Ing. ROISER CENTENO CACHAY Director (e) de la Oficina de Tecnologías de la Información
	Unidad de Modernización	UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS Abg. Carlos Francisco Grosso Vásquez JEFE DE LA UNIDAD DE MODERNIZACIÓN
	Oficina de Planeamiento y Presupuesto	UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS CPC. JESUS E. REYNA TUESTA JEFA DE LA OFICINA DE PLANEAMIENTO Y PRESUPUESTO
	Oficina de Asesoría Jurídica	UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS Abg. Karin del Rosario Burga Muñoz Jefa de la Oficina de Asesoría Jurídica
	Dirección General de Administración	UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS Milagritos del Carmen Zamora Vega Directora General de Administración

UNIVERSIDAD NACIONAL

TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS

ÍNDICE

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS

I. OBJETIVO

Normar los requisitos de seguridad de la información dentro de los diferentes procesos de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas - UNTRM, para proteger la confidencialidad, disponibilidad e integridad de la información, recursos, servicios e instalaciones.

II. ALCANCE

Las disposiciones contenidas en el presente documento son aplicables al Sistema de Gestión de Seguridad de la Información (SGSI), así como a los trabajadores, proveedores, terceros y demás partes interesadas.

III. BASE LEGAL

- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. 2da Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 166-2017-PCM, que modifica la Resolución Ministerial N° 004-2016-PCM.

IV. DOCUMENTOS DE REFERENCIA

- Norma UNE-ISO/IEC 27001:2017 "Sistemas de Gestión de Seguridad de la Información – Requisitos".
- Norma NTP-ISO/IEC 27002:2017 "Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información.

V. DEFINICIONES Y ABREVIATURAS

5.1. Definiciones

Acceso remoto	Acceso desde un equipo de cómputo hacia un recurso informático de la UNTRM.
Activos de información	Bien o servicio tangible o intangible, que genera, procesa o almacena información, en el cual se le atribuye un grado de valor según su criticidad o asociación con los procesos de negocio los cuales están alineados a sus objetivos planteados.
Activos de TI	Está referido a los activos de Tecnologías de la Información, que son los recursos tecnológicos con los que cuenta una organización como el software, hardware y servicios.
Dispositivo móvil	Dispositivos que permiten a las personas acceder a datos e información desde cualquier lugar y en cualquier momento. Comprenden los dispositivos: laptops, smartphones, tabletas electrónicas y relojes inteligentes.
Equipo desatendido	Equipo de cómputo que queda momentáneamente sin supervisión por parte del trabajador.

Medios removibles	Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.
PIN	Utilizado en ciertos sistemas, como el teléfono móvil o el cajero automático, para identificarse y obtener acceso al sistema.
Portal cautivo	Página de inicio de sesión personalizado en redes empresariales que los usuarios invitados deben pasar antes de poder conectarse a la red inalámbrica.
Propietario de activo de información	Individuo o entidad de forma responsable, que cuenta con la aprobación del órgano de dirección, para el control de la producción, desarrollo, mantenimiento, utilización y seguridad de los activos. El término propietario no significa que la persona disponga de los derechos de propiedad reales del activo.
Proveedor	Persona natural o jurídica que brinda un servicio o producto a la UNTRM.
Proyecto	Proceso único, que consiste en un conjunto de actividades coordinadas y controladas con fechas de inicio y finalización, llevadas a cabo para lograr un objetivo conforme con requisitos específicos y requerimientos específicos, incluyendo las limitaciones de tiempo, coste y recursos
Remote Desktop Protocol (RDP)	Protocolo propietario desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre un terminal (mostrando la información procesada que recibe del servidor) y un servidor Windows (recibiendo la información dada por el usuario en el terminal mediante el ratón o el teclado).
Teletrabajo	Modalidad especial de prestación de labores, de condición regular o habitual. Se caracteriza por el desempeño subordinado de aquellas labores sin presencia física del trabajador o servidor civil en el centro de trabajo, con la que mantiene vínculo laboral. Se realiza a través de la utilización de las plataformas y tecnologías digitales (Ley N° 31572 – Ley de Teletrabajo). Todas las formas de trabajo fuera de la oficina, incluyendo los ambientes de trabajo no tradicionales, tales como los ambientes denominados "trabajo a distancia", "trabajo flexible", "trabajo remoto" y "trabajo virtual" (NTP-ISO/IEC 27002).
Tercero	Toda persona que no cuentan con vínculo laboral con la UNTRM, pero requiere hacer uso de sus activos de información ya sea para la prestación de un servicio (proveedores), en calidad de visitante o administrado (empresa operadora o usuario de servicio de telecomunicaciones).

5.2. Abreviaturas

CISO	Del término inglés Chief Information Security Officer, cuya correspondencia equivale al Oficial de Seguridad de la Información y Protección de Datos Personales y Abiertos en la UNTRM.
CSIRT	Del término ingles Computer Security Incident Response Team, cuya correspondencia equivale a Equipos de Respuesta ante Incidentes de Seguridad Digital.
DGA	Dirección General de Administración

OTI	Oficina de Tecnologías de la Información
URH	Unidad de Recursos Humanos
UNTRM	Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas
TI	Tecnologías de la Información

VI. POLÍTICAS

6.1. Seguridad de la información

- La Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas, como entidad que brinda educación superior universitaria considera a la información como un activo valioso para el cumplimiento de sus funciones y alcance de sus objetivos académicos y de investigación científica.
- Por tanto, resulta necesario gestionar la seguridad de la información estableciendo mecanismos para proteger su confidencialidad, disponibilidad e integridad ante amenazas internas o externas, deliberadas o accidentales; y se compromete a cumplir con los requisitos aplicables en seguridad de la información y mejorar continuamente su Sistema de Gestión de Seguridad de la Información.

