



RES - 2026 - 691 - CS # UNNE
Sesión 26/08/2026

VISTO:

El EXP-2026-21864#UNNE, por el cual la Dirección de Gestión e Innovación de las Tecnologías de la Información (DGITI) eleva el proyecto denominado “Normativa de Ciberseguridad y Seguridad de la Información de la Universidad Nacional del Nordeste”, identificado como UNNE-CSI-POL-001; y

CONSIDERANDO:

Que el proyecto tiene por objeto establecer un marco institucional general en materia de ciberseguridad y seguridad de la información, aplicable al conjunto de la Universidad, comprendiendo sus Unidades Académicas, Institutos, Centros y demás dependencias, así como a los distintos actores que intervienen en el ecosistema digital institucional;

Que la propuesta contempla principios, responsabilidades y mecanismos de gobernanza, gestión de riesgos, protección y clasificación de activos de información, control de accesos, gestión de incidentes, respaldos y recuperación, continuidad operativa, seguridad en el desarrollo de sistemas, gestión de proveedores y servicios en la nube, capacitación, monitoreo, métricas y mejora continua;

Que la Unidad de Auditoría Interna, en ejercicio de las funciones previstas por la RES-2023-585-CS#UNNE, emitió opinión favorable respecto del diseño normativo, destacando que la propuesta contribuye al tratamiento de observaciones de auditoría pendientes vinculadas con la aprobación de una política de seguridad de la información, identificación de infraestructura crítica, inventario y etiquetado de activos, procedimientos de respaldo y recuperación y evaluación documentada de proveedores tecnológicos;

Que, asimismo, la Coordinación Ejecutiva de Planificación y Gestión de Inteligencia Artificial y Transformación Digital, prestó conformidad al proyecto y señaló su importancia como marco institucional para acompañar los procesos de transformación digital, incluyendo el desarrollo, implementación y utilización de soluciones basadas en inteligencia artificial, recomendando contemplar criterios de gobernanza de datos, trazabilidad, gestión de riesgos, supervisión humana y protección de información;

Que la Dirección General de Organización e Innovación Administrativa consideró conveniente que el marco general de la política sea aprobado por el Consejo



RES - 2026 - 691 - CS # UNNE
Sesión 26/08/2026

Superior, reservándose al Rector la aprobación, actualización e implementación de los anexos operativos, procedimientos y demás instrumentos técnicos necesarios para su desarrollo;

Que asimismo, recomendó la articulación con la RES-2024-8869-REC#UNNE, la incorporación de un cronograma de implementación progresiva y la adecuación de la documentación a los estándares institucionales de gestión documental;

Que la Secretaría General Legal y Técnica, mediante OL-2026-23-SGLT, efectuó el análisis jurídico del proyecto y concluyó que, por su naturaleza, alcance general, creación de estructuras de gobernanza y establecimiento de deberes institucionales, el instrumento reviste carácter de reglamento administrativo de alcance general;

Que, en consecuencia, corresponde que su aprobación sea efectuada por el Consejo Superior, en ejercicio de la competencia atribuida por el artículo 19º, inciso 1), del Estatuto Universitario, en cuanto le corresponde la dirección de la Universidad y el desarrollo de funciones normativas generales, de definición de políticas y de control;

Que la misma opinión jurídica considera jurídicamente admisible la delegación expresa en el Rector de las facultades relativas a la aprobación, actualización e implementación de los anexos operativos, procedimientos derivados y documentación complementaria, por tratarse de materias técnicas e instrumentales sujetas a modificaciones y actualizaciones frecuentes, sin afectar la competencia del Consejo Superior respecto de la definición de la política institucional, sus principios y su alcance;

Que el análisis jurídico efectuado tuvo especialmente en consideración la autonomía universitaria, el régimen de protección de datos personales, las garantías constitucionales, el régimen disciplinario, el régimen de contrataciones y la responsabilidad institucional, formulando observaciones destinadas a asegurar la compatibilidad del proyecto con el ordenamiento jurídico aplicable;

Que, en particular, se recomendó distinguir adecuadamente entre las normas nacionales de aplicación legal directa y obligatoria y aquellas reglamentaciones o estándares técnicos del Sector Público Nacional que son incorporados por la Universidad como referencias técnicas en ejercicio de su autonomía;



RES - 2026 - 691 - CS # UNNE
Sesión 26/08/2026

Que también se formularon observaciones vinculadas con la protección de datos personales, la transferencia internacional de información, el monitoreo de recursos institucionales, la continuidad del correo electrónico y los servicios de identidad, las consecuencias de los incumplimientos respecto de estudiantes y usuarios eventuales, la realización de pruebas de seguridad sobre sistemas institucionales, la intervención jurídica ante incidentes con posible relevancia penal, la articulación de los controles de seguridad con el régimen de contrataciones y la delimitación de las responsabilidades institucionales;

Que, con fecha 18 de agosto de 2026, la Dirección de Gestión e Innovación de Tecnologías de la Información informó la incorporación al proyecto de la totalidad de las observaciones calificadas como condición previa a su aprobación, incluyendo la adecuación de las cláusulas relativas a referencias normativas, organismos competentes, transferencia internacional de datos, monitoreo institucional, sistemas críticos, régimen aplicable a estudiantes y usuarios eventuales, dictamen de aptitud para contrataciones, verificación de idoneidad curricular, fe de erratas y uniformidad del versionado; quedando el documento identificado como Versión 2.3 – Agosto 2026;

Que corresponde, no obstante, que la aprobación de la normativa sea acompañada por medidas de implementación progresiva, en atención a la amplitud de su ámbito de aplicación y a la diversidad de sistemas, procesos, dependencias y niveles de madurez tecnológica existentes en la Universidad;

Que asimismo resulta conveniente preservar la articulación de la nueva normativa con los instrumentos institucionales actualmente vigentes, en particular con la RES-2024-8869-REC#UNNE, evitando superposiciones o contradicciones y disponiendo, de corresponder, su adecuación o refundición;

Que las medidas que eventualmente impliquen erogaciones deberán encontrarse sujetas a la disponibilidad presupuestaria y al cronograma de implementación que se establezca;

Que en mérito a todo lo expuesto, analizadas las constancias de estas actuaciones, lo dictaminado por la Dirección General de Asuntos Jurídicos y a la luz de la normativa vigente, la Comisión de Interpretación y Reglamento aconseja: 1º) Aprobar la “Normativa de Ciberseguridad y Seguridad de la Información de la Universidad Nacional del Nordeste”, identificada como UNNE-CSI-POL-001 - Versión 2.3 - Agosto 2026, que como proyecto forma parte de las presentes actuaciones, estableciendo que la misma constituye el marco institucional general en materia de ciberseguridad y



RES - 2026 - 691 - CS # UNNE
Sesión 26/08/2026

seguridad de la información, de aplicación en todo el ámbito de la Universidad conforme el alcance de las disposiciones establecidas en la misma. 2º) Delegar en el Sr. Rector la aprobación, actualización e implementación de los anexos operativos, procedimientos derivados y demás instrumentos técnicos, instructivos, registros, formularios, protocolos y/o documentación complementaria que resulten necesarios para el desarrollo, operación, mantenimiento y mejora continua de la normativa, dentro de los principios, objetivos, alcance y responsabilidades definidos por el Consejo Superior, tomando en consideración que las medidas que eventualmente impliquen erogaciones deberán encontrarse sujetas a la disponibilidad presupuestaria y al cronograma de implementación que se establezca. 3º) Disponer que la presente normativa se articulará con las reglamentaciones, procedimientos e instrumentos institucionales vigentes que resulten vinculados, en particular con la RES-2024-8869-REC#UNNE, facultando a las áreas competentes a proponer las adecuaciones que resulten necesarias;

Lo aprobado en sesión de fecha 26 de agosto de 2026;

EL CONSEJO SUPERIOR
DE LA UNIVERSIDAD NACIONAL DEL NORDESTE
RESUELVE:

ARTICULO 1º - Aprobar la “Normativa de Ciberseguridad y Seguridad de la Información de la Universidad Nacional del Nordeste”, identificada como UNNE-CSI-POL-001 -Versión 2.3- Agosto 2026, que se agrega como Anexo de la presente, estableciendo que la misma constituye el marco institucional general en materia de ciberseguridad y seguridad de la información, de aplicación en todo el ámbito de la Universidad conforme el alcance de las disposiciones establecidas en la misma.

ARTICULO 2º - Delegar en el Sr. Rector la aprobación, actualización e implementación de los anexos operativos, procedimientos derivados y demás instrumentos técnicos, instructivos, registros, formularios, protocolos y/o documentación complementaria que resulten necesarios para el desarrollo, operación, mantenimiento y mejora continua de la normativa, dentro de los principios, objetivos, alcance y responsabilidades definidos por el Consejo Superior, tomando en consideración que las medidas que eventualmente impliquen erogaciones deberán encontrarse sujetas a la disponibilidad presupuestaria y al cronograma de implementación que se establezca.

ARTICULO 3º - Disponer que la presente normativa se articulará con las reglamentaciones, procedimientos e instrumentos institucionales vigentes que resulten



RES - 2026 - 691 - CS # UNNE
Sesión 26/08/2026

vinculados, en particular con la RES-2024-8869-REC#UNNE, facultando a las áreas competentes a proponer las adecuaciones que resulten necesarias.

ARTICULO 4º - Regístrese, comuníquese y archívese.

PROF. PATRICIA B. DEMUTH MERCADO
SEC. GRAL. ACADÉMICA

PROF. GERARDO OMAR LARROZA
RECTOR

ANEXO

UNIVERSIDAD NACIONAL DEL NORDESTE

Dirección de Gestión e Innovación de las Tecnologías de la Información

NORMATIVA DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

Documento integral: política,
controles, procedimientos y anexos operativos

Versión:	2.3 — Agosto 2026. Incorporación de las 10 observaciones esenciales de la Opinión Legal SGLyT (OL-2026-23-SGLT-REC) previas a la elevación al Consejo Superior
Fecha de aprobación:	_____ de _____ de 2026
Ámbito:	Toda la UNNE
Naturaleza:	Política institucional con procedimientos y anexos operativos
Instrumento:	Resolución del Consejo Superior N° _____/2026 (marco general), con delegación en el Rector de anexos operativos, procedimientos derivados y documentación complementaria
Custodia:	Área de Ciberseguridad — DGITI
Revisión siguiente:	Marzo 2027 (o ante evento disparador)
Estado:	VERSIÓN CON OBSERVACIONES ESENCIALES DE LA SGLyT APLICADAS — PENDIENTE DE APROBACIÓN POR EL CONSEJO SUPERIOR

Marcos de referencia:

CIN CE 1669/22 · ISO/IEC 27001:2022 · ISO/IEC 27002:2022 · ISO/IEC 27005 · ISO 22301 · ISO/IEC 27031 · NIST CSF 2.0 · NIST SP 800-61 · NIST SP 800-34 · NIST SP 800-184 · ISO/IEC 27031 · Ley 25.326 · Ley 26.388 · Ley 25.506 · Ley 27.275

Ficha de control del documento

Campo	Datos
Título	Normativa de Ciberseguridad y Seguridad de la Información — UNNE
Identificador	UNNE-CSI-POL-001
Versión	2.3
Versión anterior	2.2 (Abril 2026)

Elaborado por	Dirección de Gestión e Innovación TI (DGITI)
Revisado por	Área legal / Secretaría de TI / Comité de Seguridad
Aprobado por	Consejo Superior (marco general) — Resolución CS; Rector (anexos operativos y procedimientos derivados, por delegación)
Fecha de elaboración	Marzo 2026
Próxima revisión	Marzo 2027
Distribución	Toda la comunidad universitaria UNNE
Soporte	Digital (repositorio institucional) y físico (Área de Ciberseguridad)

Control de cambios

Ver.	Fecha	Autor	Descripción del cambio
1.0	Mar 2026	DGITI	Versión integral inicial. Incorpora política, 19 cláusulas y 11 anexos operativos.
2.0	Mar 2026	DGITI	Revisión integral con observaciones: especificación de versión ISO; nueva sección 11 bis (ciberseguridad en la nube); expansión de criptografía; incorporación de Sección 20 (métricas); rol de Oficial de Privacidad; control de gestión de cambios; lineamientos DevSecOps; Anexos 12-15 nuevos; 10 procedimientos derivados (PE.DGITI.01 a PE.DGITI.10).
2.1	Mar 2026	DGITI	Revisión editorial final: consolidación de la sección 5 de riesgos, eliminación de duplicaciones, corrección de numeración, depuración de fragmentos insertados en procedimientos, homogeneización terminológica y revisión de metas de indicadores.
2.2	Abr 2026	DGITI	Incorporación del Anexo 16 sobre Política de Planes de Contingencia, Plan de Contingencia, Recuperación ante Desastres y Centro de Procesamiento de Datos de Respaldo; ajustes a Sección 18, PE.DGITI.10, Anexos 2, 10 y 11.
2.3	Ago 2026	DGITI / SGLyT	Incorporación de las 10 observaciones esenciales de la Opinión Legal SGLyT (OL-2026-23-SGLT-REC) previas a la elevación: distinción normas obligatorias/referencia técnica, corrección de organismos de referencia (7.1.6), encuadre de transferencia internacional de datos (Anexo 12), reformulación de la cláusula de monitoreo (Anexo 5), protocolo de continuidad de correo/identidad (Anexo 16), supresión de sanciones al claustro estudiantil (19.3.3), delimitación del dictamen de aptitud en contrataciones (PE.DGITI.05), reformulación de la verificación de idoneidad (8.1.2), corrección de la cláusula 6.1 y unificación de versionado / supresión de marcas [NV2].

Introducción

La Universidad Nacional del Nordeste reconoce que la información, los sistemas, las redes, los servicios digitales, la infraestructura tecnológica y los registros documentales que utiliza para el cumplimiento de sus

fines constituyen activos institucionales esenciales. La docencia, la investigación, la extensión, la administración y la vinculación con la comunidad dependen, de manera creciente, de entornos digitales interoperables, de servicios académicos y administrativos disponibles en línea —incluyendo plataformas en la nube— y de procesos de gestión sustentados en datos, expedientes electrónicos, plataformas colaborativas y recursos de procesamiento distribuidos.

La presente normativa establece el marco institucional de ciberseguridad y seguridad de la información de la UNNE. Su finalidad es fijar principios, responsabilidades, controles, procedimientos y criterios de actuación que permitan proteger la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y resiliencia de la información institucional, con un enfoque de mejora continua, gestión de riesgos y cumplimiento normativo.

A los efectos de esta normativa, se entiende por seguridad de la información el conjunto de medidas técnicas, organizativas, físicas y jurídicas orientadas a proteger los activos de información institucional, con independencia del soporte en que se encuentren. La ciberseguridad se refiere, específicamente a la protección del ecosistema digital de la Universidad: sus redes, sistemas, servicios en línea, infraestructura de conectividad y entornos de computación, frente a amenazas de origen digital. Ambas dimensiones son complementarias e inseparables en el contexto operativo de la UNNE.

La normativa se interpreta de manera armónica con el Estatuto de la Universidad, con las resoluciones del Consejo Interuniversitario Nacional vinculadas con la temática, con la normativa argentina aplicable y con estándares y buenas prácticas internacionalmente reconocidos.

El presente documento incluye: (a) la política institucional de seguridad de la información con sus diecinueve cláusulas temáticas y una sección adicional de métricas; (b) dieciséis anexos operativos; y (c) diez procedimientos derivados de la política. Todos ellos forman un cuerpo normativo integrado y deben interpretarse de manera conjunta y sistemática.

1. Misión

De conformidad con el Estatuto Universitario, la Universidad Nacional del Nordeste tiene por misión la creación, transmisión, preservación y difusión del conocimiento; la formación integral de personas; el desarrollo de actividades científicas, tecnológicas, culturales y de extensión; y la contribución al desarrollo regional y nacional.

La ciberseguridad y la seguridad de la información deben interpretarse como condiciones habilitantes para el cumplimiento efectivo de esa misión, y no como una actividad meramente instrumental o aislada del proyecto institucional. En consecuencia, la política de ciberseguridad de la UNNE se orienta a resguardar el funcionamiento continuo y confiable del ecosistema digital universitario, reducir la exposición a amenazas y vulnerabilidades, fortalecer las capacidades de prevención, detección, respuesta y recuperación frente a incidentes, y promover una cultura institucional de uso responsable, seguro y ético de la información y de las tecnologías digitales.

2. Alcance institucional

La presente normativa es de aplicación obligatoria para toda la Universidad Nacional del Nordeste. Comprende a Rectorado, Secretarías, Direcciones Generales, áreas centrales, Unidades Académicas, institutos, centros, dependencias, proyectos, laboratorios y cualquier otro ámbito que procese información o

utilice infraestructura tecnológica institucional, propia o tercerizada, bajo cualquier modalidad de prestación o soporte, incluidos los entornos de computación en la nube.

Quedan alcanzados por esta normativa el personal docente y no docente, las autoridades, investigadores, becarios, extensionistas, estudiantes, contratistas, consultores, pasantes, proveedores, socios tecnológicos, operadores externos y toda persona humana o jurídica que, por razón de sus funciones o de una relación contractual o institucional, acceda a información universitaria, utilice recursos tecnológicos de la UNNE, administre servicios o participe en procesos de tratamiento de datos.

El alcance material incluye, sin limitarse a ellos, los sistemas académicos, administrativos, documentales y de apoyo a la gestión; las plataformas de identidad y autenticación; la infraestructura de red y conectividad; los centros de datos; los servicios de almacenamiento, virtualización, respaldo y recuperación; los puestos de trabajo y dispositivos móviles; los servicios en la nube (IaaS, PaaS, SaaS); las bases de datos; los documentos en soporte físico o digital; los registros de auditoría; los certificados y credenciales digitales; y cualquier otro activo de información que sea generado, recibido, procesado, almacenado, transmitido o eliminado por la Universidad.

