UNIVERSIDAD DE TARAPACÁ
ARICA – CHILE

APRUEBA PROCEDIMIENTO DEL PLAN DE CONTINGENCIA DE LA UNIVERSIDAD DE TARAPACÁ.

DECRETO EXENTO N° 00.922/2025.

Arica, julio 24 de 2025.

Con esta fecha la Rectoría de la Universidad de Tarapacá, ha expedido el siguiente decreto:

VISTO:

Lo dispuesto en el D.F.L. N° 150, de 11 de diciembre de 1981, del Ex Ministerio de Educación Pública; D.F.L. N° 16, de 27 de diciembre de 2023, publicado el 11 de julio de 2024, del Ministerio de Educación, Resolución Nº 36 de 2024 de la Contraloría General de la República; Resolución Exenta Universitaria CONTRAL. Nº0.01/2002, de enero 14 de 2002, Resolución Exenta Universitaria CONTRAL N°0.01/2025, de marzo 26 de 2025; Decreto Exento N°00.916/2025 de fecha 24 de julio de 2025, Carta VRD N°114/2025, de fecha 23 de julio de 2025, Carta REC. N°2269/2025 de fecha 23 de julio de 2025; los documentos adjuntos y las facultades que me confiere la letra i), punto Nº 3 del artículo 11, del D.F.L. Nº 150, ya citado en relación con el decreto Nº1605/84, de diciembre 14 de 1984; Decreto TRA Nº 335/9/2025, tomado de razón el 02 de junio de 2025.

CONSIDERANDO:

Que, la Universidad de Tarapacá es una Corporación de derecho público, autónoma y con patrimonio propio, dedicada a la enseñanza y al cultivo superior de las artes, las letras y las ciencias, que goza de una triple autonomía académica, económica, administrativa, dedicada a la enseñanza y cultivo superior de las artes, las letras y las ciencias, creada por D.F.L Nº 150, de 11 de diciembre de 1981, del Ex Ministerio de Educación Pública.

Que, mediante Oficio VRD N°114/2025, el Vicerrector de Desarrollo Estratégico solicitó oficializar, mediante decreto exento, el documento denominado "Procedimiento del Plan de Contingencia de la Universidad de Tarapacá", cuyo objetivo es establecer un conjunto de directrices, acciones y procedimientos técnicos y organizativos que garanticen la continuidad de los servicios críticos de información, minimizando el impacto de eventos disruptivos, resguardando los principios de confidencialidad, integridad y disponibilidad, en coherencia con la misión y visión institucional.

Que dicho procedimiento se enmarca en la implementación de la Actualización de la Política General de Seguridad de la Información de la Universidad de Tarapacá, aprobada por la Junta Directiva mediante el Acuerdo N°2354, y formalizada a través del Decreto Exento N°00.916/2025, de fecha 24 de julio de 2025.

El mérito de lo ordenado por el Dr. Emilio Rodríguez Ponce, Rector a través de carta REC N°2269/2025, de fecha 23 de julio de 2025.

DECRETO:

1. Apruébese el documento denominado **"PROCEDIMIENTO DEL PLAN DE CONTINGENCIA DE LA UNIVERSIDAD DE TARAPACÁ",** contenido en documento adjunto compuesto de diecinueve (19) páginas, rubricadas por el Secretario de la Universidad.

2. Publíquese, en el sistema informático conforme lo señalado en el art. 7 de la Ley N°20.285 de 2008, del Ministerio Secretaria General de la Presidencia, sobre Acceso a la información pública.

Anótese, y remítase a la Contraloría de la Universidad, para su control y registro. Comuníquese una vez tramitado totalmente el acto.

UNIVERSIDAD DE TARAPACA SECRETARIO DE LA UNIVERSIDAD ARICA

ÁLVARO PALMA QUIROZ
Secretario de la Universidad

UNIVERSIDAD DE TARAPACA RECTOR ARICA

JORGE BERNAL PERALTA
Rector(S)

JBP.APQ.yvv

UNIVERSIDAD DE TARAPACA CONTRALORA (S) ARICA

25 JUL 2025

PROCEDIMIENTO DEL PLAN DE CONTINGENCIA DE LA UNIVERSIDAD DE TARAPACÁ

1. Objetivo del Plan

1.1 Objetivo General:

Establecer un conjunto de directrices, acciones y procedimientos técnicos y organizativos que garanticen la continuidad de los servicios críticos de información, minimizando el impacto de eventos disruptivos. Todo ello, resguardando los principios de confidencialidad, integridad y disponibilidad, en coherencia con la misión y visión de la Universidad de Tarapacá.