6.2. Contacto con autoridades y grupos de interés especial

El CISO debe mantener y registrar el contacto con las autoridades y grupos de interés.

6.3. Gestión de proyectos

- Las dependencias orgánicas u órganos de la UNTRM, que tenga bajo su responsabilidad la ejecución de un proyecto, independientemente de su naturaleza (informático o no), debe realizar el análisis de riesgos de seguridad de la información sobre los activos de información involucrados.
- Los responsables de los proyectos deben comunicar al CISO sobre el alcance del proyecto de forma que se definan los requisitos necesarios para preservar la seguridad de la información de los activos de información involucrados.

6.4. Teletrabajo o acceso remoto

- El trabajador que preste labores de Teletrabajo o requiera acceso remoto debe cumplir con la presente política y cualquier otra normativa interna relacionada a seguridad de la información, protección de datos personales y confidencialidad de la información.
- El trabajador que preste labores de Teletrabajo contará con un acceso remoto que le permita acceder a los recursos y servicio internos de la UNTRM, el cual será habilitado por la OTI previa autorización del responsable de la Unidad Orgánica a la que pertenece. La solicitud de acceso remoto se realiza a través del correo electrónico soporte@untrm.edu.pe
- El responsable de la Unidad Orgánica que autoriza la solicitud de acceso remoto es responsable de evaluar la adecuada correspondencia con aquellos roles que realmente requieren el acceso por cumplimiento de sus funciones; de forma que se preserve la seguridad de la información de la UNTRM a la que accederá el trabajador.
- El responsable de la Unidad Orgánica debe revisar de forma trimestral la relación de sus trabajadores con acceso remoto o preste laborares de Teletrabajo y validar su correspondencia ante la OTI.

- El trabajador que cuente con acceso remoto ya sea por Teletrabajo o porque ha sido autorizado para su uso, debe proteger la información a la que tiene acceso de amenazas como el acceso no autorizado, alteración indebida o software malicioso cumpliendo con lo siguiente:
  - ✓ Conectarse desde ambientes físicos seguros.
  - ✓ Bloquear el equipo de cómputo desde el cual se conecta, cuando se retira de su ubicación.
  - ✓ Cerrar sesión en el acceso remoto al finalizar sus actividades.
  - ✓ Conectarse desde accesos a internet confiables, no públicos o gratuitos.
- La OTI provee mecanismos tecnológicos seguros para brindar el servicio de acceso remoto garantizando la transmisión cifrada de la información, así también implementa controles con la finalidad de proteger los recursos y servicios informáticos internos.
- En caso de necesidad de asistencia remota por parte de proveedores especializados se debe contar con la autorización previa del responsable de la Unidad Orgánica y se deberá solicitar a la OTI el acceso remoto, a través del correo electrónico soporte@untrm.edu.pe. En caso Soporte Informático identifique alguna situación que pueda vulnerar la seguridad de la información, solicitará la evaluación de la solicitud por parte del CISO.
- La asistencia remota interna es realizada sólo por el personal técnico de OTI, para lo cual se utilizarán conexiones con protocolos seguros; no está autorizado el acceso remoto entre trabajadores de otras Unidades Orgánicas.
- Se encuentra prohibido cualquier otro mecanismo técnico de acceso remoto no autorizado que permita el acceso desde redes externas a la red de la UNTRM o viceversa.

6.5. Recursos Humanos

- La URH es la responsable de verificar los antecedentes, la información de grados y títulos de los nuevos trabajadores que sean incorporados bajo el régimen laboral que establece el Decreto Legislativo 276 y el Decreto Legislativo 1057, así como, cualquier otra información, dentro de los límites legales permitidos y que resulte relevante para la seguridad de la información cuando el trabajador tenga acceso a información o instalaciones de procesamiento de información privilegiadas.
- El nuevo trabajador de la UNTRM participa del proceso de inducción organizado por la URH, con la participación del CISO o quién él delegue.
- Todos los productos, creaciones, desarrollos, campañas, trabajos, investigaciones, etc. realizados en cumplimiento de sus labores y/o funciones por el trabajador durante la vigencia de su vínculo laboral o contractual, serán de propiedad de la UNTRM.
- La URH debe comunicar a la OTI y la DGA sobre las rotaciones, licencias mayores o iguales a 3 meses, y ceses que se produzcan en la UNTRM, hasta con 3 días de anticipación; de forma que se tomen las medidas de control sobre la revocación de accesos a las instalaciones físicas, recursos y servicios informáticos.
- Las cuentas de usuario de trabajadores con licencia mayor o igual a 3 meses serán deshabilitadas salvo autorización expresa del responsable de la Unidad Orgánica. En los casos de cese, las cuentas serán inicialmente deshabilitadas por 15 días, posterior a ello el buzón del correo será eliminado de los servidores.

- Todos los trabajadores de la UNTRM deben asistir a las charlas, entrenamientos o capacitaciones en Seguridad de la Información, así como cumplir con las Políticas de Seguridad de la Información.
- Todos los trabajadores tienen la responsabilidad de reportar incidentes, eventos y/o debilidades de seguridad de la información que se identifican o se genere duda al respecto.
- Todos los trabajadores están sujetos a cláusulas de confidencialidad, las cuales se mantienen vigentes aun cuando se haya finalizado el vínculo laboral con la UNTRM.

