DECRETO EXENTO Nº 412

VALPARAÍSO, 19 de mayo de 2025

V I S T O S:

1° Lo dispuesto en los DFL Nº 1 y 6, ambos de 1981; todos del entonces Ministerio de Educación Pública; en el DFL Nº 28 de 2023 Ministerio de Educación; decreto exento N°1253 de 2017; decreto exento N°1546 de 2023 que fija las normas sobre control de juridicidad de la Contraloría Interna y supervisión legal de la Fiscalía General y, en el Decreto Supremo de Educación N° 167 de 2024.

C O N S I D E R A N D O:

1º El decreto exento 406 de 2025, que aprueba el acuerdo Nº 3, adoptado en Sesión Ordinaria Nº 431, de fecha 22 de abril de 2025, de la Honorable Junta Directiva de la Universidad de Valparaíso, cuyo texto es el siguiente: *"Por la unanimidad de sus miembros presentes en la sesión, la Junta Directiva de la Universidad de Valparaíso acuerda aprobar las Políticas Generales de la Universidad"*.

2° El oficio ordinario Nº 19 de fecha 24 de abril de 2025 en que la directora general de Desarrollo Institucional y Aseguramiento de la Calidad remite al rector los antecedentes para la tramitación del decreto correspondiente, relativo a la política general de seguridad de la información y ciberseguridad.

3° La conformidad expresada por el Vicerrector de Gestión Institucional, Dirección General de Modernización y Transformación Digital y, de la directora general de Desarrollo Institucional y Aseguramiento de la Calidad en el cuerpo del presente escrito.

D E C R E T O:

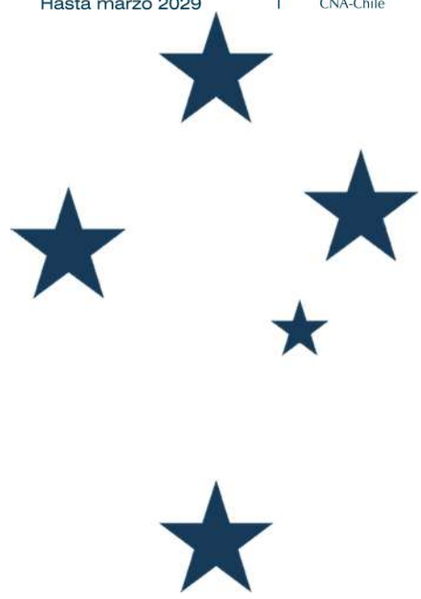
I. **APRUÉBASE** la política general de seguridad de la información y ciberseguridad, cuyo texto es el siguiente:

Inicio de la transcripción

Universidad de Valparaíso
CHILE

Universidad de Valparaíso
ACREDITADA
NIVEL DE EXCELENCIA
Gestión Institucional, Docencia de Pregrado
Investigación, Vinculación con el Medio y
Docencia de Postgrado
Hasta marzo 2029

Comisión Nacional de Acreditación
CNA-Chile



Universidad de Valparaíso
CHILE

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD SGSI-PG-001

DIRECCIÓN GENERAL DE MODERNIZACIÓN Y TRANSFORMACIÓN DIGITAL
DEPARTAMENTO DE CIBERSEGURIDAD

I.- DEFINICIONES ESTRATÉGICAS

La seguridad de la información es fundamental para el éxito y la continuidad de las operaciones de la Universidad de Valparaíso. La institución, a través de su Departamento de Ciberseguridad, presenta en este documento las características, responsabilidades y consideraciones operacionales mínimas obligatorias para la administración de los activos de información de interés a fin de garantizar la continuidad operacional y la seguridad de la información en lo que se refiere a su confidencialidad, integridad y disponibilidad.

La presente política establece directrices, responsabilidades y procedimientos para proteger la confidencialidad, integridad y disponibilidad de la información y sistemas críticos de la institución. Cada funcionario(a) de planta, suplente, contrata, reemplazo, personal a honorarios, académico/a, directivo/a, estudiantes, ex alumnos(as) titulados/as, graduados/as, proveedores/as de servicios y personal externo debe cumplir con esta política.

Un activo de información en el contexto de la norma ISO/IEC 27001 es: “algo que una empresa valora y por lo tanto debe proteger”. La información es un activo vital, y todos sus accesos, usos y procesamiento deberán estar vinculados con las políticas y procedimientos establecidos por la Universidad de Valparaíso.

La gestión de activos de información es una tarea de gestión de la información que involucra el diseño, establecimiento e implementación de un proceso que permita la identificación, valoración, clasificación y tratamiento de los activos de información más importantes del negocio.

I.1.- DECLARACIÓN INSTITUCIONAL

La Universidad de Valparaíso, a través de su Departamento de Ciberseguridad, se compromete instaurar un Sistema de Gestión de Seguridad de la Información (SGSI) para proteger los activos de información de los procesos que hacen posible la existencia de la institución, estableciendo una adecuada gestión del riesgo, aplicando y monitoreando controles para la mitigación del riesgo detectado para llevarlo a niveles compatibles con el riesgo residual tolerable. Los resultados de la aplicación del SGSI serán evaluados bajo la perspectiva de la mejora continua, asegurando el cumplimiento de los requisitos legales y aplicando una estrategia de seguridad basada en las mejores prácticas y controles sobre los activos de información.

La Universidad de Valparaíso se compromete a disponer y utilizar adecuadamente plataformas electrónicas cumpliendo con estándares de seguridad, interoperabilidad, interconexión y ciberseguridad, así como las condiciones de accesibilidad, seguridad, funcionamiento, calidad, protección y conservación de los documentos, establecidas en los estándares técnicos establecidos por los reguladores, la ley vigente y las propias definiciones estratégicas.

La Universidad de Valparaíso se compromete a colaborar con el ecosistema digital en materia de ciberseguridad, tanto es sus aspectos técnicos como jurídicos.

La Universidad de Valparaíso se compromete a establecer e incorporar en su diario quehacer los requisitos para la seguridad de la información, la continuidad operacional del servicio y la continuidad de la administración de la seguridad de la información ante situaciones adversas, es decir, durante una crisis, desastre o Estado de Excepción Constitucional.

Ante la eventual ausencia de estándares o normas fijadas por los órganos llamados a esta función, atingentes a seguridad de la información o ciberseguridad, la Universidad de Valparaíso considerará como estándar referencial válido a utilizar e implementar, los estándares vigentes ISO 27.001, ISO 27.002, ISO 27.032, ISO 22.301 y en general, los que sean técnicamente validados por Departamento de Ciberseguridad.