1.2 Objetivos Específicos

- **Prevenir** interrupciones para asegurar la continuidad de la educación y la investigación, pilares de la misión.
- **Responder** ágilmente ante incidentes que puedan entorpecer la formación de personas con espíritu crítico y reflexivo.
- **Recuperar** sistemas prioritarios para mantener la calidad y confiabilidad institucional, tal como exige la visión.
- **Coordinar** a los equipos de Tecnologías de Información (TI), académicos y administrativos, promoviendo una gestión integral.
- **Asegurar** la continuidad de los procesos académicos y administrativos (matrícula, evaluaciones, clases), fortaleciendo el desarrollo sostenible y la equidad regional, conforme a misión y visión.

1.4 Justificación reforzada con enfoque institucional

Este plan garantiza que, frente a desastres, ciberataques u otros incidentes, la institución podrá:

- Mantener su excelencia académica, base de su misión.
- Asegurar procesos formativos sólidos, promoviendo la movilidad social, conforme a su visión.
- Responder a su compromiso con el desarrollo regional, especialmente en una zona extrema y fronteriza.
- Proteger la diversidad cultural, la integración intercultural y los patrimonios ancestrales, coherente con su sello institucional.

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

2. Alcance del Plan de Contingencias

2.1 Alcance General:

Este plan aplica a todos los activos de información, infraestructura tecnológica, procesos académicos y administrativos, y servicios digitales críticos de la Universidad de Tarapacá que puedan verse afectados por incidentes que comprometan la seguridad, continuidad u operación normal de sus actividades.

2.2 Ámbitos de aplicación:

a) Cobertura organizacional

Incluye a:

- Casa Central (Arica)
- Sede Iquique
- Sedes o centros regionales conectados en red
- Áreas académicas, administrativas y de gestión institucional
- Direcciones, Vicerrectorías y Rectoría

b) Cobertura técnica

Aplica a los siguientes entornos y activos:

- Servidores físicos y virtuales (on-premise o en nube)
- Red intercampus (LAN/WAN/VPN)
- Bases de datos académicas y administrativas
- Servicios de correo institucional
- Plataformas educativas
- Sitio web institucional y portales docentes
- Sistemas ERP de matrícula, finanzas y recursos humanos
- Aplicaciones móviles institucionales (si existen)
- Sistemas de respaldo y recuperación de desastres

2.3 Procesos críticos cubiertos

Proceso	Justificación de criticidad
• **Gestión de matrícula y aranceles**	Afecta directamente a la continuidad de estudios de estudiantes
• **Evaluaciones y actas académicas**	Procesos con fechas legales y efectos académicos
• **Plataforma educativa (clases)**	Base del proceso formativo, incluso en clases presenciales
• **Acceso a red intercampus**	Comunicación y sincronización entre sedes
• **Correo institucional**	Medio oficial de comunicación docente-administrativa
• **Gestión documental**	Procesos legales, certificados, licencias, convenios

Ficha 2.1 : Matriz de Procesos Críticos

2.4 Entornos físicos y virtuales incluidos

- Salas de servidores (Data Center) en Arica e Iquique
- Oficinas administrativas con puntos de red
- Estaciones de trabajo docentes y administrativas
- Sistemas en nube bajo contrato institucional (Google Workspace, Microsoft 365, AWS, etc.)
- Sistemas de videovigilancia digital (por vulnerabilidad a ataques)

3. Contexto Institucional

3.1 Identidad institucional

La Universidad de Tarapacá (UTA) es una universidad estatal chilena, con una marcada vocación pública, regional y de frontera. Desarrolla su labor principalmente en modalidad presencial, aunque complementada por el uso intensivo de tecnologías digitales, tanto en docencia como en gestión administrativa y académica.

