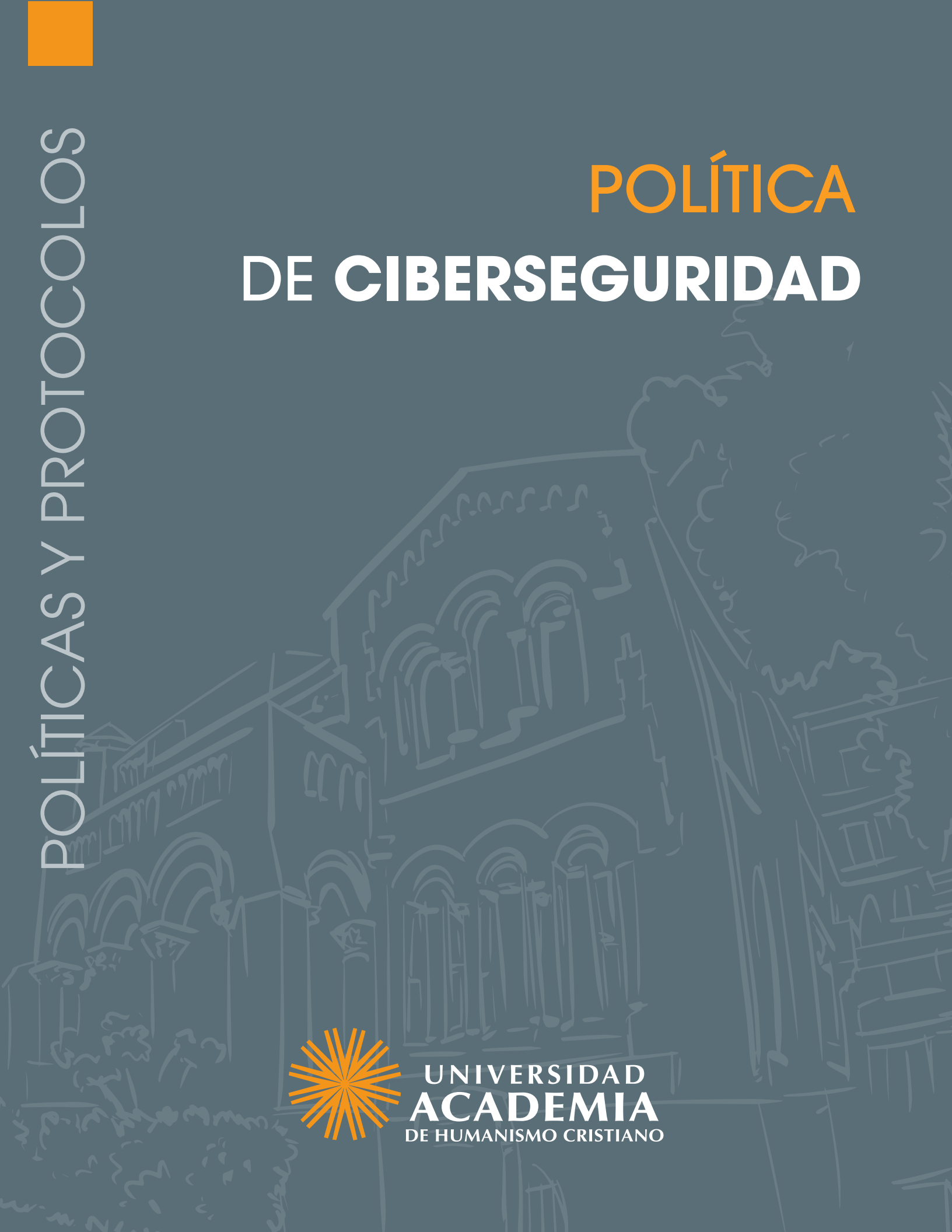
POLÍTICAS Y PROTOCOLOS

POLÍTICA DE **CIBERSEGURIDAD**



UNIVERSIDAD ACADEMIA
DE HUMANISMO CRISTIANO

Presentación

La Universidad Academia de Humanismo Cristiano, comprometida con el desarrollo seguro, sostenible y ético de sus funciones institucionales, como la docencia, investigación y vinculación con el medio, establece esta Política de Ciberseguridad como parte integral de su sistema de gestión institucional.