I.2.- OBJETIVO GENERAL

Establecer los principios y marco general de trabajo de la Universidad de Valparaíso para administrar, mantener, sensibilizar, monitorear y revisar el Sistema de Gestión de Seguridad de la Información (SGSI) acorde a las definiciones estratégicas, la misión/visión y objetivos estratégicos del negocio, asegurando la confidencialidad, integridad y disponibilidad de los activos de la información a través de su adecuada implementación, asignación de roles, funciones y responsabilidades.

I.2.1. OBJETIVOS ESPECÍFICOS

1. Asegurar el cumplimiento de los requisitos normativos, reglamentarios y contractuales, que estén orientados hacia la seguridad de la información.
2. Establecer los niveles de acceso apropiados a la información, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema, proceso, actividad crítica y usuario.
3. Apoyar al modelo de gestión de continuidad de negocio.
4. Establecer un marco de gestión de riesgo cibernético para cada sistema, proceso, actividad crítica, que permita alcanzar los objetivos estratégicos.
5. Definir el ámbito de trabajo y responsabilidades corporativas e individuales respecto al uso de los recursos tecnológicos que provee la institución y al manejo de la información.

I.3.- ALCANCE

Esta política general contiene lineamientos que aplican de forma transversal a todos los procesos de la Universidad de Valparaíso, en materias relativas a la seguridad de la información y ciberseguridad.

Esta política general, y las específicas que emanen de ella, se aplica a todos los activos de información, sistemas de tecnología de la información, funcionarios/as de planta, suplentes, contrata, reemplazo, personal a honorarios, académico/as, directivo/a, estudiantes, titulado/a, graduados, proveedores de servicios y personal externo de la Universidad de Valparaíso.

Esta política se aplica a todos los trabajadores y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de

información de la Universidad de Valparaíso, esto es, funcionarios (as) de planta, suplente, contrata, reemplazos, personal a honorarios, académicos, directivos, alumnos, ex alumnos, proveedores de servicios y personal externo que utilicen los recursos tecnológicos y sistemas de información de la Universidad de Valparaíso, sea cual fuere su nivel jerárquico y su calidad contractual. También se aplica a cualesquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información.

Esta política rige independientemente del lugar en el que el trabajador presta sus servicios a la institución, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea "presencial", "a distancia", "teletrabajo" u otra, en las condiciones que establezca la legislación vigente, los planteamientos de la Contraloría General de la República, Dirección del Trabajo o los Estados de Excepción Constitucional decretados por el Presidente de la República.

Esta política gobierna la seguridad de la información de todos los procesos de la Universidad de Valparaíso, establecidos por las Autoridades y el Consejo Superior, cubriendo a toda la organización independiente de su ubicación geográfica en el país (Chile Continental, Chile Insular o la Antártica Chilena).

I.4.- REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

El Comité de Ciberseguridad de la Universidad de Valparaíso podrá solicitar a una unidad interna u organismo auditor externo la realización de auditorías o revisiones independientes sobre el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad, las políticas específicas, los procedimientos establecidos para operativizar las políticas, el proceso de gestión del riesgo, y en general el funcionamiento y operación del Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad de Valparaíso.

I.5.- MARCO REFERENCIAL

Los contenidos y controles esenciales de carácter legal que se consideraran en las políticas de la Universidad de Valparaíso son:

1. NCh-ISO 27001/27002 - Tecnología de la Información – Código de prácticas para la gestión de seguridad de la información - INN Chile.
2. Decreto 83: Aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
3. Ley 21.180: Transformación digital del Estado.
4. Ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
5. Decreto Supremo 181, Aprueba reglamento de la ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.
6. Ley N°19.628: sobre Protección de la vida privada.
7. Ley N° 19.223: sobre Delitos informáticos.

8. Ley N° 17.336: de Propiedad Intelectual.
9. Ley N° 18.168: Ley General de Telecomunicaciones.
10. Ley N° 19.927: Modifica el código penal, el código de procedimiento penal y el código procesal penal en materia de delitos de pornografía infantil.
11. Política Nacional de Ciberseguridad 2023-2028.
12. Ley N° 21.663: Ley Marco de Ciberseguridad.

I.6.- VIGENCIA Y ACTUALIZACIÓN

La política entra en vigencia desde su aprobación por la autoridad correspondiente y será objeto de revisión cuando las condiciones internas o externas así lo requieran. Dicha revisión estará a cargo del Comité de Ciberseguridad, y será promovida de forma continua por el Departamento de Ciberseguridad, con el propósito de mantener su alineación con las amenazas emergentes, el contexto normativo, organizacional y tecnológico, así como los riesgos que puedan afectar a la Universidad de Valparaíso. Se establecen como criterios de revisión aquellos cambios que impacten significativamente la operación institucional, tales como reformas legales, incorporación de procesos críticos, cambios tecnológicos o estratégicos, reorganizaciones estructurales, o situaciones excepcionales que comprometan la seguridad de la información o las infraestructuras críticas.

I.7.- REVISIÓN DEL CUMPLIMIENTO

El Departamento de Ciberseguridad, anualmente, asignará la responsabilidad de ejecutar un proceso formal de revisión del cumplimiento a cargo de una o varias unidades organizacionales, pudiendo optar también por una revisión independiente interna o una externa ejecutada por una tercera parte.

Además, este comité determinará la metodología y los alcances que estime necesarios para cumplir los objetivos estratégicos de revisión y cumplimiento de las políticas y su mejora continua.

I.8.- CONTROL DE DOCUMENTOS

Los documentos requeridos por el Sistema de Gestión de la Seguridad de la Información (SGSI) de la Universidad de Valparaíso se deben proteger y controlar.

Las versiones pertinentes de los documentos aplicables se encontrarán disponibles para quienes lo necesiten, y serán almacenados y transferidos de acuerdo con los procedimientos aplicables a su clasificación.