3.2 Infraestructura geográfica

UTA cuenta con una Casa Central en Arica y una Sede en Iquique, además de centros universitarios o unidades que, aunque físicamente distantes, se encuentran conectados digitalmente mediante enlaces privados y/o VPN institucionales. Esta configuración interregional implica:

UNIVERSIDAD DE TARAPACÁ SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

- Dependencia de una infraestructura de red segura, resiliente y centralizada.
- Necesidad de sincronización permanente entre los sistemas académicos y administrativos de ambas ciudades.
- Riesgo de aislamiento operativo ante fallas en la red intercampus o del centro de datos.

3.3 Dependencia tecnológica crítica

- A pesar del carácter mayoritariamente **presencial de sus clases**, la universidad depende de múltiples sistemas tecnológicos para funcionar de manera eficiente:

Área funcional	Dependencia tecnológica principal
• **Docencia presencial**	Acceso a plataformas, sistemas de asistencia y evaluaciones
• **Gestión estudiantil**	Sistema de matrícula, carga académica, registro de notas
• **Finanzas y administración**	Sistema de pagos, presupuestos, RRHH
• **Comunicación interna**	Correo institucional, intranet, videollamadas
• **Seguridad física**	Cámaras IP, acceso electrónico, sensores conectados

Ficha 3.1 : Matriz de Dependencia tecnológica Crítica

3.4 Vulnerabilidades inherentes al entorno

Debido a su contexto geográfico y operacional, UTA se enfrenta a amenazas específicas:

1. **Riesgos naturales**: Zona sísmica y costera, con exposición a terremotos y tsunamis.
2. **Interrupciones de red**: Por vandalismo en tendidos de fibra, fallas ISP o cortes eléctricos.
3. **Ataques cibernéticos**: Cada vez más comunes en instituciones públicas y educativas.
4. **Falta de redundancia física**: En algunos sistemas clave, si no existen servidores espejo o nube.
5. **Dependencia de recursos críticos centralizados**: (e.g., un solo data center para múltiples servicios).

3.5 Cultura organizacional y digital

Aunque UTA ha avanzado en la implementación de plataformas digitales, aún se observa:

UNIVERSIDAD DE TARAPACÁ SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

- Heterogeneidad en el uso y capacitación digital entre usuarios (docentes, funcionarios, estudiantes).
- Prácticas informales en el uso de contraseñas, dispositivos personales o almacenamiento externo.
- Escasa formalización de roles de respuesta ante incidentes en algunas unidades.

Esto requiere:

- Capacitación continua en ciberseguridad
- Refuerzo en la concientización institucional
- Formalización de protocolos de respuesta a incidentes

3.6 Relación con el entorno nacional

Como universidad pública chilena, UTA está sujeta a:

- Las normas y estándares de seguridad de la información emanadas por el Gobierno (CSIRT, Ministerio del Interior).
- Las buenas prácticas de continuidad operativa impulsadas por Contraloría General de la República y por el Decreto Supremo N° 83.
- Las expectativas de transparencia, trazabilidad y resiliencia tecnológica que exige la ciudadanía y la comunidad educativa.

3.7 En síntesis:

El contexto institucional de UTA, marcado por su presencialidad operativa, su infraestructura tecnológica interconectada y su compromiso regional y estatal, exige un plan de contingencias robusto, que considere:

- Su realidad geográfica y organizacional.
- Sus dependencias tecnológicas distribuidas.
- Sus riesgos naturales y cibernéticos.
- Su cultura institucional en proceso de digitalización.
- Su alineamiento normativo con el Estado de Chile.

4. Amenazas Identificadas.

El análisis de amenazas permite reconocer los eventos que podrían afectar la continuidad de los servicios críticos de la universidad. Se consideran amenazas naturales, tecnológicas, humanas e intencionadas, clasificadas según su probabilidad e impacto.