Dicha política tiene por objetivo proteger la información y los activos digitales de la Universidad, asegurando la continuidad operativa de los servicios internos, y promover una cultura de seguridad digital que resguarde a toda la comunidad universitaria frente a amenazas que afecten la confidencialidad, disponibilidad e integridad de los datos.

En un entorno cada vez más digital, expuesto a riesgos crecientes como accesos indebidos, ciberataques, pérdida o filtración de datos, y uso indebido de la información, la Universidad reconoce la necesidad de contar con una política institucional alineada con los estándares internacionales y en conformidad con el marco normativo nacional vigente en materia de seguridad de la información y protección de datos personales.

Esta política se alinea en concordancia con los principios y lineamientos establecidos en la norma ISO/IEC 27001 sobre la gestión de seguridad de la información, y se complementa con la norma ISO 27701, relacionada con la privacidad de la información. De la misma forma, se articula con los enfoques de gestión del riesgo descritos en la norma ISO 31000, y con el modelo de control interno COSO ERM (Enterprise Risk Management), promoviendo la toma de decisiones informadas, la rendición de cuentas y la mejora continua.

De la misma forma, esta política da cumplimiento y aplica conceptos relevantes de las siguientes normativas chilenas vigentes:

- **Ley N° 21.719**, sobre la protección de datos personales y las buenas prácticas de seguridad institucional.
- **Ley N° 21.459**, sobre los delitos informáticos, que establece responsabilidades y medidas de prevención ante amenazas tecnológicas.
- **Ley N° 20.393**, sobre la responsabilidad penal de las personas jurídicas, incluyendo los delitos informáticos, la violación de secretos entre otros.

Adicionalmente, esta política se vincula con los objetivos estratégicos institucionales y se complementa con otras normativas internas, tales como: Uso de Recursos Computacionales, uso de cuentas de usuario/contraseña, uso de correo institucional, Protocolo de respaldo y recuperación ante desastres, como con los lineamientos sobre el uso responsable de la Inteligencia Artificial, cada uno desarrollado de forma independiente en su respectivo Anexo.

Todo con el fin de consolidar una cultura de ciberseguridad, manejo responsable de los datos personales e institucionales, y de prevención de riesgos digitales, donde cada integrante de la comunidad universitaria asuma un rol activo en la construcción de un entorno seguro, resiliente, ético y conforme a la normativa vigente.

I. Propósitos y principios de la política

La ciberseguridad y el manejo responsable de datos son elementos claves para la protección de la información institucional, ayudando a garantizar la continuidad operativa del negocio, fortaleciendo además la confianza de la comunidad universitaria. Por ende, esta política tiene como propósito establecer las directrices necesarias para prevenir, detectar y responder ante incidentes de seguridad tecnológica, protegiendo la información crítica de la universidad, como la información de todos los administrativos, docentes, estudiantes y futuros prospectos, ayudando a promover el uso ético y seguro tanto de los sistemas como de equipamiento tecnológico.

En un mundo donde la tecnología avanza muy rápido, dicha política busca fortalecer la resiliencia institucional frente a cualquier tipo de amenaza cibernética, garantizando el cumplimiento de las normativas vigentes, alineándonos con estándares internacionales como ISO/IEC 27001, ISO 27701 e ISO 31000, y con el marco de gestión de riesgos COSO ERM.

Los objetivos de la Política de Ciberseguridad comprenden los siguientes puntos:

1.1. Alcance

Esta política integra a:

- **La Comunidad Universitaria,** tanto estudiantes como académicos, administrativos, asesores o proveedores externos y cualquier tercero con acceso a los sistemas de la Universidad.

- **Todos los sistemas informáticos,** servicios digitales, plataformas educativas (tales como, Campus Virtual, titulados, entre otras), sistemas de gestión institucional (back office administrativo, VCM, SAT, portales, etc.), correo institucional, ERP financieros y administrativos, desarrollos internos, CRM y formularios de gestión, así como toda la infraestructura tecnológica y redes administradas directamente por la Universidad o por terceros bajo contrato.