La aplicación de esta política se extiende también a los entornos remotos, de teletrabajo, movilidad, acceso externo y colaboración digital, cuando dichos entornos involucren credenciales institucionales, información universitaria o infraestructura conectada a redes de la UNNE.

3. Antecedentes y marco de referencia

La UNNE toma como punto de partida el Modelo de Políticas de Seguridad de la Información aprobado por el Consejo Interuniversitario Nacional mediante Resolución CE N° 1669/22, adoptando como referencia estructural para el desarrollo de esta política institucional propia, adecuada a su organización, madurez tecnológica y escala. La relación entre los dominios del modelo CIN y las secciones de este documento se consigna en el Anexo 15 a efectos de facilitar la trazabilidad en futuras auditorías externas.

A los efectos de esta normativa se distingue expresamente entre: (a) las normas de rango legal de aplicación directa y obligatoria a la Universidad, cuyo cumplimiento no admite ponderación de compatibilidad -en particular las Leyes N° 25.326, 26.388, 25.506, 27.275 y 11.723-; y (b) las reglamentaciones dictadas por el Poder Ejecutivo Nacional o sus organismos descentralizados para el Sector Público Nacional -entre ellas la Decisión Administrativa N° 641/2021 y las Disposiciones del Centro Nacional de Ciberseguridad N° 1/2022, N° 1/2026 y N° 3/2023- así como los modelos de adopción voluntaria -entre ellos la Resolución CIN CE N° 1669/22-, que la Universidad recibe como referencia técnica orientadora por decisión propia, adoptada en ejercicio de su autonomía universitaria (artículo 75, inciso 19, de la Constitución Nacional; artículos 29 y 48 de la Ley N° 24.521), y no en virtud de una remisión obligatoria.

Asimismo, la Universidad reconoce como marco legal y de referencia: la Ley N° 25.326 de Protección de los Datos Personales; la Ley N° 26.388 sobre delitos informáticos; la Ley N° 25.506 de Firma Digital; la Ley N° 27.275 de Derecho de Acceso a la Información Pública; la normativa sobre conservación y validez de documentos digitales; las normas de control interno y auditoría del sector público; y toda otra disposición que resulte exigible.

Se consideran como referencias técnicas: los requisitos mínimos de seguridad del sector público nacional en cuanto resulten orientadores; la Segunda Estrategia Nacional de Ciberseguridad (Res. N° 44/2023); las familias de normas ISO/IEC 27000 (con la precisión de versión indicada precedentemente); ISO/IEC 27005

para gestión de riesgos; ISO 22301:2019 para continuidad; NIST Cybersecurity Framework 2.0; NIST SP 800-61 (gestión de incidentes); NIST SP 800-53; y CIS Controls v8.

Las referencias a normas nacionales de aplicación específica sobre organismos del sector público nacional se utilizarán en la medida en que resulten obligatorias para la UNNE o, en su caso, como referencia técnica orientadora, sin presentarlas como obligaciones directas cuando su alcance jurídico no así lo determine, en consonancia con la autonomía universitaria reconocida constitucionalmente.

Cuando una norma sea actualizada, derogada o sustituida, la interpretación de esta normativa deberá hacerse a la luz de la versión vigente, sin necesidad de entender por ello modificada la sustancia de los controles, siendo la actualización formal de referencias promovida en la primera revisión integral del documento.

4. Organización de la seguridad de la información

La seguridad de la información requiere una estructura de gobernanza explícita, con responsabilidades diferenciadas, mecanismos de coordinación y capacidad efectiva de decisión. La UNNE sostendrá un esquema institucional que permita definir lineamientos, aprobar prioridades, asignar responsabilidades, monitorear cumplimiento, medir el desempeño y resolver situaciones críticas, evitando superposiciones, vacíos de autoridad o enfoques exclusivamente reactivos.

4.1 Roles, funciones y responsabilidades

Las decisiones en materia de ciberseguridad se adoptarán conforme al principio de responsabilidad compartida. La existencia de un área especializada no releva a las autoridades, propietarios de información, administradores de sistemas ni usuarios de sus deberes específicos.

Propietario de la información

Autoridad o responsable funcional que determina la finalidad del tratamiento, la sensibilidad de la información, los criterios de acceso y los requisitos de resguardo. Le corresponde clasificar la información; validar necesidades de disponibilidad, integridad, confidencialidad y trazabilidad; definir perfiles de acceso; y participar en la aceptación del riesgo residual.

Responsable del servicio

Área técnica o funcional a cargo de la operación de un servicio tecnológico. Asegura la prestación conforme a niveles acordados, implementa controles, documenta procedimientos y mantiene inventarios actualizados.

Responsable de Seguridad de la Información (RSI)

Designado formalmente por la autoridad competente. Impulsa la política institucional, coordina la gestión de riesgos, promueve controles y buenas prácticas, supervisa los programas de concientización, articula la respuesta frente a incidentes y actúa como referente institucional ante organismos externos. Hasta su

designación formal, sus funciones serán ejercidas transitoriamente por la autoridad o área que la máxima autoridad determine.

Responsables de sistemas y administradores técnicos

Desarrollan, configuran, operan y mantienen sistemas, aplicaciones, redes y componentes de infraestructura. Aplican los controles definidos, mantienen configuraciones seguras, registran cambios y actúan con criterios de mínimo privilegio, segregación de funciones y trazabilidad.

Responsable del área de Recursos Humanos

Incorpora las obligaciones de seguridad en los procesos de ingreso, permanencia y egreso. Asegura que las personas alcanzadas reciban información sobre sus deberes, instrumenta compromisos de confidencialidad y coordina con las áreas técnicas el retiro o modificación de accesos ante cambios de función o desvinculaciones.

Responsable del área legal o jurídica

Asesora sobre el encuadre normativo de las medidas de seguridad, los procesos disciplinarios, la protección de datos personales, los contratos con terceros, el tratamiento de evidencias y las comunicaciones ante incidentes, requerimientos judiciales o administrativos.

Oficial de Privacidad / Referente de Protección de Datos

La UNNE tratará datos personales de gran volumen y sensibilidad diversa (datos académicos, de salud, financieros, biométricos). Sin perjuicio de que la Ley 25.326 no imponga en todos los casos la designación formal de un Oficial de Privacidad, la Universidad designará un Referente de Protección de Datos (RPD), articulado funcionalmente con el RSI y el área legal, cuya misión será supervisar el cumplimiento de las obligaciones de privacidad, asesorar en el diseño de sistemas y procesos, y actuar como punto de contacto ante titulares de datos y organismos de control. La reglamentación del cargo, sus funciones específicas y la eventual adecuación a requisitos normativos futuros serán determinadas por resolución de la autoridad competente.

Usuarios de información y recursos tecnológicos

Toda persona que utilice recursos de la UNNE o acceda a información institucional debe conocer y cumplir esta normativa, actuar con diligencia en la custodia de credenciales, reportar eventos o debilidades, participar en las instancias de capacitación y abstenerse de usos indebidos o no autorizados.

4.2 Comité de Seguridad y cargos clave

La UNNE contará con un Comité de Seguridad de la Información y Ciberseguridad como ámbito de coordinación, priorización y seguimiento estratégico. El Comité deberá integrarse, como mínimo, por: un representante de la máxima autoridad universitaria; el RSI; la autoridad del área informática central; un representante del área económica o administrativa; un representante del área legal; un representante de recursos humanos; y un representante del área académica. Podrán incorporarse representantes de auditoría interna, protección de datos, unidades académicas e infraestructura según la temática lo requiera.

El Comité se reunirá con periodicidad definida por reglamentación interna y de manera extraordinaria ante incidentes, riesgos críticos o contingencias relevantes. Sus actuaciones quedarán registradas. Entre sus funciones: proponer políticas; revisar indicadores de seguridad (ver Sección 20); impulsar planes de tratamiento del riesgo; priorizar inversiones; validar lineamientos de continuidad; y tomar conocimiento de incidentes relevantes y lecciones aprendidas.

Las decisiones que impliquen asignación presupuestaria, aceptación de riesgos de alto impacto o cambios institucionales relevantes deberán elevarse a la autoridad competente para su aprobación.

5. Evaluación y tratamiento de riesgos

La gestión de riesgos constituye un proceso institucional continuo, documentado y repetible, orientado a identificar, analizar, evaluar, priorizar, tratar y monitorear los riesgos que puedan afectar la información, los servicios digitales, la infraestructura tecnológica y la continuidad de las actividades universitarias. La metodología institucional se apoya en ISO/IEC 27005, en el Modelo de Políticas de Seguridad de la Información del CIN y en los lineamientos operativos previstos en el Anexo 9 y el Procedimiento PE.DGITI.09.

5.1 Evaluación de riesgos

La evaluación deberá contemplar, como mínimo: identificación de activos; amenazas internas y externas; vulnerabilidades técnicas, organizativas, físicas y procedimentales; controles existentes; probabilidad de materialización; impacto sobre confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y cumplimiento normativo; y determinación del riesgo residual.

La evaluación se realizará con participación de los propietarios de la información, responsables de servicios, responsables de sistemas, administradores técnicos y áreas de apoyo pertinentes. Deberá ejecutarse en ciclo anual para los sistemas y servicios críticos, y de manera extraordinaria ante cambios significativos en infraestructura, arquitectura de sistemas, proveedores críticos, procesos sustantivos, requisitos legales, contexto de amenazas o ante la ocurrencia de incidentes graves.

La UNNE utilizará una matriz de riesgo 5x5 para establecer criterios formales de valoración y aceptación. El nivel de riesgo se determinará combinando probabilidad e impacto, y deberá quedar registrado junto con los controles existentes, controles propuestos, responsable, plazo de tratamiento y estado de seguimiento. Los controles periódicos asociados a la evaluación de riesgos incluirán, como mínimo: revisión anual integral de riesgos; revisión trimestral de privilegios especiales y cuentas inactivas en sistemas críticos; revisión semestral de accesos físicos a áreas protegidas; revisión semestral de inventarios y anexos críticos; y pruebas de restauración de copias de seguridad conforme la criticidad definida en el Anexo 11 y el Procedimiento PE.DGITI.04.

5.2 Tratamiento de riesgos

El tratamiento podrá consistir en evitar, reducir, transferir o aceptar el riesgo residual. Las medidas podrán comprender controles organizativos, técnicos, físicos, jurídicos, contractuales o de capacitación. En los casos en que el tratamiento no resulte inmediato, deberá justificarse la situación, establecerse medidas compensatorias, fijarse un plazo de regularización y registrar la decisión en el plan de tratamiento de riesgos.

Los riesgos altos y críticos deberán contar con plan de tratamiento formal. Dicho plan deberá incluir responsable, controles a implementar, plazo, recursos requeridos, indicadores de seguimiento y criterio de cierre. El RSI consolidará el estado de los riesgos relevantes y lo elevará periódicamente al Comité de Seguridad.

5.2.1 Autoridad de aprobación del riesgo residual

La aceptación del riesgo residual deberá ser aprobada por la autoridad competente con intervención del RSI y del propietario de la información o servicio afectado. La aceptación no podrá utilizarse para justificar el incumplimiento de una obligación legal expresa ni para convalidar una situación que vulnere derechos de terceros.

Los riesgos bajos y medios podrán ser aceptados por el propietario de la información o responsable del servicio, con intervención del RSI y registro documental de la justificación.

Los riesgos altos deberán ser revisados por el Comité de Seguridad de la Información y Ciberseguridad, el cual deberá aprobar el plan de tratamiento o documentar formalmente la aceptación fundada del riesgo residual.

Los riesgos críticos solo podrán ser aceptados mediante intervención de la máxima autoridad competente, Rectorado o Consejo Superior según corresponda, dejando constancia de las razones técnicas, económicas, operativas o institucionales que impiden su mitigación inmediata, las medidas compensatorias adoptadas y la fecha obligatoria de próxima revisión.

6. Política de seguridad de la información

La política de seguridad de la información constituye la declaración marco de principios, objetivos y obligaciones de la UNNE. Debe ser aprobada por la autoridad competente, difundida a toda la comunidad universitaria y revisada periódicamente.

6.1 Documento de la política

El documento de política deberá redactarse en términos claros, sin contradicciones internas, con definiciones mínimas y remisión ordenada a anexos y procedimientos operativos. La versión vigente indicará responsable de custodia, fecha de aprobación, fecha de revisión, control de cambios y autoridades de aplicación. La difusión institucional garantizará que las personas alcanzadas puedan conocerla y acceder a los documentos que correspondan a su rol.

La presente normativa distingue entre requisitos de cumplimiento inmediato desde su vigencia que incluyen obligaciones organizativas, clasificación de información, controles ya operativos, y entre objetivos de madurez progresiva cuya adopción se planificará mediante cronogramas de implementación y revisión del RSI, sin que su falta de cumplimiento total en la fecha de entrada en vigencia implique incumplimiento normativo, siempre que exista un plan documentado con aceptación formal y responsable asignado.

6.2 Revisión de la política

La revisión integral deberá realizarse al menos una vez cada doce meses o ante incidentes relevantes, cambios significativos en el contexto de amenazas, actualizaciones normativas de impacto, modificaciones sustantivas en la arquitectura tecnológica o redefinición de procesos estratégicos. La revisión verificará consistencia interna, grado de implementación, claridad de responsabilidades, necesidad de nuevos controles y lecciones derivadas de auditorías, ejercicios o incidentes.

7. Organización

La organización de la seguridad asegurará independencia funcional suficiente para el control, capacidad de coordinación transversal y cercanía operativa. Las funciones críticas se distribuirán de modo que ninguna persona concentre sin control la definición, implementación y verificación de un mismo control cuando ello genere riesgos significativos.

7.1 Organización interna

Comprende la definición de responsabilidades, coordinación entre áreas, aprobación de medidas, segregación de funciones y canales para escalar riesgos, incidentes, excepciones y necesidades de mejora.

7.1.1 Compromiso de la dirección. La conducción universitaria manifestará su apoyo explícito a la política de seguridad, asignará responsabilidades, impulsará un programa sostenido de mejora, promoverá recursos razonables y requerirá información periódica sobre el estado de situación. El compromiso deberá traducirse en decisiones, prioridades y prácticas de gestión.

7.1.2 Coordinación. Se canalizará a través del RSI y del Comité de Seguridad, asegurando la participación de las áreas relevantes. Deberán existir procedimientos claros para consultas, aprobaciones, gestión de

excepciones y seguimiento de hallazgos. La coordinación contemplará la relación con unidades académicas y ámbitos descentralizados.

7.1.3 Asignación de responsabilidades. Las responsabilidades estarán expresamente asignadas y comunicadas. Toda actividad relevante en materia de seguridad contará con responsable primario, responsable de apoyo y mecanismo de trazabilidad. La asignación quedará reflejada en documentos de funciones, manuales, actos administrativos o instructivos.

7.1.4 Autorización para instalaciones de procesamiento. La instalación, ampliación, relocalización o habilitación de entornos de procesamiento de información requerirá autorización formal y revisión técnica, contemplando requisitos de energía, climatización, protección física, conectividad, respaldo, monitoreo, inventario y seguridad lógica. Para entornos en la nube, se aplicarán adicionalmente los controles del Anexo 12.

7.1.5 Acuerdos de confidencialidad. Todas las personas con acceso a información institucional de carácter confidencial o reservado suscribirán compromisos de confidencialidad apropiados a sus funciones y a la naturaleza de la información a la que acceden. Los compromisos deberán sobrevivir a la extinción del vínculo laboral, contractual o académico.

7.1.6 Contacto con otros organismos. La UNNE mantendrá canales de comunicación con organismos nacionales competentes en ciberseguridad, en particular el Centro Nacional de Ciberseguridad (Decreto N° 941/2025) y el CERT.ar (Equipo de Respuesta ante Emergencias Informáticas, actuante bajo su conducción), así como con la Agencia de Acceso a la Información Pública en materia de protección de datos personales, con el CIN y con sus pares en la comunidad universitaria, para intercambio de información sobre amenazas, incidentes, vulnerabilidades y buenas prácticas. Como fuentes técnicas de consulta extranjeras o internacionales podrán considerarse, entre otras, las guías CCN-STIC del Centro Criptológico Nacional de España y las publicaciones del Instituto Nacional de Ciberseguridad (INCIBE) de España, sin que ello implique atribuirles competencia o fuerza normativa en la República Argentina.

7.1.7 Contacto con grupos de interés especial. Se promoverá la participación activa en redes de cooperación técnica, grupos de trabajo en ciberseguridad para el sector universitario y comunidades de práctica que contribuyan a la mejora continua de las capacidades institucionales.

7.1.8 Revisión independiente. La UNNE realizará revisiones independientes de la seguridad de la información mediante auditorías internas, externas o revisiones técnicas controladas, al menos con periodicidad bienal o ante cambios significativos. Los hallazgos se incorporarán al proceso de mejora continua.

7.2 Dispositivos móviles y trabajo remoto

7.2.1 Dispositivos móviles. El uso de dispositivos móviles para acceder a información institucional deberá sujetarse a políticas de gestión de dispositivos (MDM cuando aplique), cifrado, bloqueo por inactividad, reporte de pérdida o robo y revocación remota de accesos. Se desaconsejará el almacenamiento de información confidencial o reservada en dispositivos no gestionados institucionalmente.

7.2.2 Trabajo remoto. El acceso remoto a sistemas institucionales deberá realizarse mediante canales seguros (VPN corporativa, MFA), en dispositivos que cumplan los requisitos mínimos de seguridad definidos por la DGITI. Los trabajadores remotos deberán cumplir la misma normativa aplicable al trabajo presencial.

8. Recursos humanos

8.1 Antes del empleo

8.1.1 Funciones y responsabilidades. Las funciones y responsabilidades de seguridad se definirán antes del empleo, incluyendo las obligaciones del cargo, el nivel de acceso previsto y los compromisos de confidencialidad aplicables.