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

Riesgo / Amenaza	Tipo	Probabilidad	Impacto	Riesgo	Observación institucional
Terremoto o tsunami	Natural	Alta	Alta	Muy Alto	Zona sísmica y costera
Corte eléctrico prolongado	Técnico/operacional	Media	Alta	Alto	Algunas sedes sin respaldo UPS adecuado
Falla de red troncal entre sedes	Tecnológica	Media	Alta	Alto	Interconexión crítica por fibra o VPN
Ataques de ransomware	Cibernética	Alta	Alta	Muy Alto	Riesgo creciente en instituciones públicas
Infección por malware (USB, email)	Cibernética	Alta	Media	Alto	Uso de dispositivos personales sin control
Incendio en sala de servidores	Física	Baja	Alta	Alto	Centro de datos sin redundancia completa
Errores humanos (eliminación accidental)	Humana	Alta	Media	Alto	Prácticas informales en usuarios finales
Robo de equipos o fuga de información	Humana	Media	Alta	Alto	Portátiles sin cifrado o autenticación
Fallo de plataforma Moodle	Tecnológica	Media	Alta	Alto	Dependencia en procesos académicos críticos
Falla de sistemas informáticos	Tecnológica	Baja	Muy Alta	Alto	Afecta flujo financiero y académico clave
Vulnerabilidades no parcheadas	Tecnológica	Alta	Media	Alto	Falta de revisión constante de actualizaciones

Ficha 4.1 : Matriz de Evaluación de Riesgos

4.1 Observaciones clave para UTA:

1. Riesgos naturales (sísmicos y climáticos) son inevitables, pero deben ser mitigados con redundancia, respaldo y planes de evacuación.
2. La ciberseguridad es el principal riesgo emergente, especialmente en ransomware y accesos no autorizados.
3. La interdependencia entre sedes y plataformas académicas implica que una falla puede escalar rápidamente a nivel institucional.
4. El error humano sigue siendo uno de los vectores más comunes de pérdida de datos y accesos indebidos.
5. Amenazas internas (personas autorizadas con malas prácticas) requieren medidas de formación, monitoreo y control de privilegios.

4.2 Recomendación estratégica:

Esta matriz de amenazas debe revisarse al menos una vez al año o cada vez que:

- Se implementen nuevos sistemas críticos.
- Ocurran incidentes graves.
- Se modifiquen condiciones externas (e.g. sismos, infraestructura nueva, cambios regulatorios).

5. Clasificación de Sistemas Críticos

La clasificación de sistemas críticos permite priorizar recursos y esfuerzos durante un incidente, enfocados en la disponibilidad, confidencialidad e integridad de los datos, y en la dependencia operativa de los usuarios.

5.1 Criterios de clasificación

Se evaluaron los sistemas con base en:

Criterio	Descripción
Impacto académico	¿Afecta el proceso de enseñanza-aprendizaje directamente?
Impacto administrativo	¿Detiene procesos de gestión o financieros esenciales?
Alcance institucional	¿Cuántos usuarios se ven afectados (estudiantes, docentes, administrativos)?
Nivel de dependencia	¿Existe una alternativa viable si el sistema falla?
Tiempo de recuperación	¿Cuánto tiempo puede tolerarse su interrupción sin afectar funciones clave?

Ficha 5.1 : Matriz de Criterios de Clasificación

Sistema / Servicio	Clasificación de seguridad	Nivel de criticidad	Tiempo máximo tolerado (RTO)	Justificación técnica
Sistema de matrícula y carga académica	Confidencial	Muy Alto	2 horas	Esencial para el ciclo académico
Plataforma docencia virtual	Interna	Alto	4 horas	Usado para entrega de materiales, evaluaciones y clases híbridas
Sistema financiero (aranceles, pagos)	Confidencial	Muy Alto	4 horas	Afecta finanzas institucionales y servicios estudiantiles

Correo institucional	Interna	Alto	6 horas	Medio oficial de comunicación entre áreas y con estudiantes
Red intercampus (VPN, fibra óptica)	Interna	Muy Alto	1 hora	Si se cae, las sedes quedan aisladas
Sistema de gestión documental (certificados, actas)	Confidencial	Alto	6 horas	Contiene documentos legales y académicos oficiales
Plataforma de biblioteca digital	Interna	Medio	12 horas	Apoya el aprendizaje, pero tiene menor impacto inmediato
Sitio web institucional	Pública	Medio	24 horas	No detiene funciones internas, pero afecta imagen institucional
Sistema de videovigilancia y control de acceso	Interna	Medio	24 horas	Importante para seguridad física, pero no para operación académica

Figura 5.2: Tabla de clasificación por criticidad

5.2 Clasificación de criticidad (definiciones)

- **Muy Alto**: Interrupción implica detención total de funciones críticas. Afecta cumplimiento de calendario académico o financiero.
- **Alto**: Afecta seriamente la operación, pero no impide completamente la continuidad si se recupera en pocas horas.
- **Medio**: Impacta el soporte a procesos, pero con bajo riesgo legal o financiero inmediato.
- **Bajo**: Impacto limitado, sin consecuencias operativas graves.

