Universidad de O'Higgins

# POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

*Universidad de O'Higgins*

Universidad de O'Higgins
Mayo de 2024

# Política General de Seguridad de la Información

*Prorrectoría*

Universidad de O'Higgins

# Índice

# I. CONTEXTO

La Universidad de O'Higgins (UOH) es una institución estatal de educación superior, dinámica, inclusiva, comprometida con la región a la que pertenece y conectada con el mundo, que asume con vocación de excelencia su contribución al desarrollo sostenible del país.

En su quehacer, la Universidad cultiva, desarrolla y transfiere el saber y las competencias en diversas áreas del conocimiento, a través de la formación integral de personas, la investigación de alto nivel, la creación e innovación y la vinculación con el medio. Todo su quehacer misional lo realiza escuchando a la sociedad y en permanente conexión con el progreso mundial, para mantener siempre la pertinencia y los más altos estándares.

La UOH, al ser una institución destinada a la educación superior, posee una gran cantidad de datos e información sensible y confidencial tanto de sus funcionarias y funcionarios, así como de sus estudiantes; dentro de esta información se pueden encontrar datos personales, notas, nóminas de personal, remuneraciones, investigaciones académicas, entre otras.

Es por esto que, la Universidad de O'Higgins reconoce la información como un activo y elemento crítico para el cumplimiento de sus objetivos y también como un pilar para el desarrollo estratégico que permita su desarrollo a largo plazo. La Universidad reconoce la importancia y el valor de la información para alcanzar eficiencia y eficacia en sus procesos, lo que finalmente se refleja en el cumplimiento de sus objetivos con altos niveles de calidad y pertinencia.

En consecuencia, se establece esta política que regula la gestión de la información, orientada a definir medidas que resguarden los "activos de la información" de la Universidad y la continuidad de los servicios que son necesarios para la correcta operación de esta.

Los "activos de la información" son todos los recursos y elementos que posee una organización para procesar, almacenar, transmitir y gestionar su información. Estos recursos pueden ser físicos (como computadores, dispositivos de almacenamiento USB, servidores) o lógicos (como software, bases de datos, archivos digitales) y también incluyen información confidencial o privada que la Universidad deba proteger. La gestión adecuada de los activos de la información es esencial para resguardar la confidencialidad, integridad y disponibilidad de la información, y para prevenir riesgos y amenazas como el acceso no autorizado, el robo de datos o la pérdida de información crítica.

Las personas también pueden considerarse como activos de la información en una organización, ya que poseen conocimientos, habilidades y experiencia en el manejo de la información y su participación en la gestión y protección de la misma es fundamental. Los funcionarios y funcionarias, colaboradores, clientes y proveedores son algunos ejemplos de personas que pueden ser considerados activos de la información.

Una mala gestión de los activos de información puede materializar consecuencias tales como:

- Pérdida de los activos de información (datos, equipos, documentación, investigaciones).
- Pérdida o menoscabo de imagen como institución de educación superior.
- Interrupción total o parcial de los procesos claves para el funcionamiento de la Universidad.
- Consecuencias legales derivadas del no cumplimiento de las normativas nacionales, respecto a seguridad de la información o ciberseguridad.
- Otros.

Teniendo en cuenta que existen variadas amenazas en el sector público, a nivel nacional y a nivel mundial, en contexto de seguridad de la información y ciberseguridad, es que la Universidad de O'Higgins ha asumido el compromiso de implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (desde ahora, SGSI), que permita alcanzar niveles adecuados de seguridad en todos los activos de información de la organización, de tal forma que los riesgos de seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la institución de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en el entorno y la tecnología.

De esta forma, la Universidad de O'Higgins se compromete a velar, en la medida de lo posible, por la integridad, disponibilidad y confidencialidad de la información, a través del cumplimiento de los requisitos que el sistema de gestión en sí requiera para su adecuado funcionamiento.