6.6. Activos de información

- Los responsables de la Unidad Orgánica, que son propietarios de activos de información, deben mantener el inventario de sus activos de información actualizado.
- El acceso a los activos de TI se realiza a través de una cuenta de acceso a red, la misma que es habilitada por OTI.
- La OTI es la responsable de implementar mecanismos técnicos para brindar seguridad a los activos de TI.
- Los activos de TI son parte de patrimonio de la UNTRM; por tanto, la OTI en coordinación con la DGA realizan el proceso de asignación formal.
- Los trabajadores que tengan asignado información y/o activos de TI debe hacer uso de estos en estricto cumplimiento a sus funciones y/o actividades asignadas.
- Los trabajadores cuentan con unidades de red donde deben almacenar sólo información institucional evitando la duplicidad de datos por ser un uso incorrecto del almacenamiento.
- Los trabajadores deben proteger los activos de TI y la información albergada o procesada en estos, contra el acceso (físico y lógico) no autorizado, robo, daño, saturación de recursos, consumo excesivo del ancho de banda, exposición de datos personales, u otras situaciones que puedan exponer su confidencialidad, integridad o disponibilidad.
- Los usuarios que requieran retirar activos de TI de las instalaciones de la UNTRM deberán solicitarlo a la Unidad de Bienes Patrimoniales, según los formatos establecidos y contar con la autorización previa del responsable de la Unidad Orgánica correspondiente.

6.7. Clasificación de la información

- La información confidencial contenida en documentos físicos no debe ser transferida fuera de las instalaciones de la UNTRM y debe ser almacenada en lugares seguros y/o gabinetes con llave, evitando accesos no autorizados.
- La información confidencial contenida en documentos digitales, que requiera ser transferida en consecuencia de los procedimientos de la UNTRM, deberá realizarse a través de medios seguros haciendo uso de cifrado (por ejemplo: SFTP, HTTPS, entre otros); y su almacenamiento debe contar con controles de acceso lógico y mecanismos de cifrado o contraseña.

6.7.1. Medios removibles

- ✓ La movilización y salida de medios removibles que contengan información confidencial, fuera de la UNTRM se encuentra prohibida, salvo con autorización expresa de la Dirección General de

Administración. Esta prohibición no incluye el traslado de las cintas de respaldo hacia su lugar de custodia gestionado por la OTI.

- ✓ Todo trabajador que, para el cumplimiento de sus funciones, requiera conectar un medio removible a un equipo de cómputo de la UNTRM deberá asegurarse que sea analizado previamente por el software antimalware/antivirus.
- ✓ La DGA coordinará con la OTI para garantizar que los equipos de cómputo que serán entregados a los trabajadores en calidad de préstamo y retirados de las instalaciones de la UNTRM, tengan los puertos bloqueados para el uso de medios removibles. Estos puertos sólo se habilitarán cuando exista la necesidad y se cuente con la autorización del responsable de la UO.
- ✓ El trabajador que tenga asignado un medio removible debe resguardarlo y evitar el acceso no autorizado o uso indebido.
- ✓ El trabajador que haga uso de un medio removible debe evitar dejarlo conectado a equipos desatendidos.

6.7.2. Disposición de medios

- ✓ Los equipos de cómputo que contienen medios removibles y requieran ser dados de baja, deberán pasar por un proceso de borrado seguro.
- ✓ La OTI es responsable de normar e implementar el proceso de borrado seguro y destrucción de los medios (en caso corresponda), antes que se realice la baja o reutilización de este.

6.7.3. Uso de internet

- ✓ El servicio de internet se encuentra disponible para los trabajadores como herramienta de apoyo para el cumplimiento de sus funciones y realización de actividades.
- ✓ Los trabajadores son responsables de dar buen uso al servicio de internet, así como de adoptar las medidas de seguridad necesarias que garanticen que su trabajo se llevará a cabo de una manera eficiente y productiva.
- ✓ La OTI es responsable de brindar el servicio de internet a través de mecanismos seguros para lo cual implementa controles y filtros de navegación lo cual puede implicar la restricción parcial o total de sitios web potencialmente peligrosos. Así mismo, establece las configuraciones necesarias en los navegadores web autorizados en los equipos de cómputo.
- ✓ Dentro de las instalaciones de la UNTRM, no está permitido conectar los equipos informáticos de la UNTRM a cualquier otro medio de conexión a internet de proveedores externos que no haya sido dispuesto por la OTI.
- ✓ La UNTRM cuenta con la potestad de mantener los registros de navegación de su servicio de internet, así como de toda información entrante o saliente a través de su red, con la finalidad de monitoreo y/o revisión y sin previo aviso.
- ✓ Las conexiones inalámbricas a internet se realizarán a través de los portales cautivos, los mismos que serán usados por los visitantes, en caso lo soliciten y se encuentre autorizado por el responsable de la Unidad Orgánica correspondiente; la solicitud se realiza al correo electrónico soporte@untrm.edu.pe.

- ✓ Las solicitudes de cambio en la configuración del acceso a internet son aprobadas por el Jefe de la OTI, y en caso sea necesario se elevará a evaluación por el Comité de Gobierno, Transformación Digital e Innovación.
- ✓ Los trabajadores sólo podrán hacer uso del servicio de almacenamiento en la nube institucional, previa autorización de su jefe inmediato de la Unidad Orgánica a la que pertenece y de acuerdo con los mecanismos técnicos establecidos por la OTI.
- ✓ Los trabajadores no deben divulgar o publicar información confidencial en sitios web o en servicios de almacenamiento en la nube (Dropbox, Google Drive, etc.) o aplicaciones de mensajería instantánea gratuita (como Whatsapp, Telegram u otros análogos). Adicionalmente, está prohíbo visitar sitios web con contenido inapropiado (entretenimiento, pornografía, juegos, contenido ofensivo, redes sociales, chats, conexiones P2P) o que puedan ser fuente de archivos y programas maliciosos.
- ✓ La OTI gestiona las actualizaciones de software en los equipos informáticos de forma automática, por lo cual no se requiere la descarga de parches u otro software por parte de los trabajadores.