I.9.- RESPONSABILIDADES

Roles	Responsabilidades
Consejo Superior u órgano equivalente y Consejo Universitario u órgano equivalente.	Responsables de aprobar las iniciativas para apoyar el establecimiento de una cultura de seguridad en la universidad.
Director (a) de la Dirección General de Modernización y Transformación Digital de la Universidad de Valparaíso.	Es responsable de proponer las políticas específicas, objetivos y metas en los ámbitos de modernización y transformación digital de la universidad y que se encuentren relacionadas con la presente política, y de realizar la coordinación y el seguimiento de su ejecución, disponiendo las acciones que de ello se deriven, en el marco de lo establecido en el plan de desarrollo institucional. Supervisor/a, revisor/a.
Jefe (a) del Departamento de Ciberseguridad de la Universidad de Valparaíso	Deberá supervisar y coordinar todas las actividades de seguridad de la información y ciberseguridad que garanticen el cumplimiento de la presente política y la evaluación de los riesgos. Es responsable de velar por el cumplimiento de la política general, políticas específicas, procedimientos y normativas que emanan de ella, y del seguimiento y mejora de los términos de la política, de sus revisiones, y de su difusión en la institución. Observador/a, supervisor/a, revisor/a, y ejecutor/a.
Jefe (a) del Departamento de Tecnologías de la Información y Comunicación (DTIC).	Responsable del cumplimiento de la política a nivel de unidades del Departamento de tecnologías de Información y Comunicación (DTIC), servicios de soporte y externos mediante seguimiento y verificación de la correcta aplicación de esta política. Deberá adscribirse a la presente política para efectos de todo procedimiento que se genere en las unidades internas y para dar cumplimiento cabal con las mejores prácticas en seguridad de la información. Responsable de velar por la implementación y mantenimiento de las medidas de seguridad técnicas. Revisor/a, ejecutor/a.
Funcionarios (as) (planta, contrata, suplente, reemplazos, honorarios.	Todos/as los/as funcionarios/as deberán seguir las prácticas de seguridad definidas, y reportar incidentes de seguridad de la información y ciberseguridad de inmediato, y en forma confidencial, al Departamento de Ciberseguridad.
Académicos (as)	Todos/as los/as académicos/(as) deberán seguir las prácticas de seguridad definidas, y reportar incidentes de seguridad de la información y ciberseguridad de inmediato, y en forma confidencial, al Departamento de Ciberseguridad.
Estudiantes	Todos los estudiantes deberán seguir las prácticas de seguridad definidas, y reportar incidentes de seguridad de la información y ciberseguridad de inmediato, y en forma confidencial, al Departamento de Ciberseguridad.
Titulados/as y graduados/as	Todos/as los/as titulados/as y graduados/as deberán seguir las prácticas de seguridad definidas, y reportar incidentes de

Roles	Responsabilidades
	seguridad de la información y ciberseguridad de inmediato, y en forma confidencial, al Departamento de Ciberseguridad.
Proveedores/as de servicios y personal externo a la Universidad de Valparaíso	Todos/as los/as proveedores/as de servicios y personal externo a la Universidad de Valparaíso deberán seguir las prácticas de seguridad definidas, y reportar incidentes de seguridad de la información y ciberseguridad de inmediato, y en forma confidencial, al Departamento de Ciberseguridad.
Comité de Ciberseguridad	Responsable de: • Ciclo de vida de las políticas relacionadas con seguridad de la información y ciberseguridad de la Universidad de Valparaíso. • Validar las políticas de seguridad de la información y ciberseguridad. • Velar por la implementación de los roles de seguridad en la plataforma tecnológica. • Promover la realización de campañas de concientización y formación. • Revisar, al menos 1 vez al año, el funcionamiento del SGSI (Sistema de gestión de Seguridad de la Información de la Universidad de Valparaíso). De acuerdo con lo indicado en el Decreto Exento 3752, del 20 de diciembre de 2022, el Comité de Ciberseguridad estará presidido por el vicerrector/a de Gestión Institucional e integrado por el/la director/a General de modernización y transformación digital, jefe/a del Departamento de Tecnologías de Información y Comunicación, jefe/a del Departamento de Ciberseguridad y abogada/o de Fiscalía General.
Dirección de Gestión y Desarrollo de Personas (DGDP)	Incorporar, de acuerdo con la disponibilidad de recursos, la aplicación y observancia de las políticas de seguridad de la información y ciberseguridad en el plan de capacitación institucional. Velar por la correcta inducción de los/as funcionarios/as en materia de seguridad de la información y ciberseguridad.

Las responsabilidades y funciones de la estructura de la Universidad de Valparaíso se encontrarán descritas en sus respectivas resoluciones de creación y designación.

I.9.1.- RESPONSABILIDADES EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Será responsabilidad individual inexcusable de los/as funcionarios(as) de planta, suplente, contrata, reemplazos, personal a honorarios, proveedores/as de servicios, académicos/as, estudiantes), que tengan acceso a los activos de información y al uso de las tecnologías de la información de la institución, dar cumplimiento a la presente política, políticas específicas, procedimientos o instructivos asociados al Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad de Valparaíso.

Las jefaturas y/o dueños de los procesos o responsables de los activos de información deben velar porque el personal de su dependencia conozca y cumpla la presente política general, políticas específicas, procedimientos o instructivos asociados al Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad de Valparaíso.

Los administradores/as y coordinadores/as de contrato deben velar porque los/as proveedores/as de servicios contratados y que tengan acceso a los activos de información de la Universidad de Valparaíso, den cumplimiento a la presente política general, políticas específicas, procedimientos o instructivos asociados al Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad de Valparaíso. Además, deben asegurar que, en los respectivos contratos de provisión de servicios, se incluyan cláusulas de confidencialidad de la información a la que tengan acceso a propósito de la ejecución de los servicios, cláusulas de auditoría, cláusulas relacionadas con los SLA´s, y cláusulas de responsabilidad por parte del/la proveedor/a sobre la integridad y disponibilidad de la información, servicios y continuidad de las operaciones.

I.10.- APROBACIÓN Y ENTRADA EN VIGOR

Esta política ha sido aprobada por el Consejo Superior de la Universidad de Valparaíso y entrará en vigor a partir de la fecha de aprobación.

I.11.- DIFUSIÓN

El mecanismo de difusión de la política será a través de la intranet, circulares informativas, correos electrónicos masivos o cualquier otro medio que el Departamento de Ciberseguridad estime pertinente, procurando apoyar la sensibilización con infografías que faciliten la comprensión de esta por todos los usuarios en general.

II.- PRINCIPIOS Y RESPONSABILIDADES TRANSVERSALES

II.1.- PRINCIPIOS GENERALES

La política general de seguridad de la información y ciberseguridad busca armonizar los controles necesarios con la debida funcionalidad de los procesos, de cara a los usuarios/as que utilizan los servicios y productos, alineados con las diferentes normativas, en función de la evaluación de riesgo y costo de los procesos.