5.3 Observaciones específicas para Universidad de Tarapacá:

- Los sistemas informáticos deben ser restaurados con prioridad absoluta, especialmente en periodos de inscripción, clases o cierre de semestre.
- La red intercampus requiere redundancia física o enlaces alternativos, dado que cualquier corte podría aislar totalmente las sedes.
- El correo institucional debe contar con planes de contingencia off-platform (SMS o comunicación física) en caso de caída prolongada.

6. Estrategias de Contingencia.

Las estrategias de contingencia se estructuran en tres fases principales: Prevención, Respuesta y Recuperación. Cada una contiene medidas técnicas, organizativas y comunicacionales diseñadas para mitigar riesgos identificados en los puntos anteriores.

6.1 Prevención

Acciones orientadas a reducir la probabilidad de que un incidente ocurra o a minimizar su impacto en caso de que ocurra.

6.1.1 Medidas preventivas clave:

1. **Respaldo de información**
   - Respaldos automáticos diarios de bases de datos académicas, administrativas.
   - Almacenamiento de respaldos en ubicaciones off-site (otra sede o nube).
   - Pruebas semestrales de restauración de respaldos.
2. **Redundancia en redes y servidores**
   - Enlaces redundantes entre sedes (fibra alternativa o enlaces móviles).
   - Balanceo de carga en servicios críticos si aplica.
   - Uso de entornos virtualizados para facilitar recuperación rápida.
3. **Seguridad lógica y física**
   - Autenticación multifactor (MFA) en sistemas administrativos y docentes.
   - Control de acceso físico a salas de servidores y puntos críticos.
   - Segmentación de red para aislar servicios y minimizar propagación de incidentes.
4. **Gestión de parches y vulnerabilidades**
   - Aplicación programada de actualizaciones de seguridad.
   - Escaneos mensuales con herramientas de análisis de vulnerabilidades.
   - Listas de software autorizado por la dirección que los administre.
5. **Capacitación y concientización**
   - Talleres semestrales de ciberseguridad para docentes, administrativos y estudiantes.
   - Difusión de buenas prácticas en manejo de contraseñas, correo, y dispositivos extraíbles.

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

- Campañas internas ante eventos críticos (inicio de semestre, periodos de matrícula).

6.2 Respuesta

Acciones a ejecutar inmediatamente después de detectar un incidente, con el fin de controlar y limitar los daños.

6.2.1 Medidas de respuesta:

1. **Activación del Comité de Seguridad de la Información**
   - Encabezado por el Oficial de Seguridad de la Información (OSI), con participación de unidades afectadas, si aplica.
2. **Escalamiento y registro**
   - Registro del incidente en bitácora digital.
   - Notificación inmediata a:
     - Dirección de Gestión Digital y Transparencia
     - Rectoría o Vicerrectoría de Desarrollo Estratégico
     - CSIRT Gobierno de Chile (en caso de ciberataques)
3. **Aislamiento del incidente**
   - Desconexión de sistemas comprometidos de la red.
   - Desactivación temporal de accesos externos si hay sospecha de ataque activo.
   - Interrupción de servicios no esenciales para proteger los prioritarios.
4. **Comunicación institucional**
   - Mensaje claro y coherente hacia la comunidad universitaria.
   - Uso de canales alternativos si el correo institucional está afectado.
   - Indicación de tiempos estimados de resolución y medidas transitorias.

6.3 Recuperación

Fase orientada a restablecer los servicios afectados y garantizar la vuelta a la normalidad operativa.

