EL CONSEJO UNIVERSITARIO DE LA UNIVERSIDAD DE CUENCA, en uso de sus atribuciones establecidas en la Constitución de la República; las Leyes y Reglamentos; su Estatuto; y sus Reglamentos internos, con el voto unánime a favor, expresado por los miembros presentes en la sesión,

CONSIDERANDO:

Que, el art. 226 de la Constitución de la República del Ecuador, dispone: "*Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución";*

Que, el artículo 350 de la Constitución de la República del Ecuador, dispone: *"El sistema de educación superior tiene como finalidad la formación académica y profesional con visión científica y humanista; la investigación científica y tecnológica; la innovación, promoción, desarrollo y difusión de los saberes y las culturas; la construcción de soluciones para los problemas del país, en relación con los objetivos del régimen de desarrollo*";

Que, el artículo 355 de la Constitución de la República del Ecuador, dispone: "*El Estado reconocerá a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los objetivos del régimen de desarrollo y los principios establecidos en la Constitución. Se reconoce a las universidades y escuelas politécnicas el derecho a la autonomía, ejercida y comprendida de manera solidaria y responsable. Dicha autonomía garantiza el ejercicio de la libertad académica y el derecho a la búsqueda de la verdad, sin restricciones; el gobierno y gestión de sí mismas, en consonancia con los principios de alternancia, transparencia y los derechos políticos; y la producción de ciencia, tecnología, cultura y arte. (...)";*

Que, el artículo 17 de la Ley Orgánica de Educación Superior, dispone: *"Reconocimiento de la autonomía responsable. - El Estado reconoce a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los principios establecidos en la Constitución de la República. En el ejercicio de autonomía responsable, las universidades y escuelas politécnicas mantendrán relaciones de reciprocidad y cooperación entre ellas y de estas con el Estado y la sociedad; además observarán los principios de justicia, equidad, solidaridad, participación ciudadana, responsabilidad social y rendición de cuentas. Se reconoce y garantiza la naturaleza jurídica propia y la especificidad de todas las universidades y escuelas politécnicas";*

Que, el artículo 18 de la Ley Orgánica de Educación Superior, dispone: "*Ejercicio de la autonomía responsable.- La autonomía responsable que ejercen las instituciones de educación superior consiste en: (...) e) La libertad para gestionar sus procesos internos; (...)";*

Que la Norma de Control Interno de la Contraloría General del Estado 410-04 establece que "*La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria"* y su sección 410-10 establece requisitos de Seguridad de tecnología de información.

Que, el artículo 17 del Estatuto de la Universidad de Cuenca dispone "*Son atribuciones del Consejo Universitario: (...) b) Aprobar y expedir los reglamentos y normas de carácter general, que regulan el régimen académico y administrativo del plantel y la elección de las autoridades y miembros de los organismos de cogobierno" y "d) Definir, aprobar y evaluar las políticas académicas e institucionales de la Universidad, así como la creación, suspensión o clausura de facultades, departamentos, institutos universitarios y demás unidades académicas"*;

Que, el artículo 5 del Reglamento de Conformación y Funcionamiento del Comité Estratégico de Tecnologías de Información de la Universidad de Cuenca dispone: *"*Funciones y atribuciones: El Comité Estratégico de Tecnologías de Información de la Universidad de Cuenca, tiene como funciones y atribuciones las siguientes: "1. Revisar y recomendar el rol de las tecnologías en la estrategia de la Universidad de Cuenca y la planificación estratégica de TI, asegurando que las iniciativas, procesos y soluciones de tecnología entreguen valor, mediante el adecuado aprovisionamiento de recursos y la vigilancia de los indicadores claves, así como la gestión de sus riesgos para establecer medidas de control. 2. Seleccionar la estrategia adecuada para enfrentar cada una de las diferentes problemáticas de la institución, identificando las tecnologías de información actuales y, o emergentes para satisfacer las necesidades, estrategias y objetivos. (…) 6. Revisar la solidez y los riesgos asociados con las tecnologías en la cual, la Universidad de Cuenca ha invertido o tiene la intención de invertir, y hacer las recomendaciones pertinentes a los encargados de la adquisición"; y,

Que, mediante memorando Nro. UC-DTIC-2022-0290-M suscrito por el Ing. Rodrigo Padilla Verdugo, Director de Tecnologías de la Información y Comunicación y dirigido a la señora Rectora se señala textualmente "Luego de un cordial y atento saludo, pongo a su consideración y por su intermedio al H. Consejo Universitario la aprobación de las *"Políticas de seguridad de la información de la Universidad de Cuenca", las cuales tienen por objetivo establecer lineamientos que permitan salvaguardar los activos de información de la institución. Comunico a su autoridad que, la propuesta de las Políticas de Seguridad de la Información de la Universidad de Cuenca fue conocida y tratada por el Comité Estratégico de Tecnologías de la Información, en la sesión ordinaria del 7 de junio del 2022, mismo que resolvió lo siguiente: "En atención al punto No. 7 del orden del día, denominado "CONOCIMIENTO Y RESOLUCIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE CUENCA", se resuelve recomendar la aprobación de las Políticas de Seguridad de la Información al Consejo Universitario.";*