Esta política estará basada en un supuesto que permita a la institución enfrentar el riesgo sujeto a los recursos económicos, tecnológicos y humanos disponibles.

Se han de considerar los diferentes desafíos que afecten la seguridad de la información y ciberseguridad con criterios de priorización, privilegiando los procesos que permitan el cumplimiento de los objetivos estratégicos de la institución y las regulaciones vigentes.

II.1.1. PRINCIPIOS ESPECÍFICOS

1. **Constitucionalidad y legalidad**: la presente política se deberá interpretar de manera tal que su aplicación se concilie con las normas constitucionales y legales vigentes, referidas a los derechos y libertades de las personas. Toda acción técnica de monitoreo, restricción, intervención o análisis de cuentas, comunicaciones o accesos digitales deberá fundarse en hechos verificables, ser proporcional al riesgo involucrado y respetar en todo momento la legislación nacional vigente, incluyendo las garantías constitucionales de privacidad, inviolabilidad de las comunicaciones, protección de datos personales y libertad académica. El Departamento de Ciberseguridad deberá actuar dentro de los límites de la ley y exclusivamente bajo mandatos institucionales expresos.
2. **Responsabilidad transversal**: toda la comunidad universitaria, incluyendo autoridades, académicos/as, funcionarios/as, estudiantes y también los/as proveedores/as de servicios que operen en el entorno institucional, deberán conocer, comprender y cumplir con lo establecido en la presente política. La seguridad de la información es una responsabilidad compartida que exige el compromiso activo y permanente de todos los integrantes de la Universidad de Valparaíso.
3. **Buen uso de los recursos institucionales:** el uso de los sistemas de información y comunicación debe enmarcarse en el ámbito de competencia de la institución, teniendo como finalidad el ejercicio de las funciones propias e inherentes para las cuales el/la usuario/a ha sido contratado/a o se ha convenido su prestación de servicios. Se promueve el buen uso de los sistemas de información y comunicación, especialmente para aquellas prácticas que protejan a los sistemas de eventuales daños ocasionados por amenazas cibernéticas, entre las que se pueden mencionar: físicas, desastres naturales, pérdida de servicios esenciales, perturbación debido a radiación, compromiso de información sensible, fallas técnicas, acciones no autorizadas, compromiso de funciones, acción de hacker, acción de ciberdelincuentes, acción terrorista, espionaje industrial, acción interna y otros.

4. **Obtención de prueba en procedimientos disciplinarios o auditorías internas**: en el contexto de procedimientos de investigación sumaria o auditorías internas, y previa autorización expresa del Fiscal sumariante o del Contralor universitario, el Departamento de Ciberseguridad podrá ejecutar, en sistemas o servidores administrados por la unidad correspondiente, procesos técnicos definidos orientados a la obtención de información necesaria para la investigación, procurando en todo momento que dichas acciones se realicen con el menor impacto posible en la privacidad del/la trabajador/a involucrado/a.
5. **Responsabilidad por uso malicioso**: la apertura de archivos adjuntos o la ejecución de programas que se reciban por medios electrónicos, constituyen acciones que pueden vulnerar la estabilidad, calidad o seguridad de las redes o de los sistemas de información. El personal no debe guardar, abrir o ejecutar en el equipo, programas o documentos electrónicos; si la fuente de éstos no es conocida; si no está autorizado por el propietario intelectual o industrial; como tampoco, si no se ha adquirido la licencia respectiva.
6. **Acciones especiales de seguridad**: el personal autorizado del Departamento de Ciberseguridad podrá dar recomendaciones al Departamento de Tecnologías de Información y Comunicación (DTIC) para restringir, bloquear o cancelar el acceso de un/a usuario/a a los servicios tecnológicos o a otro servicio o sistema de información, siempre que dicha acción de seguridad sea indispensable en los siguientes casos:
   a) Cuando existan requerimientos legales o judiciales, ante la presunta perpetración de algún ilícito en conocimiento del Oficial de Prevención y Cumplimiento.
   b) Cuando existan antecedentes fundados, previa calificación de las autoridades de la Universidad de Valparaíso, que den cuenta de la violación grave de la normativa interna o de la comisión de un ilícito, en conocimiento del Oficial de Prevención y Cumplimiento con la asesoría del Comité de Prevención del Modelo de Prevención de Delito de la Universidad de Valparaíso.
   c) Cuando por motivo del acceso se cause o pueda causar un daño grave e inminente a la calidad o estabilidad de la continuidad operacional de los servicios informáticos o de las redes institucionales. Esta circunstancia deberá ser informada por la jefatura del Departamento de Ciberseguridad a la autoridad de la unidad, dirección, carrera o facultad afectada, a más tardar dentro del día hábil siguiente desde que se inició la acción de seguridad.
   d) Cuando el acceso a los sistemas sea realizado por un agente externo sin vinculación directa con la Universidad de Valparaíso.
   e) Asimismo, el Departamento de Ciberseguridad deberá informar al/la usuario/a afectado/a por la acción de seguridad, con excepción de los casos contemplados en la Ley 20.393 donde el Oficial de Prevención y Cumplimiento con la asesoría del Comité de Prevención del Modelo de Prevención del Delito de la Universidad de Valparaíso dispongan lo contrario.
   f) Los procedimientos de intervención descritos no podrán ser utilizados con fines de supervisión de contenidos personales, control ideológico, vigilancia académica ni recopilación de datos sensibles sin consentimiento informado. Todo procedimiento de intervención deberá quedar debidamente documentado, indicando fecha, justificación, responsables técnicos, alcance y unidades afectadas, resguardar los derechos de privacidad de los usuarios, no obstaculizar el normal cumplimiento de los fines institucionales y estar previamente autorizado, en los términos que se contemplan en esta Política. El usuario tendrá derecho a conocer los fundamentos de la medida, a acceder al informe técnico y a presentar observaciones o reclamos ante el Comité de Prevención, la Contraloría Universitaria o el fiscal sumariante, en su caso, con excepción de que una

investigación u órgano judicial indique lo contrario.

g) Ninguna medida técnica de ciberseguridad podrá restringir, condicionar o interferir en el ejercicio legítimo de la libertad de cátedra, la autonomía de investigación o la libre expresión académica, conforme lo establece la Ley N°21.094. Las acciones de seguridad digital deberán respetar los principios de pluralismo, diálogo crítico, y no discriminación ideológica o disciplinaria. Con todo, el ejercicio de las mencionadas libertades y autonomías académicas se encuentra sujeto al cumplimiento de las disposiciones, deberes y estándares de la Ley N° 21.663, no pudiendo eximir de su observancia.