6.7.4. Uso del Correo Electrónico

- ✓ El servicio de correo electrónico se encuentra disponible para los trabajadores como herramienta de apoyo para el cumplimiento de sus funciones y realización de actividades.
- ✓ La OTI es responsable de brindar el servicio de correo a través de mecanismos seguros y confiables para lo cual implementa controles y filtros que pueden implicar la restricción parcial o total de cuentas de correo que remiten información potencialmente peligrosa.
- ✓ Los trabajadores no deben hacer uso de correos electrónicos gratuitos personales (Gmail, Hotmail, Yahoo, Outlook, etc.) con excepción de la Alta Dirección, directores, subdirectores, asesores y jefes.
- ✓ Los trabajadores no deben enviar información confidencial de la UNTRM por correo electrónico hacia cuentas de terceros y/o gratuitos.
- ✓ Los trabajadores que remitan información a cuentas grupales o listas de correo deben asegurarse de que los destinatarios tienen necesidad de conocer la información a remitir, entendiéndose que esta información es estrictamente laboral.
- ✓ Los trabajadores no deben remitir información de su entorno privado a través de cuentas de correo electrónico de la UNTRM, tampoco deben usar su cuenta de correo institucional para suscribirse a boletines, revistas, programas u otros medios de notificaciones de carácter personal.
- ✓ Los trabajadores que reciban un correo electrónico con contenido malicioso, fraudulento o donde se alerte situaciones que comprometan la seguridad de la información deberá remitir el mensaje a la cuenta de correo soporte@untrm.edu.pe con la finalidad de que se brinde el tratamiento adecuado, así como evitar su difusión o reenvío a otros destinatarios.
- ✓ Los trabajadores deben cuidar y hacer buen uso del servicio de correo electrónico de la UNTRM, toda acción contraria (envío de publicidad, correos masivos, suplantación de identidad, correos cadenas, virus,

código malicioso, contenido inapropiado u ofensivo, entre otros) y/o que ponga en peligro la información almacenada o transmitida por el servicio de correo, así como su infraestructura, está prohibida y será considerada como un ataque.

- ✓ Los trabajadores y/o Unidades Orgánicas que requieran enviar comunicaciones a todos los estudiantes, docentes, personal administrativo de la UNTRM deberán solicitarlo al correo electrónico soporte@untrm.edu.pe
- ✓ Los trabajadores deben hacer uso de firmas (resumen de datos) estandarizadas que lo identifiquen en el intercambio de correos electrónicos. La estructura de la firma seguirá lo normado por la OTI.
- ✓ Los trabajadores son responsables controlar el espacio de almacenamiento en su correo de forma que garantice su disponibilidad contando con opciones de eliminación, copia a carpetas del equipo local, entre otras.
- ✓ El trabajador que requiera acceder al servicio de correo electrónico institucional desde fuera del Perú, con motivo al cumplimiento de sus labores, deberá contar con la autorización del responsable de su Unidad Orgánica y solicitarlo a la OTI a través del correo electrónico soporte@untrm.edu.pe

6.7.5. Pantalla y escritorios limpios

- ✓ Los trabajadores deben bloquear su equipo de cómputo cuando se ausenten de su lugar de trabajo, así como guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial. Si los trabajadores están ubicados cerca de zonas de atención al público, deben guardar también los documentos y medios que contengan información de uso interno.
- ✓ Al finalizar la jornada de trabajo, el usuario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.
- ✓ La OTI configura el bloqueo automático de los equipos de cómputo ante la inactividad por 5 minutos, de forma que se proteja el acceso no autorizado.
- ✓ El trabajador debe mantener su escritorio virtual con la menor cantidad de archivos o accesos directos debido a que estos generan degradación del performance de los equipos de usuario.

6.8. Control de acceso

- ➢ El acceso a la información, a los recursos y servicios de TI debe ser controlado con la finalidad de preservar su confidencialidad, integridad y/o disponibilidad.
- ➢ Los propietarios de los activos de información son los responsables de definir las reglas de acceso y restricciones que son requeridas; así como la revisión periódica de los derechos de acceso a los mismos.
- ➢ La OTI es responsable de normar e implementar los mecanismos técnicos para controlar el acceso lógico a los recursos y servicios de TI, por tanto, no debe existir equipamiento informático y/o software que no cumpla con las condiciones de seguridad exigidos por este.
- ➢ Las Unidades Orgánicas deben comunicar a la OTI la relación de proveedores que requieren acceso a los sistemas de información con la debida autorización

y evidenciar el vínculo contractual con estos, así también comunicar la culminación del contrato para las bajas correspondientes en los accesos.