Que, mediante memorando Nro. UC-SG-2022-0759-M, de fecha 05 de agosto de 2022, el Dr. Claudio Quevedo Troya, Secretario General Procurador, en referencia a la solicitud de aprobación de las Políticas de seguridad de la información de la Universidad de Cuenca, concluye señalando textualmente *"En virtud de lo expuesto, una vez que se han acogidas todas las observaciones esta dependencia procedió a realizar los ajustes pertinentes al referido instrumento, el mismo que cumple con los parámetros legales pertinentes, se recomienda que sea conocido, evualuado y resuelto por el Consejo Universitario, esto, dando cumplimiento a lo dispuesto en el art. 17.d) del Estatuto de la Universidad de Cuenca".*

RESUELVE:

1. Dar por conocidas y aprobar, con las observaciones expuestas en la presente sesión, las mismas que deben ser incorporadas por la Dirección de Tecnologías de la Información y la Comunicación, el documento que contiene las Políticas de seguridad de la información de la Universidad de Cuenca, que fuera presentado mediante memorando Nro. UC-DTIC-2022-0290-M suscrito por el Ing. Rodrigo Padilla Verdugo, Director de Tecnologías de la Información y Comunicación y que consta en 23 hojas que se anexan como parte integrante de la presente resolución.
2. Notificar con el contenido de la presente resolución a la señora Rectora, al señor Vicerrector Académico, a la Señora Vicerrectora de Investigación, al Director de Tecnologías de la Información y la Comunicación, al Director de Planificación; al Secretario General Procurador, a las Facultades y Dependencias Universitarias para su conocimiento y fines pertinentes; y, a la Unidad de Relaciones Públicas y Comunicación, para que proceda con la respectiva publicación en la página Web Institucional.

Dado en sesión del Consejo Universitario de la Universidad de Cuenca, a los nueve días del mes de agosto de dos mil veinte y dos.

Firmado electrónicamente por:
MARCIA FERNANDA CEDILLO DIAZ

Abg. Marcia Cedillo Díaz,
SECRETARIA DEL CONSEJO UNIVERSITARIO

UNIVERSIDAD DE CUENCA

Políticas de Seguridad de la Información

Versión 1.0

Agosto 2022

TABLA DE CONTENIDO

1. ANTECEDENTES

La información constituye uno de los activos más importantes de las instituciones y de manera particular para la Universidad de Cuenca es fundamental para su desarrollo adecuado, en un mundo en el que la hiperconectividad impulsada tras la aparición de la pandemia del COVID-19 presenta nuevas y constantes amenazas para la información y como tal, requiere de mecanismos que garanticen su seguridad.

Aspectos de orden regulatorio contemplados en la Constitución de la República, la Ley Orgánica de Transparencia y Acceso a la Información Pública, Ley de Protección de Datos Personales, Normas de Control Interno de la Contraloría General del Estado, entre otras, requieren que las instituciones públicas adopten medidas de control en materia de seguridad de información.

La administración actual de la Universidad de Cuenca consciente de la importancia de identificar y proteger los activos de información de la destrucción, divulgación, modificación y utilización no autorizada de la información considerada sensible, se compromete a desarrollar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI), articulado con los objetivos estratégicos institucionales que permita un tratamiento sistemático de los riesgos que afectan a la información.

En este sentido, las Políticas de Seguridad de la Información constituyen un pilar importante que aporta al mejoramiento del ambiente de control, guiando la operatividad, los procesos institucionales y la entrega de servicios con la finalidad de proteger la información institucional, basando sus prácticas en estándares de general aceptación.

2. CONTEXTO ORGANIZACIONAL

La Universidad de Cuenca es una institución pública de educación superior de la República del Ecuador, que cuenta con más de 150 años de vida institucional, regulada por el Consejo de Educación Superior y por el Consejo de Aseguramiento de la Calidad de la Educación Superior, acoge alrededor de 16 mil estudiantes de diversas regiones y sectores sociales del país en sus 12 facultades ubicadas en sus cinco campus universitarios, ofertando alrededor de 50 carreras de grado, más de 20 programas de maestría, 17 especializaciones y dos programas de doctorado.

Visión

Al 2027 la Universidad de Cuenca es una comunidad universitaria innovadora y resiliente, integrada al mundo a través de la generación de conocimiento pertinente, de calidad y comprometida con la sociedad.

Misión

Formar investigadores y profesionales comprometidos con una sociedad justa, diversa y sostenible, dispuestos a ser agentes de transformación.

Principios y valores institucionales

La Universidad de Cuenca se rige por los principios establecidos en la Constitución de la República, en la Ley Orgánica de Educación Superior, por el humanismo, la libertad, la inclusión y la no discriminación, la equidad de género, el pensamiento creativo y plural, la gratuidad de la educación hasta el tercer nivel, la rendición de cuentas y la igualdad de oportunidades para los profesores, investigadores, estudiantes, servidores y trabajadores.