6.3.1 Medidas de recuperación:

1. **Restauración desde respaldos**
   - Prioridad a sistemas clasificados como "Muy Alto" y "Alto" (matrícula, Moodle, red).
   - Verificación de integridad antes de poner el sistema en producción.
2. **Conmutación a servicios espejo o alternativos**
   - Si hay servidores en otra sede o en nube, activar operación desde ahí.
   - Reasignación de tareas en unidades académicas si hay impacto prolongado.
3. **Análisis post-incidente**
   - Revisión de logs, vectores de ataque y puntos vulnerables.
   - Elaboración de informe técnico y comunicacional.
   - Recomendaciones de mejora y actualizaciones al plan.
4. **Apoyo a usuarios**
   - Guías prácticas para volver a operar los sistemas.
   - Canal de soporte extendido por parte de Dirección de Gestión Digital y Transparencia durante la reanudación.

7. Roles y Responsabilidades

Un plan de contingencia efectivo requiere una estructura organizacional clara que coordine la prevención, respuesta y recuperación ante incidentes que afecten la seguridad de la información y la continuidad operativa.

7.1 Estructura operativa de respuesta

Comité de Seguridad de la Información

Es el equipo que **coordina la gestión integral del incidente**. Se activa ante cualquier evento que comprometa sistemas críticos o interrumpa funciones relevantes.

Cargo / Área	Rol en el Comité
Oficial de Seguridad de la Información (OSI)	Lidera el comité, dirige las acciones, asesora a rectoría
Director(a) de Gestión Digital y Transparencia	Ejecuta planes técnicos, asigna equipos y recursos
Director(a) de Comunicaciones Estratégicas	Coordina la información oficial y canales alternativos

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

Representante jurídico / Secretaría General	Asesora en aspectos legales y contractuales
Encargado(a) de cada unidad afectada	Proporciona contexto funcional y prioridades

Figura 7.1: Tabla de Roles y Responsabilidades

Unidades operativas involucradas

Área / Unidad	Responsabilidades específicas
Dirección de Gestión Digital y Transparencia	Mantención de servidores, redes, UPS, respaldos, virtualización, red intercampus
	Atención directa a usuarios, reconfiguración de estaciones, restauración de accesos
	Verificación de integridad de sistemas internos, parches, respaldo de bases de datos
Dirección de Calidad Institucional	Coordinación con docentes y jefaturas para continuidad educativa
Dirección de Administración y Finanzas	Activación de procedimientos alternativos ante caída del ERP o pagos
Dirección de Admisión Comunicaciones Estratégicas	Redacción de mensajes, avisos a la comunidad, uso de redes sociales o medios externos

Figura 7.2: Tabla de Unidades involucradas

7.2 Responsabilidades documentales y legales

- **El OSI** debe documentar todos los incidentes mayores, generar informes post-incidente y proponer mejoras.
- **Rectoría y Secretaría General** deben evaluar el impacto institucional y si corresponde emitir comunicados públicos o notificaciones legales.
- **La Dirección de Gestión Digital y Transparencia** debe mantener actualizados los inventarios de sistemas críticos y respaldos.

Responsabilidad de notificación externa (casos críticos)

En caso de ciberataques, fugas de información o interrupciones mayores:

- **Notificar a CSIRT Gobierno (https://www.csirt.gob.cl/)**: obligación para instituciones públicas o con sistemas financiados por el Estado.
- **Notificar a proveedores de nube o servicios críticos** si el incidente involucra plataformas contratadas.

UNIVERSIDAD DE TARAPACÁ SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

8. Planes de Escenario Específicos

Cada escenario contempla una situación de contingencia concreta, con sus correspondientes acciones preventivas, de respuesta inmediata y de recuperación, definidas por áreas responsables.

A. Corte prolongado de energía eléctrica

Riesgo:

Fallo eléctrico generalizado en campus o sedes, sin respaldo suficiente.

Impacto:

- Caída de servidores y redes locales.
- Interrupción de clases presenciales y servicios administrativos.
- Riesgo de corrupción de datos si no hay apagado controlado.

Estrategia:

Fase	Acción
Prevención	Instalación de UPS en servidores y switches principales; evaluación de generadores
Respuesta	Apagar ordenadamente servidores no respaldados, notificar a usuarios
Recuperación	Encendido secuencial tras restablecer energía, verificación de sistemas críticos

Figura 8.1 Estrategia ante cortes prolongados

B. Ataque de ransomware o ciberataque mayor

Riesgo:

Cifrado malicioso de información en servidores o estaciones; pérdida de acceso.