7. **Confidencialidad e integridad de la información**: se deberá garantizar y mantener la confidencialidad e integridad de toda la información y datos de los/as usuarios/as que tengan a los activos de información de la Universidad de Valparaíso.
8. **Seguridad ante la navegación en la internet**: el personal autorizado del Departamento de Tecnologías de Información y Comunicación (DTIC), previa autorización del Departamento de Ciberseguridad podrá ejecutar sistemas de filtro, monitoreo y registro del tráfico de la navegación en la internet que se realice a través de las redes de la institución, incluyendo la extranet (VPN) sólo para efectos de mantener protegida la seguridad y estabilidad de los recursos tecnológicos de la universidad, así como también para procurar que su uso común y regular esté abocado a los fines establecidos.

II.2.- DIFUSIÓN

II.2.1. OBLIGACIÓN DE CONOCIMIENTO Y CUMPLIMIENTO

El personal o terceras partes que usen los recursos informáticos de la red de la institución deberán conocer y dar cumplimiento a esta política general de Seguridad de la Información y Ciberseguridad.

II.2.2. INCORPORACIÓN DE LA NORMA A LAS ACTAS ADMINISTRATIVAS Y CONTRATOS

Las normas y políticas expresadas en este documento se considerarán parte integrante de los contratos de trabajo, y de cualquier otro contrato de servicio que signifique el uso de los recursos tecnológicos proporcionados por la Universidad de Valparaíso.

II.2.3. PUBLICIDAD Y FOMENTO DE SU CUMPLIMIENTO

Se deberán mantener publicadas en la intranet institucional las políticas, procedimientos y normas que formarán parte del SGSI de la Universidad de Valparaíso. A su vez, se difundirá con la frecuencia que el Departamento de Ciberseguridad en conjunto con el Comité de Ciberseguridad determine o que los/as actores/rices internos/as relacionados impulsen, a través de correo masivo, invitando a conocerlas, cada vez que sean modificadas, tanto la política general como las específicas, guías, procedimientos y protocolos atingentes que hayan sido aprobadas, incorporando en lo posible estrategias comunicacionales que simplifiquen educativamente los contenidos para hacerlos fácilmente comprensibles, interpretables, asimilables y adoptables por todo el personal.

Así mismo, el Departamento de Ciberseguridad en coordinación con la Dirección de Gestión y Desarrollo de Personas (DGDP) favorecerán acciones destinadas a sensibilizar, entrenar, capacitar y educar a los/as usuarios/as para operar los servicios y sistemas informáticos en conformidad a dichas normas y políticas.

La Dirección de Gestión y Desarrollo de Personas (DGDP) será la encargada de gestionar la capacitación del personal y deberá incorporar las materias de seguridad de la información y ciberseguridad como elemento informativo relevante dentro de sus planes anuales. En este sentido, deberá velar por la asignación de recursos para estos entrenamientos y sensibilización. Se considera como un aspecto clave para el éxito de esta política el hacer llegar el conocimiento a los diferentes niveles jerárquicos, razón por la que el plan de capacitación y de difusión de estas materias debe contemplar las diferentes necesidades del público objetivo, adecuando los niveles de profundidad del material a entregar y seleccionando las tecnologías óptimas que permitan una entrega eficiente y eficaz de los conocimientos.

II.3.- POLÍTICAS ESPECÍFICAS

Se deberán aprobar, validar y mantener, según corresponda, de acuerdo con los compromisos de revisión establecidos, al menos las siguientes políticas específicas para cubrir en detalle los dominios recomendados como buena práctica en la normativa vigente, junto con los procedimientos, normas e instructivos que sean necesarios para la implementación y operación de estas.

1. PE-SGSI-001: Política específica de organización de la seguridad de la información y ciberseguridad.
2. PE-SGSI-002: Política específica de gestión de administración de activos de información, equipamiento y plataforma de servicios informáticos para usuarios.
3. PE-SGSI-003: Política específica de uso, desarrollo, adquisición e instalación de las tecnologías de la información y comunicación.
4. PE-SGSI-004: Política específica de seguridad de la información y ciberseguridad ligada a los recursos humanos.
5. PE-SGSI-005: Política específica de seguridad física y del ambiente.
6. PE-SGSI-006: Política específica de gestión de comunicaciones y operaciones.
7. PE-SGSI-007: Política específica de control de acceso físico.
8. PE-SGSI-008: Política específica de control de acceso lógico.
9. PE-SGSI-009: Política específica de creación, uso y gestión de las contraseñas de acceso.
10. PE-SGSI-010: Política específica de respaldos de la información.
11. PE-SGSI-011: Política específica de proceso de desarrollo seguro de software.
12. PE-SGSI-012: Política específica de gestión de incidentes y vulnerabilidades de seguridad de la información y ciberseguridad.
13. PE-SGSI-013: Política específica del uso del correo electrónico institucional.
14. PE-SGSI-014: Política específica de planificación de la continuidad de la seguridad de la información.
15. PE-SGSI-015: Política específica de trabajo a distancia, remoto y teletrabajo.

16. PE-SGSI-016: Política específica de medios de almacenamiento, removibles y dispositivos móviles.
17. PE-SGSI-017: Política específica de seguridad de uso, acceso y administración de la red de datos y sistemas de comunicación.
18. PE-SGSI-018: Política específica de eliminación o reutilización segura de las tecnologías de información y comunicación.
19. PE-SGSI-019: Política específica de pantallas y escritorios limpios.
20. PE-SGSI-020: Política específica de seguridad en la continuidad de operaciones.
21. PE-SGSI-021: Política específica de seguridad en la relación con proveedores.
22. PE-SGSI-021: Política específica de privacidad y protección de datos personales.
23. PE-SGSI-022: Política específica de segregación de funciones.
24. PE-SGSI-023: Política específica de uso de los controles criptográficos.
25. PE-SGSI-024: Política específica contra código malicioso.

II.4.- SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD EN LA UNIVERSIDAD DE VALPARAÍSO

La política general de Seguridad de la Información y Ciberseguridad deberá mantener un lineamiento acorde a las directrices definidas por la Universidad de Valparaíso, siempre considerando el marco constitucional y legislativo en nuestro país, particularmente en lo referido a los derechos y libertades de las personas y otras leyes aplicables al campo de la información y la tecnología.