Valores institucionales

La Universidad de Cuenca ha acordado los siguientes valores institucionales:

- Excelencia
- Respeto
- Sentido de Comunidad
- Equidad
- Adaptabilidad
- Trabajo en equipo

Partes interesadas

Se establecen como partes interesadas para el contexto de la seguridad de la información de la Universidad de Cuenca las siguientes:

Externas

- Consejo de Educación Superior (CES)
- Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES)

Internas

- Consejo Universitario
- Rectorado
- Vicerrectorado Académico
- Vicerrectorado de Investigación
- Facultades
- Dependencias académicas, de investigación y administrativas
- Comunidad universitaria en general

Localización geográfica

La gestión de seguridad de la información y sus políticas serán aplicables a los servicios y procesos relacionados con los ejes de docencia, investigación, vinculación con la sociedad, así como de los procesos de gestión académica y administrativa, de acuerdo con las siguientes ubicaciones geográficas:

- Ciudad de Cuenca, Campus Central. Av. 12 de abril s/n y Agustín Cueva.
- Ciudad de Cuenca, Campus El Paraíso. Av. El Paraíso.
- Ciudad de Cuenca, Campus Centro Histórico. Tarqui y Sangurima.
- Ciudad de Cuenca, Eco Campus Balzay. Víctor Albornoz y Calle de los Cerezos.
- Ciudad de Cuenca, Campus Yanuncay. Av. 12 de octubre y Diego de Tapia.
- Ciudad de Cuenca, Dirección de Cultura
- Ciudad de Cuenca, Campus Huayna Cápac.
- Ciudad de Cuenca, Granja Universitaria Nero, Parroquia Baños.
- Cantón Guachapala, Granja Universitaria El Romeral.
- Ciudad de Cuenca, Granja Universitaria Irquis, Victoria del Portete.

Referencias

La institución toma como referencia los siguientes estándares para gestionar la seguridad de información:

- ISO 27001:2013
- ISO 27002:2013

3. CONSIDERACIONES LEGALES

Para la definición de las Políticas de Seguridad de la Información de la Universidad de Cuenca se consideran las siguientes normativas legales:

La Constitución de la República en su artículo 66 numeral 19 reconoce "*El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley"*.

El artículo 92 de la Carta Magna reconoce que "*Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información*

personal y el tiempo de vigencia del archivo o banco de datos".

El artículo 6 de la Ley Orgánica de Transparencia y Acceso a la Información Pública dispone que "*Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 66 y 76 de la Constitución Política de la República"*

El artículo 10 de la Ley Orgánica de Transparencia y Acceso a la Información Pública dispone: *"Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción (…)*".

El artículo 17 de la Ley Orgánica de Transparencia y Acceso a la Información Pública establece que *"No procede el derecho a acceder a la información pública, exclusivamente en los siguientes casos: a) Los documentos calificados de manera motivada como reservados por el Ministerio de Coordinación de Seguridad, por razones de defensa nacional, de conformidad con el artículo 91 de la Constitución Política de la República y que son: (…) b) Las informaciones expresamente establecidas como reservadas en leyes vigentes"*.

El artículo 1 de la Ley del Sistema Nacional de Archivos establece que *"Constituye Patrimonio del Estado la documentación básica que actualmente existe o que en adelante se produjere en los archivos de todas las Instituciones de los sectores públicos, y privado, así como de las personas particulares, que sean calificadas como tal Patrimonio por el Comité Ejecutivo previsto en el Art. 9 de esta Ley, y que sirva de fuente para estudios históricos, económicos, sociales, jurídicos y de cualquier índole. (…)".*

El artículo 1 de la Ley Orgánica de Protección de Datos Personales dispone que *"El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principio, derechos, obligaciones y mecanismos de tutela"*.

Las Normas de Control Interno de la Contraloría General del Estado en su sección 410-04 establece que "*La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria*" y su sección 410-10 establece requisitos de Seguridad de tecnología de información.

El Consejo de Educación Superior, mediante Resolución RPC-SO-41 –No.856-2016 define la "*Propuesta de directrices para el diseño, consolidación y administración de Sistema de Gestión de Documentos y Archivos de las Instituciones de Educación Superior.*"

El Estatuto de la Universidad de Cuenca dentro de su Título II, Capítulo IV, Subcapítulo I, Sección Quinta establece: "*Art. 32.- Son funciones de esta Dirección: (…) b) Operar y mantener los sistemas de información y de la infraestructura tecnológica, garantizar la seguridad de la información y de las instalaciones y el soporte a usuarios (…)*".

4. GLOSARIO DE TÉRMINOS

Activo de Información: Se refiere a cualquier elemento relacionado con el tratamiento de la información que tenga valor para la institución y que requiere ser protegido. Comprende los sistemas de información, aplicaciones, herramientas de software, bases de datos, equipos de computación, dispositivos móviles, documentos físicos o electrónicos, instalaciones, entre otros.

Amenaza: Causa potencial de un incidente no deseado, que puede causar daños a un activo de información, sistema o a la institución.

Ataque: Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo de información.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencia suficiente y objetiva para determinar si cumplen los criterios de evaluación.

Autenticación: Es el acto o proceso de confirmar que algo es quien dice ser. En este punto no se garantiza quién dice ser, para ello es necesario que se sigan los tres ámbitos: autenticación, autorización y acceso.

Certificado de firma electrónica: Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.

Confidencialidad: Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados.

Conformidad: Cumplimiento de un requisito.

Control: Son medidas de seguridad técnicas o administrativas para evitar, contrarrestar o mitigar la pérdida o falta de disponibilidad debido a las amenazas que actúan por una vulnerabilidad asociada a la amenaza.

Entidad de certificación: Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República.

Disponibilidad: Propiedad de la información de ser accesible y utilizable a solicitud de una entidad autorizada. La información debe ser asequible en todo momento que se requiera, pero solo para aquellos con autorización para acceder a ella.

Dato sensible: Es aquel dato personal que en caso de ser tratado de manera inadecuada podría derivar en importantes riesgos para los derechos y las libertades fundamentales de una persona. Por ejemplo, ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, identificación personal, datos biométricos, condición migratoria, entre otros.