Impacto:

- Secuestro de datos críticos (Moodle, matrícula, finanzas).
- Caída de servicios y redes.
- Posible daño reputacional.

UNIVERSIDAD DE TARAPACÁ SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

Estrategia:

Fase	Acción
Prevención	Copias de seguridad offline y pruebas de restauración; filtrado de correo
Respuesta	Desconectar inmediatamente sistemas infectados; activar Comité de Seguridad de la Información
Recuperación	Restaurar desde respaldos limpios; cambio de contraseñas institucionales

Figura 8.2 Estrategia ante ataques cibernéticos

C. Falla de red intercampus o colapso de conexión a internet

Riesgo:

Caída del enlace troncal entre Arica e Iquique o interrupción general del ISP.

Impacto:

- Incomunicación total entre sedes.
- Pérdida de acceso a plataformas externas y correo.
- Imposibilidad de sincronizar datos entre sistemas.

Estrategia:

Fase	Acción
Prevención	Redundancia de enlaces (segundo ISP, enlaces móviles, VPN alterna)
Respuesta	Derivar tráficos críticos a enlaces alternativos, uso de plataformas locales
Recuperación	Reestablecer comunicación, verificar integridad de datos sincronizados

Figura 8.3 Estrategia ante fallas de comunicación

D. Incendio o daño físico en sala de servidores

Riesgo:

Pérdida o destrucción de infraestructura TI local por fuego, agua o sismo.

Impacto:

- Interrupción total de servicios alojados en sitio afectado.
- Posible pérdida de datos si respaldos son locales únicamente.

Estrategia:

Fase	Acción
Prevención	Detectores térmicos, extintores especializados, sala con climatización y control de acceso
Respuesta	Corte de energía, activación de protocolo de emergencia institucional, respaldo de data reciente
Recuperación	Activar servidores espejo o nube (si existen), restaurar desde respaldo off-site

Figura 8.4 Estrategia ante daño en Sala de Servidores

E. Pérdida de datos por error humano o eliminación accidental

Riesgo:

Borrado de registros académicos, archivos docentes o configuraciones clave.

Impacto:

- Dificultad para recuperar evaluaciones, actas, certificados, etc.
- Repetición de procesos administrativos o académicos.

Estrategia:

Fase	Acción
Prevención	Política de respaldo automático y puntos de restauración por sistema
Respuesta	Notificación inmediata a la Dirección de Gestión Digital y Transparencia, detención del sistema afectado si es necesario
Recuperación	Restaurar datos desde última copia disponible, revisión de logs para auditoría

Figura 8.5 Estrategia ante pérdida de datos

9. Comunicación y Notificación

En una contingencia, una buena gestión de la comunicación es tan importante como la respuesta técnica. Esta sección define cómo, cuándo, a quién y por qué medios se debe comunicar un incidente, garantizando la fluidez de la información y evitando desinformación, pánico o rumores.

Objetivos de la comunicación institucional en contingencias

1. Informar de forma **oportuna y clara** a toda la comunidad afectada.
2. Coordinar acciones entre unidades internas y autoridades institucionales.
3. Notificar a organismos estatales (como **CSIRT Chile**) cuando corresponda.

4. Proteger la imagen pública y la confianza en la institución.
5. Facilitar el retorno ordenado a la normalidad operativa.

Niveles de comunicación

A. Comunicación interna

Incluye rectoría, vicerrectorías, direcciones, unidades académicas y administrativas.

Medio	Uso previsto
Correo institucional (Google/M365)	Canal primario si está disponible
Intranet universitaria	Publicación de comunicados oficiales
Mensajería directa / llamadas	Para equipos técnicos y jefaturas claves
Grupos de WhatsApp institucionales	Apoyo informal si otros canales están caídos

Figura 9.1 Estrategia de Comunicación Interna

B. Comunicación externa (comunidad universitaria)

Estudiantes, docentes, administrativos, apoderados, público general.