6.8.1. Identificación y contraseñas

- ✓ Todo acceso a recursos y servicios de TI se realiza con una cuenta de usuario que es un identificador único compuesto por un usuario y contraseña.
- ✓ La contraseña está clasificada como información confidencial por lo cual no se debe compartir o mantener anotaciones de esta, ya sea en papeles o archivos digitales.
- ✓ Las empresas operadoras que deban hacer uso de las aplicaciones informáticas de la UNTRM, designarán a sus usuarios autorizados, estas cuentas deberán ser diferenciadas de las cuentas internas de los trabajadores y mantener una nomenclatura estandarizada por OTI.
- ✓ Los trabajadores o terceros tienen prohibido usar una cuenta de usuario de otra persona o suplantar su identidad.
- ✓ El uso de cuentas genéricas solo está permitido para el uso de servicios específicos, previa autorización de la Unidad Orgánica responsable y en coordinación con la OTI.
- ✓ Las contraseñas deben ser robustas para mitigar riesgos de acceso no autorizado, por lo cual debe ser de una longitud mínima de 8 caracteres cumpliendo una combinación de números, símbolos, letras mayúsculas y minúsculas.
- ✓ Las cuentas de usuario serán bloqueadas ante 5 intentos de autenticación fallida.
- ✓ Las contraseñas almacenadas deben hacer uso de cifrados robustos como AES256 o superior.
- ✓ Las cuentas de usuario deben permitir que los usuarios realicen su cambio con una frecuencia máxima de 90 días, no se podrán reutilizar contraseñas anteriores. El usuario de una nueva cuenta de acceso debe cambiar su contraseña la primera vez que inicie sesión.
- ✓ El trabajador o tercero es responsable de que su contraseña cumpla con la fortaleza o robustez establecida en la presente política.
- ✓ La OTI, dentro de las características técnicas de las herramientas involucradas, establecerá los mecanismos para el cumplimiento de la fortaleza o robustez de la contraseña, bloqueo de intentos de autenticación fallida, cifrado robusto, tiempo de vigencia, reutilización y cambio de contraseña por defecto.
- ✓ El restablecimiento de contraseña por olvido debe ser solicitada a OTI que es responsable de realizar la validación de la identificación del solicitante bajo los mecanismos que establezca y asignando una contraseña temporal que cumpla con las características de fortaleza ya definidas.
- ✓ La entrega de la primera contraseña o clave temporal deben ser brindadas en cumplimiento del procedimiento establecido por la OTI.
- ✓ Todos los equipos y/o dispositivos conectados a la red de la UNTRM (routers, firewalls, switches, etc.) deben contar con contraseñas u otro mecanismo superior de control de acceso. La OTI es responsable de la seguridad de la red de la UNTRM por tanto norma los procedimientos adecuados para su cumplimiento.

- ✓ Ningún equipo o dispositivo conectado a la red de la UNTRM debe mantener contraseñas por defecto u omisión, incluyendo aquellas provistas por fabricantes o proveedores de equipamiento o software.

6.8.2. Usuarios privilegiados

- ✓ Las cuentas de usuarios del tipo administrador, súper administrador y/o administradores del dominio son de uso exclusivo de la OTI y deben ser usados solo para labores de mantenimiento, configuración y/o soporte de la plataforma tecnológica institucional.
- ✓ Las cuentas de administración local deberán ser desactivadas por defecto para los equipos de cómputo de usuario final.
- ✓ Las contraseñas de cuentas de usuario que son usadas por servicios (sistemas, IIS, SQL, Directorio Activo, Contrafuegos, almacenamiento etc.) e infraestructura son de uso exclusivo de la OTI y deben de tener una longitud mínima de 30 caracteres, combinación de números, símbolos, letras mayúsculas y minúsculas.
- ✓ Los usuarios que gestionen bases de datos con información confidencial y/o datos personales deben contar con controles que prevengan la pérdida de confidencialidad de la información como una adecuada gestión de accesos, controles en el equipo de usuario, controles de red, entre otros.

6.9. Seguridad física y del entorno

- ➢ Toda persona que ingrese a las instalaciones de la UNTRM debe identificarse y ser registrado tanto en el ingreso como en la salida. Los trabajadores y los terceros deben usar en todo momento su fotocheck o el identificador que se les haya sido asignado, portándolo en un lugar visible.
- ➢ La URH es la responsable de normar e implementar los mecanismos técnicos para asegurar el control del acceso físico a las instalaciones y a través de su Coordinador de Seguridad establece los procedimientos necesarios para cumplir con tal fin.
- ➢ No se encuentra permitido tomar fotografías o filmar dentro de los ambientes donde se almacene o procese información confidencial, como los archivos de las Unidades Orgánicas, el archivo central y el centro de datos.
- ➢ Las oficinas o instalaciones donde se almacene o procese información confidencial (Centro de Datos, Archivo, entre otras) deben contar con acceso restringido y monitoreado con cámaras de videovigilancia. El ingreso y salida de los trabajadores autorizados debe ser registrado por las Unidades Orgánicas responsables de dichos ambientes y, de ser el caso, emplear mecanismos biométricos.
- ➢ Las oficinas o instalaciones que contengan equipos de comunicaciones (switches, routers, firewalls) y consolas de administración, deben contar con acceso restringido y monitoreado con cámaras de videovigilancia.
- ➢ La OTI es responsable de mantener en condiciones razonablemente seguras el cableado de datos del UNTRM, así como los servicios de suministro (UPS) del centro de datos.
- ➢ El mantenimiento y supervisión de adecuada operación del grupo electrógeno es responsabilidad de la OTI.
- ➢ El mantenimiento de los equipos de cómputo e infraestructura tecnológica de la UNTRM están bajo la responsabilidad de la OTI.