1.2. Principios Rectores

Los siguientes principios fundamentales rigen la aplicación de esta política:

- **Confidencialidad:** acceso autorizado a la información.
- **Integridad:** trazabilidad y bases de datos con información exacta y protegida de modificaciones no autorizadas.
- **Disponibilidad:** Alta disponibilidad de los servicios y sistemas, además de un correcto manejo de los plazos y tiempos en que los datos estén accesibles, según definición de la universidad.
- **Legalidad**: cumplimiento de la legislación chilena vigente en materia de ciberseguridad, delitos informáticos y seguridad de la información, así como de los estándares y buenas prácticas recomendadas.
- **Responsabilidad Compartida:** a ciberseguridad es una responsabilidad transversal, donde cada integrante de la comunidad universitaria debe adoptar conductas seguras en el uso de sistemas y tecnologías, cumplir los lineamientos institucionales y reportar oportunamente incidentes o vulnerabilidades detectadas.

1.3. Roles y Responsabilidades

La aplicación efectiva de la presente política se articula en distintos niveles de responsabilidad, con el fin de asegurar continuidad, claridad y adaptabilidad institucional.

1.3.1 Nivel Estratégico — Alta dirección

- Aprueba la Política de Ciberseguridad y sus actualizaciones.
- Supervisan su cumplimiento institucional, con el seguimiento y coordinación entre la Dirección de Informática/ Encargado de ciberseguridad y el Delegado institucional de protección de datos personales.
- Autoriza medidas excepcionales o cambios relevantes que afecten la seguridad de la información y los activos digitales críticos.

1.3.2 Nivel Táctico — Dirección de Informática/Encargado de ciberseguridad

- Lideran la planificación, implementación y mejora continua de la seguridad digital.
- Asegurar la articulación operativa entre ciberseguridad y los marcos institucionales de la política de protección y manejo de datos, en coherencia con la gobernanza de datos.
- La Dirección de informática dirige el plan de continuidad operativa (PCO) y del Plan de Recuperación ante Desastres (DRP).
- La Dirección de informática define los lineamientos generales sobre accesos, manejo de credenciales, resguardo de información, clasificación de datos, transferencia y almacenamiento y con concordancia a la Política de Protección, Gobernanza y Manejo de datos.

1.3.3 Nivel Operativo— Unidades Especializadas

Corresponde a las unidades técnicas encargadas de la ciberseguridad en los distintos ámbitos, como el encargado de ciberseguridad, el jefe de soporte informático y el jefe de sistemas.

Responsabilidades clave:

- Implementar, operar y monitorear los controles técnicos de seguridad definidos por la Dirección de Informática.

- Administrar accesos, permisos y credenciales institucionales (AD/M365/SSO), enlazado a los sistemas institucionales.
- Realizar auditorías técnicas (según solicitud formal del director de informática), monitoreos (diarios), gestión de vulnerabilidades y revisión de logs (semestral), así como la validación de los respaldos diarios.
- Coordinar y ejecutar la respuesta técnica ante incidentes de seguridad.
- Mantener inventarios de activos tecnológicos y asegurar el cumplimiento de políticas de contraseñas, MFA y acceso seguro.
- Aplicar medidas técnicas, lógicas de la red conforme a los protocolos operativos vigentes (segregación de redes, bloqueos de puertos, accesos privilegiados, respaldo, cifrado, etc.).
- Gestionar limpieza de las BD de los sistemas, actualizaciones y parches de seguridad.

Todos estos requerimientos deben ir en concordancia a los otros requerimientos y solicitudes abordadas en la Política de Protección, Gobernanza y Manejo de datos, que permiten dar cumplimiento a los marcos normativos que regulan a la Universidad.

1.3.4 Nivel Funcional — Unidades Académicas y Administrativas

Comprende todas las direcciones de gestión y/o unidades administrativas que gestionan información personal, académica y financiera o inclusive datos de encuestas o de prospectos, por medio de los distintos sistemas o plataformas institucionales o redes externas.