DTIC: Dirección de Tecnologías de Información y Comunicaciones.

Firma Electrónica: Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Gestión de Identidad: Proceso que permita administrar el ciclo de vida de los usuarios y controlar el acceso a sistemas de información.

Gestión de Riesgos: Proceso mediante el cual las instituciones identifican, miden, priorizan, controlan, monitorean y comunican los riesgos a los que se encuentran expuestas.

Identificación de Riesgos: Proceso de encontrar, reconocer y describir riesgos.

Identificador de Usuario - ID de Usuario: Es un texto único que identifica al usuario dentro de un servicio o sistema.

Incidente de Seguridad de la Información: Un evento o una serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones institucionales y amenazar la seguridad de la información.

Inventario de Activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, etc.) que tengan valor para la institución y por lo tanto requieren ser protegidos de potenciales riesgos.

Malware o software malicioso: Software que contiene características o capacidades que potencialmente pueden causar daño directa o indirectamente a los sistemas informáticos.

Mensaje de datos: Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

Mejora continua: Actividad recurrente para mejorar el rendimiento.

Monitoreo: Determinar el estado de un sistema, un proceso o una actividad, en un determinado punto del tiempo, y bajo unos parámetros definidos que indiquen la tolerancia de la operación de un sistema.

Nivel de riesgo: Magnitud de un riesgo expresada en términos de la combinación de consecuencias y su probabilidad.

Personal Universitario: Refiérase a profesores, investigadores, empleados y trabajadores de la Universidad de Cuenca.

Principios de la Seguridad de la Información: Guían el accionar de las estrategias de seguridad enfocadas en proteger la disponibilidad, integridad y confidencialidad de la información.

Propietario de Activos de información: se refiere a la persona que se establece como dueño de uno o más activos de información o titular de datos.

Responsable de Activos de información: Persona que tiene a su cargo uno o más activos de información institucionales.

Responsable de Seguridad de la Información: Personal que establece, implementa, mantiene y mejora continuamente uno o más procesos en la gestión de seguridad de la información.

Requisito de Seguridad: Necesidad o expectativa que se declara, generalmente implícita u obligatoria.

Riesgo de Seguridad de la Información: Está asociado con la posibilidad de que las amenazas aprovechen las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a la institución.

Sistema Informático: Conjunto de elementos de hardware y software relacionados entre sí que permiten el procesamiento automatizado de información.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Vulnerabilidad técnica: Fallo o brecha de seguridad en los sistemas operativos, programas, aplicaciones y demás software que lo expone a una posibilidad de ataque informático.

Usuarios: Se refiere al conjunto de docentes, investigadores, empleados, trabajadores, estudiantes, proveedores y demás terceros con acceso a sistemas y servicios tecnológicos de la Universidad de Cuenca.

5. OBJETIVO DE LAS POLÍTICAS DE SEGURIDAD DE INFORMACIÓN

Establecer lineamientos de estricto cumplimiento que permitan salvaguardar los activos de información de la Universidad de Cuenca.

6. ORGANIZACIÓN SEGURIDAD DE LA INFORMACIÓN

La implementación de una gestión efectiva de seguridad de la información en la Universidad de Cuenca requiere la participación activa de sus actores. Para esto se definen las siguientes responsabilidades:

Consejo Universitario

a) Conocer, analizar y aprobar las políticas de seguridad de la información y demás documentación que requiera este nivel de aprobación, para el adecuado funcionamiento del sistema de gestión de seguridad de la información.

Comité Estratégico de Tecnologías de Información

b) Conocer y analizar los objetivos, políticas, procesos, procedimientos y metodologías de seguridad de la información considerando las mejores prácticas y ponerlas en consideración de las autoridades correspondientes para su aprobación.

Director de TIC

a) Supervisar y revisar la gestión de seguridad de la información.
b) Supervisar al equipo responsable por la definición e implementación de la planificación de la continuidad para los sistemas y servicios informáticos de la Universidad de Cuenca.

Responsable de Seguridad de Información

a) Guiar, implementar, mantener y documentar la gestión de seguridad de la información de la institución.
b) Asegurar que la implementación de los controles de seguridad de la información se coordine en toda la institución.
c) Revisar en forma periódica los documentos, controles y procesos de seguridad de la información de la institución.
d) Coordinar la gestión de los riesgos de seguridad de la información en base a una metodología y tratamiento de los riesgos identificados.
e) Identificar cambios significativos en las amenazas y la exposición a riesgos de los activos de información.
f) Promover la difusión, concientización y formación en seguridad de la información en la institución.

Autoridades académicas, de investigación y administrativas de la Universidad de Cuenca

a) Cumplir y velar por el cumplimiento de las políticas de seguridad de la información por parte del personal bajo su cargo.

b) Colaborar con los proyectos de seguridad de la información.
c) Levantar y mantener un inventario actualizado de los activos de información en las unidades académicas y administrativas a su cargo.
d) Gestionar los riesgos de seguridad asociados a sus activos de información.

Docentes, investigadores, empleados y trabajadores

a) Observar y cumplir las normas, políticas, procedimientos, instrucciones y demás disposiciones relativas a seguridad de la información que establezca la Universidad de Cuenca.