6.9.1. Acceso al Centro de Datos

- ✓ El Centro de Datos es considerado una instalación crítica por almacenar y procesar información importante para la UNTRM.
- ✓ El acceso al Centro de Datos está permitido sólo al personal técnico autorizado de la OTI. El ingreso y salida es previa identificación biométrica.
- ✓ El personal técnico de la OTI, deberá registrar las acciones que realizará en el Centro de Datos, a manera de bitácora o registro de sucesos.
- ✓ Los terceros que requieran ingresar deben contar con autorización del responsable del Centro de Datos y estar acompañados por un personal técnico autorizado de la OTI quién supervisará los trabajos o actividades a realizar.
- ✓ Todo equipamiento que sea instalado debe ser inspeccionado antes de la entrega a fin de determinar si su contenido representa un peligro para la seguridad del centro de datos, de igual manera, esta tarea será supervisada por un personal técnico autorizado de la OTI.
- ✓ Cualquier mantenimiento efectuado en las áreas continuas al Centro de Datos que impliquen uso de químicos o agentes emisores de humo, polvo, gases o cualquier otra sustancia que afecte las alarmas del Centro de Datos, debe ser comunicado y coordinado con la OTI con el fin de prevenir alguna alteración del Centro de Datos.
- ✓ En mención a lo anterior, se debe realizar el correcto sellado de todas las puertas del Centro de Datos (deberá asegurarse el sellado de todo el marco de las puertas, para evitar ingreso de gases) así como ductería (cableado de fibra óptica, cableado de cobre, cableado eléctrico, etc.) y falso piso contiguos a sus instalaciones de ser necesario, utilizando para ello cinta de enmascarar - Hogar y Obra (cinta azul) de remoción limpia, este sellado lo deberá realizar el área responsable del mantenimiento o trabajo. Asimismo, 24 horas después de la finalización de los trabajos, dicha cinta deberá ser retirada sin dejar residuos en los marcos de las puertas.

6.9.2. Reutilización o baja de equipos informáticos

- ✓ Todo equipo de cómputo que contenga medios de almacenamiento debe pasar por un proceso de borrado seguro ante la necesidad de su reutilización o baja.
- ✓ La OTI es responsable de normar e implementar el proceso de borrado seguro y destrucción de los componentes informáticos (en caso corresponda), antes que se realice la baja o reutilización de este.

6.10. Relación con proveedores

6.10.1. Seguridad en las relaciones con proveedores

- ✓ Todo proveedor se asegurará que su personal designado para formar parte o brindar el servicio conozca y cumpla la presente política.
- ✓ Aquellos proveedores que hayan sido autorizados por los responsables de la Unidad Orgánica donde brindan servicio, para contar con una cuenta de correo electrónico deberán seguir los lineamientos establecidos en el ítem 6.6.5. Uso del Correo Electrónico.
- ✓ Todo personal del proveedor que en prestación de su contrato esté involucrado o en contacto con información, recursos o servicios tecnológicos de la UNTRM, debe protegerlos del acceso o uso no

autorizado, alteración de operaciones, destrucción, mal uso o robo, cumpliendo con los lineamientos de la presente política y con toda aquella normativa que sea aplicable a estos.

- ✓ Toda información albergada en la red corporativa, de forma estática o circulando a través de ella mediante elementos de comunicación o transmisión, es propiedad de la UNTRM y debe ser tratada como confidencial por todo proveedor.
- ✓ Todo personal del proveedor de servicio con responsabilidades en áreas de operación o administración de sistemas y redes debe:
  - Asegurar que la integridad, autenticación, control de acceso, auditoría y registro se contemplan e incorporan al diseñar, implantar y operar los Sistemas de Información y Redes de Comunicaciones.
  - Asegurar la confidencialidad de la información almacenada, tanto en formato electrónico como físico.
- ✓ Todo personal del proveedor que tenga contacto o haya obtenido conocimiento de información de la UNTRM debe guardar absoluta confidencialidad, esta obligación permanece vigente aún posterior a la extinción del contrato y por tiempo indefinido.
- ✓ Toda información (física o digital) que haya sido puesta a disposición del personal del proveedor es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.
- ✓ Todo personal del proveedor debe notificar inmediatamente a la UNTRM cualquier evento o incidente de seguridad o violación de datos que involucre información de la UNTRM a través del correo soporte@untrm.edu.pe, y colaborar en la mitigación y resolución del incidente, en caso sea necesario.
- ✓ Todo proveedor que tenga acceso a las instalaciones de la UNTRM deberá cumplir con lo especificado en la sección 6.8. Seguridad física y del entorno de la presente política. Así mismo, deberán cumplir con otras secciones, según la naturaleza del producto o servicio que brinden a la UNTRM, y que sean relevantes y esenciales para asegurar la seguridad de la información de la UNTRM.

6.10.2. Gestión de la provisión de servicios de proveedores

- ✓ El acceso a los activos de información por parte del personal del proveedor debe ser autorizado por el propietario del activo de información de la UNTRM.
- ✓ Las Unidades Orgánicas solicitantes de servicios o productos suministrados por proveedores deben de coordinar con la DGA para que se garantice la inclusión de cláusulas de seguridad en los contratos.
- ✓ La Unidad Orgánica usuaria en calidad de supervisor de la ejecución contractual deberá asegurarse que aquellos proveedores y/o su personal que brindan servicio dentro de las instalaciones de la UNTRM y/o realizan actividades donde se involucre el manejo de información y servicios informáticos, participen en una actividad de sensibilización en seguridad de la información.
- ✓ La Unidad Orgánica usuaria en su calidad de supervisor de la ejecución contractual deberá revisar de forma trimestral la relación de sus

proveedores con acceso remoto y con acceso a los sistemas de información de la UNTRM y validar su correspondencia ante la OTI.

- ✓ La Unidad Orgánica usuaria en su calidad de supervisor de la ejecución contractual será la encargada de monitorear y revisar el cumplimiento de los servicios o productos brindados por el proveedor, en coordinación con la DGA.