Se declara que todo activo de información cuyo tratamiento sea propio de realizar por personas, sistemas o cualquier otra entidad al interior de la Universidad de Valparaíso, deberá implementar los mecanismos necesarios para resguardar la confidencialidad, integridad y disponibilidad de la información, permitiendo controlar los riesgos inherentes a los cuales por su naturaleza se pueda ver expuesto.

Por lo anterior, la seguridad de la información y ciberseguridad tiene como objetivo proteger aquellos activos de información que tengan una relevancia para la institución, para asegurar confidencialidad, integridad y disponibilidad de estos con el objetivo de mantener y asegurar la continuidad operativa de la Universidad de Valparaíso.

La implementación de la seguridad de la información y ciberseguridad se llevará a cabo de manera continua, a través de un proceso de mejora, el cual deberá considerar prioritariamente la información de mayor valor para la institución, abarcando la relación funcionarios(as) de planta, suplentes, contratas, reemplazos, personal a honorarios, académicos/as, directivos/as, estudiantes, titulados/as y graduados/as, proveedores/as de servicios, personal externo y otros grupos interesados. La Universidad de Valparaíso podrá alinear la implementación, manteniendo el marco correspondiente a los objetivos y alcances definidos en la presente política general.

II.5.- RESPONSABILIDAD DE LAS PERSONAS

Toda persona, ya sea funcionario(a) de planta, suplente, contrata, reemplazo, personal a honorarios, académico/a, directivo/a, estudiante, titulado/a y graduada/o, proveedores/as de servicios, personal externo, y que tenga acceso a la información de esta, será responsable de mantener el resguardo adecuado de la seguridad de los datos y la información, para lo cual se destinará la siguiente clasificación de tipos de usuarios/as:

1. Propietario de la información: persona responsable de una información en particular, como también de su valorización y clasificación.
2. Administrador/a de información: persona encargada de resguardar la información y administrar las definiciones establecidas por el propietario de la información.
3. Usuario/a de información: persona que solicita acceso para realizar tratamiento sobre la información resguardada por el administrador/a de información.

Los recursos tecnológicos (hardware y software) proporcionados para el desempeño de las funciones, cualquiera sea su origen y función, deben ser usados única y exclusivamente en las labores propias y específicas del cargo del/la trabajador/a, según su contrato individual de trabajo, estando por lo tanto estrictamente prohibido cargar software en los equipos sin la licencia respectiva y efectuar modificaciones de cualquier naturaleza a los equipos, tanto en lo que respecta a software, hardware como a la configuración de la red sin la debida autorización de su jefatura directa y del Departamento de Tecnologías de la Información y Comunicación (DTIC), siguiendo para todo efecto los procedimientos vigentes que al respecto ha emitido la Universidad de Valparaíso.

Respecto a las responsabilidades de usuarios/as se debe tener presente que:

1. Todo usuario es responsable de la seguridad de la información que se le ha confiado y, por lo tanto, debe tomar todas las precauciones para evitar su pérdida, extravío, hurto o robo, en especial de las credenciales de acceso. El usuario será asimismo responsable en caso de manejos de copias de software no autorizados y de la introducción de virus o juegos en los equipos a su cargo. Deberá cuidar las máquinas, materiales y útiles que tenga a su cargo o que le sean entregados para el desempeño de sus labores.
2. A los/as usuarios/as y personal externo que, por encargo de la Universidad de Valparaíso, diseñen, programen, codifiquen y/o modifiquen sistemas computacionales, procedimientos, software y/o programas, les será aplicable la disposición contenida en el Art. 8 de la Ley N° 17.336 sobre propiedad intelectual, por lo que la institución será titular del derecho de autor sobre toda obra intelectual que derive en forma directa o indirecta en el desarrollo de dichas funciones. Además, a los/as funcionarios/as y externos les estará prohibido realizar versiones sucesivas o derivadas de la idea matriz, o transferir parte alguna.
3. Proteger, evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la información que disponen y cumplir los lineamientos generales y especiales dados por la organización referidos a la protección de datos.
4. Solicitar autorización previa antes de suministrar información de la organización a cualquier requirente.
5. Velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.
6. Resguardar sus claves de acceso a los recursos informáticos, las que son personales e intransferibles.
7. Son responsables de todas las actividades llevadas a cabo con su clave de acceso.

8. Almacenar y respaldar la información que es soportada por la infraestructura de tecnología informática de acuerdo con las normas emitidas por DTIC, de tal forma que se garantice su disponibilidad.
9. Respaldar la información relevante de su estación de trabajo utilizando los protocolos de respaldo establecidos por DTIC.
10. Cumplir con los protocolos y procedimientos de almacenamiento de información establecidos por DTIC.

De acuerdo con lo indicado en el Decreto Exento N°3752, DTIC estará a cargo de:

1. Proponer y ejecutar las políticas específicas, objetivos y metas en los ámbitos de seguridad informática, normas de uso de los recursos computacionales, acceso a la red de datos y telefonía, renovación de equipamiento e infraestructura que garanticen la operación continua del servicio y del desarrollo de sistemas informáticos, así como de realizar la coordinación y el seguimiento de su ejecución, disponiendo las acciones que de ello se deriven, en el marco de lo establecido en el Plan de desarrollo estratégico institucional.
2. Establecer la utilización de las claves de acceso a los recursos informáticos, los parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los/as usuarios/as deben cambiar su contraseña y los períodos de vigencia de estas, entre otras.
3. Definir las especificaciones y requerimientos de seguridad necesarios para cada sistema de información o aplicación que se desarrolle en la unidad.
4. Aprobar y certificar la conexión entre sistemas internos de la Universidad de Valparaíso y otros de terceros, con el fin de no comprometer la seguridad de la información interna de la institución.
5. Regular las conexiones de redes externas de tiempo real que accedan a la red interna de la organización, la cuales deben pasar a través de los sistemas de defensa electrónica que incluyen servicios de cifrado y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autentificación de usuarios/as.
6. Borrar, de forma definitiva, los datos contenidos en los equipos informáticos y medios digitales que sean usados en el almacenamiento y/o procesamiento de información de la Universidad de Valparaíso antes de ser dados de baja.