7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

7.1. POLÍTICAS DE TÉRMINOS Y CONDICIONES EN LA RELACIÓN LABORAL

a) La Dirección de Talento Humano requerirá al personal universitario y demás individuos que presten sus servicios a la Universidad de Cuenca, suscribir un acuerdo de confidencialidad de información, independientemente de su relación contractual.
b) Los usuarios de los sistemas de información de la Universidad de Cuenca suscribirán un acuerdo de términos y condiciones de uso de los sistemas de información a través de la Dirección de Talento Humano.
c) Al término de la relación laboral o contractual la Dirección de Talento Humano iniciará un procedimiento que asegure que remuevan todos los accesos de los sistemas informáticos.

7.2. POLÍTICAS PARA LA GESTIÓN DE ACTIVOS DE INFORMACIÓN

7.2.1. Inventario de activos de información

Las dependencias académicas, de investigación y administrativas mantendrán un inventario preciso y actualizado de los activos de información inherentes a sus procesos y designarán un responsable para cada activo. La identificación de estos activos se basará en el catálogo definido para el efecto.

7.2.2. Responsabilidad y uso aceptable de los activos de Información

a) El responsable de un activo de información asegurará su buen uso, custodia y protección adecuada.

b) Los activos de información de la Universidad de Cuenca y los que se encuentren dentro de sus instalaciones, deberán ser utilizados de acuerdo con las leyes y reglamentos vigentes, y en fiel cumplimiento de estas políticas de

seguridad de la información.

c) Los usuarios se abstendrán de instalar, copiar o reproducir materiales de otras fuentes que vulneren los derechos de propiedad intelectual.

7.2.3. Clasificación de información

Los responsables de los activos de información deberán clasificar la información de la Universidad de Cuenca en función de su nivel de acceso, para lo cual se definen tres categorías:

UCuenca-Pública: Es la información que puede estar disponible para la sociedad en general, así como, la información requerida por la Ley Orgánica de Transparencia y Acceso a la Información Pública.

UCuenca-Uso-Interno: Es la información que puede ser conocida o usada únicamente por usuarios o funcionarios debidamente autorizados.

UCuenca-Confidencial o Reservada: Es la información que requiere de una autorización explícita de su propietario para su divulgación, que no afecten derechos personalísimos.

7.2.4. Etiquetado de la información

La información de la Universidad de Cuenca que se encuentre clasificada como UCuenca-Confidencial o Reservada, contenida en documentos físicos o digitales, deberá estar debidamente etiquetada.

7.2.5. Protección antimalware

a) La DTIC garantizará la implementación de soluciones antimalware de gestión centralizada con bases de firmas actualizadas, distribuidas permanentemente para la protección de los equipos servidores y dispositivos de usuario final que pertenecen a la institución.
b) La DTIC analizará periódicamente los sistemas informáticos en búsqueda de software malicioso.
c) La DTIC deberá contar con controles que prevengan o detecten el uso de software no autorizado en los dispositivos institucionales.

7.2.6. Escritorio limpio

Los usuarios deberán almacenar la información reservada o de uso interno en condiciones seguras y evitarán exponer documentos impresos, dispositivos de almacenamiento como memorias USB, discos duros, tarjetas de memoria, entre otros, que contengan estos tipos de información.

7.2.7. Pantalla limpia

Los usuarios deberán bloquear la pantalla de su equipo al ausentarse de su lugar de trabajo por un periodo corto, si su ausencia es mayor, procederán a apagar el equipo, procurando además la eficiencia energética.

7.2.8. Uso de Internet

a) El uso del Internet se limitará a las actividades laborales, académicas, investigativas, operativas, y cualquier otra relacionada con las actividades institucionales.
b) La Coordinación de Redes y Comunicaciones bloqueará el acceso a determinados sitios de Internet maliciosos y/o no autorizados. El usuario no debe intentar eludir por su cuenta la mencionada restricción.

7.2.9. Correo electrónico y mensajería instantánea

a) Las cuentas de correo institucionales serán usadas para el cumplimiento de las actividades laborales, académicas y de investigación.
b) Los usuarios de correo electrónico no deben responder o reenviar correo no solicitado (spam), cadenas de mensajes, correos de remitentes desconocidos, debiendo borrarlos inmediatamente de todas sus bandejas de correo.
c) Para el envío, recepción y/o almacenamiento de información clasificada como “UCuenca-Confidencial o Reservada” o “UCuenca-Uso-Interno”, se emplearán únicamente cuentas de correo y/o aplicaciones institucionales.
d) El contenido de las cuentas de correo bajo el dominio de la Universidad de Cuenca será tratado como información institucional.

7.2.10. Uso prohibido de los activos de información

Se encuentra prohibido en la Universidad de Cuenca:

a) Instalar software propietario en un equipo informático de la Universidad de

Cuenca que no cuente con una licencia de uso.

b) Utilizar los activos de información de la Universidad de Cuenca para fines personales o que pongan en riesgo la seguridad de la información de la institución.
c) Escanear puertos de equipos informáticos o redes que pertenecen a la infraestructura universitaria, sin la autorización de la Coordinación de Redes y Comunicaciones.
d) Explotar las vulnerabilidades presentes en la infraestructura o en el software utilizado por la institución, sin la autorización de la Unidad de Seguridad de la Información.
e) Violentar la seguridad de los activos de información, dañar, alterar, destruir, borrar o afectar en alguna forma, en beneficio propio o de un tercero.
f) Acceder sin autorización a un dispositivo, sistema o recurso informático.
g) Revelar ilegalmente el contenido de las bases de datos, ficheros, archivos, o similares que afecten su confidencialidad, la intimidad o privacidad de las personas.
h) Utilizar el servicio de Internet para almacenamiento, divulgación o transmisión de cualquier información, archivos, documentos, imágenes, audios, entre otros, que puedan infringir normas de propiedad intelectual, marcas o patentes.
i) Emplear los recursos y activos de información institucionales para ver, descargar, guardar, reenviar material que: fomente la discriminación basada en nacionalidad, etnia, sexo, edad, estado civil, orientación sexual, discapacidad, afinidad política, religiosa u otras; que promueva el comportamiento amenazante o violento; o que incite cualquier tipo de actividad ilegal.