8.1.2 Verificación de idoneidad. Se realizará la verificación de la información curricular y de los requisitos de idoneidad exigidos por la normativa de ingreso aplicable al personal docente y no docente (Estatuto Universitario, convenios colectivos y ordenanzas de concursos), con el alcance que dicha normativa determine. Esta normativa no crea ni habilita investigaciones de antecedentes penales u otras indagaciones no previstas en el marco legal de ingreso aplicable; el tratamiento de datos relativos a antecedentes penales está reservado por el artículo 7°, inciso 4), de la Ley 25.326 a las autoridades públicas competentes.

8.1.3 Términos y condiciones de contratación. Los términos de contratación reflejarán las obligaciones de seguridad de la información, incluyendo la política de uso aceptable de activos (Anexo 5) y el deber de reportar incidentes.

8.2 Durante el empleo

8.2.1 Responsabilidad de la dirección. La conducción deberá asegurar que el personal conozca y cumpla la política y que existan canales accesibles para consultas, reportes y gestión de excepciones.

8.2.2 Concientización, formación y capacitación. La UNNE mantendrá un programa institucional sostenido de concientización y capacitación en seguridad de la información, estructurado por públicos objetivo, con contenidos diferenciados para usuarios generales, personal técnico, administradores y autoridades. El programa incluirá, como mínimo, formación anual obligatoria, inducción para nuevos ingresos, y simulacros periódicos de ingeniería social y phishing. El Procedimiento PE.DGITI.07 establece el marco operativo del programa.

8.2.3 Proceso disciplinario. Los incumplimientos de esta normativa serán tratados mediante los procedimientos disciplinarios aplicables, proporcionales a la gravedad, intencionalidad y daño causado. El proceso disciplinario no interrumpirá la respuesta técnica al incidente ni la preservación de evidencia.

8.3 Cese del empleo o cambio de puesto

8.3.1 Responsabilidad del cese o cambio. El área de Recursos Humanos notificará con anticipación razonable a la DGITI ante cese, desvinculación, cambio de función o inicio de licencia especial. Para situaciones urgentes (causa disciplinaria, incidente), la notificación será inmediata.

8.3.2 Devolución de activos. Al cese, el personal devolverá todos los activos institucionales a su cargo: equipos, credenciales físicas, documentos, tokens, tarjetas de acceso y cualquier otro recurso entregado.

8.3.3 Retiro de derechos de acceso. Los accesos a sistemas críticos se revocarán el mismo día hábil del cese o notificación de baja. Los accesos a sistemas de menor criticidad, en el plazo máximo definido en el Procedimiento PE.DGITI.01. La revocación incluirá correo institucional, VPN, sistemas académicos y administrativos, repositorios y credenciales de nube.

9. Gestión de activos

9.1 Responsabilidad sobre los activos

Todo activo de información deberá contar con un propietario funcional identificado, responsable de su clasificación, de la definición de los criterios de acceso y de la participación en la evaluación de riesgos. Los activos sin propietario identificado representan una brecha de gobernanza inadmisibles. El inventario institucional se gestionará conforme al Procedimiento PE.DGITI.06 y al Anexo 11.

9.2 Clasificación de la información

La información se clasificará en cuatro niveles: Pública, Interna, Confidencial y Reservada. La clasificación determinará los controles de acceso, almacenamiento, transmisión, reproducción y eliminación aplicables. El Procedimiento PE.DGITI.06 y el Anexo 5 desarrollan los criterios de cada nivel y las conductas asociadas.

9.3 Manejo de soportes y activos

Los activos deberán gestionarse conforme a su clasificación durante todo su ciclo de vida: creación, uso, almacenamiento, transmisión y eliminación. La eliminación de activos de información deberá garantizar la irrecuperabilidad de la información sensible, mediante técnicas apropiadas al soporte (borrado seguro, destrucción física certificada, desmagnetización).

10. Control de acceso

El control de accesos se regirá por los principios de identificación individual, mínimo privilegio, necesidad de saber, segregación de funciones, trazabilidad, revisión periódica y revocación oportuna. El Procedimiento PE.DGITI.01 y el Anexo 1 establecen el marco operativo detallado.

10.1 Requerimientos para la gestión de acceso

Deberá existir una política formal de control de acceso, comunicada a todas las personas con acceso a sistemas institucionales, que establezca los criterios de otorgamiento, modificación, revisión y revocación de accesos, y los principios de mínimo privilegio y segregación de funciones.

10.2 Gestión de acceso de usuarios

Las altas de acceso responderán a necesidades funcionales comprobables, con solicitud formal y aprobación del responsable competente. Todo cambio de rol o función motivará una revisión y adecuación de accesos. Las bajas se ejecutarán conforme a los plazos del PE.DGITI.01. Las cuentas privilegiadas serán nominativas, protegidas con controles reforzados y sujetas a registro de actividad.

10.3 Gestión de acceso a redes

El acceso a las redes institucionales estará controlado mediante segmentación, autenticación, listas de control de acceso y monitoreo de tráfico. Los usuarios remotos accederán mediante VPN institucional con autenticación multifactor. Las redes inalámbricas institucionales contarán con autenticación 802.1X o equivalente.

10.4 Control de acceso al sistema operativo

Los sistemas operativos de servidores y puestos de trabajo aplicarán configuraciones de hardening, autenticación obligatoria, bloqueo por inactividad y registro de accesos. Las cuentas de administración local serán gestionadas de manera centralizada y rotadas periódicamente.

10.5 Control de acceso a la información y aplicaciones

El acceso a sistemas de información y aplicaciones estará basado en roles (RBAC) o perfiles predefinidos. La autenticación multifactor se implementará progresivamente para todos los sistemas críticos identificados en el Anexo 11, comenzando por los de mayor exposición.

10.6 Computación móvil y teletrabajo

El acceso desde dispositivos móviles o en modalidad de teletrabajo deberá cumplir los requisitos de la sección 7.2 y del Anexo 1. Los dispositivos no gestionados institucionalmente no deberán almacenar información clasificada como Confidencial o Reservada.

11. Criptografía

La criptografía es una herramienta fundamental para garantizar la confidencialidad, integridad y autenticidad de la información en tránsito y en reposo. Su implementación deberá respetar la legislación vigente (Ley 25.506 y normativa complementaria), los estándares técnicos reconocidos y las definiciones institucionales sobre administración de claves.

11.1 Política de uso de controles criptográficos

La UNNE establecerá criterios mínimos para el uso de criptografía, que incluirán:

- Cifrado en tránsito: toda comunicación de información Confidencial o Reservada a través de redes públicas o semipúblicas deberá utilizar protocolos seguros (TLS 1.2 o superior, SSH, SFTP). Se evitará el uso de protocolos sin cifrado (HTTP, FTP, Telnet) para sistemas en producción que manejen información institucional.
- Cifrado en reposo: las bases de datos con datos personales sensibles, información académica confidencial y credenciales deberán cifrarse en reposo con estándar AES-256 o equivalente. Los respaldos de sistemas críticos deberán cifrarse conforme al Anexo 2.
- Algoritmos: se utilizarán únicamente algoritmos reconocidos como seguros por estándares actuales (AES, RSA $\geq$ 2048 bits, ECDSA, SHA-256 o superiores). Se evitará el uso de algoritmos obsoletos o deprecados (MD5, SHA-1, DES, RC4).
- Firma digital: la implementación de firma digital se articulará con las disposiciones de la Ley 25.506 y la infraestructura de clave pública (PKI) vigente o disponible para el sector universitario.

11.2 Gestión de claves

La gestión del ciclo de vida de claves criptográficas y certificados digitales contemplará: generación segura, distribución, almacenamiento protegido, rotación periódica, revocación y destrucción. El Anexo 13 establece los lineamientos operativos para la PKI institucional, los certificados de servidor, los certificados de usuario y la gestión de secretos en entornos de desarrollo y producción.

11 bis. Ciberseguridad en la nube

La adopción de servicios de computación en la nube por parte de la UNNE deberá estar precedida de una evaluación de seguridad documentada conforme al Procedimiento PE.DGITI.05, y deberá contemplar el modelo de responsabilidad compartida como principio rector: el proveedor cloud es responsable de la seguridad de la infraestructura; la UNNE es responsable de la seguridad de los datos, configuraciones, identidades y accesos que opera sobre esa infraestructura.

11 bis.1 Criterios de adopción de servicios cloud

Antes de adoptar un servicio cloud que involucre información institucional, la DGITI y el RSI evaluarán: clasificación de la información a tratar; residencia y localización de los datos; portabilidad y reversibilidad; garantías de disponibilidad (SLA); capacidades de auditoría y registro; modalidad de acceso y controles de identidad; cumplimiento normativo del proveedor (ley de protección de datos aplicable); y derechos de auditoría contratables.

11 bis.2 Gestión de identidades en la nube

El acceso a servicios cloud institucionales deberá integrarse, en la medida de lo técnicamente posible, con el directorio central de identidades de la UNNE, habilitando SSO mediante protocolos estándar (SAML 2.0, OIDC). Se evitará la proliferación de cuentas cloud desconectadas del ciclo de vida de identidades institucional. La autenticación multifactor será obligatoria para accesos de administración cloud.

11 bis.3 Configuración segura y postura de seguridad

Los servicios cloud se configurarán conforme a los lineamientos de seguridad del proveedor (CIS Benchmarks, Security Best Practices) y revisados periódicamente mediante herramientas de Cloud Security Posture Management (CSPM) cuando corresponda. Los recursos cloud sin uso o abandonados serán inventariados y eliminados periódicamente.

12. Seguridad física y ambiental

12.1 Áreas seguras

Las instalaciones que alberguen infraestructura de procesamiento de información crítica contarán con controles de acceso físico proporcionales a su criticidad: identificación y registro de accesos, control de visitas, protección perimetral, vigilancia y procedimientos de acceso de emergencia. El acceso a salas de servidores y centros de datos estará restringido a personal autorizado.

12.2 Seguridad de los equipos

Los equipos de procesamiento de información estarán protegidos contra amenazas físicas y ambientales: energía redundante (UPS), climatización controlada, protección contra incendio, monitoreo ambiental y

mantenimiento preventivo documentado. El traslado, baja y reutilización de equipos seguirá procedimientos que garanticen la irrecuperabilidad de la información almacenada.

13. Seguridad en las operaciones

13.1 Procedimientos operativos y responsabilidades

Los procedimientos operativos de administración de sistemas, configuración, puesta en marcha y baja de servicios estarán documentados, actualizados y disponibles para el personal autorizado. Los cambios en entornos de producción seguirán el Procedimiento PE.DGITI.08 (gestión de cambios).

13.2 Protección contra código malicioso

Todos los sistemas de usuario final y servidores de propósito general contarán con protección contra malware activa, actualizada y con capacidad de detección y respuesta (EDR preferentemente sobre antivirus tradicional). Las actualizaciones de firmas y motores serán automáticas. Se implementarán controles adicionales de filtrado de correo electrónico y navegación web para reducir la superficie de ataque de phishing y malware.

13.3 Resguardo de la información

La estrategia de respaldos se define en el Anexo 2, los lineamientos de software en el Anexo 8 y los lineamientos para máquinas virtuales críticas en el Anexo 10. El Procedimiento PE.DGITI.04 establece el proceso operativo de gestión de respaldos y pruebas de restauración, incluyendo frecuencias mínimas, verificación de integridad y documentación de resultados.

13.4 Registro y monitoreo de actividad

Los sistemas críticos generarán registros de actividad (logs) de autenticación, accesos, cambios de configuración, errores y eventos de seguridad. Los registros deberán conservarse por un período mínimo definido por el RSI (mínimo 90 días en línea, 12 meses en archivo). Se implementará monitoreo activo de los sistemas más expuestos, con revisión periódica de alertas y correlación de eventos cuando la capacidad tecnológica lo permita.

13.5 Gestión de vulnerabilidades técnicas

La gestión de vulnerabilidades técnicas se llevará a cabo conforme al Procedimiento PE.DGITI.03 y al Anexo 7. Los plazos de remediación serán proporcionales a la severidad y criticidad del activo: vulnerabilidades críticas en sistemas expuestos serán atendidas en un plazo máximo de 48 horas desde su identificación o publicación con exploit activo conocido. En sistemas cuya remediación dependa de terceros (fabricante, ecosistema SIU u otro proveedor), el plazo se contará desde la disponibilidad del parche o mitigación oficial publicada por el tercero; mientras tanto, la UNNE aplicará controles compensatorios documentados y registrará el seguimiento ante dicho proveedor.

14. Gestión de las comunicaciones

14.1 Gestión de la red

La infraestructura de red de la UNNE estará segmentada para separar entornos de distinta criticidad y sensibilidad (gestión, producción, desarrollo, estudiantes, investigación, visitantes). Los dispositivos de red contarán con configuraciones de hardening documentadas, contraseñas seguras, firmware actualizado y acceso de administración restringido. El tráfico de red será monitoreado para detectar anomalías.

14.2 Transferencia de información

La transferencia de información Confidencial o Reservada con terceros deberá realizarse mediante canales seguros y cifrados. Los acuerdos de transferencia de información con terceros establecerán las responsabilidades de cada parte respecto de la protección, uso y eliminación de la información transferida. Se evitará el uso de servicios de almacenamiento o transferencia en la nube no autorizados institucionalmente para información clasificada.

15. Adquisición, desarrollo y mantenimiento de sistemas

15.1 Requerimientos de seguridad

Los requerimientos de seguridad deberán definirse en las etapas iniciales de adquisición o desarrollo de sistemas, incluyendo autenticación, autorización, cifrado, registro de auditoría, validación de entradas, gestión de sesiones y manejo seguro de errores.

15.2 Seguridad en los sistemas de aplicación

Los sistemas de aplicación deberán validar todas las entradas, gestionar errores sin revelar información sensible, proteger la integridad de la información procesada, implementar controles de sesión seguros y

registrar actividad de seguridad relevante. El desarrollo seguirá buenas prácticas reconocidas (OWASP Top 10, CWE/SANS Top 25).

15.3 Seguridad en el desarrollo y soporte

Los ambientes de desarrollo y pruebas estarán segregados de producción. Los datos de producción no deberán utilizarse en ambientes de prueba sin anonimización adecuada. Los repositorios de código fuente estarán protegidos y no contendrán secretos, claves o credenciales embebidos. Los pipelines de integración continua integrarán controles de seguridad automatizados (análisis estático, revisión de dependencias).

15.4 Gestión de vulnerabilidades en desarrollo

Las vulnerabilidades detectadas en sistemas desarrollados internamente o customizados serán gestionadas con la misma priorización que las vulnerabilidades en productos de terceros, conforme al Procedimiento PE.DGITI.03. Los parches de seguridad sobre plataformas SIU u otras bases institucionales

se aplicarán en las ventanas de mantenimiento aprobadas, dentro de los 5 días hábiles posteriores a la publicación del parche oficial, salvo exploit activo que justifique ventana excepcional.

16. Relaciones con proveedores

Los contratos con proveedores que accedan a información institucional o administren componentes de la infraestructura de la UNNE incluirán requisitos mínimos de seguridad conforme al Anexo 4 y al Procedimiento PE.DGITI.05. La evaluación de seguridad de proveedores es un requisito previo a la contratación.

16.1 Seguridad en las relaciones con proveedores

Los contratos incluirán, como mínimo: deber de confidencialidad; obligación de notificación de incidentes en ≤ 24 hs; cumplimiento de la Ley 25.326; controles de acceso de mínimo privilegio; restricción de subcontratación sin autorización; derechos de auditoría; RTO/SLA acordados; y procedimiento de devolución o eliminación certificada de información al cierre.

16.2 Administración de prestación de servicios de proveedores

El desempeño de los proveedores será monitoreado conforme a los SLA acordados. Los accesos otorgados a proveedores serán temporales o renovables, limitados al alcance contractual, y revocados inmediatamente al finalizar el vínculo. Los cambios significativos en la prestación o subcontratación serán informados y evaluados antes de su implementación.

17. Gestión de incidentes de seguridad

La gestión de incidentes comprende un ciclo completo desde la preparación hasta las lecciones aprendidas. El Procedimiento PE.DGITI.02 y el Anexo 6 establecen el proceso operativo detallado.

17.1 Reporte de eventos y debilidades

17.1.1 Reporte de eventos. Todo evento de seguridad observado deberá reportarse al canal designado (mesa de ayuda / RSI) sin demora, independientemente de si el usuario considera que constituye o no un incidente. El reporte temprano es clave para la detección y contención.

17.1.2 Reporte de debilidades. Las debilidades en controles, configuraciones, procedimientos o comportamiento de usuarios deberán reportarse aun sin evidencia de incidente consumado. El reporte de debilidades permite la acción preventiva.

17.1.3 Anomalías de software. Los errores, comportamientos inesperados o fallas recurrentes con posible impacto en seguridad deberán documentarse y escalar. Ante posibilidad de vulnerabilidad o explotación, la evaluación se priorizará con intervención de las áreas técnicas y de seguridad.

17.2 Gestión de incidentes y mejoras

17.2.1 Responsabilidades y procedimientos. El procedimiento de respuesta definirá roles de las áreas técnicas, funcionales, legales y de comunicación. Contemplará criterios de escalamiento, severidades, tiempos de atención, supuestos de activación del Comité de Seguridad, interacción con proveedores, criterios de aislamiento y reglas para la toma y resguardo de evidencia digital.

17.2.2 Aprendizaje de los incidentes. Todo incidente relevante generará una revisión posterior de causa raíz, factores contribuyentes, oportunidades de mejora, necesidades de ajuste normativo o técnico y acciones de capacitación. Las conclusiones se traducirán en planes verificables.