6.11. Adquisición, Desarrollo y Mantenimiento de Sistemas

- ➢ La UNTRM no realiza actividades de desarrollo de sistemas con recursos internos. Cualquier nuevo desarrollo es realizado o adquirido a terceros y en casos menores realiza mantenimiento de sus sistemas legados.
- ➢ Las Unidades Orgánicas que requieran la adquisición de sistemas de información deberán de coordinarlo con la OTI.
- ➢ La OTI cuenta con requisitos de seguridad de la información para el desarrollo (tercerizado), la adquisición y mantenimiento de sistemas de información, los cuales forman parte de los términos de referencia o requisitos mínimos en sus proyectos.
- ➢ La OTI es responsable de normar, solicitar e implementar los mecanismos técnicos que protejan los sistemas e información alojados en estos.
- ➢ La OTI es responsable de controlar el acceso y respaldo del código fuente de los sistemas de información de la UNTRM.
- ➢ La OTI es responsable de gestionar las pruebas de seguridad y funcionales necesarias para los nuevos sistemas o mantenimientos.
- ➢ La OTI establece un procedimiento para el control de cambios, el cual debe seguir principios de seguridad para los sistemas de información.
- ➢ No está permitido el uso de data de producción para desarrollos y pruebas, salvo que esta sea previamente enmascarada para evitar la pérdida de confidencialidad de la información.

6.12. Gestión de las Operaciones

6.12.1. Gestión del cambio

- ✓ La OTI es la responsable de gestionar los cambios en la infraestructura tecnológica y/o sistemas de información, y normar los procedimientos necesarios para este fin, así como mantener información documentada sobre este proceso.
- ✓ Los cambios deberán ser planificados e incluir la identificación de los posibles compromisos en seguridad de la información; los cuales, de ser el caso, serán comunicados al CISO para su evaluación de acuerdo con las políticas y requisitos de seguridad de la información.
- ✓ Los cambios de emergencia que requieren ser aplicados para resolver un incidente, deberán realizarse de forma rápida y controlada.
- ✓ Los cambios realizados deben ser verificados para asegurar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente.
- ✓ Los cambios deben de incluir un plan de roll-back (volver al estado anterior), que incluyan las actividades a seguir para abortar los cambios que se ejecutaron sin éxito y/o eventos imprevistos.

6.12.2. Gestión de la capacidad

- ✓ La OTI analiza la demanda de capacidad y realiza proyecciones de crecimiento de los recursos administrados (capacity planning) de

manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica de la UNTRM. Este análisis considera aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

6.12.3. Protección contra Software Malicioso

- ✓ La OTI es responsable del control del software por ello establece e implementa los mecanismos técnicos que protejan los recursos y servicios de TI, así como la información alojada.
- ✓ Los equipos de cómputo cuentan con software de protección contra malware, virus y troyanos.
- ✓ Los usuarios tienen restricciones de instalación de software con la finalidad de evitar la propagación de software malicioso,
- ✓ El servicio de correo cuenta con un servicio antispam para detectar correos maliciosos y bloquearlos.
- ✓ Los usuarios son responsables de reportar cualquier evento que identifiquen como potencialmente peligroso (archivos modificados sin autorización, ventanas emergentes, etc.) a soporte informático.
- ✓ Dentro de las actividades de concientización, el CISO, establece contenido relacionado al software malicioso.
- ✓ El Equipo de Respuesta ante Incidentes de Seguridad Digital de la UNTRM cuenta con un servicio que monitorea los eventos de seguridad del software antimalware.

6.12.4. Respaldo de Información

- ✓ La OTI es responsable de gestionar el respaldo de la información en formato digital, así como del software y sistemas.
- ✓ El respaldo de información debe almacenarse en lugares remotos para evitar cualquier daño en caso de desastre en las instalaciones de la UNTRM.
- ✓ La OTI establece los requisitos necesarios para la protección ambiental y física de las copias de respaldo.
- ✓ Se realiza copias de respaldo de la información de los servicios en producción de la UNTRM, los cuales incluyen código fuente, bases de datos y unidades de red y se encuentran administrados por la OTI.
- ✓ Las copias de respaldo diarias son conservadas por 30 días, las copias de respaldo semanales son conservadas por 4 semanas y las copias de respaldo mensuales son conservadas de forma indefinida.
- ✓ La OTI revisará periódicamente la vigencia tecnológica de los equipos y software utilizados para el respaldo y recuperación de la información.
- ✓ La OTI realizará pruebas periódicas (mínimo anual) de recuperación del respaldo, para asegurar que son confiables; para lo cual seleccionará una muestra de información y coordinará la verificación con la correspondiente Unidad Orgánica propietaria. Adicionalmente, en caso un área usuaria requiera la restauración de una copia de respaldo, esta será considerada como una prueba de recuperación de respaldo.

6.12.5. Protección de información de registros

- ✓ La OTI es responsable de asegurar que los componentes principales de la infraestructura tecnológica y sistemas de información cuenten con registros de auditoría sobre fallas y eventos de seguridad.

- ✓ Se deben contar con registros (logs de auditoría) de acceso a las bases de datos que contengan datos personales, así como registro de las acciones relevantes sobre estas.