7.2.11. Devolución de activos de información

Al finalizar la relación laboral, contractual o acuerdo, los activos de información de la Universidad de Cuenca que hayan sido generados y/o entregados a su responsable, deberán ser transferidos a su jefe inmediato.

7.2.12. De la gestión de riesgos de seguridad de información

Los activos de información críticos se someterán a un proceso sistemático de gestión de riesgos de seguridad de información, identificando los riesgos que amenazan a dichos activos, cuantificando el nivel de impacto y el tratamiento sugerido.

7.2.13. Protección y tratamiento de la información

a) La información reservada contenida en bases de datos y discos de almacenamiento serán protegidos de preferencia mediante técnicas de

cifrado de información.

b) El acceso a información confidencial o reservada para modificaciones debe registrarse en los respectivos registros de eventos o pistas de auditoría.
c) La Universidad de Cuenca priorizará el almacenamiento centralizado de la información.

7.2.14. Divulgación de Información de uso interno, confidencial o reservada

a) La información clasificada como UCuenca-Confidencial o Reservada no debe presentarse en eventos, foros, seminarios o similares.
b) La divulgación de información clasificada como UCuenca-Confidencial o Reservada requiere autorización previa de su propietario siempre y cuando no afecten derechos personalísimos.

7.2.15. Eliminación de medios físicos

a) Se debe proceder con la eliminación segura de datos mediante el borrado criptográfico, destrucción física del medio, o cualquier otra técnica considerada segura, que garantice que su contenido sea ilegible para medios de almacenamiento que contengan información de uso interno o reservada.
b) Los datos que requieran conservarse deben copiarse a otros medios y ser verificados antes de la eliminación de los medios físicos o digitales considerando el tiempo de retención de información.
c) La información de uso interno confidencial o reservada contenida en papel debe ser destruida con trituradoras de papel.

7.3. POLÍTICAS DEL CONTROL DE ACCESO

7.3.1. De la gestión de identidad

a) El acceso a los sistemas o servicios institucionales se realizará por medio de un identificador único de usuario.
b) Las credenciales de acceso (ID de usuario y contraseña o similares) para cada servicio o aplicativo informático serán entregados formalmente a los solicitantes, quienes deberán conocer sus obligaciones y responsabilidades en su uso.
c) Los identificadores de súper usuario tipo admin, root o similares, establecidas por defecto, en sistemas o dispositivos, no deben ser usados. Siempre que sea posible las mismas deben ser deshabilitadas o eliminadas, según

aplique, además de modificadas sus contraseñas por defecto.

d) Los ID de súper usuario serán entregados únicamente a los administradores de sistemas, redes, bases de datos y demás recursos tecnológicos para el mantenimiento de los sistemas que requieran de tales privilegios. Preferentemente usarán un identificador de usuario con privilegios estándar para sus actividades operativas de rutina.
e) No se permite utilizar ID de usuario genéricos y/o compartidos, salvo casos excepcionales debidamente analizados y justificados por la dependencia o unidad a cargo.
f) Todo identificador de usuario de la Universidad de Cuenca debe tener asignado al menos un factor de autenticación: contraseña, biométrico, token o similar.
g) Las credenciales de acceso (usuarios y contraseñas o similares) asignadas por la Universidad de Cuenca son personales e intransferibles.

7.3.2. De la Autenticación

a) La autenticación a los aplicativos de la institución se realizará por medio de un sistema centralizado.
b) Siempre que sea posible, se emplearán mecanismos de doble factor de autenticación en los sistemas de información.

7.3.3. Del control de acceso a los sistemas informáticos

a) Se emplearán perfiles para simplificar la concesión y el mantenimiento de los derechos de acceso a los sistemas y/o servicios informáticos.
b) Los responsables de unidades administrativas, académicas y de investigación establecerán los permisos que corresponden a cada perfil de usuario en los sistemas de información, al que podrá acceder el personal bajo su cargo.
c) Los responsables de unidades académicas, administrativas y de investigación son los únicos autorizados a solicitar el acceso a los diferentes sistemas informáticos de su personal académico y administrativo, estudiantes, proveedores o terceros, según aplique; especificando los privilegios de acceso vinculados al usuario.
d) La Coordinación de Servicios Informáticos será responsable de la asignación del acceso a los sistemas de información, conforme los permisos que correspondan a cada perfil.
e) Los usuarios de la Universidad de Cuenca deberán acceder únicamente a los sistemas de información para los cuales han sido formalmente admitidos. Se prohíbe intentos de acceso ilegítimos.

f) La Dirección de Talento Humano en conjunto con la Coordinación de Servicios Informáticos implementarán procedimientos definidos formalmente que cubran las altas, bajas y modificaciones de usuarios y de sus derechos de acceso, asegurando que sólo los usuarios debidamente autorizados tengan derecho a utilizar determinados servicios.