17.2.3 Procesos disciplinarios. Cuando el incidente se vincule con incumplimientos, usos indebidos o conductas intencionales, se dará intervención a las áreas competentes para evaluar las medidas disciplinarias, administrativas o judiciales que correspondan, sin afectar la continuidad de la respuesta técnica ni la preservación de evidencia.

18. Gestión de la continuidad

La UNNE integrará la seguridad de la información con la gestión de continuidad, contingencia y recuperación ante desastres, de modo que los servicios críticos puedan sostenerse, degradarse de manera controlada o restablecerse dentro de parámetros aceptables frente a interrupciones graves, incidentes de ciberseguridad, fallas de infraestructura, indisponibilidad de proveedores, eventos físicos o desastres que afecten la operación universitaria.

La gestión de continuidad se referencia en ISO 22301:2019, ISO/IEC 27031, NIST SP 800-34, NIST SP 800-184 y en los lineamientos técnicos nacionales aplicables. Su desarrollo operativo se documenta en el Procedimiento PE.DGITI.10 y en los Anexos 2, 10, 11 y 16, que deberán interpretarse de manera integrada.

18.1 Política de planes de contingencia

La UNNE contará con una Política de Planes de Contingencia que defina propósito, alcance, roles, responsabilidades, coordinación entre áreas, mecanismos de actualización periódica y actualización reactiva ante eventos relevantes. Esta política se desarrolla en el Anexo 16 y deberá ser revisada, como mínimo, una vez al año o ante cambios significativos en sistemas críticos, arquitectura tecnológica, dependencias, proveedores, riesgos o normativa aplicable.

18.2 Inventario, criticidad y análisis de impacto

Todo plan de continuidad partirá del inventario institucional de sistemas críticos. Dicho inventario deberá identificar, para cada sistema o servicio, propietario funcional, responsable técnico, funcionalidades, dependencias de aplicaciones, datos, infraestructura, comunicaciones y proveedores, dimensiones de impacto, nivel de criticidad, RTO, RPO, orden de recuperación y recursos mínimos requeridos. La estructura del inventario se establece en el Anexo 11 y se complementa con el Anexo 16.

El Análisis de Impacto al Negocio o al Servicio (BIA) determinará las consecuencias de una interrupción prolongada y fijará parámetros de recuperación. Como mínimo, deberá considerar impacto sobre seguridad de las personas, continuidad de servicios universitarios, impacto económico u operativo, cumplimiento legal o regulatorio, reputación institucional, protección de datos, docencia, investigación, extensión y gestión administrativa.

18.3 Planes de continuidad y recuperación

Los planes de continuidad, contingencia y recuperación ante desastres deberán contener procedimientos concretos de activación, conmutación, recuperación, operación degradada, retorno a la normalidad, roles de decisión, contactos de emergencia, bitácora de eventos, medidas de seguridad durante la recuperación, criterios de validación y evidencias de cierre. Para los servicios críticos, estos planes deberán adoptar el formato mínimo definido en el Anexo 16 y ejecutarse conforme al PE.DGITI.10.

18.4 Estrategia de respaldo, recuperación y sitio alternativo

La estrategia de respaldo y recuperación deberá estar alineada con la criticidad del sistema, sus RTO y RPO, el orden de recuperación institucional y la disponibilidad de infraestructura alterna. Los respaldos se rigen por el Anexo 2 y el PE.DGITI.04; las máquinas virtuales críticas por el Anexo 10; y los requerimientos de centro de procesamiento de datos de respaldo por el Anexo 16.

18.5 Ensayos, mantenimiento y mejora continua

Los planes deberán ser probados de manera periódica mediante simulacros de mesa, pruebas técnicas parciales, pruebas de restauración, ejercicios de conmutación y pruebas integrales, según la criticidad del servicio. Toda prueba generará informe de resultados, métricas, desvíos, acciones correctivas, responsables y plazos. Las fallas detectadas deberán incorporarse al plan de tratamiento de riesgos y al ciclo de mejora continua.

19. Cumplimiento

La Universidad asegurará que sus controles, procesos y decisiones en materia de seguridad se mantengan compatibles con el marco normativo aplicable, con los compromisos contractuales asumidos y con sus propias políticas y procedimientos internos.

19.1 Cumplimiento de requisitos legales

19.1.1 Legislación aplicable. La Universidad mantendrá un repertorio razonablemente actualizado de normativa aplicable, incluyendo protección de datos personales, delitos informáticos, firma digital, acceso a la información pública, propiedad intelectual, conservación documental, procedimientos administrativos, control interno, contrataciones y relaciones laborales. Las normas nacionales de aplicación específica sobre organismos del PEN se utilizarán como referencia técnica orientadora en la medida en que resulten compatibles con la autonomía universitaria, sin presentarlas como obligaciones directas cuando su alcance jurídico no así lo determine.

En tal sentido, integran el bloque de aplicación directa y obligatoria las Leyes N° 25.326, 26.388, 25.506, 27.275 y 11.723, entre otras de igual carácter. Operan, en cambio, como referencia técnica orientadora -incorporada por decisión propia del órgano de gobierno universitario- la Decisión Administrativa N° 641/2021, las Disposiciones del Centro Nacional de Ciberseguridad N° 1/2022, N° 1/2026 y N° 3/2023, y la Resolución CIN CE N° 1669/22, en la medida en que resulten compatibles con la autonomía universitaria.

19.1.2 Propiedad intelectual. La Universidad garantizará el respeto de licencias, derechos de autor, restricciones de uso y condiciones contractuales aplicables a software, bases de datos, contenidos y demás activos protegidos. Solo se instalarán, utilizarán o distribuirán elementos para los cuales exista autorización suficiente.

19.1.3 Protección de registros. Los registros institucionales se preservarán contra pérdida, alteración, destrucción no autorizada o falsificación. Existirán criterios de retención, archivo, acceso, disponibilidad y eliminación compatibles con su valor administrativo, académico, probatorio, legal o histórico.

19.1.4 Protección de datos personales. El tratamiento de datos personales se realizará de conformidad con la Ley 25.326 y normativa complementaria, respetando principios de licitud, finalidad, proporcionalidad, calidad, seguridad, confidencialidad y ejercicio de derechos. El Referente de Protección de Datos colaborará con las áreas responsables para asegurar el cumplimiento de estas obligaciones.

19.1.5 Uso inadecuado de recursos. Los recursos tecnológicos institucionales deberán utilizarse prioritariamente para fines académicos, científicos, administrativos, de extensión y demás finalidades compatibles con la misión universitaria. El uso abusivo, contrario a derecho, riesgoso o incompatible con las políticas vigentes podrá ser restringido y sancionado.

19.1.6 Criptografía y firma digital. La implementación de criptografía y firma digital respetará la legislación vigente (Ley 25.506), los estándares aceptados y las definiciones institucionales sobre administración de claves y certificación. Se evitarán referencias obsoletas o no pertinentes.

19.1.7 Recolección de evidencia. La recolección, preservación, custodia y presentación de evidencia digital deberá realizarse de modo que preserve integridad, trazabilidad, autenticidad y valor probatorio, limitándose al personal autorizado.

19.1.8 Delitos informáticos. La Universidad promoverá el conocimiento básico de las conductas tipificadas como delitos informáticos (Ley 26.388) y de sus consecuencias jurídicas.

19.2 Revisiones de compatibilidad técnica

19.2.1 Cumplimiento de la política. Cada responsable de unidad organizativa velará por la implementación efectiva de los controles que le correspondan y colaborará en las revisiones que disponga el RSI, el Comité o auditoría interna.

19.2.2 Verificación técnica. La verificación podrá comprender revisiones de configuración, pruebas controladas, análisis de registros, escaneos, revisiones de código o pruebas de penetración autorizadas, realizadas por personal competente, con alcance definido y autorización previa.

19.3 Auditorías de sistemas

19.3.1 Controles de auditoría. Las actividades de auditoría sobre sistemas de información se planificarán para maximizar eficacia y reducir interferencias operativas, preservando la integridad de los entornos auditados. El acceso a información o ambientes de producción se limitará a lo estrictamente necesario.

19.3.2 Protección de herramientas de auditoría. Las herramientas, datos, scripts y repositorios utilizados en auditorías se resguardarán adecuadamente para evitar uso indebido o afectación de entornos productivos.

19.3.3 Sanciones por incumplimiento. Las sanciones por incumplimiento se sustanciarán conforme al ordenamiento jurídico aplicable, con observancia de competencia, procedimiento y debido proceso. La responsabilidad disciplinaria no excluye otras responsabilidades que pudieran corresponder.

Respecto de quienes no revisten la calidad de agentes de la Universidad -estudiantes, becarios, extensionistas, pasantes y usuarios eventuales-, y en tanto la Universidad no cuenta con un régimen disciplinario que les resulte aplicable, las consecuencias del incumplimiento de esta normativa se limitan a las medidas de gestión de acceso en ella previstas -suspensión, restricción o revocación de credenciales-, adoptadas por el área competente mediante acto fundado y notificado, susceptible de los recursos administrativos previstos en el ordenamiento, y sin perjuicio de las acciones civiles o penales que pudieran corresponder. Ninguna disposición de esta normativa podrá interpretarse como creación de un régimen disciplinario estudiantil.

20. Métricas e indicadores de seguridad

La UNNE establecerá y mantendrá un conjunto de indicadores clave de desempeño (KPIs) y de riesgo (KRIs) en materia de seguridad de la información, que permitan evaluar objetivamente el grado de implementación de los controles, la evolución del perfil de riesgo y la efectividad de los programas de mejora.

20.1 Indicadores de gestión operativa

Indicador	Meta mínima	Frecuencia de reporte
% de sistemas críticos con respaldo exitoso en el período	>= 95 %	Mensual
Tiempo medio de revocación de accesos ante baja	<= 1 día hábil en sistemas críticos	Mensual
Vulnerabilidades críticas sin remediación en plazo	0	Mensual
% de incidentes con informe post-incidente	100 % (niveles 2-4)	Mensual
% de personal con capacitación anual completada	>= 80 % anual; 100 % para administradores de sistemas críticos	Anual
Tasa de clics en simulacros de phishing	Tendencia decreciente; objetivo <= 10 %	Por simulacro
Riesgos altos/críticos con plan de tratamiento activo	100 %	Trimestral
Pruebas de restauración realizadas según plan	100 %	Trimestral
Cambios en producción con RFC documentado	100 %	Mensual
% de proveedores con dictamen RSI previo a contratación	100 %	Por contratación

20.2 Reporte al Comité de Seguridad

El RSI presentará al Comité de Seguridad un informe trimestral de seguridad que incluirá: estado de los indicadores operativos; evolución del perfil de riesgo institucional; resumen de incidentes y tendencias; estado de los planes de tratamiento de riesgos; y propuestas de mejora para el período siguiente. El informe anual será elevado a la autoridad universitaria competente.

Anexo 1

Política de control de accesos e identidades

Referencia normativa

Sección 10 / Procedimiento PE.DGITI.01 / ISO 27002:2022 A.5.15-5.18

- 1. Objeto.** Establecer criterios mínimos para la administración del ciclo de vida de los accesos a sistemas, redes, aplicaciones, bases de datos y demás recursos tecnológicos de la UNNE, asegurando que el acceso se otorgue, mantenga y retire de manera controlada y trazable.
- 2. Principios.** El control de accesos se regirá por: identificación individual; mínimo privilegio; necesidad de saber; segregación de funciones; trazabilidad; revisión periódica; revocación oportuna; y autenticación multifactor progresiva para sistemas críticos.
- 3. Altas.** Toda alta de acceso responderá a una necesidad funcional comprobable, con solicitud formal (FORM-ACC-001) y aprobación del responsable competente. Las cuentas se vincularán a una persona identificable. No se crearán cuentas genéricas o duplicadas.
- 4. Modificaciones.** Todo cambio de rol, dependencia, función o nivel de responsabilidad motivará una revisión y adecuación de accesos. La reasignación incluirá eliminación de permisos que hayan dejado de ser necesarios.
- 5. Bajas.** Los accesos a sistemas críticos se revocarán el mismo día hábil de la notificación de cese. Los accesos de menor criticidad, en un máximo de 2 días hábiles. No se reutilizarán nombres de usuario de personas desvinculadas.
- 6. Cuentas privilegiadas.** Las cuentas administrativas serán limitadas, nominativas, protegidas con controles reforzados (MFA obligatorio), sujetas a revisión periódica y con registro de actividad. Las elevaciones temporales de privilegio se justificarán y documentarán.
- 7. Contraseñas y autenticación.** Las credenciales se gestionarán conforme a criterios de complejidad, confidencialidad, no reutilización y cambio ante sospecha de compromiso. La autenticación multifactor se adoptará progresivamente para todos los sistemas críticos, comenzando por los de mayor exposición.
- 8. Revisiones periódicas.** Los responsables funcionales y técnicos revisarán trimestralmente los accesos sobre sistemas críticos, dejando evidencia documentada. Los accesos sin uso prolongado serán investigados y revocados si no se justifican.
- 9. Accesos de terceros.** Los accesos a proveedores serán temporales, limitados al alcance contractual, monitoreados en la medida posible y revocados al finalizar la necesidad operativa. Ver Anexo 4 y PE.DGITI.05.
- 10. Excepciones.** Toda excepción se fundará, aprobará por la autoridad competente y contará con medidas compensatorias documentadas.

Anexo 2

Política de respaldos

- 1. Objeto.** Establecer criterios para la realización, protección, verificación y restauración de copias de seguridad de información y sistemas institucionales, asegurando su alineación con los objetivos de recuperación definidos para cada sistema o servicio.
- 2. Alcance.** Bases de datos, archivos, máquinas virtuales, configuraciones de red, sistemas operativos, servicios críticos, documentación, repositorios, plataformas de identidad, aplicaciones institucionales y demás activos definidos por los responsables de sistemas, propietarios funcionales y el RSI.

3. Relación con RTO y RPO. Todo respaldo deberá responder a un RPO documentado y toda estrategia de restauración deberá ser consistente con el RTO del sistema o servicio. Los valores de RTO y RPO se registrarán en el Anexo 11 y se utilizarán para definir frecuencia, retención, ubicación, tipo de respaldo y prioridad de restauración.

Nivel de criticidad	Estrategia mínima de respaldo	Pruebas mínimas de restauración
Crítico / Alto	Respaldo completo semanal, incremental o diferencial diario, retención mínima de 30 días y al menos una copia lógicamente aislada o fuera de sitio. Para servicios con RPO reducido, evaluar replicación o snapshots consistentes.	Mensual para servicios críticos y trimestral para servicios de alta criticidad, con comparación contra RTO/RPO.
Medio	Respaldo completo periódico e incremental según ventana operativa, retención definida por el propietario funcional y al menos una prueba semestral.	Semestral o ante cambios relevantes.
Bajo	Respaldo conforme a valor operativo y requisitos legales.	Anual o por muestreo documentado.

4. Diversidad y aislamiento. Siempre que resulte técnica y económicamente razonable, deberá existir diversidad de medios, repositorios o ubicaciones, incluyendo al menos una copia fuera del sitio o lógicamente aislada para contingencias severas, ransomware o indisponibilidad del sitio principal. 5. Protección. Los respaldos con información Confidencial o Reservada se cifrarán con estándar AES-256 o equivalente. Las claves de cifrado se custodiarán de manera independiente al repositorio. El acceso a sistemas de respaldo será restringido, nominativo, monitoreado y con autenticación reforzada. 6. Retención. Los plazos de retención se definirán según criticidad, requisitos legales, valor operativo y necesidades de recuperación. La retención no será arbitraria ni ilimitada. 7. Pruebas de restauración. La eficacia de un respaldo se acredita mediante restauración exitosa. Las pruebas deberán documentar fecha, sistema, alcance, responsable, repositorio utilizado, tiempo efectivo de restauración, punto de recuperación alcanzado, brechas respecto de RTO/RPO y acciones correctivas. 8. Integración con continuidad. Los resultados de pruebas de restauración son insumo obligatorio del PE.DGITI.10, del Anexo 10 y del Anexo 16. Toda brecha relevante deberá incorporarse al plan de tratamiento de riesgos. 9. Fallas. Las fallas de respaldo se registrarán, escalarán y corregirán con prioridad acorde al activo afectado, su criticidad y el riesgo de incumplimiento de RTO/RPO.

Referencia normativa

Sección 13.3 / Procedimiento PE.DGITI.04 / ISO 27002:2022 A.8.13

Anexo 3

Política marco de seguridad de la información

Referencia normativa

Sección 6 / Principios rectores de la normativa

1. Protección integral. La seguridad de la información protege la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de todos los activos de información de la UNNE.

2. Gestión basada en riesgos. Las decisiones de seguridad se priorizan en función del riesgo y del impacto sobre la misión universitaria, evitando tanto la omisión de controles esenciales como la imposición de medidas desproporcionadas.

3. Responsabilidad compartida. Toda persona que trate información o utilice recursos institucionales tiene obligaciones de seguridad acordes a su rol. La seguridad no es responsabilidad exclusiva del área técnica.

- 4. Seguridad por diseño.** Los sistemas y procesos nuevos incorporarán requerimientos de seguridad desde su concepción, con configuraciones seguras por defecto y mínima exposición innecesaria.
- 5. Privacidad.** Toda iniciativa que implique tratamiento de datos personales contemplará medidas adecuadas de protección, minimización y cumplimiento normativo.
- 6. Mejora continua.** La política se revisará periódicamente y se actualizará a la luz de auditorías, incidentes, ejercicios, cambios tecnológicos y nuevas necesidades institucionales.

