Universidad Central

SECRETARÍA GENERAL

RESOLUCIÓN N° 5030

MAT: APRUEBA EL PROTOCOLO DE AMENAZAS CON ARMAS EN REDES SOCIALES U OTROS MEDIOS DE LA UNIVERSIDAD CENTRAL DE CHILE.

Santiago, 04 de junio de 2026.

CONSIDERANDO:

1° Que el Protocolo tiene por objeto establecer un procedimiento institucional claro, sistemático y oportuno para la detección, evaluación, gestión y respuesta frente a amenazas que puedan afectar la seguridad de la comunidad universitaria, resguardando la integridad física de las personas, la continuidad operacional y la protección de las instalaciones universitarias;

2° Que el presente Protocolo será aplicable a todas las sedes, campus y dependencias de la Universidad Central de Chile, comprendiendo a estudiantes, académicos(as), funcionarios(as), proveedores y visitantes;

3° Que la Dirección de Administración y Servicios ha elaborado y propuesto el Protocolo de Amenazas con Armas en Redes Sociales u Otros Medios de la Universidad Central de Chile, con el propósito de fortalecer los mecanismos institucionales de prevención y respuesta frente a situaciones que puedan comprometer la seguridad de la comunidad universitaria.

VISTOS:

1° La Ley N° 19.628 sobre Protección de la Vida Privada, y sus modificaciones, que establece normas sobre el tratamiento y protección de los datos personales, debiendo resguardarse la confidencialidad, privacidad y dignidad de las personas involucradas en los procedimientos institucionales;

2° La Resolución N° 1156, de fecha 31 de enero de 2020, que Promulga acuerdo de la H. Junta Directiva que modifica la Resolución N° 4835/2018, sobre el Reglamento de Convivencia y Vida Estudiantil;

3° La Resolución N° 7438, de fecha 20 de noviembre de 2024, que Promulga acuerdo de la Junta Directiva que aprueba modificación del Reglamento Interno de Orden, Higiene y Seguridad de la Universidad Central de Chile;

4° El Memorándum N° 10/2026, de fecha 15 de mayo de 2026, del Jefe de Gabinete de Rectoría, mediante el cual solicita a esta Secretaría General la emisión de la correspondiente resolución que apruebe el Protocolo de Amenazas con Armas en Redes Sociales u Otros Medios de la Universidad Central de Chile;

5 El correo electrónico de fecha 04 de junio de 2026, remitido por la Directora de Administración y Servicios, mediante el cual adjunta el referido protocolo;

6° Las atribuciones contenidas en el Estatuto Orgánico de la Corporación.

RESUELVO:

1° Apruébase el "Protocolo de Amenazas con Armas en Redes Sociales u Otros Medios de la Universidad Central de Chile", cuyo texto se adjunta a la presente resolución y se entiende formar parte integrante de ella para todos los efectos legales e institucionales;

Universidad Central

SECRETARÍA GENERAL

2° *Las disposiciones contenidas en el Protocolo aprobado mediante la presente resolución deberán ser observadas por todas las autoridades, académicas y administrativas, así como por todas aquellas personas que, directa o indirectamente, intervengan en la gestión de situaciones comprendidas dentro de su ámbito de aplicación;*

3° *La presente resolución entrará en vigencia a contar de la fecha de su dictación.*

Anótese, comuníquese y archívese.

UNIVERSIDAD CENTRAL DE CHILE VICERRECTOR VICERRECTORÍA DE ADMINISTRACIÓN Y FINANZAS

MARIO PINTO ASTUDILLO
VICERRECTOR DE ADMINISTRACIÓN Y FINANZAS

UNIVERSIDAD CENTRAL RECTOR SANTIAGO - CHILE

SANTIAGO GONZÁLEZ LARRAÍN
RECTOR

UNIVERSIDAD CENTRAL DE CHILE FISCAL

UNIVERSIDAD CENTRAL DE CHILE SECRETARIO GENERAL SANTIAGO - CHILE

NEFTALÍ CARABANTES HERNÁNDEZ
SECRETARIO GENERAL

NCH/JGS/JLM/ngf
c.c.: Junta Directiva - Rectoría - Secretaría General - Fiscalía - Contraloría - Vicerrectorías - Facultades - Direcciones de Carreras - Sede Región de Coquimbo - Dirección de Gestión de la Docencia - Dirección de Comunicaciones Corporativas - Dirección de Aseguramiento de la Calidad - Dirección de Desarrollo de Personas - Archivo.

Universidad Central

SECRETARÍA GENERAL

PROTOCOLO DE AMENAZAS CON ARMAS EN REDES SOCIALES U OTROS MEDIOS.

1. OBJETIVO

El presente protocolo tiene por objeto establecer un procedimiento institucional claro, sistemático y oportuno para la detección, evaluación, gestión y respuesta frente a amenazas que puedan afectar la seguridad de la comunidad universitaria, resguardando la integridad física de las personas, la continuidad operacional y la protección de las instalaciones.

Asimismo, busca estandarizar los criterios de actuación, asegurar la coordinación entre las distintas unidades involucradas y permitir la trazabilidad completa de cada evento, facilitando la mejora continua de los procesos de seguridad Universidad.

2. ALCANCE

Este protocolo será aplicable a todas las sedes, campus y dependencias de la Universidad, incluyendo a estudiantes, funcionarios, académicos, proveedores y visitantes, sin excepción.

Las disposiciones contenidas en este documento deberán ser observadas por todas las unidades que, directa o indirectamente, participen en la gestión de situaciones de riesgo o emergencias.

3. PRINCIPIOS GENERALES DE ACTUACIÓN

Toda gestión de amenazas deberá regirse por los siguientes principios:

- ***Prevención:***
  *Se establece mediante la implementación de **sistemas de monitoreo permanente**, levantamiento de información relevante y evaluación continua. Toda señal o indicio de amenaza deberá ser sometido a un **proceso breve de análisis técnico de seguridad**, evitando su desestimación sin fundamentos ejecutable.*

- ***Oportunidad:***
  *Las acciones de respuesta deberán ejecutarse bajo criterios de **inmediatez y eficiencia**, reduciendo al mínimo los tiempos de reacción desde la detección de la amenaza. Este principio implica la activación expedita de protocolos, la utilización de canales de comunicación expeditos y la toma de decisiones, con el objetivo de **proteger la integridad física de la comunidad universitaria,** evitando la escalada del riesgo mayor.*

- ***Proporcionalidad:***
  *Toda medida adoptada deberá responder a un criterio de **ajuste y coherencia con el nivel de riesgo evaluado**, evitando tanto la sobrerreacción como la subestimación del evento. La respuesta operativa deberá basarse en una **evaluación de riesgos**, considerando variables como credibilidad de la amenaza, capacidad del agresor, inmediatez y nivel de exposición. Este principio busca optimizar recursos y asegurar intervenciones objetivas y técnicamente justificadas.*

- ***Reserva:***
  *La gestión de la información deberá regirse por criterios de **reserva, control y trazabilidad**, limitando su acceso exclusivamente a personal autorizado o comprometido en el proceso. Se deberán implementar mecanismos de resguardo de la información sensible (digital y física), **evitando filtraciones que puedan generar alarma pública**, interferir en procedimientos operativos del área de seguridad o afectar procesos investigativos. Asimismo, se deberá asegurar la integridad de la evidencia para fines legales y administrativos de la Universidad.*

- ***Coordinación:***
  *Las decisiones y acciones deberán desarrollarse bajo un enfoque de **articulación interinstitucional**, integrando de manera eficiente a las distintas áreas internas (seguridad, autoridades académicas, comunicaciones) y organismos externos (policías, servicios de emergencia). Este principio implica la existencia de **canales formales de comunicación, roles definidos, cadena de mando clara y protocolos de actuación conjunta**, con el fin de garantizar una respuesta sincronizada, eficaz y alineada con los objetivos de seguridad institucional.*

4. ACTIVACIÓN DEL PROTOCOLO

El protocolo se activará ante la recepción o detección de cualquier amenaza, entendida como toda comunicación, señal o indicio que sugiera la posible ocurrencia de un hecho que pueda afectar la seguridad.

Cualquier integrante de la comunidad universitaria que tome conocimiento de una amenaza deberá reportarla de manera inmediata a los canales oficiales definidos por la institución. Para estos efectos, se considerarán canales válidos:

- *Teléfono institucional de seguridad informados en la Alerta Ucentral.*
- *Correo electrónico seguridad@ucentral.cl / rodrigo.alvarado@ucentral.cl (Jefe de Seguridad)*
- *Presencial ante los Guardias de Seguridad o el Jefe de Seguridad de la Universidad.*

Desde el momento en que la amenaza es recepcionada por el Área de Seguridad, se entenderá activado el protocolo, debiendo iniciarse el registro del evento y la aplicación de las acciones descritas en el presente documento.

Toda amenaza deberá ser considerada potencialmente real hasta que su descarte sea efectuado mediante análisis técnico del área de seguridad.

5. PROCEDIMIENTO DE GESTIÓN DE LA AMENAZA

a) Recepción, registro e identificación inicial:

Una vez recepcionada la amenaza, el personal de seguridad deberá registrar de manera inmediata la información disponible, incluyendo fecha y hora, forma de ingreso, contenido del mensaje y antecedentes del emisor. Además de todos los registros del desarrollo del procedimiento.

b) Validación preliminar de la información:

El Área de Seguridad deberá efectuar un análisis inicial del contenido de la amenaza, evaluando su coherencia, lenguaje, nivel de detalle, referencias espaciales o temporales y posibles vínculos con hechos anteriores asignándole un nivel de riesgo.

Este proceso deberá ejecutarse de manera inmediata desde la recepción de la amenaza.

c) Captura y resguardo de evidencia:

Toda evidencia asociada a la amenaza deberá ser recopilada y resguardada de manera íntegra, incluyendo correos electrónicos, capturas de pantalla, enlaces, registros de llamadas y otros.

El tratamiento de esta información deberá garantizar la integridad de los datos y la correcta custodia de la evidencia, con el fin de permitir su eventual utilización por parte de las autoridades competentes.

d) Identificación del emisor y coordinación interna:

En la medida de lo posible, se deberá determinar el origen de la amenaza, identificando si corresponde a un estudiante, funcionario, proveedor o actor externo.

Para estos efectos, el Área de Seguridad deberá coordinarse con las unidades pertinentes, tales como Direcciones Académicas, Dirección de Desarrollo de Personas, Dave o áreas administrativas, según corresponda.

e) Evaluación del nivel de riesgo:

La amenaza será evaluada considerando su nivel de especificidad, la inmediatez de su posible ejecución, la capacidad operativa del emisor y la existencia de antecedentes previos.

En base a estos criterios, se clasificará el riesgo en tres niveles:

- ***Riesgo Alto:*** *Existe una amenaza específica, creíble e inminente, con potencial de afectar directamente a la comunidad Universitaria.*
- ***Riesgo Medio:*** *La amenaza presenta elementos de probabilidad, pero carece de evidencia concreta o inmediata.*
- ***Riesgo Bajo:*** *La amenaza es genérica o presenta baja probabilidad de materialización.*

6. ACTIVACIÓN DE LA COMISIÓN SEGURIDAD

En caso de que la evaluación determine un nivel de riesgo medio o alto, se procederá a la activación de la Comisión de Seguridad, en instancias Pasivas y Activas, señalando los responsables de la toma de decisiones estratégicas.

La convocatoria deberá realizarse inmediatamente desde la clasificación del riesgo, estableciendo un mando unificado que permita coordinar las acciones institucionales de la comunidad universitaria, en ausencia de los titulares, serán reemplazados por respectivos suplentes de los cargos.

La Comisión estará integrada por las autoridades definidas para cada sede y contará con el apoyo técnico del Área de Seguridad.

Comisión de Seguridad (Activo)

- *Sede Santiago: VRA, VRAF, DCC y Jefe de Seguridad.*
- *Sede Coquimbo: VRR, DA, DAF, DCC y Jefe de Seguridad.*

7. GESTIÓN DE LA COMUNICACIÓN

La comunicación interna y externa será centralizada a través de la Dirección de Comunicaciones, la cual será responsable de elaborar y difundir los mensajes oficiales.

Las comunicaciones deberán ser claras, oportunas y basadas en información verificada, evitando generar alarma innecesaria o desinformación.

Se establecerá un control estricto sobre la difusión de información, quedando prohibida la comunicación no autorizada por canales informales o redes sociales.

8. COORDINACIÓN CON AUTORIDADES EXTERNAS

Ante situaciones de riesgo medio o alto, el Jefe de Seguridad deberá establecer contacto inmediato con las autoridades policiales correspondientes, entregando los antecedentes disponibles para su evaluación y eventual intervención.

La coordinación con dichas instituciones deberá realizarse de manera permanente mientras la situación se mantenga activa.

9. IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

En función del nivel de riesgo, se podrán adoptar diversas medidas operativas, tales como el refuerzo de controles de acceso, la restricción de ingresos, la delimitación de perímetros de seguridad, la suspensión de actividades y el monitoreo intensivo mediante sistemas de cámaras de televigilancia.

Estas medidas deberán ser proporcionales al riesgo identificado y orientadas prioritariamente a la protección de las personas.

10. MEDIDAS DE RESPUESTA OPERATIVA

La Comisión de Seguridad evaluará la necesidad de implementar acciones extraordinarias, tales como evacuación o confinamiento, considerando factores como la ubicación de la amenaza, el tiempo de respuesta y las recomendaciones de las autoridades.

La ejecución de estas medidas deberá realizarse conforme a los planes de emergencia vigentes.

11. REGISTRO Y TRAZABILIDAD

Durante todo el proceso se deberá mantener un registro detallado de las acciones realizadas, decisiones adoptadas y comunicaciones emitidas, asegurando la trazabilidad completa del evento.

12. NORMALIZACIÓN DE LAS OPERACIONES

Una vez controlada la situación, la Comisión de Seguridad evaluará las condiciones para la reanudación de las actividades, autorizando el retorno a la normalidad de manera progresiva y segura.

Esta decisión deberá ser comunicada oficialmente a la comunidad mediante comunicado oficial.

13. CIERRE Y MEJORA CONTINUA

Finalizada la contingencia, se deberá elaborar un informe técnico que documente la gestión del evento, incluyendo la cronología de los hechos, las decisiones adoptadas, las brechas detectadas y las oportunidades de mejora.

14. NORMATIVA APLICABLE AL PROTOCOLO

En relación a la Ley N° 19.628 sobre Protección de la Vida Privada, establece y exige a la Universidad Central de Chile, que todo proceso de indagación o averiguación, que se realicen con la finalidad de esclarecer o constatar un hecho que vulneren o infrinjan las normativas de la Universidad, los participantes vinculados al proceso, debe resguardar la confidencialidad y dignidad de los involucrados, garantizando que el tratamiento de sus datos personales se realice conforme a principios de legalidad.

Finalmente, durante el esclarecimiento de una infracción o hechos constitutivos de delitos, la Universidad Central de Chile, deberá asegurar que el procedimiento se conduzca bajo los principios del debido proceso y en plena observancia de los ***Derechos Humanos****. Es indispensable garantizar la dignidad humana, evitando cualquier forma de discriminación o estigmatización, y respetar la presunción de inocencia, asegurando que las decisiones se basen en pruebas verificables y no en juicios anticipados.*

La imparcialidad debe regir las averiguaciones, evitando conflictos de interés y asegurando objetividad. Asimismo, se recomienda permitir el acompañamiento de la Dirección de Apoyo y Vida Estudiantil (DAVE), lo que refuerza la seguridad emocional y la transparencia. La Universidad Central de Chile, debe proteger contra represalias y garantizar la confidencialidad, evitando cualquier afectación a la reputación de la persona involucrada.

Finalmente, el proceso debe alinearse con los estándares internacionales de derechos humanos y los principios de igualdad y no discriminación, reafirmando que las denuncias o averiguaciones de esclarecimiento de un hecho, es también una oportunidad para fortalecer la justicia, la convivencia y el respeto en el ámbito educativo.

15. CONCLUSIÓN

El protocolo constituye una herramienta institucional clara y eficaz para enfrentar amenazas que afecten la seguridad universitaria. Su estructura integra principios de prevención, oportunidad, proporcionalidad, reserva y coordinación, asegurando un marco de actuación coherente y técnicamente fundamentado. La definición de procedimientos de activación, clasificación de riesgos y coordinación con autoridades internas y externas fortalece la capacidad de respuesta y evita improvisaciones.