Responsabilidades:

- Garantizar el uso adecuado, legal y responsable de los datos bajo su administración, incluyendo el uso de herramientas tecnológicas externas, tales como plataformas de inteligencia artificial, automatización o análisis, evitando la exposición de información clasificada como confidencial o sensible.

- Mantener actualizada la información que gestionan y asegurar su tratamiento conforme a la clasificación institucional.
- Abstenerse de utilizar datos personales, académicos, financieros o institucionales en plataformas de inteligencia artificial u otras herramientas externas no autorizadas institucionalmente.
- Reportar incidentes, irregularidades o accesos indebidos según los protocolos vigentes.
- Solicitar formalmente altas, modificaciones y bajas de cuentas institucionales asociadas a estudiantes, académicos, funcionarios o terceros.
- Todo requerimiento que implique modificaciones a los sistemas o a los procesos definidos en los protocolos de manejo de datos de cada unidad, o en la presente Política, deberá ser derivado y gestionado por la unidad respectiva ante el Delegado de Protección de Datos y el Encargado de Ciberseguridad.

  Dichas instancias evaluarán la procedencia de la solicitud y definirán su aplicación o no. En caso de tratarse de accesos excepcionales, requerimientos especiales de tratamiento de la información o necesidades específicas de reportería, será responsabilidad de la unidad solicitante coordinar y elevar el caso a la Alta Dirección o al Comité Institucional de Datos, según corresponda, para su análisis y resolución.

1.3.5 Comunidad Universitaria — Académicos, Funcionarios, Estudiantes y Terceros

- Usar responsablemente las cuentas institucionales y proteger sus credenciales de acceso.
- Mantener un uso aceptable y responsable de los sistemas y cumplir con la ley de privacidad y protección de datos.
- Reportar inmediatamente a la unidad de soporte informático, cualquier incidente de seguridad o sospecha de vulneración.
- Proveedores y terceros deben cumplir estrictamente las cláusulas contractuales de seguridad, confidencialidad y tratamiento adecuado de la información institucional.

2. Lineamientos Generales

- Gestión de accesos: uso obligado de las credenciales institucionales (SSO M365) y el correcto uso de contraseñas robustas.
- Protección de datos personales: accesos restringidos en base al rol y permiso de cada cuenta, cumplimiento y acuerdo de resguardo y manejo adecuado de la información privada (proveedores, terceros y trabajadores), conforme a las políticas institucionales vigentes.
- Uso controlado de softwares o servicios: prohibición de instalar software no autorizado, no compartir claves de acceso (claves de uso personal e intransferible), reinstalar o reconfigurar el SO de equipamiento tecnológico (labor exclusiva soporte informático) o el utilizar recursos institucionales con fines ilícitos.
- Actualizaciones de software: obligación de mantener sistemas, aplicaciones y servidores actualizados con parches de seguridad.
- Seguridad en infraestructura y sistemas: reglas y control desde el firewall, antivirus, segmentación de las redes, creación de VLAN y optimización de flujo de datos, VPNS con permisos específicos, manejo adecuado de servicios y permisos restringidos, bloqueo de puertos, etc.
- Respaldo y recuperación: copias de seguridad y plan de recuperación ante desastres, permisos actualizados acceso data center.
- Gestión de incidentes de ciberseguridad: todo incidente debe ser reportado inmediatamente al Encargado de Ciberseguridad, conforme a los protocolos institucionales vigentes.
- Concientización y capacitación: programas de formación periódica en buenas prácticas de ciberseguridad dirigidos a toda la comunidad universitaria (correos de recomendación de buenas prácticas, avisos periódicos a la comunidad, advertencias por nuevas amenazas, etc.).

2.1 Gobierno de Datos

El Gobierno de Datos corresponde al marco rector que define cómo la institución organiza, regula y supervisa el uso de sus datos durante todo su ciclo de vida. Incluye lineamientos, roles, estándares y responsabilidades que garantizan que la información sea confiable, íntegra, trazable, disponible y utilizada correctamente conforme a la Ley 21.719. El cual se detalla profundamente en la Política de Protección, Gobernanza y Manejo de Datos.