Anexo 4

Política de seguridad en la relación con proveedores

Referencia normativa

Sección 16 / Procedimiento PE.DGITI.05 / ISO 27002:2022 A.5.19-5.22

- 1. Objeto.** Regular los requisitos mínimos de seguridad aplicables a la contratación y supervisión de terceros que presten servicios tecnológicos o traten información institucional.
- 2. Evaluación previa.** Antes de contratar, se evaluarán: criticidad del servicio, tipo de información involucrada, modalidad de acceso, dependencia operativa, localización del tratamiento, capacidad de respuesta ante incidentes y antecedentes del proveedor. El RSI emitirá dictamen de aptitud de seguridad (ver PE.DGITI.05).
- 3. Requisitos contractuales mínimos.** Confidencialidad; protección de datos; notificación de incidentes en ≤ 24 hs; controles de acceso de mínimo privilegio; restricción de subcontratación sin autorización; derecho de auditoría; RTO/SLA acordados; y procedimiento de devolución o eliminación de información al cierre.
- 4. Accesos de soporte.** Los accesos remotos o presenciales de proveedores serán autorizados, limitados en alcance y tiempo, monitoreados en la medida posible y revocados al finalizar la intervención.
- 5. Cambios y subcontratación.** Todo cambio significativo en la prestación o uso de subproveedores que altere el perfil de riesgo será informado y evaluado previamente.
- 6. Cierre del vínculo.** Al concluir la relación, el proveedor devolverá, transferirá o eliminará la información y activos conforme a lo acordado, y cesará sus accesos de manera verificable.

Anexo 5

Política de uso aceptable de activos

Referencia normativa

Sección 8.2.2, 9.3 / ISO 27002:2022 A.5.10

- 1. Objeto.** Establecer pautas de uso responsable de los recursos tecnológicos, de información y de comunicación puestos a disposición por la UNNE.
- 2. Uso institucional.** Los activos se asignan para el cumplimiento de fines académicos, científicos, administrativos, de extensión y de gestión compatibles con la misión universitaria.
- 3. Conductas prohibidas.** Son conductas no admitidas: compartir credenciales; instalar software no autorizado; acceder sin permiso a información ajena; desactivar controles de seguridad; utilizar recursos para actividades ilícitas; distribuir malware; realizar capturas o divulgaciones indebidas de información institucional; emplear mecanismos de almacenamiento o transferencia no autorizados para información Confidencial o Reservada; responder a correos de phishing o proveer credenciales ante solicitudes no verificadas.

4. Uso personal ocasional. El uso personal ocasional, cuando no esté prohibido, deberá ser excepcional, razonable, no interferir con las tareas ni comprometer la seguridad, el rendimiento ni el cumplimiento normativo.

5. Monitoreo. La Universidad podrá aplicar controles y monitoreo sobre sus recursos con finalidades de seguridad, operación, auditoría o investigación, sujeto a los siguientes estándares mínimos: a) notificación previa, expresa y documentada a todos los usuarios sobre el carácter institucional de los recursos, las finalidades del monitoreo y su alcance; b) principio de finalidad determinada y prohibición de utilizar la información obtenida para fines distintos de los declarados; c) principio de mínima intervención, privilegiando el tratamiento de datos de tráfico y metadatos por sobre el acceso al contenido de las comunicaciones; d) registro documentado de todo acceso, con individualización del agente, la fecha, el alcance y la finalidad; y e) intervención del Referente de Protección de Datos.

6. Responsabilidad del usuario. Cada usuario es responsable del uso de su cuenta, de la custodia de los

— 2026 — AÑO DE LA GRANDEZA ARGENTINA

Anexo 6

Procedimiento de gestión de incidentes de seguridad

Referencia normativa

Sección 17 / Procedimiento PE.DGITI.02 / NIST SP 800-61 / ISO 27035

1. Definiciones. Evento: toda ocurrencia observable en un sistema o red. Incidente: evento que compromete o amenaza comprometer la seguridad de la información o la continuidad del servicio.

2. Fases. El procedimiento comprende: preparación; detección y análisis; contención; erradicación; recuperación; y revisión posterior.

3. Preparación. Incluye roles, contactos, herramientas, plantillas, canales de reporte, criterios de severidad (niveles 0-4), mecanismos de preservación de evidencia y coordinación con áreas de apoyo.

4. Detección y análisis. Todo evento reportado se registrará, validará y clasificará. Se evaluará alcance, sistemas afectados, impacto potencial, indicios de compromiso, necesidad de escalar y urgencia de contención.

5. Contención. Las medidas podrán incluir aislamiento de equipos, suspensión de cuentas, bloqueo de comunicaciones, preservación de registros, activación de respaldos, con criterio de mínima afectación necesaria y documentación de cada acción.

6. Erradicación. Consiste en eliminar la causa raíz o los artefactos de compromiso, aplicar parches, corregir configuraciones y reemplazar credenciales comprometidas.

7. Recuperación. Implica restablecer sistemas y datos, validar integridad, monitorear recurrencia y asegurar que el servicio vuelva a condiciones aceptables.

8. Evidencia. Toda evidencia digital se preservará con trazabilidad, registrando quién accede, cuándo, dónde y con qué finalidad. Las copias se realizarán con técnicas apropiadas.

9. Comunicación. Las comunicaciones internas y externas serán canalizadas por los responsables definidos, evitando difusiones prematuras o imprecisas.

10. Lecciones aprendidas. Cerrado el incidente, se documentarán causas, impactos, tiempos, decisiones, desvíos y acciones de mejora. Ver PE.DGITI.02.

Anexo 7

Proceso de monitoreo y seguimiento de vulnerabilidades

Referencia normativa

Secciones 13.5, 15.4 / Procedimiento PE.DGITI.03 / CIS Controls v8 #7

- 1. Fuentes.** NVD (NIST), CERT.ar, CISA KEV, boletines de fabricantes, comunidades técnicas, monitoreo interno, escaneos automatizados y reportes recibidos por la Universidad.
- 2. Registro.** Toda vulnerabilidad relevante identificada se registrará con: referencia (CVE), activo afectado, CVSS score, exposición, fecha de detección, responsable y estado.
- 3. Priorización.** La prioridad considera: CVSS score, criticidad del activo (Anexo 11), exposición a Internet, existencia de exploit público activo (CISA KEV), presencia de datos personales y riesgo para la continuidad.
- 4. Plazos de tratamiento.** Crítica (CVSS ≥ 9.0 o exploit activo): 48 hs. Alta (CVSS 7.0-8.9 en sistema crítico): 7 días. Media (CVSS 4.0-6.9): 30 días. Baja (CVSS < 4.0): 90 días.
- 5. Tratamiento.** Parche oficial del fabricante preferente. Cuando no esté disponible: controles compensatorios temporales documentados y aceptación formal del riesgo residual por el RSI.
- 6. Seguimiento y reporte.** El RSI consolidará reportes periódicos sobre vulnerabilidades críticas, activos más expuestos y demoras significativas. Ver PE.DGITI.03.
- 7. Dependencia de terceros / SIU.** El plazo de 48 hs corre desde la publicación del parche oficial por el proveedor. Plazo de aplicación en UNNE: **5 días hábiles** desde disponibilidad, con controles compensatorios mientras tanto.

Anexo 8

Lineamientos sobre software y herramientas de respaldo

Referencia normativa

Sección 13.3 / Procedimiento PE.DGITI.04

- 1. Selección.** Las soluciones de respaldo se elegirán por compatibilidad con la infraestructura, capacidad de automatización, seguridad, trazabilidad, soportabilidad, restauración granular y costos de operación.
- 2. Configuración y documentación.** Toda herramienta de respaldo se documentará indicando activos cubiertos, credenciales asociadas, repositorios, políticas de retención, alertas y responsables de administración.
- 3. Seguridad del sistema de respaldo.** Las consolas, repositorios y cuentas de administración del software de respaldo se protegerán con controles reforzados, segmentación y revisión periódica. El sistema de respaldo no deberá convertirse en punto de compromiso.
- 4. Actualización.** Las herramientas de respaldo se mantendrán en versiones soportadas y con parches de seguridad aplicados.
- 5. Restauración.** Las capacidades de recuperación serán conocidas y probadas periódicamente por el equipo responsable conforme al PE.DGITI.04.

Anexo 9

Matriz de riesgos — lineamientos mínimos

Referencia normativa

Sección 5 / Procedimiento PE.DGITI.09 / ISO/IEC 27005

- 1. Campos mínimos de la matriz.** Activo o proceso; propietario; amenaza; vulnerabilidad; controles existentes; probabilidad (1-5); impacto (1-5); nivel de riesgo inherente ($P \times I$, escala 1-25); tratamiento propuesto (evitar/reducir/transferir/aceptar); responsable; plazo; riesgo residual; y autoridad que aprueba la aceptación cuando corresponda.
- 2. Clasificación de riesgos.** Bajo (1-4), Medio (5-9), Alto (10-16), Crítico (17-25). Los riesgos Altos y Críticos requieren plan de tratamiento documentado y aprobación expresa.
- 3. Diferenciación por criticidad.** La matriz distinguirá servicios críticos, información sensible, dependencias con terceros y riesgos que comprometan continuidad o cumplimiento normativo.
- 4. Trazabilidad.** Se conservará historial de actualizaciones para trazabilidad del tratamiento y las decisiones adoptadas. La matriz es un documento vivo que se actualiza al menos anualmente y ante eventos disparadores.

Anexo 10

Lineamientos para respaldo de máquinas virtuales críticas

- 1. Identificación.** Son máquinas virtuales críticas aquellas cuya indisponibilidad afecte significativamente procesos académicos, administrativos, documentales, de identidad, comunicaciones, conectividad, seguridad, continuidad operativa o prestación de servicios digitales esenciales. Su criticidad deberá coincidir con el inventario del Anexo 11.
- 2. Alineación con criticidad.** La frecuencia, retención, tipo de respaldo, replicación, snapshot, ubicación y prioridad de recuperación se definirán según el nivel de criticidad, RTO, RPO y orden de recuperación establecidos en el Anexo 11 y en el Anexo 16.

Criticidad	Estrategia de recuperación recomendada para MV	Consideraciones mínimas
Crítico / Alto	Replicación, snapshots controlados, respaldos consistentes y capacidad de recuperación en infraestructura alterna o sitio de respaldo.	Validar dependencias, redes, almacenamiento, credenciales, DNS, certificados, bases de datos y orden de encendido.
Medio	Respaldos completos e incrementales con restauración en entorno controlado o alterno según disponibilidad.	Documentar tiempos reales de restauración y brechas frente a RTO/RPO.
Bajo	Respaldos periódicos y restauración por demanda o por muestreo.	Mantener documentación mínima para reconstrucción del servicio.

- 3. Consistencia.** Cuando la carga lo requiera, se implementarán mecanismos de respaldo consistentes a nivel de aplicación o base de datos, evitando depender únicamente de snapshots no consistentes.
- 4. Pruebas.** Las MV críticas integrarán el plan de pruebas de restauración del PE.DGITI.04 y los ejercicios del PE.DGITI.10. Las pruebas deberán validar arranque, integridad de datos, conectividad, autenticación, servicios dependientes y cumplimiento de RTO/RPO.
- 5. Documentación de dependencias.** Para cada MV crítica se consignarán dependencias entre máquinas, servicios, almacenamiento, redes, balanceadores, certificados, credenciales, reglas de firewall, tareas programadas y proveedores involucrados.
- 6. Orden de recuperación.** La secuencia de restauración de MV no será definida únicamente por conveniencia técnica, sino por el orden de recuperación institucional del Anexo 11, considerando servicios de identidad, seguridad, conectividad, datos, aplicaciones críticas y servicios de soporte.

Referencia normativa

Sección 13.3 / Procedimiento PE.DGITI.04 / Anexo 2

Anexo 11

Inventario y clasificación de sistemas críticos

- 1. Objeto.** Establecer el formato mínimo del inventario institucional de sistemas, servicios y procesos

tecnológicos relevantes para la seguridad de la información, la continuidad operativa y la recuperación ante contingencias.

2. Campos del inventario. El inventario deberá contener, como mínimo: nombre del sistema o servicio; identificador único; propietario funcional; responsable técnico; unidad organizativa; descripción de funcionalidades; entorno (on-premises/cloud/híbrido); datos tratados; clasificación de la información; dependencias de aplicaciones, bases de datos, infraestructura, comunicaciones, identidad, certificados y proveedores; exposición a Internet; usuarios o población afectada; criticidad; RTO; RPO; orden de recuperación; recursos mínimos; fecha de actualización; y aprobación de la autoridad designada.

Dimensión de impacto Aspectos a evaluar

Seguridad / vida / bienestar Riesgos para personas, seguridad física, servicios esenciales o condiciones de operación segura.

Continuidad de servicios universitarios Impacto en docencia, investigación, extensión, gestión administrativa, trámites, identidad, comunicaciones y servicios digitales.

Económico / operativo Costos de indisponibilidad, reprocesos, pérdida de productividad, afectación presupuestaria o contractual.

Legal / regulatorio Incumplimiento de leyes, resoluciones, obligaciones de guarda, protección de datos, transparencia, auditoría o contratos.

Reputacional / institucional

Impacto en confianza, imagen pública, relación con comunidad universitaria, organismos externos y ciudadanía.

3. Niveles de criticidad. La UNNE utilizará la clasificación Crítico/Alto, Medio y Bajo, compatible con la categorización técnica del Anexo 16. Cuando se mantenga la escala interna 1 a 4, se aplicará la siguiente equivalencia: 1=Crítico, 2=Alto, 3=Medio, 4=Bajo.

Nivel	Criterio general	RTO orientativo	RPO orientativo
Crítico / Alto	Indisponibilidad con impacto severo en funciones esenciales, servicios digitales institucionales críticos, identidad, seguridad, datos sensibles o continuidad universitaria.	Menor a 4 horas para críticos; hasta 24 horas para alta criticidad según BIA.	Menor a 1 hora para críticos; hasta 4 horas para alta criticidad según BIA.
Medio	Impacto grave pero manejable mediante procedimientos alternativos temporales, con afectación relevante a áreas o procesos.	Hasta 24 horas o plazo definido por BIA.	Hasta 4 horas o plazo definido por BIA.
Bajo	Impacto acotado, tolerable o recuperable mediante trabajo manual o postergación sin comprometer funciones esenciales.	Entre 1 y 5 días, según BIA.	Hasta 24 horas o según valor operativo.

4. Dependencias y orden de recuperación. Cada sistema deberá registrar sus dependencias y precondiciones de recuperación. El orden de recuperación deberá priorizar identidad y autenticación, conectividad, seguridad perimetral y monitoreo, bases de datos y almacenamiento, sistemas académicos y documentales críticos, sistemas económicos y administrativos, comunicaciones y servicios de menor criticidad. El orden podrá modificarse por decisión del Comité o de la autoridad designada ante un escenario concreto, dejando constancia en bitácora.

5. Mantenimiento. El inventario se actualizará, como mínimo, una vez al año y ante altas, bajas, migraciones, cambios de arquitectura, incorporación o baja de proveedores, modificación de criticidad, cambios de RTO/RPO, incidentes relevantes o pruebas de continuidad con resultados significativos. 6. Uso como insumo. El inventario es insumo obligatorio para los Procedimientos PE.DGITI.03 (vulnerabilidades), PE.DGITI.04 (respaldos), PE.DGITI.09 (riesgos) y PE.DGITI.10 (continuidad), así como para los Anexos 2, 10 y 16.

Referencia normativa

Anexo 12

Lineamientos de ciberseguridad en entornos de computación en la nube

Referencia normativa

Sección 11 bis / Procedimiento PE.DGITI.05 / ISO 27002:2022 A.5.23 / CSA CCM v4

- 1. Objeto.** Establecer los criterios y controles mínimos de seguridad para la adopción, configuración y gestión de servicios de computación en la nube (IaaS, PaaS, SaaS) utilizados por la UNNE.
- 2. Modelo de responsabilidad compartida.** El proveedor cloud es responsable de la seguridad de la infraestructura subyacente. La UNNE es responsable de la seguridad de los datos, configuraciones, identidades, accesos y aplicaciones que opera sobre esa infraestructura. Esta distinción debe ser comprendida y documentada para cada servicio cloud contratado.
- 3. Evaluación previa de servicios cloud.** Antes de adoptar un servicio cloud que trate información institucional, la DGITI y el RSI evaluarán y documentarán: clasificación de la información a tratar; residencia y localización de datos, conforme a la prohibición de transferencia internacional del artículo 12 de la Ley 25.326 -aplicable a la totalidad de los datos personales y no solo a la información sensible- y al régimen que lo complementa (Disposición DNPDP N° 60-E/2016 y Resoluciones AAIP N° 34/2019 y N° 198/2023); toda transferencia a países que no cuenten con nivel de protección adecuado -entre ellos, Estados Unidos- deberá encuadrarse en alguna excepción del artículo 12, en el consentimiento expreso de los titulares, o en las cláusulas contractuales modelo aprobadas por dicha normativa, con intervención previa del Referente de Protección de Datos y de la Secretaría General Legal y Técnica; portabilidad y reversibilidad (plan de salida); garantías de disponibilidad (SLA mínimo 99,5% para servicios críticos); capacidades de auditoría y registro exportables; cumplimiento del proveedor con Ley 25.326 o equivalente; y derechos de auditoría contratables.
- 4. Gestión de identidades y accesos cloud (IAM).** El acceso a servicios cloud institucionales se integrará, en la medida de lo posible, con el directorio central de identidades de la UNNE mediante SSO (SAML 2.0, OIDC). La autenticación multifactor será obligatoria para cuentas de administración cloud. Las cuentas cloud seguirán el ciclo de vida definido en el PE.DGITI.01 y el Anexo 1.
- 5. Configuración segura.** Los servicios cloud se configurarán conforme a los lineamientos de seguridad del proveedor (CIS Benchmarks, Security Best Practices). Se evitará el acceso público no intencional a recursos de almacenamiento o bases de datos cloud. Los recursos cloud sin uso serán inventariados y eliminados periódicamente.
- 6. Monitoreo y registros.** Los logs de actividad de los servicios cloud críticos se habilitarán y conservarán durante el período mínimo definido por el RSI. Se configurarán alertas ante eventos de seguridad relevantes: accesos no habituales, cambios de configuración, elevación de privilegios.
- 7. Cifrado en la nube.** La información Confidencial o Reservada almacenada en servicios cloud deberá cifrarse en reposo y en tránsito, preferentemente con claves gestionadas por la UNNE (Customer Managed Keys) cuando el servicio lo permita.
- 8. Continuidad y portabilidad.** Los contratos con proveedores cloud incluirán garantías de recuperación ante fallos, procedimientos de migración y eliminación de datos al cierre del vínculo. No se adoptarán servicios que generen dependencia tecnológica irreversible (vendor lock-in) sin evaluación y aprobación formal del RSI y la DGITI.