6.12.6. Gestión de vulnerabilidades técnicas

- ✓ Todo proyecto informático que sea implementado en la UNTRM debe ser coordinado con la OTI y el CISO de forma que se incluya los requisitos de seguridad necesarios que eviten posibles vulnerabilidades.
- ✓ La OTI incluye dentro de los requisitos de adquisición o mantenimiento de software pruebas o análisis de vulnerabilidades.
- ✓ El CISO realiza periódicamente pruebas de vulnerabilidades sobre los servicios e infraestructura tecnológica, comunicará los resultados a las Unidades Orgánicas encargadas de la remediación para que planifiquen las acciones necesarias.
- ✓ La OTI como responsable de la seguridad de los recursos y servicios informáticos, realiza tareas de actualización periódica sobre el software de los servidores, equipos de cómputo, comunicaciones o seguridad perimetral.
- ✓ Los trabajadores o terceros que detecten vulnerabilidades o debilidades que puedan poner en peligro la información, recursos o servicios de TI, debe comunicarlo al CISO.
- ✓ Los trabajadores o terceros que detecten vulnerabilidades no deben aprovecharse de estas para acceder o difundir información no autorizada, así como producir alguna interrupción o daño en los recursos y servicios de TI.

6.12.7. Restricciones a la instalación y uso de software

- ✓ Los trabajadores o terceros no deben realizar instalación de software en los equipos informáticos, esta actividad es exclusiva del personal técnico de OTI.
- ✓ La OTI es responsable de la seguridad de los recursos y servicios de TI, por tanto, norma e implementa los mecanismos técnicos necesarios para protegerlo de amenazas que afecten su adecuado funcionamiento.
- ✓ Está prohibido difundir software o contenidos que violen derechos de autor o programas no licenciados o cuyo propietario de licencia no sea de la UNTRM. La OTI establece estos y otros lineamientos para la gestión adecuada del software legal.
- ✓ La actualización de software especializado que no se realice automáticamente a través de las herramientas de la OTI deberán ser solicitadas a Soporte Técnico como un requerimiento a través del correo electrónico soporte@untrm.edu.pe.

6.12.8. Controles de auditoría de sistemas de información

- ✓ Las pruebas de auditoría que afecten la disponibilidad de los sistemas deben ejecutarse fuera del horario de oficina previa coordinación entre el auditor, CISO, OTI y los responsables de las Unidades Orgánicas cuya información se encuentre involucrada en la auditoría.

6.13. Transferencia de información

- ➢ Las solicitudes de información por parte de organismos externos deben ser autorizadas por los propietarios de los activos de información y cuando

corresponda debe ponerse en conocimiento de la Dirección General de Administración – DGA UNTRM.

- La transferencia de información por medios informáticos desde o hacia organismos externos se deberá realizar usando mecanismos seguros (SFTP, TLS, IPSEC, etc.).
- La publicación de documentos en el portal web institucional (.docx, .xlsx, .pdf, etc.) se realizarán previa eliminación de los metadatos que puedan contener.
- Toda publicación web que haga referencia a información autorizada de la UNTRM debe utilizar el dominio untrm.edu.pe, no se acepta publicaciones que usen direcciones IP directamente.

6.14. Protección de datos personales

- La UNTRM, en cumplimiento de la Ley N° 29733 - Ley de Protección de Datos Personales, su reglamento, directiva y demás normas modificatorias, complementarias y conexas, realiza tratamiento de datos personales única y exclusivamente para el fin establecido, garantizando su confidencialidad, integridad y disponibilidad.
- En tal sentido, la UNTRM se compromete a:
  - ✓ Designar a un responsable por cada banco de datos personales; así como un responsable del tratamiento de estos.
  - ✓ Promover la toma de conciencia del personal responsable sobre la protección de los datos personales.
  - ✓ Cumplir con los requisitos legales, normativos y regulatorios aplicables.
  - ✓ Fomentar la mejora continua sobre las medidas adoptadas en protección de los datos personales a fin de minimizar los riesgos e incidentes de seguridad relacionados a los datos personales.

6.15. Controles criptográficos

- Los controles criptográficos son utilizados para la protección de la información clasificada como confidencial durante su transmisión por redes públicas a través de los protocolos HTTPS, SFTP, IPSEC, SSH. La OTI establece el uso de algoritmos de cifrado sólido.
- La OTI establece los controles necesarios para protección durante la generación, almacenamiento y archivo de las claves criptográficas, incluyendo los respaldos y accesos correspondientes.

6.16. Continuidad de la seguridad de la información

- En situaciones adversas, la UNTRM establece los siguientes lineamientos de seguridad de la información y de continuidad para la gestión de seguridad de la información:
  - ✓ Mantener el uso de credenciales de acceso a los sistemas de información de acuerdo con los lineamientos establecidos en "6.7.1 Identificación y contraseñas" de la presente política.
  - ✓ Mantener activados los logs de auditoría, en cumplimiento de lo establecido en "6.11.5 Protección de información de registros" de la presente política.
  - ✓ El acceso a las copias de respaldo solo está permitido a la OTI.
  - ✓ Mantener la configuración de copias de respaldo de archivos y bases de datos.

- ✓ Verificar que la documentación (física o digital) con clasificación confidencialidad esté protegida durante los traslados o restauración, incluyendo copias de respaldo.
- ✓ Mantener la misma configuración de los perfiles y usuarios de las aplicaciones en el ambiente de contingencia.
- ✓ En caso de verse afectados equipos de usuario final y estos requieran ser reemplazados, se debe mantener la configuración base.

➢ La OTI cuenta con un Plan de contingencia Informático, que establece las acciones a realizar ante escenarios adversos definidos.

VII. ACCIONES ANTE DESVIACIONES A LAS POLÍTICAS

El incumplimiento de las disposiciones establecidas en las políticas de seguridad de la información, procedimientos, manuales o cualquier otro documento derivado de estas, tendrá como resultado la aplicación de medidas correctivas y de mejora necesarias. En caso de encontrar responsabilidad en un trabajador y/o tercero, se dará inicio al procedimiento administrativo disciplinario correspondiente y/o a las acciones legales que la ley faculte.