Lo anteriormente descrito se desarrollará bajo la convicción que tiene la Universidad de que los datos e información de sus académicas, académicos, estudiantes, funcionarias, funcionarios y todas y todos sus colaboradores, son de vital importancia, por lo que deben gestionarse al más alto nivel posible en lo relativo a su seguridad. De esta forma, la Universidad de O'Higgins sigue avanzando y fomentando la creación de calidad, con el fin de entregar siempre lo mejor en todo ámbito posible relacionado a su quehacer.

## II. OBJETIVO GENERAL

Establecer los lineamientos que regulen la gestión de la información y sus activos. Estos deben estar orientados también a definir medidas que resguarden la confidencialidad, integridad y disponibilidad de la información y la continuidad de los servicios que de ella dependen, así como dar cumplimiento a las normativas legales dictadas por el Estado de Chile en materias de ciberseguridad.

## III. OBJETIVOS ESPECÍFICOS

I. Establecer las directrices sobre el uso correcto de los activos de información y de las medidas para su resguardo.

II. Establecer necesidades de seguridad de la información e incentivar la comprensión de las responsabilidades individuales en todo el personal de la Universidad.

III. Determinar las medidas que deban ser adoptadas para protegerse de amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de la información; controlar, prevenir y mitigar los riesgos a los que la información de la Universidad está expuesta, identificando las vulnerabilidades y amenazas a las que se enfrenta.

IV. Proporcionar a la Universidad opciones que faciliten la toma de decisiones apropiadas en situaciones relacionadas con la preservación de la seguridad de la información.

V. Identificar los activos de información críticos presentes en todos los procesos considerados como cruciales en la Universidad, de manera de poder catalogar y clasificar dichos activos en un inventario de activos de información.

VI. Establecer un responsable que vele por la confidencialidad, integridad y disponibilidad de cada activo crítico de información.

VII. Establecer la gobernanza y el liderazgo necesario dentro de la organización para la implementación del SGSI.

VIII. Generar planes de capacitación anual, observando los requerimientos de la seguridad de la información.

IX. Auditar periódicamente el Sistema de Gestión de Seguridad de la Información para asegurar su eficacia y eficiencia.

# IV. ALCANCE

## I. Personas

La Política General de Seguridad de Información se aplica a todo el personal de la Universidad, en cualquier modalidad de contratación, al personal externo que presta servicios y a todo integrante o colaborador que tenga acceso a algún activo de la información.

## II. Activos

La Política General de Seguridad de la Información se aplica a todos los activos de información, independiente de su forma (digital, físico, escrito, transmitido de forma oral, o cualquier otro medio de almacenaje y distribución) que contengan información de la Universidad. Finalmente, esta política será aplicable a todas las estructuras organizacionales (Rectoría, Prorrectoría, Vicerrectorías, Direcciones, Secretarías, Gabinetes, Unidades y cualquier otra subdivisión de la Universidad). Esta política es aplicable a todos los proveedores, al igual que a todos aquellos que tengan relación con el procesamiento, almacenamiento y/o tratamiento de la información y sus activos de información relacionados en cualquiera de sus formas.