Anexo 13

Criptografía y gestión de certificados digitales

Referencia normativa

Sección 11 / ISO 27002:2022 A.8.24 / Ley 25.506

- 1. Objeto.** Definir los lineamientos de uso de controles criptográficos, gestión de claves y administración de certificados digitales en la UNNE.
- 2. Algoritmos permitidos.** Se utilizarán únicamente algoritmos reconocidos como seguros: AES-256 para cifrado simétrico; RSA de 2048 bits o superior (preferiblemente RSA-4096 o ECDSA P-256/P-384) para criptografía asimétrica; SHA-256 o superior para funciones hash. Se prohíbe el uso de algoritmos obsoletos: MD5, SHA-1, DES, 3DES, RC4, RSA < 1024 bits.
- 3. Cifrado en tránsito.** Toda comunicación de información Confidencial o Reservada a través de redes públicas o semipúblicas utilizará TLS 1.2 o superior. Se deshabilitarán TLS 1.0, TLS 1.1 y SSL en todos los servicios en producción. Los servicios expuestos a Internet deberán contar con certificados emitidos por CA reconocida.
- 4. Cifrado en reposo.** Las bases de datos con datos personales sensibles, credenciales o información académica confidencial se cifrarán en reposo. Los respaldos de sistemas críticos se cifrarán conforme al Anexo 2.
- 5. Gestión de certificados.** La DGITI mantendrá un inventario de todos los certificados digitales de la UNNE (certificados de servidor, de usuario, de firma de código) con: autoridad emisora, dominio o entidad cubierta, fecha de emisión, fecha de vencimiento y responsable de renovación. Se implementarán alertas de vencimiento con 60 días de anticipación mínima.
- 6. Gestión de secretos y claves.** Las claves criptográficas, contraseñas de servicio, tokens de API y demás secretos de aplicación no deberán almacenarse en repositorios de código fuente ni en texto plano. Se utilizarán mecanismos de gestión de secretos (vault, variables de entorno seguras, servicios de secretos del proveedor cloud) para todos los entornos de producción.
- 7. Firma digital.** La implementación de firma digital para documentos y actos administrativos se articulará con la Ley 25.506 y la infraestructura de clave pública (PKI) disponible para el sector universitario. Los certificados de firma digital de autoridades universitarias deberán ser de firma digital reconocida (Nivel 1 o superior de la IAFRA).

Anexo 14

Dashboard de métricas de seguridad

Referencia normativa

Sección 20 / Comité de Seguridad

- 1. Objeto.** Definir el conjunto mínimo de indicadores de seguridad para el reporte periódico al Comité de Seguridad y a la autoridad universitaria.
- 2. Estructura del informe trimestral.** El informe incluirá: resumen ejecutivo; semáforo de estado por dominio (verde/amarillo/rojo); indicadores operativos (ver Sección 20.1); estado de riesgos; resumen de incidentes; estado de programas de mejora; y recomendaciones.
- 3. Indicadores adicionales de seguimiento.** Además de los KPIs de la Sección 20.1, el dashboard incluirá: número de incidentes por mes y tendencia; % de accesos privilegiados con MFA habilitado; % de sistemas críticos con cobertura de monitoreo activo; deuda técnica de vulnerabilidades (vulnerabilidades CVSS ≥ 7 pendientes acumuladas); cobertura del inventario de activos (% con propietario asignado y ficha completa).
- 4. Formato y herramienta.** El RSI y la DGITI definirán la herramienta o plantilla de reporte conforme a las capacidades tecnológicas disponibles. El informe se presentará en formato que permita comparación histórica (mínimo 4 trimestres).

5. Distribución. El informe trimestral se distribuirá al Comité de Seguridad. El informe anual se elevará a la autoridad universitaria competente y se pondrá a disposición de auditoría interna.

Anexo 15

Gestión de identidades y accesos (IAM) — ecosistema UNNE

Referencia normativa

Sección 10 / Procedimiento PE.DGITI.01 / ISO 27002:2022 A.5.15-5.18 / Res. CIN CE 1669/22

1. Objeto. Definir lineamientos para la gestión unificada del ciclo de vida de identidades en el ecosistema tecnológico de la UNNE, abarcando sistemas SIU, directorio corporativo, servicios en la nube y accesos federados.

2. Fuente de verdad de identidades. El directorio corporativo institucional (LDAP/Active Directory o equivalente) constituirá la fuente de verdad para todas las identidades del personal docente, no docente y autoridades. Los sistemas SIU (Guaraní, Pilagá, Mapuche) y los servicios en la nube se integrarán, en la medida de lo técnicamente posible, con este directorio central.

3. Identidades de estudiantes. Las identidades de los estudiantes activos serán provisionadas automáticamente a partir del sistema SIU-Guaraní, con ciclo de vida vinculado a la condición académica. Se definirán criterios de desactivación automática ante egreso, abandono o inactividad prolongada.

4. Single Sign-On (SSO). La UNNE implementará progresivamente SSO para los sistemas institucionales, utilizando protocolos estándar (SAML 2.0, OIDC/OAuth 2.0). Se priorizará la integración de sistemas de alta frecuencia de uso y mayor criticidad. El SSO reducirá la proliferación de credenciales y mejorará la experiencia de usuario manteniendo la trazabilidad.

5. Federación de identidades. La UNNE explorará la participación en esquemas de federación de identidades del sistema universitario nacional (CAFEI/ARede u equivalente) que permitan la autenticación federada entre instituciones, facilitando la movilidad académica y el acceso a recursos compartidos.

6. Aprovisionamiento y desaprovisionamiento automático. Se implementarán mecanismos de aprovisionamiento automático de cuentas a partir de altas en el sistema de RRHH o académico, y desaprovisionamiento automático a partir de bajas o cambios de estado. Esto reducirá el riesgo de cuentas huérfanas o accesos residuales.

7. Autenticación multifactor (MFA). La MFA se implementará de manera progresiva: en primer lugar para cuentas de administración de sistemas críticos, accesos VPN y consolas cloud; luego para toda la comunidad universitaria. Los métodos de MFA admitidos serán: aplicaciones de autenticación (TOTP), llaves de seguridad hardware (FIDO2/WebAuthn) o SMS como último recurso. Se desaconseja el uso de SMS como único factor adicional ante la vulnerabilidad al SIM swapping.

8. Trazabilidad. Todos los eventos de autenticación, cambios de contraseña, resets de MFA y modificaciones de atributos de identidad quedarán registrados en el directorio o en sistema de logging centralizado, con retención mínima de 12 meses.

9. Mapeo de correspondencia CIN CE 1669/22. Este anexo incluye la tabla de correspondencia entre los dominios del Modelo CIN y las secciones de esta normativa, para facilitar la trazabilidad en revisiones externas. La DGITI mantendrá actualizada dicha tabla en la siguiente revisión.

Anexo16

Política de Planes de Contingencia, Recuperación ante Desastres y Centro de Procesamiento de Datos de Respaldo

1. **Objeto.** Establecer el marco técnico y operativo para la elaboración, implementación, prueba, actualización y mejora de los planes de contingencia y recuperación ante desastres de los sistemas y servicios tecnológicos de la UNNE, incluyendo criterios para el centro de procesamiento de datos de respaldo cuando corresponda.

2. **Alcance.** Este anexo alcanza a los sistemas, servicios, datos, plataformas, redes, componentes de infraestructura, proveedores y procesos institucionales que resulten necesarios para sostener o recuperar servicios digitales de la Universidad ante eventos disruptivos. Comprende tanto contingencias tecnológicas como incidentes de ciberseguridad, indisponibilidad de instalaciones, fallas energéticas, fallas de comunicaciones, indisponibilidad de proveedores, daño físico, errores operativos y desastres.

3. **Política de planes de contingencia.** La UNNE elaborará y mantendrá una Política de Planes de Contingencia que defina propósito, alcance, roles, responsabilidades, coordinación entre áreas, criterios de activación, mecanismos de actualización y procedimientos asociados. La actualización será periódica y también reactiva ante eventos relevantes, tales como cambios de arquitectura, incorporación de sistemas críticos, incidentes graves, cambios de proveedor, resultados insatisfactorios de pruebas o modificaciones normativas.

4. **Autoridad designada.** La autoridad designada para impulsar la política, coordinar su actualización y consolidar los planes será el RSI, con intervención de la DGITI, los propietarios funcionales, responsables técnicos, Comité de Seguridad, áreas legales, comunicación institucional y proveedores críticos cuando corresponda.

5. **Inventario y clasificación.** La política se apoyará en el inventario del Anexo 11. Cada sistema deberá estar identificado de manera unívoca, con descripción funcional, dependencias, criticidad, RTO, RPO, orden de recuperación y recursos requeridos. El inventario será aprobado por la autoridad designada y revisado al menos anualmente.

Campo mínimo	Descripción
Sistema / proceso	Nombre e identificador único del sistema o proceso soportado.
Funcionalidad institucional	Descripción de los servicios o funciones que sostiene.
Dependencias	Aplicaciones, datos, infraestructura, comunicaciones, identidad, proveedores y recursos humanos requeridos.
Impacto de interrupción y reputacional.	Impacto por dimensiones: seguridad/vida, continuidad de servicios, económico/operativo, legal/regulatorio
Criticidad	Nivel Alto/Medio/Bajo o equivalencia interna Crítico/Alto/Medio/Bajo.
RTO / RPO	Tiempo objetivo de recuperación y punto objetivo de recuperación.
Orden de recuperación	Prioridad de restauración y recursos mínimos necesarios.

6. **Categorización por criticidad.** La criticidad se definirá en función del impacto de la indisponibilidad. La clasificación deberá orientar la inversión, la estrategia de respaldo, la arquitectura de recuperación, las pruebas y la priorización durante una contingencia.

Nivel	Descripción	Exigencia orientativa
Alto / Crítico	Sistemas cuya indisponibilidad compromete funciones esenciales de la Universidad, identidad, seguridad, continuidad de servicios críticos, datos sensibles o cumplimiento legal relevante.	RTO preferente menor a 4 horas; RPO preferente menor a 1 hora; sitio alternativo caliente o tibio cuando sea viable; pruebas integrales anuales y tabletop semestrales.
Medio	Sistemas cuya interrupción genera efectos adversos graves pero manejables mediante alternativas temporales.	RTO preferente menor a 24 horas; RPO preferente menor a 4 horas; recuperación mediante infraestructura alterna, backups o procesos manuales; pruebas anuales y tabletop periódicos.
Bajo	Sistemas con impacto limitado o recuperable sin afectar funciones esenciales.	RTO entre 1 y 5 días o según BIA; pruebas por muestreo, verificación de copias y documentación mínima de recuperación.

7. Contenido mínimo del Plan de Contingencia y Recuperación. Todo plan deberá incluir: alcance; resumen del BIA; sistemas y procesos alcanzados; RTO y RPO; estrategia de respaldo y recuperación; sitio alternativo o modalidad de operación degradada; roles y responsabilidades; contactos de emergencia; proveedores involucrados; procedimientos de activación; conmutación; recuperación; validación; retorno a la normalidad; comunicación; seguridad física y lógica; bitácora; pruebas; revisión; aprobación; actualización y mejora continua.

8. Procedimientos de activación, conmutación, recuperación y retorno. Los planes deberán contener playbooks paso a paso para: declarar la contingencia; activar el equipo de recuperación; preservar evidencia cuando se trate de incidente de ciberseguridad; conmutar a sitio o modalidad alternativa; restaurar sistemas y datos; validar integridad; operar en contingencia; retornar al sitio o servicio normal; y cerrar formalmente el evento con informe post-contingencia.

9. Seguridad durante la recuperación. La recuperación no deberá debilitar controles esenciales. Se mantendrán o restablecerán autenticación robusta, segmentación, reglas de firewall, monitoreo, cifrado, protección de credenciales, control de accesos físicos y lógicos, resguardo de evidencia y trazabilidad de decisiones. En eventos de ciberseguridad, la recuperación se coordinará con el procedimiento de respuesta a incidentes para evitar reinfección, pérdida de evidencia o exposición prematura de información.

10. Bitácora y evidencia. Durante toda contingencia se llevará una bitácora cronológica con fecha, hora, evento, decisión, responsable, acción ejecutada, resultado, evidencia asociada y estado. Se archivarán informes de pruebas, reportes de backups, registros de replicación, validaciones de integridad, comunicaciones, autorizaciones y lecciones aprendidas.

11. Programa de pruebas. Los planes serán probados con periodicidad acorde a la criticidad. Las pruebas podrán ser tabletop, restauración de backups, failover, recuperación de datos, conmutación de red, pruebas de comunicación, validación de sitio alternativo o pruebas integrales. Toda prueba deberá concluir con informe de resultados, brechas, plan de remediación y responsable.

12. Centro de Procesamiento de Datos de Respaldo. Cuando resulte aplicable por criticidad, obligación normativa, decisión institucional o estrategia de continuidad, la UNNE definirá un Centro de Procesamiento de Datos de Respaldo o modalidad funcional equivalente. Su diseño deberá considerar independencia geográfica, disponibilidad de energía, conectividad redundante, capacidad de cómputo y almacenamiento, compatibilidad tecnológica, seguridad física y lógica equivalente y mecanismos de replicación o restauración consistentes con RTO/RPO.

13. Requisitos técnicos de referencia para el sitio de respaldo. Como objetivo técnico de referencia, y sin perjuicio del análisis de viabilidad y normativa aplicable a la UNNE, el sitio de respaldo deberá

contemplar: ubicación dentro del territorio nacional; distancia geográfica suficiente respecto del sitio principal para evitar exposición simultánea a eventos disruptivos; conectividad redundante por rutas diferenciadas y, preferentemente, proveedores distintos; energía con UPS y generación de respaldo; climatización redundante; hardware compatible y dimensionado; controles de acceso físico; detección y supresión de incendios; monitoreo; firewalls; IDS/IPS; autenticación robusta; segmentación; cifrado; y procedimientos de mantenimiento concurrente.

14. Nivel Tier y mantenibilidad. Para servicios de criticidad alta o crítica, la planificación del centro de datos de respaldo deberá tomar como referencia estándares de disponibilidad y mantenibilidad concurrente equivalentes a Tier 3, ANSI/TIA-942 o Uptime Institute, en la medida en que resulten aplicables, viables y aprobados por la autoridad institucional competente. No constituye requisito de cumplimiento inmediato. Cuando no sea posible cumplir de manera inmediata, deberá documentarse brecha, riesgo residual, medidas compensatorias, plazo de adecuación y autoridad que acepta el riesgo.

15. Revisión y aprobación. Los planes de contingencia y recuperación serán aprobados por la autoridad designada, con intervención del propietario funcional y del responsable técnico. Los planes vinculados con sistemas críticos deberán ser informados al Comité de Seguridad.

16. Mejora continua. Toda prueba, incidente, contingencia real, cambio significativo o hallazgo de auditoría deberá retroalimentar el inventario del Anexo 11, la política de respaldos del Anexo 2, los lineamientos de MV críticas del Anexo 10, el PE.DGITI.10 y los planes específicos de recuperación.

17. Continuidad de los servicios de identidad y correo institucional. Por constituir el correo institucional el domicilio electrónico de los agentes de la UNNE (RES-2024-8869-REC # UNNE), los servicios de identidad, autenticación y correo institucional se clasifican expresamente como sistemas críticos en el inventario del Anexo 11, con valores de RTO y RPO acordes a esa naturaleza. Ante indisponibilidad prolongada de dichos servicios, el PE.DGITI.10 aplicará un protocolo específico que contemple: constancia documentada del hecho, publicidad institucional de la contingencia, intervención de la Secretaría General Legal y Técnica, y evaluación de la suspensión o prórroga de los plazos administrativos en curso mientras subsista la indisponibilidad.

Procedimientos derivados de la política

Los procedimientos que se presentan a continuación fueron elaborados por la Dirección de Gestión e Innovación de las Tecnologías de la Información (DGITI) de la UNNE, en su rol de dirección operativa de la seguridad de la información. Cada procedimiento se deriva directamente de una o más cláusulas o anexos de la Normativa de Ciberseguridad UNNE y establece pasos concretos, roles, registros e indicadores de desempeño para su implementación.

Criterio de priorización de implementación: se recomienda adoptar PE.DGITI.01, PE.DGITI.02, PE.DGITI.03 y PE.DGITI.04 en el primer año de vigencia, por su impacto directo en la reducción del riesgo operativo. PE.DGITI.09 y PE.DGITI.10 consolidan el enfoque estratégico y son el fundamento para las revisiones anuales del sistema.