7.3.4. De las contraseñas

a) Se emplearán contraseñas con estructuras complejas las cuales mínimamente deben cumplir con los siguientes requerimientos:
   - Contar con una longitud de por lo menos 12 caracteres.
   - Contener al menos 3 tres de los siguientes grupos de caracteres: mayúsculas, minúsculas, numéricos, especiales.
   - No usar nombres, fechas de nacimiento, domicilios o palabras de diccionario relacionadas con su identificador de usuario.

b) Los sistemas informáticos obligarán al usuario a cambiar su contraseña en su primer uso y/o luego de ser asignada por un administrador de sistema.
c) Se realizará el bloqueo de la cuenta de usuario luego de 5 intentos fallidos de inicio de sesión.
d) Las aplicaciones, sistemas operativos y demás recursos tecnológicos deben hacer cumplir los lineamientos para contraseñas seguras.

7.3.5. Repositorios de Identidad

a) Se emplearán mecanismos seguros de cifrado sobre las contraseñas o similares que reposan en bases de datos, archivos o contenedores.
b) La DTIC garantizará el resguardo de las credenciales de súper usuario de los diferentes recursos tecnológicos en repositorios seguros.

7.3.6. De los registros de eventos

Se deberán configurar *logs* o registros de auditoría en los sistemas de información, según sea aplicable, de los eventos realizados por el usuario que correspondan a:

- Número de intentos de inicio de sesión fallido
- Intento de inicio de sesión exitoso
- Última fecha de inicio de sesión
- Fecha de último cambio de contraseña
- Dirección IP desde donde se conecta (si es aplicable)
- Cambio de estado de usuario (activo, inactivo, bloqueado)

- Acciones que correspondan al: ingreso, actualización o eliminación de datos.

7.3.7. Revocatoria de acceso

a) La Dirección de Talento Humano comunicará de forma inmediata a la Coordinación de Servicios Informáticos de la DTIC, la solicitud de revocatoria de acceso del personal académico y administrativo, una vez terminada su relación laboral, contractual o vinculación con la Universidad de Cuenca.
b) La revocatoria de privilegios de acceso a estudiantes de pregrado deberá realizarse de forma automática un mes después de finalizado su proceso de estudios o de no haber registrado matrícula.
c) Únicamente el personal de la DTIC autorizado deberá crear, modificar, bloquear y suspender cuentas de usuarios. Los funcionarios responsables de la administración de accesos atenderán la solicitud de la revocatoria de acceso en un plazo no mayor a 16 horas laborables.

7.3.8. De las responsabilidades del usuario en el uso de contraseñas

Para mitigar el riesgo de acceso no autorizado, los usuarios cumplirán con:

a) No revelar sus contraseñas a terceros.
b) No almacenar claves en papel o medios físicos. Si se tiene registros electrónicos estos deberán estar adecuadamente protegidos mediante contraseñas y/o técnicas de cifrado.
c) Las contraseñas empleadas en los sistemas o servicios institucionales no deben usarse en servicios, sistemas o aplicaciones personales.
d) Cambiar inmediatamente sus contraseñas cuando tenga indicios de que esta se encuentra comprometida o representa un riesgo para la seguridad de la información de la institución.
e) A toda persona a la que se haya entregado un identificador de usuario, es responsable de la actividad asociada al mismo en los sistemas de información, dispositivos, aplicativos y otros a los que tenga acceso de acuerdo a su perfil de usuario.

7.4. POLÍTICAS DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

a) La DTIC deberá contar con procedimientos para la gestión de incidentes de seguridad de la información que aborden las fases de: preparación, detección y

análisis, contención, erradicación y recuperación.

b) Los incidentes de seguridad de la información que afecten a un activo de información de la Universidad de Cuenca deberán ser reportados por sus docentes, empleados, trabajadores o estudiantes, a través de los canales que se definan para el efecto.

7.5. POLÍTICAS DEL LICENCIAMIENTO DE SOFTWARE

a) El software empleado por la Universidad de Cuenca deberá contar con la respectiva licencia de uso.
b) Se prohíbe descargar archivos o cualquier otro material, sin contar con los derechos, los permisos, las licencias que correspondan o cualquier otro formalismo que deba cumplirse y se omita intencionalmente.
c) La Coordinación de Servicios Informáticos será la responsable de la administración de licencias de software institucional.

7.6. POLÍTICAS DE LA CONTINUIDAD DE LOS SISTEMAS Y SERVICIOS INFORMÁTICOS

a) Las DTIC deberá implementar un plan de continuidad a fin de garantizar la operación de los servicios y procesos críticos.
b) Se deberán planificar y realizar pruebas a la continuidad de los sistemas y servicios informáticos de forma periódica.
c) El Comité Estratégico de Tecnologías de Información velará por que se cuente con los medios y recursos tecnológicos, humanos y de cualquier otra índole necesarios para operar en una localización diferente al sitio principal de procesamiento.

7.7. POLÍTICAS DE LA SEGURIDAD FÍSICA DE LAS ÁREAS DE PROCESAMIENTO DE INFORMACIÓN

a) Las áreas de procesamiento de información como: centros de datos, cuartos de comunicaciones y las instalaciones de la DTIC, deberán contar con mecanismos que aseguren el registro y control del acceso físico, con lectores de tarjetas magnéticas, identificación por radiofrecuencia (RFID) o sistemas biométricos.
b) El sistema de control de acceso mantendrá información histórica de accesos a las áreas de procesamiento de información.
c) Los centros de datos deberán contar con un sistema cerrado de TV.
d) Los centros de datos deberán contar con medidas de seguridad física y ambiental apropiados, que aseguren la protección principalmente de los

servidores y equipos de comunicaciones.

e) Se prohíbe el ingreso al centro de datos con alimentos, líquidos, material combustible, o cualquier producto que pudiera ocasionar daño a la infraestructura del centro de datos.