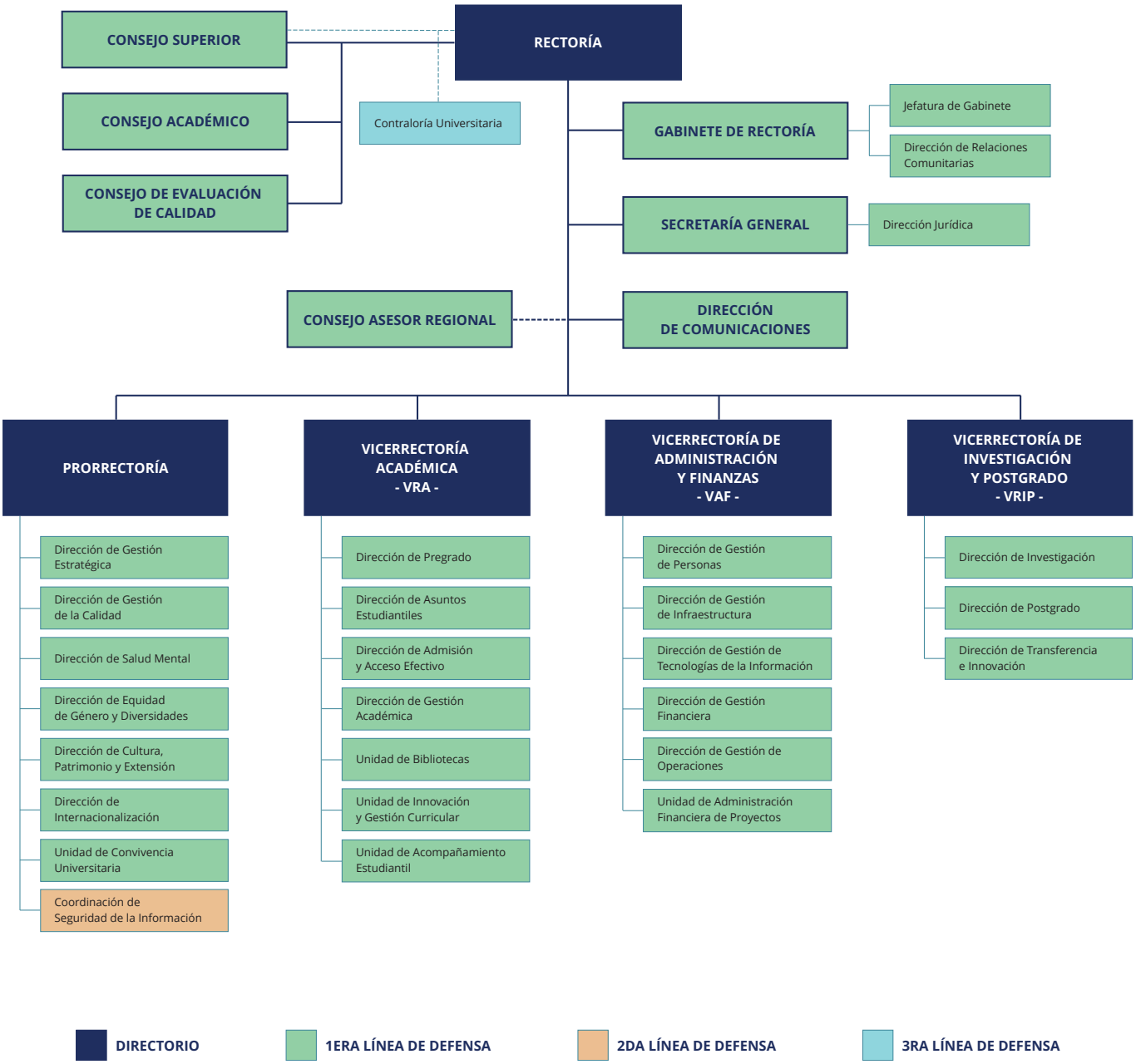
## III. Estructuras Organizacionales

La Política General de Seguridad de la Información se aplica a toda la Universidad.

En la siguiente hoja, se puede apreciar la estructura organizacional basada en el modelo de gestión de riesgos de 3 líneas de defensa de COSO (marco de referencia para el diseño, implementación y evaluación de controles internos en las organizaciones), que se utilizará para el SGSI.

El modelo de 3 líneas de defensa de COSO es una herramienta que las organizaciones pueden utilizar para asegurar una gestión adecuada de los riesgos. En este modelo, se establecen tres áreas de responsabilidad: la primera línea, que es responsable de la gestión diaria de los riesgos y oportunidades; la segunda línea, que proporciona supervisión y monitoreo de los procesos de gestión de riesgos; y la tercera línea, que es responsable de la auditoría interna y la evaluación independiente de los procesos de gestión de riesgos y controles internos. De esta forma, el modelo de 3 líneas de defensa de COSO permite una distribución clara de responsabilidades y una mejor gestión de los riesgos en una organización, lo que puede contribuir a su éxito y sostenibilidad a largo plazo.