ID	Título	Cláusulas/Anexos de origen	Prioridad
PR-01	Gestión del ciclo de vida de accesos e identidades	Secc.10 / Anexo 1 / Anexo 15	Alta — Año 1
PR-02	Respuesta a incidentes de seguridad	Secc.17 / Anexo 6	Alta — Año 1

PR-003	Gestión de vulnerabilidades técnicas	Secc.13.5, 15.4 / Anexo 7	Alta — Año 1
PR-004	Respalos y pruebas de restauración	Secc.13.3 / Anexos 2, 8, 10	Alta — Año 1
PR-005	Evaluación de seguridad de proveedores TI	Secc.16 / Anexo 4	Media — Año 1
PR-006	Clasificación y etiquetado de activos	Secc.9 / Anexo 11	Media — Año 1
PR-007	Concientización y capacitación en seguridad	Secc.8.2.2 / Anexo 5	Media — Año 1
PR-008	Gestión de cambios en infraestructura y sistemas	Secc.13.1, 15	Media — Año 2
PR-009	Evaluación periódica de riesgos	Secc.5 / Anexo 9	Alta — Año 1
PR-010	Gestión de continuidad, contingencia y recuperación	Secc.18 / Anexos 2, 10, 11, 16	Alta — Año 2

PE.DGITI.01

Gestión del Ciclo de Vida de Accesos e Identidades

Ref.: Secc.4.1, 10 / Anexo 1, 15 / ISO 27002:2022 A.5.15-5.18 / NIST CSF PR.AC

Versión: 1.0	Estado: Vigente	Revisión: Anual	Dirección: DGITI
---------------------	------------------------	------------------------	-------------------------

Objeto: Definir el proceso de alta, modificación, baja y revisión periódica de accesos, asegurando mínimo privilegio, trazabilidad y revocación oportuna en todo el ecosistema tecnológico de la UNNE.

Roles

Rol	Responsabilidad en este procedimiento
Propietario de la información	Aprueba perfiles de acceso y valida necesidad funcional.
Responsable del servicio	Ejecuta altas, modificaciones y bajas. Mantiene registro actualizado.
RRHH / Talento Humano	Notifica ingresos, egresos y cambios de función.
RSI	Supervisa cumplimiento, valida accesos privilegiados y autentica excepciones.
DGITI	Mantiene el procedimiento y los sistemas de IAM. Reporta KPIs.

Disparadores

- Ingreso de nuevo personal, docente, becario o contratista.
- Cambio de función, dependencia o responsabilidad.
- Cese, desvinculación, licencia especial o finalización de contrato.
- Detección de acceso indebido o cuenta inactiva en revisión periódica.
- Revisión periódica programada (trimestral para sistemas críticos).

Pasos del procedimiento

Fase 1 — Solicitud y aprobación

1.1. El solicitante o responsable de RRHH completa el FORM-ACC-001 indicando: nombre, función, sistema(s) solicitado(s), nivel de privilegio, justificación funcional y plazo si es temporal.

1.2. El propietario de la información aprueba la solicitud. El RSI revisa las solicitudes de acceso privilegiado o a sistemas de criticidad alta antes de su implementación.

Fase 2 — Implementación

2.1. El responsable del sistema implementa el acceso en el plazo definido: máx. 2 días hábiles para altas ordinarias, inmediato para bajas urgentes.

2.2. Se asignan roles o perfiles predefinidos. Se evitan cuentas genéricas. Las cuentas temporales de terceros tendrán fecha de expiración automática.

2.3. Se registra en REG-ACC-001: usuario, sistema, nivel, fecha y responsable de implementación.

Fase 3 — Revisión periódica

3.1. Cada trimestre, el responsable del servicio genera reporte de cuentas activas por sistema crítico para validación del propietario de la información.

3.2. El RSI consolida resultados y reporta al Comité los hallazgos: cuentas sin uso, accesos huérfanos, privilegios excesivos.

Fase 4 — Baja y revocación

4.1. RRHH notifica a DGITI con al menos 24 hs de anticipación. Para bajas urgentes, la notificación es inmediata.

4.2. Accesos a sistemas críticos: revocados el mismo día hábil. Sistemas de menor criticidad: máx. 2 días hábiles.

4.3. Se verifica la devolución de credenciales físicas y se documenta el cierre en REG-ACC-001.

Registros requeridos

- FORM-ACC-001: Formulario de alta/modificación/baja de acceso.
- REG-ACC-001: Registro de implementación y cambios de acceso (por sistema).
- REP-ACC-001: Reporte periódico de revisión de accesos.

Indicadores de desempeño

Indicador	Meta	Frecuencia
Tiempo promedio de baja de acceso ante desvinculación (sistemas críticos)	≤ 1 día hábil	Mensual
% de cuentas con revisión periódica al día	$\geq 95\%$	Trimestral
Accesos privilegiados sin justificación documentada	0	Trimestral

Revisión: Anual o ante cambio significativo en arquitectura de identidades o incidente vinculado a gestión de accesos.

PE.DGITI.02

Respuesta a Incidentes de Seguridad

Ref.: Secc.17 / Anexo 6 / NIST SP 800-61 Rev.3 / ISO 27035

Versión: 1.0	Estado: Vigente	Revisión: Anual	Dirección: DGITI / RSI
---------------------	-----------------	-----------------	------------------------

Objeto: Establecer el proceso coordinado de detección, análisis, contención, erradicación, recuperación y documentación de incidentes de seguridad, con preservación de evidencia.

Roles

Rol	Responsabilidad en este procedimiento
DGITI / Mesa de ayuda	Primer punto de contacto. Registra y escala según severidad.
RSI	Coordina la respuesta. Activa fases. Decide escalamiento al Comité.
Responsable del sistema afectado	Ejecuta medidas técnicas. Preserva evidencia.
Área legal	Interviene ante requerimientos judiciales y preservación de evidencia.
Comunicación institucional	Gestiona comunicación externa ante incidentes con impacto público.
Comité de Seguridad	Se activa para incidentes Severos (N3) o Críticos (N4).

Clasificación de severidad

Nivel	Denominación	Criterio	Escalamiento
N0	Sin impacto	Evento sin afectación real	Mesa de ayuda — cierra sin escalar
N1	Bajo	Impacto limitado a un usuario o sistema no crítico	Responsable técnico + RSI (informativo)
N2	Medio	Impacto en sistema no crítico o afectación parcial de datos	RSI coordina. Informe post-incidente obligatorio
N3	Severo	Servicio crítico afectado, datos personales comprometidos, ransomware	RSI + Comité. Área legal si corresponde
N4	Crítico	Múltiples servicios críticos, impacto institucional grave, APT detectado	RSI + Comité + Máxima autoridad. Comunicación controlada

Pasos del procedimiento

Fase 1 — Detección y registro

- 1.1. Todo evento se registra en TICK-INC-001 con fecha/hora, reportante, descripción, sistemas aparentemente afectados y fuente.
- 1.2. Se clasifica en N0-N4 usando MAT-INC-001. Incidentes N2+ se escalan al RSI en ≤ 30 minutos.

Fase 2 — Análisis y validación

- 2.1. RSI y responsable del sistema analizan: sistemas comprometidos, loC, vector de ataque, alcance, datos personales involucrados.
- 2.2. La clasificación se actualiza si el análisis revela mayor alcance. N3+ activa al Comité de Seguridad.

Fase 3 — Contención y evidencia

- 3.1. Se implementan medidas: aislamiento de equipo, bloqueo de cuenta, revocación de acceso remoto, regla de firewall, activación de respaldo limpio.
- 3.2. Toda acción de contención se documenta con timestamp y responsable en TICK-INC-001.
- 3.3. Se preservan evidencias en estado original: volcado de memoria, imagen forense, copia de logs, capturas de tráfico. Cadena de custodia en FORM-EVID-001.

Fase 4 — Erradicación y recuperación

- 4.1. Se eliminan causas raíz y artefactos: malware, configuraciones comprometidas, credenciales expuestas, backdoors.
- 4.2. La recuperación sigue el orden del Anexo 11 (criticidad). El RSI autoriza el alta al servicio productivo previa validación de integridad.

Fase 5 — Cierre y lecciones aprendidas

- 5.1. Se redacta INF-INC-001: cronología, causa raíz, impacto, acciones, loC, tiempos de resolución y recomendaciones.
- 5.2. En los 10 días hábiles siguientes, el RSI convoca reunión de lecciones aprendidas. Las mejoras se incorporan al plan de tratamiento de riesgos.

Registros requeridos

- TICK-INC-001: Ticket de incidente.
- MAT-INC-001: Matriz de clasificación de incidentes.
- FORM-EVID-001: Cadena de custodia de evidencia digital.
- INF-INC-001: Informe post-incidente.

Indicadores de desempeño

Indicador	Meta	Frecuencia
Tiempo de respuesta inicial (N3-N4)	≤ 30 min desde detección	Mensual
% de incidentes con informe post-incidente (N2-N4)	100%	Mensual
Tiempo medio de contención (N3)	≤ 4 horas	Por incidente

PE.DGITI.03

Gestión de Vulnerabilidades Técnicas

Ref.: Secc.13.5, 15.4 / Anexo 7 / NIST CSF ID.RA / CIS Controls v8 #7

Versión: 1.0	Estado: Vigente	Revisión: Semestral	Dirección: DGITI
---------------------	-----------------	---------------------	------------------

Objeto: Identificar, priorizar, tratar y hacer seguimiento de vulnerabilidades técnicas en todos los activos institucionales, con plazos de remediación proporcionales al riesgo.

Roles

Rol	Responsabilidad en este procedimiento
Responsables de sistemas	Ejecutan escaneos, aplican parches, documentan el tratamiento.
RSI	Define la estrategia, aprueba excepciones y consolida reportes.
DGITI	Mantiene el inventario, coordina el proceso y reporta KPIs.
Propietario de la información	Aprueba ventanas de mantenimiento y acepta riesgo residual si aplica.

Plazos de remediación por severidad

Prioridad	Criterio	Plazo máximo de remediación
Crítica	CVSS $\geq$ 9.0 o exploit activo (CISA KEV) en sistema crítico	48 horas
Alta	CVSS 7.0-8.9 en sistema de criticidad alta	7 días
Media	CVSS 4.0-6.9	30 días
Baja	CVSS $<$ 4.0	90 días

Pasos del procedimiento

Fase 1 — Identificación y registro

1.1. La DGITI mantiene fuentes: NVD, CERT.ar, CISA KEV, boletines de fabricantes.

Escaneos automatizados: mensual para sistemas críticos, trimestral para el resto.

1.2. Toda vulnerabilidad se registra en REG-VUL-001 con: CVE, activo, CVSS, exposición, estado de parche y responsable.

Fase 2 — Priorización

2.1. Se combina CVSS score + criticidad del activo (Anexo 11) + exposición a Internet + presencia en CISA KEV + datos personales involucrados.

Fase 3 — Tratamiento

3.1. Tratamiento preferente: parche oficial. Cuando no disponible: controles compensatorios temporales documentados (WAF, regla de firewall, deshabilitación de componente).

3.2. Parches en sistemas productivos requieren autorización del propietario para ventana de mantenimiento. Para críticos, la ventana no excederá 48 hs. Para sistemas SIU/plataformas de terceros, el plazo corre desde disponibilidad del parche oficial, con seguimiento documentado y controles compensatorios hasta su aplicación.

3.3. Si el tratamiento no es factible en el plazo: excepción en REG-VUL-001 con control compensatorio y aceptación formal del riesgo residual por el RSI.

Fase 4 — Verificación y cierre

4.1. Tras la aplicación del parche/control: verificación mediante re-escaneo o prueba técnica. Cierre registrado en REG-VUL-001 con fecha, responsable y método de verificación.

4.2. El RSI consolida mensualmente el estado del parque de vulnerabilidades y reporta al Comité.

Indicadores de desempeño

Indicador	Meta	Frecuencia
Tiempo medio de remediación de vulnerabilidades críticas	≤ 48 horas	Por ciclo
Tiempo medio de aplicación post-disponibilidad (SIU / terceros)	≤ 5 días hábiles	Por ciclo
% de activos críticos escaneados mensualmente	100%	Mensual
Vulnerabilidades CVSS ≥ 7 pendientes >30 días sin justificación	0	Mensual

PE.DGITI.04

Gestión de Respaldos y Pruebas de Restauración

Ref.: Secc.13.3 / Anexos 2, 8, 10 / ISO 27002:2022 A.8.13 / NIST CSF RC.RP

Versión: 1.0	Estado: Vigente	Revisión: Anual	Dirección: DGITI
---------------------	-----------------	-----------------	------------------

Objeto: Establecer criterios, frecuencias y verificación de copias de seguridad, incluyendo pruebas de restauración periódicas.

Roles

Rol	Responsabilidad en este procedimiento
Responsable del sistema	Implementa y supervisa la ejecución de los respaldos. Reporta fallas.
DGITI	Define estándares técnicos y coordina pruebas de restauración.
Propietario de la información	Define criticidad, RPO/RTO y valida la estrategia.
RSI	Supervisa coherencia con gestión de riesgos y continuidad.

Pasos del procedimiento

Fase 1 — Diseño y configuración

- 1.1. Para cada sistema del Anexo 11, el responsable documenta en REG-BCK-001: tipo de respaldo, frecuencia, horario, retención, repositorio, herramienta, credenciales y responsable.
- 1.2. Estrategia mínima para sistemas críticos: respaldo completo semanal + incremental diario + retención 30 días. Al menos una copia lógicamente aislada o fuera de sitio.
- 1.3. Respallos con datos personales o información Confidencial/Reservada: cifrado AES-256 obligatorio. Claves custodias de manera independiente al repositorio.

Fase 2 — Ejecución y monitoreo

- 2.1. Ejecución automatizada. El sistema genera alertas ante fallas.

2.2. El responsable del sistema verifica diariamente el estado de respaldos de sistemas críticos. Fallas no resueltas en 4 horas se escalan a la DGITI.

2.3. El RSI recibe reporte semanal consolidado del estado de respaldos de sistemas críticos.

Fase 3 — Pruebas de restauración

3.1. Frecuencias mínimas de pruebas: Criticidad 1 (Críticos): mensual. Criticidad 2 (Alto): trimestral. Resto: semestral.

3.2. Cada prueba se documenta en FORM-REST-001: sistema, fecha, responsable, tipo de restauración, tiempo efectivo, integridad validada, desvíos y resultado.

3.3. Los resultados se comparan con RTO y RPO del Anexo 11. Las brechas se incorporan al plan de tratamiento de riesgos.

Indicadores de desempeño

Indicador	Meta	Frecuencia
% de sistemas críticos con respaldo exitoso en el período	≥ 99%	Semanal
% de pruebas de restauración realizadas según frecuencia	100%	Trimestral
% de restauraciones que cumplen el RTO definido	≥ 90%	Por prueba

PE.DGITI.05

Evaluación de Seguridad en la Contratación de Proveedores TI

Ref.: Secc.16 / Anexo 4 / ISO 27002:2022 A.5.19-5.22 / NIST CSF GV.SC

Versión: 1.0	Estado: Vigente	Revisión: Anual	Dirección: DGITI
--------------	-----------------	-----------------	------------------

Objeto: Establecer criterios y actividades mínimas de evaluación de seguridad antes, durante y al cierre de la contratación de proveedores de tecnología.

Roles

Rol	Responsabilidad en este procedimiento
Área de contrataciones	Inicia el proceso. Incorpora cláusulas de seguridad al pliego.
DGITI	Realiza la evaluación técnica de seguridad previa a la contratación y supervisa durante la vigencia.
RSI	Define criterios, emite dictamen y gestiona excepciones.
Área legal	Redacta y valida las cláusulas contractuales de seguridad.
Propietario de la información	Valida la criticidad de la información que el proveedor tratará.

Pasos del procedimiento

Fase 1 — Evaluación previa

1.1. La DGITI completa FORM-PROV-001: tipo de servicio, información involucrada, criticidad, modalidad de acceso, localización de datos y subproveedores.

1.2. Para servicios cloud: se evalúa el modelo de responsabilidad compartida, residencia de datos, portabilidad, SLA y derechos de auditoría.

1.3. El RSI emite dictamen: Apto, Apto con condiciones o No apto. El dictamen se articula dentro del circuito del Reglamento de Compras y Contrataciones aprobado por RES-1009/24 C.S. y sus modificatorias, y es requisito previo y esencial para continuar el proceso de contratación exclusivamente en aquellos casos que involucren tecnologías de la información, acceso a información institucional o tratamiento de datos personales, conforme el criterio objetivo (tipo de servicio, criticidad y/o monto) que defina la DGITI. El RSI emitirá el dictamen dentro de los diez (10) días hábiles de recibida la solicitud; vencido el plazo sin pronunciamiento, el área de contrataciones podrá continuar el trámite dejando constancia de la omisión, que resultará subsanable en cualquier estado del procedimiento previo a la adjudicación.

Fase 2 — Requisitos contractuales

2.1. El área legal incorpora cláusulas mínimas: confidencialidad; notificación de incidentes ≤ 24 hs; Ley 25.326; mínimo privilegio; restricción de subcontratación; derecho de auditoría; RTO/SLA; y devolución/eliminación de información al cierre.

Fase 3 — Supervisión durante la vigencia

3.1. La DGITI mantiene REG-PROV-001 con proveedores activos, accesos otorgados y estado de revisión.

3.2. Los accesos de proveedores son temporales o renovables. Ante incidente vinculado a un proveedor, se activa PE.DGITI.02 y se evalúa suspensión del acceso.

Fase 4 — Cierre del vínculo

4.1. Al finalizar el contrato, la DGITI verifica la revocación de todos los accesos y documenta la verificación en REG-PROV-001.

4.2. Se coordina la devolución, transferencia o eliminación certificada de la información institucional.

Indicadores de desempeño

Indicador	Meta	Frecuencia
% de contrataciones TI con dictamen RSI previo	100%	Por contratación
Accesos de proveedores vigentes sin contrato activo	0	Mensual
Tiempo de revocación de acceso al cierre del contrato	≤ 1 día hábil	Por cierre

PE.DGITI.06

Clasificación y Etiquetado de Activos de Información

Ref.: Secc.9 / Anexo 11 / ISO 27002:2022 A.5.10-5.12

Versión: 1.0	Estado: Vigente	Revisión: Anual	Dirección: DGITI
---------------------	-----------------	-----------------	------------------

Objeto: Identificar, clasificar, etiquetar y mantener el inventario de activos de información institucional como base para la gestión de riesgos y la aplicación proporcional de controles.