2.2 Manejo de Datos

El Manejo de Datos corresponde a la implementación operativa del Gobierno de Datos. Son las actividades prácticas que realizan las unidades para capturar, ingresar, validar, depurar, integrar y disponer datos, siguiendo los lineamientos institucionales. Este concepto se aborda en la Política de Protección, Gobernanza y Manejo de Datos.

2.3 Ciberseguridad

La Ciberseguridad comprende los controles, procesos y tecnologías destinadas a proteger sistemas, redes y datos institucionales frente a accesos no autorizados, vulneraciones, ataques y pérdidas. Siendo abordado en la presente Política.

3. Relación entre Gobierno de Datos, Manejo de Datos y Ciberseguridad

El Gobierno de Datos es definido por la Alta Dirección y Comité de Datos; el Manejo de Datos es ejecutado por cada unidad académica/administrativa; y la Ciberseguridad es responsabilidad de la Dirección de Informática.

Complementariamente, la Universidad clasifica la información que administra según su nivel de sensibilidad y criticidad, con el fin de establecer los controles que deben aplicarse para su adecuada protección. Esta clasificación permite condicionar el tipo y nivel de controles requeridos, los cuales se detallan en función de las características del dato, su uso y los riesgos asociados. El cual es abordado en la Política de Protección, Gobernanza y Manejo de Datos.

La coordinación entre los responsables del Gobierno, Protección y Manejo de Datos, y aquellos encargados de la Ciberseguridad, se encuentra definida y articulada en ambas políticas, asegurando una gestión integrada, coherente y alineada con los objetivos institucionales.

4. Gestión de accesos

- Toda cuenta debe usar credenciales institucionales y MFA (Microsoft 365).
- Se aplica estrictamente el principio de privilegio mínimo (perfilamiento).

5. Uso controlado de software

- Solo personal técnico autorizado puede instalar software.
- Solo se usa software licenciado o en su defecto open source (validado por el equipo técnico).

Actualizaciones

- Todo sistema operativo debe mantenerse actualizado (cada usuario es responsable de mantener actualizado su equipo asignado, el sistema operativo siempre lo solicitará en caso de ser necesario).
- Actualización de parches de seguridad FW (Encargado de ciberseguridad).
- Actualizaciones sistemas, plataformas de desarrollo interno, plugins, etc. (jefe de sistemas).

Seguridad perimetral

- Firewalls, segmentación de la red, VLAN con servicios separados, VPNs autorizadas, antimalware.
- Toda transferencia de documentación e información se realiza por medios protegidos, cifrados y autorizados (SFT, Onedrive con permisos a usuarios definidos), permisos de enlace directo VPNs, permisos de IP, etc. (definido por la dirección de informática).

7. Continuidad operativa

La continuidad operativa es fundamental para asegurar que los servicios, procesos y sistemas críticos de la Universidad puedan mantenerse en funcionamiento ante eventuales interrupciones, incidentes o desastres que afecten la infraestructura tecnológica o la disponibilidad de la información. Su propósito es garantizar que la institución cuente con mecanismos preventivos, procedimientos de respuesta y planes de recuperación que permitan minimizar el impacto operacional, proteger los activos de información y asegurar la reanudación oportuna de las actividades esenciales. En este marco, la continuidad operativa se rige por los siguientes lineamientos:

1. **Respaldo y recuperación:** La Universidad ejecuta respaldos diarios de sus sistemas y bases de datos críticas. Dichos respaldos se almacenan en entornos seguros, tanto en la nube como en la infraestructura local. Los respaldos deben estar cifrados y contar con procedimientos de verificación y restauración periódica para garantizar su integridad y operatividad.
2. **Gestión de incidentes de Ciberseguridad:** Todo incidente o sospecha de incidente de ciberseguridad debe ser reportado inmediatamente a la Dirección de Informática para su análisis, contención y mitigación oportuna, cualquier acción paliativa será trabajada con en conjunto con el Encargado de Ciberseguridad, informando a la brevedad a las autoridades afectadas y a comunicaciones para difusión en caso de corresponder.
3. **Concientización y Capacitación:** Se implementarán programas de formación periódica en buenas prácticas de ciberseguridad, dirigidos a toda la comunidad universitaria. Estos programas pueden incluir el envío de correos de recomendación, así como advertencias oportunas sobre nuevas amenazas detectadas.