## Estructura organizacional de 3 líneas de defensa, según contexto de la Universidad:




*Prorrectoría*

## Primera línea de defensa, funciones:

- Identificar los activos de la información en sus procesos para dar cumplimiento a la Política General de Seguridad de la Información.

- Resguardar los activos de la información en términos de seguridad física, ambiental y los relativos a personal externo.

- Analizar e implementar medidas o controles para detectar y mitigar riesgos y potenciales amenazas a la seguridad de la información de la Universidad.

- Detectar, investigar y generar acciones de mitigación de impacto para amenazas o incidentes de seguridad de la información y ciberseguridad y resguardar la confidencialidad, disponibilidad e integridad de sus activos de información.

- Evaluar oportunamente los riesgos asociados a la seguridad de la información y ciberseguridad que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades y/o definir nuevos procesos.

- Gestionar sus alertas o amenazas e incidentes de seguridad de la información y ciberseguridad, con el fin de detectar, investigar y generar acciones de mitigación de impacto de estos eventos, y resguardar la confidencialidad, disponibilidad e integridad de sus activos de información.

- Identificar las amenazas y vulnerabilidades que puedan comprometer los activos de información, de manera que se pueda resguardar la operatividad de los procesos críticos.

- Permitir la evaluación, a través de auditorías internas, de los controles existentes para así conocer su eficacia y suficiencia.

- Identificar las consecuencias que puedan tener en los activos de información las pérdidas de confidencialidad, integridad y disponibilidad.

- Realizar un proceso de análisis de riesgo, que considera elementos como la evaluación de la probabilidad de ocurrencia de incidentes y su consecuencia o impacto en los activos de información.

## Segunda línea de defensa, funciones:

- Colaborar en el desarrollo y difusión de planes de capacitación y concientización para todos los funcionarios y funcionarias en materia de seguridad de la información y ciberseguridad.
- Gestionar la evaluación de los riesgos asociados a la seguridad de la información y ciberseguridad con las distintas áreas de la Universidad.
- Asegurar el cumplimiento de las leyes y normativas vigentes en relación a seguridad de la información y ciberseguridad.
- Diseñar y mantener un adecuado sistema de identificación, seguimiento, control y mitigación de los riesgos de seguridad de la información y ciberseguridad
- Desarrollar un proceso formal tendiente a comunicar los riesgos de seguridad de la información a la Universidad.
- Verificar que los riesgos resultantes sean concordantes con la tolerancia a los riesgos definida.
- Verificar con al menos una periodicidad anual, el proceso de gestión de riesgos de seguridad de la información y ciberseguridad, de manera de identificar oportunamente la necesidad de efectuar ajustes en las metodologías y/o herramientas utilizadas.
- Elaborar un plan de tratamiento del riesgo.
- Prestar apoyo tanto a la primera como tercera línea de defensa en las gestiones que deban realizar.

### Tercera línea de defensa, funciones:

- Llevar a cabo revisiones regulares de la eficacia del SGSI. Incluir en estas revisiones el cumplimiento de la política y los objetivos del SGSI y revisar las prácticas de seguridad y privacidad.
- Realizar auditorías de SGSI a intervalos planificados.
- Realizar periódicamente una revisión de la gestión del SGSI para asegurar que el alcance sigue siendo adecuado y que se identifican mejoras en el proceso del SGSI.
- Registrar acciones y eventos (observaciones y seguimientos a estas) que podrían tener un impacto en la eficacia o el rendimiento del SGSI.
- Hacer aportes (oportunidades de mejora) para el mantenimiento de los planes de seguridad, para tener en cuenta los hallazgos de las actividades de monitorización y revisión.
- Proporcionar evaluaciones imparciales y objetivas, así como proporcionar asesoramiento sobre la adecuación y eficacia del gobierno y la gestión de riesgos. Esto se realiza en colaboración con el Oficial de Seguridad de la Información.
- Apoyar el logro de los objetivos de la Universidad, promover y facilitar la mejora continua de los procesos y procedimientos.
- Informar al directorio las deficiencias en la independencia y la objetividad y aplicar las medidas de mitigación necesarias.