De acuerdo con lo indicado en el Decreto Exento N°3752, el Departamento de Ciberseguridad estará a cargo de:

1. Proponer, ejecutar políticas específicas, objetivos y metas en el ámbito de la ciberseguridad, en coordinación con el Departamento de Tecnologías de Información y Comunicación, y con los organismos competentes, públicos y privados.
2. Establecer actividades para cubrir brechas en la documentación actual, así como diseñar nuevos documentos o añadir lineamientos a la documentación existente.
3. Identificar la documentación se seguridad de la información y ciberseguridad a modificar/actualizar. La actualización de la documentación se debe llevar a cabo reflejando la realidad operativa de la organización.
4. Definir y formalizar responsables de actualizar o crear la documentación según el área específica. Estos encargados deberán presentar avances periódicos del proceso.
5. Establecer un tiempo máximo para el cumplimiento de los lineamientos de seguridad de la información y ciberseguridad definidos.
6. Establecer un procedimiento formal para actualizar y probar formalmente los ajustes en la documentación.
7. Publicar y difundir las nuevas versiones a toda la comunidad universitaria (dependiendo del contenido del documento).
8. Desarrollar actividades de gestión de los activos de información de la Universidad de Valparaíso.

9. Realizar campañas de concientización en materia de seguridad de la información y ciberseguridad.
10. Desarrollar actividades de gestión de fallos e incidentes de seguridad.
11. Desarrollar actividades de gestión y monitoreo de cuentas de acceso y privilegios.
12. Preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, maremoto, explosión, terrorismo, inundación etc.
13. Aprobar y certificar la conexión entre sistemas internos de la Universidad de Valparaíso y otros de terceros, con el fin de no comprometer la seguridad de la información interna de la institución.
14. Establecer la utilización de las claves de acceso a los recursos informáticos, parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los/as usuarios/as deben cambiar su contraseña y los períodos de vigencia de estas, entre otras.
15. Definir las especificaciones y requerimientos de seguridad necesarios para cada sistema de información o aplicación que se desarrolle en la unidad.
16. Establecer lineamientos de seguridad de la información y ciberseguridad para la continuidad del negocio.

II.6.- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

El Departamento de Ciberseguridad de la Universidad de Valparaíso mantendrá una adecuada organización relacionada con la seguridad de la información y ciberseguridad, para lo cual gestionará a través del Comité de Ciberseguridad políticas, procedimientos, normativas, estándares, o cualquier otro mecanismo de control que ayude a mejorar la seguridad de la información y ciberseguridad.

Tanto el Comité de Ciberseguridad como el/la jefe/a del Departamento de Ciberseguridad podrán dictaminar marcos de trabajo de seguridad con entidades externas a la institución y/o terceros que presten servicios de seguridad de la información y ciberseguridad.

La formalización de las tareas, funciones y responsabilidades sobre los procesos de tratamiento y gestión de la información, por su amplitud, son establecidos en la primera política específica, denominada:

PE-SGSI-001: POLÍTICA DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

II.7.- GESTIÓN DE ACTIVOS DE INFORMACIÓN

Para hacer más eficiente el proceso de implementación de la seguridad de la información y ciberseguridad en procesos, sistemas y recursos humanos, la Universidad de Valparaíso desarrolla estrategias focalizadas de trabajo para optimizar el uso de los recursos de seguridad, por lo mismo se establecen métodos para la identificación, clasificación y valorización de los activos de información, considerando también la asignación de responsabilidades sobre su tratamiento, permitiendo mantener claramente identificación sobre los activos de información relevantes para la institución y mantener mecanismos acordes para el control de los riesgos de información.

Para clasificar la información el criterio se basará en la confidencialidad de la información, llevando a cabo los siguientes pasos:

1. Incluir la información en el inventario de activos, para lo cual es necesario conocer formatos y medios, además de los/as responsables de generarla y recibirla. Como ejemplo están los documentos de carácter electrónico, bases de datos, documentos en formato papel, correos electrónicos, medios de almacenamiento, etc.
2. Clasificar la información anterior según el carácter confidencial de la misma:
   - Confidencial o reservado: cuando el nivel de confidencialidad de la información sea alto.
   - Restringido: para niveles medios de confidencialidad.
   - Uso interno: información con un nivel bajo de confidencialidad.
   - Público: cuando todas las personas pueden ver la información.
   - El/la propietario/a del activo de información es la persona encargada de proceder a realizar la clasificación de la información, por lo que se realizará según los resultados obtenidos tras la evaluación del riesgo.
3. Realizada la anterior clasificación de la información, se debe etiquetar de forma adecuada. Es necesario que se defina una serie de pautas a seguir para cada tipo de activo de información. La Universidad de Valparaíso podría establecer las reglas para indicar el carácter confidencial en cada uno de los documentos en papel que posee, como por ejemplo, indicar en la esquina superior del lado derecho del documento concreto el nivel de confidencialidad atribuido al mismo y que aparezca en el frente de la portada y en la carpeta donde se archive tal documento. También en el encabezado de un correo electrónico es posible señalar la clasificación de la información.
4. Hacer un manejo y tratamiento seguro de la información clasificada. La Universidad de Valparaíso deberá definir una serie de reglas que guíen sobre cómo proteger cada tipo de información según el nivel de confidencialidad de cada una. Por ejemplo, los documentos en formatos papel, que se encuentran categorizados como de carácter “restringido”, deben ser guardados en un gabinete. Es necesario que se transfiera dentro o fuera de la institución, pero siempre que se encuentren en sobres cerrados. En caso de enviarse fuera, el documento tiene que enviarse con un servicio de devolución.

II.8.- SEGURIDAD LIGADA A LAS PERSONAS

Debido a la importancia que tienen las personas en la Universidad de Valparaíso, se considera fundamental gestionar la seguridad de la información aplicada su ciclo de vida y mientras presten servicios en la institución. Por lo mismo, se incorporarán términos legales de confidencialidad y responsabilidades de seguridad en los contratos y descripciones de cargos, adicionalmente se desarrollarán planes orientados a incorporar la cultura de seguridad en toda la comunidad universitaria, en conjunto con otros mecanismos complementarios a este ámbito, permitiendo entregar un apoyo permanente a la gestión del cambio frente a temas de seguridad de la información en las personas.

Toda la información que se recibe o se obtiene a partir de fuentes al interior de la Universidad de Valparaíso solo podrá ser revelada a aquellas personas autorizadas dentro de la institución, dependiendo de sus funciones y del tipo de información, que requieran conocer esta información para prestar algún servicio o para desempeñar funciones relacionadas con su cargo, y cuya posición no origine un conflicto de intereses o induzca a un mal uso de dicha información.