4. **Controles para la resiliencia tecnológica:** La implementación de controles adecuados permite garantizar la confidencialidad, integridad y disponibilidad de la información, fortaleciendo la continuidad operativa y la resiliencia tecnológica de la institución. Estos mecanismos actúan como herramientas preventivas y correctivas

que permiten anticipar, detectar y mitigar incidentes de seguridad, asegurando el cumplimiento de la normativa vigente y los estándares internacionales aplicables.

Los controles de acceso y seguridad fortalecen la gobernanza de la información, al establecer responsabilidades claras, mecanismos de trazabilidad y procedimientos de auditoría que resguardan los activos digitales universitarios. En este contexto, el acceso a los sistemas y datos debe gestionarse bajo el principio de privilegio mínimo, de modo que solo las personas autorizadas y debidamente registradas puedan interactuar con la infraestructura o información institucional.

5. **Plan de Recuperación ante Desastres (DRP):** La Universidad dispone de un DRP formal, el cual considera un protocolo de restauración (de sistemas, bases de datos, etc.) dentro de Tiempos Objetivos de Recuperación (RTO) y Objetivos de Punto de Recuperación (RPO) previamente definidos.

Revisión y Actualización

La presente política será revisada al menos una vez al año por la Dirección de Informática o quien esta designe. Este proceso contará con el apoyo de los integrantes del comité interno de seguridad, el cual está compuesto por el Encargado de Ciberseguridad, el Jefe de Soporte y Redes, y el Jefe de Sistemas. La política se actualizará de manera obligatoria cuando se produzcan cambios normativos, tecnológicos o estratégicos que así lo requieran, pasando por la autorización final del alto comité, determinando la pertinencia de la actualización.

Vigencia

La presente Política de Ciberseguridad entrará en vigor a partir de su aprobación por las autoridades competentes de la Universidad Academia de Humanismo Cristiano.

Toda situación no prevista, vacío normativo o duda interpretativa que surja con ocasión de la aplicación de la presente Política de Ciberseguridad, y que no se encuentre regulada en la Política de Protección y Manejo de Datos, será resuelta por la Rectoría de la Universidad o por la unidad en la cual esta delegue expresamente dicha facultad, velando en todo momento por la coherencia con los principios éticos, normativos e institucionales.

Anexos

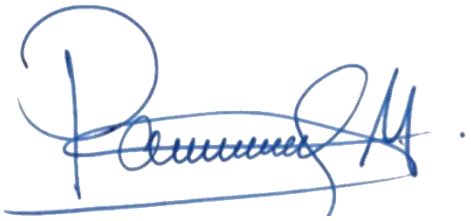
La Política de Ciberseguridad se complementa con los siguientes documentos, divididos en Anexos Normativos y Operativos, siendo cumplimiento obligatorio y forman parte integrante del sistema de control institucional:

Anexos Normativos

- Protocolo de Identidad Digital y Cuentas Institucionales.
- Protocolo de Privacidad y Uso de la Plataforma Campus Virtual
- Protocolo Uso de Recursos Computacionales.

Anexos Operativos

- Protocolo de Respaldo y Recuperación.
- Plan de Recuperación ante Desastres (DRP).



Paulina Miranda Santana, Secretaria General y ministra de fe de la Universidad Academia de Humanismo Cristiano, certifica que, con fecha 28 de enero de 2026, en sesión extraordinaria del Consejo Superior Universitario se aprueba la Política de Ciberseguridad, ratificada por Decreto de Rectoría N° 033/2026 de fecha 29 de enero de 2026.