Roles

Rol	Responsabilidad en este procedimiento
Propietario de la información	Clasifica sus activos y aprueba el inventario de su área.
Responsable del sistema	Mantiene la información técnica del activo en el inventario.
DGITI	Establece la metodología, gestiona la herramienta y consolida el catálogo.
RSI	Supervisa la coherencia del inventario con la gestión de riesgos.

Niveles de clasificación de la información

Nivel	Definición	Controles mínimos aplicables
Pública	Sin restricción de acceso ni difusión	Sin restricciones especiales. Integridad básica.
Interna	Uso general de la comunidad universitaria	Acceso autenticado. No difundir sin autorización.
Confidencial	Acceso restringido a grupos específicos	Cifrado en tránsito. Acceso basado en roles. Registro de accesos.
Reservada	Acceso estrictamente limitado. Impacto grave si divulga	Cifrado en tránsito y en reposo. MFA. Auditoría de accesos. Aprobación del propietario para cada acceso.

Pasos del procedimiento

Fase 1 — Identificación

1.1. La DGITI provee la plantilla del Inventario de Activos (basada en Anexo 11). Cada área completa el inventario para los activos bajo su responsabilidad.

Fase 2 — Clasificación

2.1. El propietario de la información asigna el nivel de clasificación de la información (Pública/Interna/Confidencial/Reservada) y el nivel de criticidad del activo (1=Crítico a 4=Bajo) conforme al Anexo 11.

Fase 3 — Mantenimiento

3.1. El inventario se actualiza ante toda alta, baja o modificación significativa de activo, en plazo máximo de 5 días hábiles desde el cambio.

3.2. Revisión integral anual coordinada por la DGITI, con validación de cada propietario.

Indicadores de desempeño

Indicador	Meta	Frecuencia
% de sistemas críticos con ficha de activo completa y actualizada	100%	Semestral
Activos identificados sin propietario asignado	0	Semestral

PE.DGITI.07

Concientización y Capacitación en Seguridad

Ref.: Secc.8.2.2 / Anexo 5 / NIST CSF PR.AT / ISO 27002:2022 A.6.3

Versión: 1.0	Estado: Vigente	Revisión: Anual (Q1)	Dirección: DGITI
---------------------	-----------------	----------------------	------------------

Objeto: Mantener un programa institucional sostenido de concientización y capacitación en seguridad, con contenidos diferenciados por rol y medición de efectividad.

Roles

Rol	Responsabilidad en este procedimiento
DGITI	Diseña, ejecuta y evalúa el programa. Coordina con RRHH y Área Académica.
RSI	Define contenidos prioritarios según contexto de amenazas e incidentes recientes.
RRHH	Incorpora la capacitación de inducción en el proceso de ingreso.
Área académica	Facilita canales de comunicación con la comunidad estudiantil y docente.

Pasos del procedimiento

Fase 1 — Planificación anual

1.1. En Q1, la DGITI elabora el Plan Anual de Concientización (PAC-SEC-001) con: públicos objetivo, temas prioritarios, modalidades, cronograma, métricas y recursos.

Fase 2 — Contenidos por público objetivo

2.1. Todos los usuarios: contraseñas seguras, reconocimiento de phishing, uso aceptable, reporte de incidentes. E-learning obligatorio (≤ 30 min) + recordatorio semestral.

2.2. Personal con acceso a datos sensibles o sistemas críticos: protección de datos (Ley 25.326), información confidencial, teletrabajo seguro. Taller anual (90 min).

2.3. Administradores de sistemas: hardening, parches, respuesta a incidentes, seguridad en la nube, DevSecOps. Capacitación técnica semestral.

2.4. Autoridades y directivos: gobernanza de ciberseguridad, obligaciones del propietario de la información, gestión de riesgos. Sesión informativa anual (45 min).

Fase 3 — Simulacros de ingeniería social y phishing

3.1. Al menos 2 simulacros anuales de phishing sobre muestra representativa de usuarios, con análisis de tasa de clics y reportes generados. Los usuarios que interactúan reciben capacitación inmediata de refuerzo.

3.2. Los resultados son anónimos a nivel individual pero se reportan por área y se incorporan al plan de mejora.

Fase 4 — Medición y mejora

4.1. Al finalizar cada actividad: evaluación de conocimientos y encuesta de satisfacción.

4.2. El RSI elabora informe anual con: cobertura, tasas de completitud, resultados de evaluaciones y simulacros, y propuestas de mejora.

Indicadores de desempeño

Indicador	Meta	Frecuencia
% de personal con capacitación básica completada en el año	$\geq 80\%$	Anual
Tasa de clics en simulacros de phishing	Reducción $\geq 20\%$ interanual	Por simulacro
% de nuevos ingresos con inducción de seguridad en 30 días	$\geq 95\%$	Trimestral

PE.DGITI.08

Gestión de Cambios en Infraestructura y Sistemas

Ref.: Secc.13.1, 15 / ISO 27002:2022 A.8.32 / ITIL v4 Change Enablement

Versión: 1.0	Estado: Vigente	Revisión: Anual	Dirección: DGITI
---------------------	------------------------	------------------------	-------------------------

Objeto: Establecer un proceso controlado para la planificación, evaluación, aprobación, implementación y documentación de cambios en sistemas y entornos productivos, con evaluación de impacto en seguridad.

Roles

Rol	Responsabilidad en este procedimiento
Solicitante del cambio	Describe el cambio, justificación, impacto estimado y plan de rollback.
DGITI (CAB simplificado)	Evalúa, prioriza y aprueba o rechaza el cambio.
RSI	Evalúa el impacto en seguridad de cambios Normal, Urgentes y Mayores.
Responsable del sistema	Implementa el cambio y documenta el resultado.
Propietario de la información	Aprueba ventanas de mantenimiento y cambios que afecten disponibilidad.

Clasificación de cambios

Tipo	Descripción	Proceso de aprobación
Estándar	Pre-aprobados, bajo riesgo, procedimiento conocido	Ejecutar con documentación posterior
Normal	Requiere evaluación y aprobación	DGITI + RSI (si impacta seguridad)
Urgente	Emergencias, parche crítico activo	Aprobación expedita RSI + DGITI. Documentación posterior inmediata
Mayor	Alto impacto, cambio arquitectónico significativo	Propietario + RSI + DGITI + aprobación formal

Pasos del procedimiento

Fase 1 — Solicitud

1.1. Todo cambio en producción se solicita mediante RFC en FORM-CAM-001: descripción técnica, sistemas afectados, criticidad, ventana propuesta, plan de rollback e impacto en disponibilidad.

Fase 2 — Evaluación de seguridad

2.1. El RSI evalúa el impacto en seguridad de cambios Normal, Urgentes y Mayores. Criterios: modificación de controles de acceso, apertura de puertos, nuevos componentes con dependencias externas, cambios en autenticación o cifrado.

2.2. El rechazo del RSI es vinculante salvo autorización del Comité de Seguridad.

Fase 3 — Implementación y verificación

3.1. Se implementa en la ventana aprobada. Se verifica que exista respaldo del sistema antes de comenzar.

3.2. Ante desvíos significativos del plan, se activa el rollback y se notifica a la DGITI. El RSI verifica el estado de los controles de seguridad si el cambio los afectó.

Indicadores de desempeño

Indicador	Meta	Frecuencia
% de cambios Normal/Mayor/Urgente con RFC documentado	100%	Mensual
% de cambios sin incidente post-implementación	≥ 95%	Mensual

PE.DGITI.09

Evaluación Periódica de Riesgos de Seguridad

Ref.: Secc.5 / Anexo 9 7ISO/IEC 27005 / NIST CSF ID.RA

Versión: 1.0	Estado: Vigente	Revisión: Anual	Dirección: RSI / DGITI
---------------------	-----------------	-----------------	------------------------

Objeto: Evaluar formalmente y de manera periódica los riesgos de seguridad de la información, asegurando que los riesgos sean identificados, analizados, priorizados y tratados con planes documentados y aprobados.

Roles

Rol	Responsabilidad en este procedimiento
RSI	Conduce el proceso, consolida la matriz y presenta al Comité.
DGITI	Aporta datos de vulnerabilidades (PE.DGITI.03) e incidentes (PE.DGITI.02).
Propietarios de la información	Participan en la valoración de impacto.
Responsables de sistemas	Aportan información técnica sobre vulnerabilidades y dependencias.
Comité de Seguridad	Revisa y aprueba la matriz. Valida aceptaciones de riesgo alto.

Pasos del procedimiento

Fase 1 — Preparación

1.1. El RSI convoca a los participantes con al menos 10 días hábiles de anticipación. Se parte del inventario actualizado (PE.DGITI.06), resultados de PE.DGITI.03 e historial de incidentes (PE.DGITI.02).

Fase 2 — Identificación y análisis

2.1. Para cada activo se identifican amenazas y vulnerabilidades. Se estima Probabilidad (1-5) e Impacto (1-5) sobre CIA + cumplimiento.

2.2. Nivel de riesgo = $P \times I$ (escala 1-25): Bajo (1-4), Medio (5-9), Alto (10-16), Crítico (17-25).

Fase 3 — Tratamiento y registro

3.1. Cada riesgo se documenta en MAT-RIE-001 con: activo, propietario, amenaza, vulnerabilidad, controles existentes, riesgo inherente, tratamiento (evitar/reducir/transferir/aceptar), responsable, plazo y riesgo residual.

3.2. Riesgos Alto y Crítico requieren plan de tratamiento aprobado. Riesgos Críticos se elevan al Comité. La aceptación de riesgo residual alto requiere firma del propietario y del RSI.

Fase 4 — Seguimiento

4.1. El RSI reporta trimestralmente al Comité el estado de los planes de tratamiento de riesgos altos y críticos.

Indicadores de desempeño

Indicador	Meta	Frecuencia
Evaluación de riesgos integral realizada	1 vez / año	Anual
% de riesgos altos/críticos con plan de tratamiento documentado	100%	Trimestral
% de planes de tratamiento con avance verificado en el período	≥ 80%	Trimestral

PE.DGITI.10

Gestión de Continuidad, Contingencia y Recuperación ante Desastres

Ref.: Secc.18 / Anexos 2, 10, 11, 16 / ISO 22301 / ISO/IEC 27031 / NIST SP 800-34 / NIST SP 800-184

Versión: 1.0	Estado: Vigente	Revisión: Anual	Dirección: RSI / DGITI
--------------	-----------------	-----------------	------------------------

Objeto: Planificar, implementar, probar y mantener la continuidad, contingencia y recuperación ante desastres de los servicios críticos de la UNNE, incluyendo criterios de activación, conmutación, recuperación, retorno a la normalidad, pruebas, bitácora y mejora continua.

Roles

RSI: coordina la activación del procedimiento, evalúa el impacto de seguridad, articula con el Comité y asegura el registro de decisiones. DGITI: conduce la recuperación técnica, coordina administradores, redes, infraestructura, sistemas y proveedores. Propietario funcional: prioriza el servicio, valida la recuperación y aprueba el retorno a la operación normal. Responsable técnico: ejecuta playbooks, restaura componentes y documenta evidencias. Comunicación institucional: gestiona mensajes internos y externos autorizados. Comité de Seguridad: interviene en contingencias críticas, aceptación de riesgos residuales y priorización institucional.

Disparadores

El procedimiento podrá activarse ante indisponibilidad de sistemas críticos, pérdida o corrupción de datos, incidente de ciberseguridad con impacto operativo, ransomware, falla masiva de infraestructura, indisponibilidad prolongada del centro de datos, interrupción energética o de comunicaciones, desastre físico, falla de proveedor crítico o resultado insatisfactorio de pruebas que exija operación de contingencia.

Pasos del procedimiento

Fase 1 — BIA, planificación y preparación

- 1.1. La DGITI, con intervención del RSI y los propietarios funcionales, conduce el Análisis de Impacto al Negocio o al Servicio (BIA-001) al menos anualmente para identificar servicios críticos, procesos sustentantes, consecuencias por período de interrupción, dependencias y recursos mínimos de recuperación.
- 1.2. El BIA determina RTO, RPO, criticidad, orden de recuperación y modalidad de recuperación por servicio, actualizando el Anexo 11 y los planes específicos PLAN-CONT-001.
- 1.3. Para cada servicio crítico se documenta un plan con: alcance, responsables, contactos 24x7, dependencias, ubicación de respaldos, recursos requeridos, estrategia de recuperación, procedimientos manuales de emergencia, criterios de validación, riesgos residuales y evidencias esperadas.
- 1.4. Los planes deberán alinearse con el Anexo 2, Anexo 10, Anexo 11 y Anexo 16. La existencia de respaldos no reemplaza la obligación de contar con procedimientos de recuperación probados.

Fase 2 — Detección, evaluación y activación

- 2.1. Ante una contingencia o evento con impacto en un servicio crítico, el responsable técnico notifica inmediatamente al RSI, a la DGITI y al propietario funcional, indicando servicio afectado, alcance conocido, hora de detección, impacto preliminar, sistemas dependientes y medidas iniciales.
- 2.2. El RSI y la DGITI evalúan el alcance y determinan si corresponde activar el plan. Para criticidad alta o crítica, se informa al Comité de Seguridad y a la máxima autoridad que corresponda.
- 2.3. La activación debe quedar registrada en BIT-CONT-001 con fecha, hora, responsable, causa, servicio afectado, decisión adoptada, nivel de criticidad, plan activado y próximos pasos.
- 2.4. Cuando el evento tenga posible origen malicioso, se coordinará con el procedimiento de respuesta a incidentes, preservando evidencia y evitando restaurar sistemas comprometidos sin validación previa.

Fase 3 — Conmutación y operación en contingencia

3.1. La DGITI ejecuta el playbook de conmutación correspondiente: activación de sitio alternativo, restauración en infraestructura alterna, operación degradada, uso de procedimientos manuales o derivación temporal de servicios, según el escenario previsto.

3.2. La conmutación deberá respetar el orden de recuperación del Anexo 11, salvo decisión fundada del Comité o de la autoridad designada. Toda alteración del orden se registrará en la bitácora.

3.3. Durante la operación en contingencia se mantendrán controles mínimos de seguridad: autenticación, autorización, segmentación, logging, cifrado cuando corresponda, protección de credenciales y monitoreo de eventos.

Fase 4 — Recuperación técnica y validación

4.1. La recuperación se ejecuta conforme al plan específico del servicio. Incluye restauración de datos, recuperación de máquinas virtuales, validación de integridad, verificación de conectividad, autenticación, dependencias, configuraciones, certificados, reglas de firewall y controles de seguridad.

4.2. Los tiempos reales de recuperación y el punto de recuperación alcanzado se comparan contra RTO y RPO. Toda desviación deberá documentarse, analizarse y elevarse como brecha para tratamiento. 4.3. El servicio no se declara recuperado hasta que el responsable técnico confirme la operación técnica, el RSI valide los controles de seguridad aplicables y el propietario funcional confirme que el servicio cumple su función institucional mínima.

Fase 5 — Retorno a la normalidad

5.1. El retorno al sitio o servicio normal requiere plan de reversa, ventana de ejecución, respaldo previo, validación de integridad, comunicación a usuarios afectados y autorización del propietario funcional con intervención del RSI.

5.2. Se verificará que no queden datos divergentes entre el ambiente de contingencia y el ambiente normal. En caso de divergencia, se documentará conciliación, pérdida máxima aceptada, responsable y decisión de negocio.

5.3. Finalizada la reversa, se confirmará normalización de monitoreo, respaldos, alertas, accesos, certificados, tareas programadas y controles de seguridad.

Fase 6 — Pruebas, bitácora y mejora continua

6.1. Los planes se probarán con periodicidad acorde a criticidad: tabletop semestral para servicios críticos, prueba técnica integral anual para servicios críticos, pruebas de restauración conforme PE.DGITI.04 y pruebas por muestreo para servicios de menor criticidad.

6.2. Toda prueba o contingencia real generará informe FORM-ENS-001 o INF-CONT-001 con alcance, participantes, tiempos alcanzados, RTO/RPO comparados, fallas, brechas, evidencias, acciones correctivas, responsables y plazos.

6.3. La bitácora BIT-CONT-001 será obligatoria durante contingencias reales y recomendable durante ejercicios integrales. Deberá incluir eventos, decisiones, responsables, evidencias y comunicaciones relevantes.

6.4. Las lecciones aprendidas actualizarán el Anexo 11, los planes PLAN-CONT-001, la política de respaldos, los lineamientos de máquinas virtuales críticas y el plan de tratamiento de riesgos.

Indicadores de desempeño

Indicador	Meta mínima	Frecuencia
% de servicios críticos con BIA vigente	100 %	Anual
% de servicios críticos con PLAN-CONT-001 vigente	100 %	Anual
% de pruebas de continuidad ejecutadas según plan	100 %	Anual / semestral según criticidad
% de pruebas con informe y plan de	100 %	Por prueba

remediación

Brechas RTO/RPO sin plan de tratamiento	0	Trimestral
Tiempo de activación del plan desde detección	Según criticidad definida	Por contingencia
% de contingencias con bitácora Complete	100 %	Por evento

Fin de los procedimientos derivados

Los diez procedimientos conforman el cuerpo operativo de la Normativa de Ciberseguridad UNNE versión 2.3. Todos deben ser formalizados mediante resolución del área competente, asignarse a un responsable de custodia documental y revisarse conforme al ciclo establecido en cada procedimiento. La DGITI coordinará la implementación progresiva conforme al criterio de priorización indicado en la tabla de índice de procedimientos.

Hoja de firmas



Sistema: sudocu

Fecha: 27/08/2026 08:27:44

Cargado por: CECILIA INES VIEYRA



Sistema: sudocu

Fecha: 27/08/2026 10:00:09

Autorizado por: PATRICIA BEL DEMUTH MERCADO



Sistema: guarani

Fecha: 27/08/2026 12:12:06

Autorizado por: GERARDO OMAR LARROZA