## V. CONTENIDO DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y SUS POLÍTICAS ESPECÍFICAS

La Política General de Seguridad de la Información, y sus políticas específicas, establecen la declaración de intenciones de la Universidad respecto a la seguridad de la información, así como los deberes de los usuarios y usuarias con respecto a la utilización de los activos de la información entregados por la Universidad de O'Higgins, para que puedan desarrollar sus labores diarias con el debido apoyo tecnológico.

Los usuarios y usuarias deberán respetar las medidas de seguridad que se indiquen en las políticas, las cuales revisten, cada una, el carácter de obligatorias para todas las personas que trabajan o cumplen labores en la Universidad de O'Higgins, no importando su calidad contractual.

# VI. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

- La Política de Seguridad de la Información de la Universidad de O'Higgins ha sido elaborada en concordancia con la legislación vigente y en base a los requisitos de la NCh ISO 27001.

- El Equipo Directivo de la Universidad se compromete a realizar las acciones que estén a su alcance para velar por la seguridad de la información, la prestación de servicios y la continuidad operativa de todos sus activos de información (disponibilidad).

- El Equipo Directivo de la Universidad, a través del Sistema de Gestión de Seguridad de la Información (SGSI), establecerá las acciones necesarias para proteger los sistemas de información críticos que reportan información en todas las áreas de la Universidad.

- El Equipo Directivo de la Universidad se compromete a realizar las acciones que sean necesarias para velar por la confidencialidad de la información de todo el personal de la Universidad, así como de sus estudiantes.

- El Equipo Directivo de la Universidad se compromete a mantener la disponibilidad de los sistemas de información necesarios para el desarrollo de sus procesos, a fin de asegurar las condiciones de trabajo óptimas para todo el personal.

- El Equipo Directivo de la Universidad se compromete a realizar las acciones que sean necesarias para mantener la integridad de los datos almacenados en los sistemas de información de la Universidad.

- La estructura documental para la gestión de la seguridad de la información en la Universidad, estará compuesta por esta Política General de Seguridad de la Información, políticas asociadas o específicas de seguridad de la información, procesos, procedimientos, reglamentos e instructivos.

- El incumplimiento de la Política General de Seguridad de la Información, políticas específicas, procesos, procedimientos, reglamentos e instructivos, podría dar pie a la aplicación de diversas sanciones de acuerdo con el Estatuto y Procedimiento Administrativo vigente establecidos en la Ley, o aquellas deliberadas por el Comité de Seguridad de la Información o el Equipo Directivo de la Universidad.

- El desarrollo y las modificaciones de esta Política General de Seguridad de la Información, será responsabilidad del Comité de Seguridad de la Información de la Universidad.

- El Oficial de Seguridad de la Información (CISO) es el responsable del ciclo de vida del SGSI y actuará en la segunda línea de defensa de la organización, trabajando y colaborando con Contraloría Universitaria, cuyo ámbito de trabajo será en la tercera línea de defensa.

# VII. POLÍTICAS ESPECÍFICAS

La Política General de Seguridad de la Información de la Universidad de O'Higgins establecerá las siguientes sub políticas asociadas o políticas específicas para todo el personal de la institución:

- Política de uso de sistemas de información.
- Política organizacional del SGSI.
- Política de uso de contraseñas.
- Política de conexión o conectividad wifi.
- Política de escritorio limpio.
- Política de correo electrónico.
- Política de control de acceso físico y ambiental.
- Política de privacidad.
- Política de antivirus.
- Política de instalación de software.
- Política de acceso y uso de la internet.
- Política de vulnerabilidades técnicas.
- Política de gestión de incidentes.
- Política de desarrollo seguro.
- Política de continuidad de seguridad de la información.
- Política de intercambio de información.
- Política de gestión de personas del SGSI.

- Política de gestión de activos de información.
- Política de respaldos.

En todos los contratos que la Universidad de O'Higgins celebre con proveedores o empresas externas, en los que se requiera usar activos de información o tener acceso a los sistemas de información, el ítem de cumplimiento de la Política General de Seguridad de la Información y sus políticas específicas deberá estar presente explícitamente.

## VIII. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades del SGSI, se encuentran definidos en la Política Organizacional del SGSI.

## IX. REVISIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La presente política y todas sus políticas específicas deberán ser revisadas y actualizadas, según corresponda, a lo menos una vez al año, para asegurar su conveniencia, suficiencia y eficacia continua.

La Política General de Seguridad de la Información y sus políticas específicas, también podrán ser revisadas y actualizadas en caso de generarse incidentes o contingencias que afecten drásticamente a la Universidad, o por cambios legales o normativos que lo ameriten.

La revisión del cumplimiento de todas las políticas estará a cargo de la Contraloría Universitaria, la cual se efectuará a través de auditorías al SGSI. Asimismo, el Oficial de Seguridad de la Información también deberá velar por el cumplimiento de las políticas y sus revisiones periódicas.

## X. EXCEPCIONES A LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En casos especiales en donde se necesite no aplicar la Política General de Seguridad de la Información y sus directrices, el Comité de Seguridad de la Información deberá evaluar dicha solicitud para adoptar las medidas puntuales respecto a la excepción solicitada. Dicha resolución deberá ser justificada y quedar como información documentada para revisiones o para las auditorías pertinentes, o en efecto, para futuras mejoras de esta.

## XI. SANCIONES POR INCUMPLIMIENTO

El no cumplimiento de las declaraciones y directrices de la Política General de Seguridad de la Información o de sus políticas asociadas o específicas dará pie a ejecutar procedimientos disciplinarios, los cuales podrían terminar en sanciones administrativas, conforme a los reglamentos internos de la Universidad y a las leyes con la que esta debe cumplir.

El dictamen de si los incumplimientos son de carácter grave con respecto a los reglamentos internos de la Universidad, deberá ser evaluado por el Comité de Seguridad de la Información en conjunto con el área legal y la Contraloría de la institución.

## XII. DIFUSIÓN DE LA POLÍTICA

La difusión de la Política General De Seguridad de la Información se realizará a través de correo electrónico a todo el personal de la Universidad (indistintamente de su calidad de contrato), colaboradores y personal externo. Asimismo, se deberá publicar en el sitio web de la Universidad y en su intranet para facilitar su acceso y su conocimiento.

## XIII. REFERENCIAS NORMATIVAS

- Ley N°18.834: Ley sobre Estatuto Administrativo.
- Ley 20285: Principio de Transparencia de la función pública y el derecho de acceso a la información.
- Ley 19.880: Sobre el Procedimiento Administrativo.
- Ley 17.336: Ley sobre propiedad Intelectual.
- Ley 20.435: Modifica Ley sobre propiedad Intelectual.
- Ley N°19.628: Ley sobre protección de la vida privada.
- Decreto supremo 83, que aprueba una norma técnica para los órganos de administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
- ISO 27001: Sistema de Gestión de la Seguridad de Información.
- ISO 27002: Prácticas para la gestión de la seguridad de la información.

Universidad de O'Higgins

| Versión | Realizado por | Aprobado por | Fecha |
|---|---|---|---|
| 1.0 | Oficial de Seguridad de la Información | Prorrectoría | 24/05/2024 |

| Versión | Cambios de la versión | Fecha |
|---|---|---|
| 1.0 | Emisión del documento | 24/05/2024 |