7.8. POLÍTICAS DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN

a) La DTIC contará con procedimientos formalizados para realizar copias de seguridad de la información de servidores, bases de datos, aplicaciones, código fuente y objeto, así como, la documentación técnica correspondiente considerando aspectos como: frecuencia, tiempo de retención, verificación, almacenamiento en una ubicación remota.
b) Los respaldos permanecerán en un lugar externo adecuado para el almacenamiento seguro con medidas de protección ambiental y deberán ser probados periódicamente a efectos de garantizar su efectividad, en caso de emergencia.
c) Se considerará la confidencialidad de la información contenida en los respaldos, en caso de que sea requerido, estos deberán permanecer cifrados.

7.9. POLÍTICAS DE LA GESTIÓN DE VULNERABILIDADES TÉCNICAS

a) La DTIC implementará un procedimiento formal para gestionar las vulnerabilidades técnicas presentes en su infraestructura tecnológica.
b) Se deberá emplear únicamente aquellas herramientas autorizadas para la identificación de vulnerabilidades técnicas.
c) El personal técnico dará el tratamiento adecuado en función del riesgo que representen las vulnerabilidades para los activos de información institucionales.
d) El análisis de vulnerabilidades se realizará integralmente sobre los servidores y servicios institucionales cuando menos semestralmente y previo a la salida a producción de un servicio nuevo.
e) La aplicación de parches o actualizaciones deberán ser evaluadas y probadas previamente en ambientes no productivos a fin de garantizar su efectividad y que no presenten efectos no deseados sobre el funcionamiento de los servicios informáticos en producción.

7.10. POLÍTICA DE USO DE EQUIPOS DE CÓMPUTO FUERA DE LAS INSTALACIONES

a) El equipo de cómputo que requiera utilizarse fuera de las instalaciones de la Universidad de Cuenca será solicitado por el responsable de la unidad

administrativa correspondiente y autorizado por el responsable de la unidad de bienes.

b) Todos los equipos de cómputo mantendrán una cobertura de seguro adecuada para proteger el equipamiento fuera de las instalaciones universitarias.

7.11. POLÍTICA SOBRE EL USO DE FIRMAS ELECTRÓNICAS

a) El personal universitario que en el ámbito de su trabajo requiera el uso de firmas electrónicas empleará certificados de firma electrónica emitidos por las entidades certificadoras acreditadas por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).
b) Los documentos firmados electrónicamente podrán ser validados a través de un sistema validación de firma.
c) La DTIC garantizará que los documentos digitales firmados electrónicamente a través de los sistemas de información centralizados de la institución, se conserven perpetuamente en medios y condiciones de almacenamiento seguros, manteniendo su formato original.
d) La seguridad de las contraseñas y dispositivos empleados en los procesos de firma electrónica es responsabilidad del usuario.

8. SUPERVISIÓN

La supervisión del cumplimiento de las políticas de seguridad lo realizará el Responsable de Seguridad de la Información.

9. REVISIÓN

Las Políticas de Seguridad de la Información deben ser revisadas periódicamente.

10. VIOLACIONES A LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Las violaciones a las políticas expresadas en este documento serán conocidas y se procederá conforme el Estatuto, los reglamentos internos, el Código de Ética de la Universidad de Cuenca, o la ley, según aplique, sin perjuicio de las acciones civiles y penales que dieran lugar.

11. DISPOSICIONES GENERALES

Las facultades, dependencias o unidades académicas y administrativas involucradas,

con el apoyo de la Dirección de Tecnologías de Información y Comunicaciones, deberán documentar los procedimientos que correspondan, para la aplicación de la presente política, en un plazo de 180 días.

12. APROBACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Ing. Rodrigo Padilla V. **Director de la DTIC** Ing. Jaime Inga I., **Unidad de Seguridad de la Información** Ing. María José Torres, **Coordinadora de Redes y Comunicaciones** Ing. Edison Casanova Y., **Coordinador de Sistemas de Información** Ing. Pablo Palacios M., **Coordinador de Servicios Informáticos**	Dra. Ma. Augusta Hermida P. **Presidenta del CETI** Miembros: Dra. Monserrath Jerves H. Ing. Juan Leonardo Espinoza A. Ing. Rodrigo Padilla V. Eco. Fernando Martínez T. Eco. Pedro Mora P.	H. Consejo Universitario **Rectora**

SECRETARIA DEL CONSEJO UNIVERSITARIO DE LA UNIVERSIDAD DE CUENCA

Certifica,

Que, la información que antecede en veinte y tres fojas, corresponde a las Políticas de Seguridad de la Información de la Universidad de Cuenca, aprobado mediante resolución No. UC-CU-RES-165-2022 adoptada por el Consejo Universitario en sesión del 09 de agosto de 2022, de la cual se constituye en parte integrativa.

Cuenca, 09 de agosto de 2022.

Firmado electrónicamente por:
MARCIA FERNANDA CEDILLO DIAZ

Abg. Marcia Cedillo Díaz
Secretaria del Consejo Universitario.