Medio	Uso previsto
Sitio web institucional	Comunicados generales ante incidentes mayores
Redes sociales oficiales (UTA)	Difusión rápida y amplia (Facebook, Twitter, Instagram)
Correo masivo (SMTP alterno)	En caso de caída de Google Workspace o similar
Carteles o notas físicas en sedes	Contingencia total o caídas prolongadas

Figura 9.2 Estrategia de Comunicación Externa

C. Comunicación a entidades externas y autoridades

Destinatario	Condición para notificación
CSIRT Gobierno de Chile	Ante ciberataques, fuga de datos, ransomware, etc.
Proveedor de nube / software	Si el incidente afecta infraestructura contratada externamente
Contraloría / MINEDUC	Solo si afecta procesos auditables o procesos financieros críticos
Medios de comunicación	Solo bajo aprobación de rectoría y comunicado institucional oficial

Figura 9.3 Estrategia de Comunicación a entidades externas

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

Protocolo para incidentes críticos

1. El **Oficial de Seguridad de la Información (OSI)** informa al Director de Gestión Digital y Transparencia y al Comité de Seguridad de la Información.
2. Se redacta un **comunicado oficial interno y externo** (si aplica) validado por Rectoría y Comunicaciones.
3. Se publica por **canales oficiales y alternativos** según la disponibilidad de sistemas.
4. Se mantiene una **bitácora de comunicaciones** con fecha, contenido y medio utilizado.

Contenido mínimo de una comunicación de contingencia

- Fecha y hora del incidente
- Sistemas afectados
- Medidas en curso
- Acciones que debe tomar la comunidad (si aplica)
- Tiempo estimado de recuperación (si es conocido)
- Contacto oficial para dudas o reportes

Medidas complementarias

- **Simulacros de comunicación** institucional al menos una vez al año.
- Definición clara de **voceros oficiales** (ejemplo: Rector(a), Director de Gestión Digital y Transparencia, Director(a) de Admisión y Comunicaciones Estratégicas).
- Manual actualizado de **mensajes tipo** para incidentes comunes (caída de red, Moodle, ERP, etc.).

APC

UNIVERSIDAD DE TARAPACÁ
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

10. Pruebas y Actualizaciones del Plan

Un plan de contingencia no es estático: debe ser probado regularmente, ajustado tras cada incidente real o simulacro, y revisado conforme a la evolución institucional y normativa. Esto asegura que los procedimientos definidos no solo existan, sino que realmente funcionen cuando más se necesiten.

Historial de revisiones

El plan debe incluir un registro con fecha, responsable y motivo de cada actualización. Esto garantiza trazabilidad y mejora continua.

11. Referencias Normativas

El presente plan se elabora en cumplimiento y coherencia con el marco normativo chileno, así como con los estándares internacionales de seguridad de la información y continuidad operativa.

A. Normativa nacional y del sector público

Documento / Norma	Aplicación al plan
Decreto Supremo N° 83 (2004) – MINSEGPRES	Establece la Política de Seguridad de la Información del Estado. Fundamento general del presente plan.
Norma Técnica de Seguridad de la Información (DS N° 100, 2006)	Define principios de confidencialidad, integridad y disponibilidad para organismos públicos.
Ley N° 19.628 sobre Protección de la Vida Privada	Regula el tratamiento de datos personales y su protección.
Ley N° 21.180 de Transformación Digital del Estado	Promueve servicios digitales resilientes y seguros en organismos públicos.
Normas y recomendaciones del CSIRT de Gobierno	Aplicación directa ante ciberincidentes; modelo de respuesta, guías y reporte de eventos.
Contraloría General de la República (CGR) – Instrucciones sobre control interno y continuidad operativa en instituciones públicas.	

B. Normas y estándares internacionales

Estándar / Guía	Relevancia
ISO/IEC 27001	Norma internacional para sistemas de gestión de seguridad de la información (SGSI).

UNIVERSIDAD DE TARAPACÁ SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

ISO/IEC 27002	Buenas prácticas para implementar controles de seguridad.
ISO 22301	Gestión de continuidad del negocio. Marco clave para definir prioridades, impactos y recuperación.
NIST SP 800-34 Rev.1 (USA)	Guía para planes de contingencia en sistemas de información.
ITIL v4 – Gestión de Incidentes y Continuidad	Buenas prácticas para respuesta y recuperación operativa en entornos TI.

UNIVERSIDAD DE TARAPACÁ
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE