



Universidad
Católica
de Cuenca

JEFATURA DE SEGURIDAD DE LA INFORMACIÓN

CÓDIGO: UC-JSI-
POL-001

Página 1 de 12



Universidad
Católica
de Cuenca

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

JUNIO, 2026

www.ucacue.edu.ec



CONTROL DE VERSIONES

Versión	Fecha	Descripción del cambio	Responsable	Clasificación
v1.0	15/06/2026	Creación inicial.	Seguridad de la Información	Confidencial — Uso interno institucional



1. INTRODUCCIÓN.

La Universidad Católica de Cuenca reconoce que la información institucional, en cualquier formato o soporte, constituye un activo esencial para el cumplimiento de sus funciones académicas, administrativas, investigativas y de vinculación con la sociedad.

La seguridad de la información y la protección de datos personales forman parte del marco de control institucional, de la transformación digital y de la responsabilidad de la Universidad frente a sus estudiantes, docentes, personal administrativo, graduados, proveedores y demás partes interesadas.

La presente Política se sustenta principalmente en la Constitución de la República del Ecuador, Reglamento de la Jefatura de Seguridad de la Información, el Reglamento de Estructura Orgánico Institucional, la Ley Orgánica de Educación Superior (LOES), Ley Orgánica de Protección de Datos Personales (LOPDP), en el Estatuto de la Universidad Católica de Cuenca, y en la norma ISO/IEC 27001:2022 como estándar internacional de referencia para la implementación del Sistema de Gestión de Seguridad de la Información.

En consecuencia, la Universidad emite la presente Política General de Seguridad de la Información como instrumento rector del SGSI institucional.

2. OBJETO.

Esta política establece los principios, compromisos, lineamientos y responsabilidades que rigen la seguridad de la información en la universidad, con el propósito de proteger la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y resiliencia de sus activos de información.

Sirve de base para la elaboración de políticas específicas, procedimientos, estándares, guías y demás documentación del Sistema de Gestión de Seguridad de la Información (SGSI). En caso de conflicto entre esta política y cualquier documento subordinado, prevalece la presente política general.

3. ALCANCE.

Esta Política es de cumplimiento obligatorio para toda la comunidad universitaria, así como para toda persona natural o jurídica que, por razón de su cargo, vínculo, contrato o relación funcional con la Universidad, acceda, utilice, trate, procese, almacene, custodie o transmita información institucional.

Aplica a la información física y digital, y a los activos que la soportan, en todas las sedes, campus y extensiones de la Universidad, incluyendo entornos de trabajo remoto y servicios tecnológicos operados en la nube o por proveedores externos autorizados.

4. DECLARACION DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN.

La Universidad declara que la presente Política constituye el marco rector para la protección de sus activos de información. Su finalidad es preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de dicha información.

 Universidad Católica de Cuenca	JEFATURA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: UC-JSI-POL-001 Página 4 de 12
---	--	--

La Universidad se compromete a implementar, mantener y mejorar de manera continua un SGSI basado en gestión de riesgos, alineado con la norma ISO/IEC 27001:2022, la normativa legal vigente y los objetivos institucionales. Para ello, promoverá una cultura de seguridad de la información en toda su comunidad, asegurando el cumplimiento de esta Política y el desarrollo progresivo de controles, procedimientos y mecanismos que permitan gestionar adecuadamente los riesgos e incidentes en esta materia.

5. MARCO NORMATIVO Y DOCUMENTOS DE REFERENCIA.

Instrumento	Descripción	Ámbito
Constitución de la República del Ecuador	Reconoce el derecho a la protección de datos personales y el habeas data como garantías fundamentales.	Nacional
Ley Orgánica de Educación Superior (LOES)	Establece las obligaciones de las instituciones de educación superior en materia de gestión segura y transparente de información institucional.	Nacional
Ley Orgánica de Protección de Datos Personales (LOPDP)	Define el régimen de protección de datos personales aplicable a la institución en su calidad de responsable del tratamiento.	Nacional
Reglamento General a la LOPDP	Desarrolla las obligaciones del responsable y encargado del tratamiento de datos personales.	Nacional
ISO/IEC 27001:2022	Estándar internacional para la implementación del Sistema de Gestión de Seguridad de la Información. Marco de referencia para la certificación institucional.	Internacional
Esquema Gubernamental de Seguridad de la Información (EGSI V3)	Marco de referencia técnico para la implementación de controles de seguridad en el sector público y entidades asimiladas.	Nacional - Referencial
Estatuto de la Universidad Católica de Cuenca	Instrumento rector del funcionamiento institucional; base para la adopción de políticas y normativa interna.	Institucional
Reglamento de Estructura Orgánico Institucional	Instrumento rector del funcionamiento institucional; base para la adopción de políticas y normativa interna.	Institucional
Reglamento de la Jefatura de Seguridad de la Información de la UCACUE.	Instrumento rector del funcionamiento del SGSI institucional.	Institucional



6. PRINCIPIOS RECTORES.

Principio	Descripción
Confidencialidad	La información será accesible únicamente a personas, procesos o sistemas expresamente autorizados.
Integridad	La información deberá mantenerse exacta, completa y protegida frente a modificaciones no autorizadas.
Disponibilidad	Los activos de información deberán estar accesibles para los usuarios autorizados cuando sean requeridos.
Responsabilidad proactiva	La institución demuestra el cumplimiento de sus obligaciones mediante documentación, evidencias y controles verificables, sin esperar a ser requerida para ello.
Proporcionalidad	Los controles de seguridad se diseñan en proporción al riesgo, la criticidad del activo y el contexto institucional. No se sobredimensionan ni se minimizan.
Mejora continua	El SGSI se revisará y fortalecerá de forma periódica, conforme al ciclo PDCA y a la evolución de riesgos y necesidades institucionales.
Privacidad por diseño y por defecto	La protección de la información se incorpora desde la concepción y configuración inicial de procesos, sistemas y servicios, no como un añadido posterior.
Mínimo privilegio	El acceso a la información y a los sistemas se limita a lo estrictamente necesario para el ejercicio de las funciones autorizadas de cada usuario.
Zero Trust	Ningún acceso se considera confiable por defecto. Toda solicitud de acceso se valida de acuerdo con el nivel de riesgo y los controles definidos, independientemente del origen.

7. DEFINICIONES.

Activo de información: Todo dato, sistema, servicio, proceso, infraestructura o recurso que tenga valor para la Universidad y requiera protección.

SGSI: Sistema de Gestión de Seguridad de la Información implementado por la Universidad para gestionar de forma sistemática la seguridad de la información.

JSI: Jefatura de Seguridad de la Información, unidad técnica responsable de coordinar e impulsar el SGSI institucional.

DTD: Dirección de Transformación Digital responsable de la gestión tecnológica institucional y de la articulación técnica con la JSI.

Incidente de seguridad: Evento que compromete o amenaza comprometer la confidencialidad, integridad o disponibilidad de la información o de los sistemas que la soportan.

LOPD: Ley Orgánica de Protección de Datos Personales del Ecuador.

MFA: Autenticación multifactor.



Riesgo de seguridad: Efecto de la incertidumbre sobre los objetivos de seguridad de la información, expresado mediante la probabilidad de ocurrencia y su impacto.

Propietario o dueño del activo: Unidad o autoridad responsable de un activo de información y de definir sus necesidades de protección y uso.

RAT: Registro de Actividades de Tratamiento de datos personales.

Tratamiento de datos personales: Toda operación realizada sobre datos personales, conforme a la LOPDP.

Zero Trust: Modelo de seguridad basado en verificación explícita y ausencia de confianza implícita por defecto.

8. COMPROMISO DE LAS AUTORIDADES.

Las autoridades de la Universidad, reconocen la seguridad de la información como un componente estratégico para la gestión institucional y se compromete a:

- Brindar respaldo visible al SGSI y promover su integración en la gestión universitaria.
- Asignar, en la medida de las posibilidades institucionales, los recursos humanos, técnicos, financieros y organizativos necesarios para el desarrollo progresivo del SGSI.
- Conocer y respaldar las políticas, planes, informes y propuestas que la Jefatura de Seguridad de la Información eleve a su consideración.
- Promover el cumplimiento de la normativa aplicable en seguridad de la información y protección de datos personales.
- Impulsar la mejora continua del SGSI a través de mecanismos de seguimiento, revisión y toma de decisiones.
- Establecer, mantener y revisar periódicamente objetivos de seguridad de la información alineados con esta Política y al Sistema de Gestión de Seguridad de la Información.

9. ROLES Y RESPONSABILIDADES.

9.1. Estructura de gobernanza.

La gobernanza de la seguridad de la información en la Universidad se articula a través de los siguientes niveles:

Nivel	Instancia	Responsabilidad principal
Estratégico	Comité de Seguridad de la Información (CSI)	Aprobar las Políticas de Seguridad de la Información y Protección de Datos Personales, así como, respaldar estratégicamente el SGSI. Supervisar, coordinar y dar seguimiento al SGSI, conforme a su resolución de conformación y reglamento interno.



Operativo	Jefatura de Seguridad de la Información	Coordinar, implementar, operar y mejorar el SGSI. Reportar al Comité y proponer políticas, planes y controles.
Operativo	Propietarios de activos y responsables de áreas	Identificar activos de información, valorar riesgos asociados y apoyar la aplicación de controles en sus unidades.
Usuario	Comunidad universitaria y terceros autorizados	Cumplir esta Política, reportar incidentes, eventos sospechosos, situaciones de riesgo o vulnerabilidades a la Jefatura de Seguridad de la Información.

9.2. Comité de Seguridad de la Información.

El Comité de Seguridad de la Información es la instancia colegiada de apoyo estratégico a la gobernanza del SGSI. Su composición, funciones y funcionamiento se rigen por la Resolución Rectoral de conformación correspondiente y por el reglamento interno del Comité.

9.3. Responsabilidades generales de la comunidad universitaria.

Todos los miembros que conforman la comunidad universitaria tienen las siguientes responsabilidades:

- Conocer y cumplir esta Política y los documentos derivados que resulten aplicables a su rol o función.
- Utilizar los activos de información institucionales exclusivamente para fines autorizados y dentro del marco de las funciones o actividades permitidas.
- Custodiar responsablemente las credenciales de acceso, dispositivos, documentos y demás recursos bajo su responsabilidad.
- Reportar de inmediato a la JSI cualquier incidente, evento sospechoso o vulnerabilidad que pueda afectar la seguridad de la información, a través de los canales habilitados para el efecto.
- Participar activamente en los programas de sensibilización y capacitación dispuestos por la Universidad.
- Devolver los activos institucionales y facilitar la revocación de los accesos correspondientes al término de la relación funcional, contractual o académica.
- El cumplimiento de las obligaciones previstas en esta Política se realizará respetando los derechos constitucionales, el debido proceso y la normativa aplicable. Asimismo, las actividades de control, monitoreo y revisión que ejerza la Jefatura de Seguridad de la Información en el ámbito de sus competencias se ejecutarán bajo criterios de necesidad, proporcionalidad, trazabilidad y confidencialidad, conforme a los procedimientos institucionales autorizados para garantizar la continuidad y seguridad de los servicios.



10. LINEAMIENTOS GENERALES.

Los lineamientos que se enumeran a continuación serán desarrollados progresivamente mediante políticas específicas, procedimientos y controles en el marco de la implementación del SGSI. Su inclusión en esta Política General establece el compromiso institucional de abordarlos de forma sistemática.

10.1. Gestión de activos de información.

La Universidad mantendrá un inventario progresivo y controlado de sus activos de información, asignando responsables y criterios de clasificación conforme a su criticidad, sensibilidad y uso de cada activo institucional.

10.2. Control de acceso e identidad.

El acceso a sistemas, redes, aplicaciones y repositorios institucionales se concederá de acuerdo con el principio de mínimo privilegio y Zero Trust. Los accesos deberán gestionarse mediante procesos formales de alta, modificación, revisión y baja.

10.3. Clasificación y tratamiento de la información.

La información institucional se clasificará según su nivel de sensibilidad y los riesgos asociados a su divulgación, alteración o indisponibilidad. Los datos personales recibirán el tratamiento que establece la LOPDP y la política institucional de privacidad y protección de datos personales.

10.4. Seguridad en talento humano.

La seguridad de la información se incorporará en el ciclo de vida de la relación institucional con autoridades, personal, practicantes, pasantes y terceros, incluyendo compromisos de confidencialidad, inducción, controles de acceso y devolución de activos.

La Dirección de Talento Humano, en coordinación con la JSI y las unidades competentes, deberá garantizar que los procesos de vinculación, cambio de funciones, desvinculación, suspensión o terminación de la relación laboral o contractual incluyan medidas de seguridad, confidencialidad, devolución de activos, revocatoria de accesos, transferencia ordenada de información institucional y recordatorio de obligaciones posteriores a la terminación de la relación.

10.5. Seguridad física y del entorno.

La Universidad establecerá medidas razonables de protección física para áreas, equipos y recursos críticos, de acuerdo con la naturaleza de cada activo y el riesgo identificado.

10.6. Seguridad de las operaciones y comunicaciones.

Las operaciones tecnológicas se ejecutarán bajo criterios de seguridad, con control de cambios, respaldo, monitoreo y uso de medios autorizados. El intercambio de información institucional sensible por canales no aprobados queda expresamente prohibido.

10.7. Ciberseguridad y monitoreo.



La Universidad implementará controles de ciberseguridad orientados a prevenir, detectar y responder a amenazas que afecten su infraestructura y servicios digitales, apoyándose en capacidades internas y, cuando corresponda, en servicios especializados de terceros autorizados.

Las actividades de monitoreo, revisión de logs, análisis de tráfico, auditoría de accesos, revisión de cuentas institucionales, inspección de dispositivos o investigación de incidentes deberán ejecutarse bajo criterios de necesidad, proporcionalidad, trazabilidad, confidencialidad, conforme a los procedimientos institucionales autorizados.

10.8. Protección de datos personales.

Todo tratamiento de datos personales deberá sustentarse en una base legal válida, una finalidad legítima y controles proporcionales al riesgo, conforme a la LOPDP, su reglamento y la política institucional de privacidad y protección de datos personales.

10.9. Gestión de incidentes de seguridad.

La Universidad contará con un proceso documentado para la gestión de incidentes de seguridad de la información, que contemplará las etapas de reporte, clasificación, atención, contención, recuperación, análisis y mejora.

10.10. Continuidad y resiliencia.

La Universidad promoverá medidas de continuidad y recuperación para sus procesos y servicios críticos, incluyendo respaldos, criterios de recuperación y planes progresivos de continuidad operativa.

10.11. Relaciones con proveedores y terceros.

Todo proveedor o tercero que acceda a información institucional deberá sujetarse a obligaciones de seguridad, confidencialidad y, cuando corresponda, de encargo de tratamiento de datos personales, conforme a la normativa y a los instrumentos contractuales aplicables.

10.12. Cumplimiento normativo.

La Universidad identificará y observará los requisitos legales, reglamentarios, contractuales e institucionales aplicables a la seguridad de la información y la protección de datos personales.

10.13. Concienciación y capacitación.

La Universidad promoverá una cultura institucional de seguridad de la información mediante programas de sensibilización, capacitación y comunicación adaptados a los distintos perfiles de usuarios. La participación en estos programas será obligatoria cuando así lo disponga la institución.

11. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

La Universidad adopta un enfoque basado en riesgos para gestionar la seguridad de la información, conforme a los lineamientos de ISO/IEC 27001:2022. Este enfoque implica:



- Identificar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.
- Evaluar dichos riesgos considerando su probabilidad de ocurrencia e impacto potencial.
- Definir e implementar medidas de tratamiento para mitigar, transferir, evitar o aceptar los riesgos identificados, con criterios documentados.
- Mantener la gestión de riesgos como un proceso continuo y dinámico, sujeto a revisión periódica y actualización ante cambios del entorno institucional o tecnológico.

La Universidad establecerá progresivamente metodologías, criterios y herramientas para la adecuada gestión de los riesgos de seguridad de la información, en función de las capacidades y prioridades institucionales.

12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

La Universidad establecerá y mantendrá un proceso documentado para la gestión de incidentes de seguridad de la información, con el fin de minimizar su impacto y evitar su recurrencia. Dicho proceso contemplará:

- La obligación de todo usuario de reportar oportunamente a la JSI cualquier evento o sospecha de incidente de seguridad, a través de los canales habilitados.
- La clasificación de los incidentes por nivel de severidad y su atención conforme a los procedimientos definidos por la JSI.
- Las etapas de reporte, clasificación, contención, recuperación, análisis de causa raíz y mejora como parte integral del ciclo de gestión.
- La revisión y fortalecimiento continuos del proceso de gestión de incidentes, a medida que el SGSI institucional madure.

13. VIGENCIA Y MEJORA CONTINUA.

Esta Política entra en vigencia a partir de su aprobación por la autoridad competente y será objeto de revisión periódica, al menos una vez al año o cuando se produzcan cambios normativos, institucionales, tecnológicos o en el nivel de riesgo que así lo demanden.

Cada revisión busca asegurar la adecuación, eficacia y mejora continua de la Política, conforme al ciclo PDCA y a los principios de ISO/IEC 27001. Las revisiones podrán complementarse con auditorías internas y revisiones formales por parte de la Alta Dirección.

Toda modificación deberá cumplir con los procedimientos institucionales de revisión y aprobación establecidos en el marco del SGSI.

14. INCUMPLIMIENTO.

El incumplimiento de esta Política y de los documentos derivados podrá dar lugar a medidas administrativas, disciplinarias, académicas, contractuales, civiles o legales, según la calidad del sujeto involucrado y la gravedad de los hechos. En el caso de trabajadores, se aplicará el Reglamento Interno de Trabajo y el Código del Trabajo; en el caso de estudiantes, la normativa académica y disciplinaria



estudiantil; y, en el caso de proveedores o terceros, los contratos, convenios, acuerdos de confidencialidad, encargos de tratamiento y demás instrumentos jurídicos aplicables. En todos los casos se garantizará proporcionalidad, debido proceso, derecho a la defensa y autoridad competente

15. DEROGATORIA.

La presente Política deroga y reemplaza todas las versiones anteriores de la Política de Seguridad de la Información de la Universidad, a partir de la fecha de su aprobación formal y entrada en vigencia.

16. DISPOSICIÓN TRANSITORIA.

En el plazo de noventa (90) días contados a partir de la aprobación y entrada en vigencia de la presente Política, la Dirección de Talento Humano, con el apoyo técnico de la Jefatura de Seguridad de la Información y la revisión del Procuraduría, elaborará y someterá a aprobación de la autoridad competente la reforma correspondiente al Reglamento Interno de Trabajo de la Universidad, con el objeto de incorporar las siguientes disposiciones:

- La obligación expresa de todos los trabajadores de la institución de conocer y cumplir la Política General de Seguridad de la Información y los documentos normativos derivados de ella, como condición inherente al ejercicio de sus funciones.
- La tipificación de las conductas que constituyen incumplimiento de las obligaciones de seguridad de la información como faltas disciplinarias, distinguiendo entre faltas leves, graves según la naturaleza, reiteración e impacto del hecho.
- El catálogo de sanciones aplicables por cada tipo de falta, en correspondencia con las disposiciones del Código del Trabajo, el Estatuto Universitario y el propio Reglamento Interno, garantizando la proporcionalidad y el debido proceso.
- El procedimiento disciplinario aplicable, con indicación de los órganos competentes, los plazos, el derecho a la defensa del trabajador y los mecanismos de impugnación.

En el mismo plazo, las unidades competentes deberán revisar y proponer, cuando corresponda, reformas o anexos a la normativa estudiantil, contratos con proveedores, acuerdos de confidencialidad, contratos de encargo de tratamiento, términos de uso de plataformas institucionales y demás instrumentos aplicables, a fin de asegurar la exigibilidad de la presente Política frente a todos los sujetos comprendidos en su alcance.

Hasta tanto no entre en vigencia la reforma prevista en esta Disposición Transitoria, los incumplimientos de la presente Política podrán ser tratados conforme a las disposiciones disciplinarias actualmente vigentes en el Reglamento Interno de Trabajo, en cuanto resulten aplicables, sin perjuicio de las responsabilidades administrativas o contractuales que correspondan.



17. FIRMAS DE RESPONSABILIDAD

Realizado por:	Aprobado por:
 Validar únicamente en FirmaEC. Firmado electrónicamente por: JUAN CARLOS ORTEGA CASTRO <i>Ing. Juan Carlos Ortega, PhD.</i> Jefe de Seguridad de la Información	CORNELIO AGUSTIN BORJA POZO Firmado digitalmente por CORNELIO AGUSTIN BORJA POZO Fecha: 2026.09.25 17:26:24 -05'00' <i>Abg. Agustín Borja Pozo, PhD.</i> Rector de la Universidad Católica de Cuenca