La información confidencial recibida en la institución, para un fin específico, no deberá proporcionarse a terceros para ser utilizada con un propósito distinto, sin tener el consentimiento previo, salvo que se trate de requerimientos de los tribunales de justicia u otros organismos públicos debidamente autorizados. Los informes de reuniones u otros documentos que contengan información confidencial no se podrán enviar o poner a disposición de personas dentro de la institución que no cuenten con la debida autorización para acceder a dicha información. En caso de que se entregue información confidencial a alguien que cuente con la debida autorización para recibirla, se deberá informar al/la receptor/a que dicha información es confidencial, y se le deberá instruir respecto de las restricciones en lo que diga relación con una mayor divulgación.

II.9.- SEGURIDAD FÍSICA Y AMBIENTAL

Los activos de información físicos, tales como las oficinas, áreas de procesamiento y almacenamiento de información, equipos tecnológicos, de soporte, de respaldo, información en medios físicos, inventario de activos tangibles e intangibles, entre otros, son la base para el cumplimiento de los objetivos de la institución. Los activos de información físicos, como oficinas, áreas de procesamiento y almacenamiento de información, equipos tecnológicos, de soporte y respaldo, información en medios físicos, inventario de activos tangibles e intangibles, entre otros, son esenciales para alcanzar los objetivos institucionales. Por ello, se implementarán políticas, procedimientos, normativas, controles y otros mecanismos que aseguren la seguridad de las instalaciones y los entornos de trabajo, el acceso a las áreas, la gestión de documentos, los mecanismos físicos de tratamiento de la información, y el hardware que apoya los procesos. Todo esto permitirá proteger los activos de información contra amenazas físicas, ambientales y naturales.

II.9.1.- ADMINISTRACIÓN DEL EQUIPAMIENTO COMPUTACIONAL

Todo equipamiento computacional que esté o sea conectado a la red de la Universidad de Valparaíso, o aquel que en forma autónoma se tenga y que sea propiedad de la institución, debe sujetarse a las normas y procedimientos de instalación, uso y administración que emite la institución.

DTIC deberá tener un registro de todos los equipos que son propiedad de la Universidad de Valparaíso. En el caso de que estos sean adquiridos por otras unidades administrativas o académicas deberán ser informados a DTIC.

El equipo de la institución que sea de propósito específico y que tenga asignada una misión crítica, debe estar ubicado en un área que cumpla con los requerimientos de seguridad física, condiciones ambientales y de alimentación eléctrica normadas por DTIC.

La protección física de los equipos computacionales es responsabilidad de las personas a las cuales en un principio se les asigna, y les corresponde a estos notificar a DTIC los movimientos en caso de que existan.

A DTIC le corresponde la supervisión del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y el acondicionamiento específico a que tenga lugar. El traslado o reubicación de un equipo se realizará satisfaciendo las normas y procedimientos determinados por DTIC.

En el caso de los equipos gestionados por terceros, DTIC deberá establecer las normativas correspondientes y llevar a cabo estas tareas de manera coordinada con los encargados de la administración del equipamiento.

Los/as responsables de las áreas de tecnologías de la información de una unidad pueden otorgar mantenimiento preventivo y correctivo, a partir del momento en que sean autorizados/as por DTIC informando periódicamente de las actividades indicadas.

Corresponde a DTIC dar a conocer las listas de las personas que puedan tener acceso a los equipos y brindar los servicios de soporte básico, a excepción de los atendidos por terceros, los cuales deben ser informados a DTIC.

DTIC y los soportes informáticos de la universidad no realizarán mantenimiento ni otorgarán ningún tipo de soportes a equipamiento que no sea de propiedad de la institución.

II.10.- SEGURIDAD EN LAS COMUNICACIONES Y OPERACIONES

Gran parte de la información que se manipula en la Universidad de Valparaíso se encuentra en formato digital, por lo mismo se considera de vital necesidad gestionar los riesgos asociados a las comunicaciones y operaciones relacionados con los activos de información, definir responsabilidades y segregación de funciones, documentar las operaciones en el tratamiento de información, establecer criterios de calidad para la aceptación de los sistemas de información, administrar planes de respaldo y recuperación, implementar mecanismos de monitoreo y supervisión de la ciberseguridad, así como también en el manejo de los soportes y la seguridad de la redes tecnológicas. Todo esto permite la protección de los activos de información y asegurar el cumplimiento adecuado de la presente política.

Es fundamental supervisar y revisar los acuerdos establecidos para la gestión de los servicios proporcionados por terceros. Esta supervisión debe enfocarse tanto en la calidad como en la seguridad con la que se prestan dichos servicios, incluyendo la gestión de cambios entre las partes. Especial atención se debe prestar a los acuerdos de confidencialidad y al intercambio de información con entidades externas e internas de la Universidad de Valparaíso, garantizando en todo momento la protección y el resguardo de la información.

II.10.1.- ACCESO Y ADMINISTRACIÓN DE LA RED DE DATOS Y SISTEMAS DE COMUNICACIÓN

El otorgamiento de acceso a la red de datos y sistema de comunicación está regulado mediante las políticas y procedimientos definidos por la Universidad de Valparaíso, las cuales siguen los siguientes lineamientos generales:

1. Todos/as los/as usuarios/as podrán tener acceso a la red de datos y sistemas de comunicación necesarios para el desarrollo de sus actividades.
2. Todos los accesos a la red de datos y sistemas de comunicación de la Universidad de Valparaíso deben terminar inmediatamente después de que el/la trabajador/a deje de prestar sus servicios a la organización
3. DTIC será el responsable de efectuar el seguimiento a los accesos realizados por los/as usuarios/as a la información de la organización, mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica. Cuando se presenten eventos que pongan en riesgo la integridad, validez y consistencia de la información el/la usuario/a deberá documentar y realizar las acciones tendientes a su solución, informando a los/as responsables de los respectivos sistemas.
4. La configuración e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la organización serán considerados y tratados como información confidencial.

II.10.2.- SEGURIDAD EN EL ACCESO A LA INFORMACIÓN

La Universidad de Valparaíso considera fundamental controlar el acceso a los activos de información para mantener su confidencialidad, por tanto, los archivos digitales, documentos electrónicos, bases de datos, software y aplicativos, plataformas de almacenamiento y procesamiento de información, entre otros, son componentes esenciales para lograr el cumplimiento de los objetivos de la institución. Por lo mismo, y en relación con este principio, es que los sistemas de información de la organización cuentan con medidas de control que son adecuadas para mantener el resguardo de la información, considerando normativas de acceso, gestionando cuentas de usuarios/as autorizados/as, estableciendo responsabilidades por parte de las personas, controlando el ingreso a las redes de comunicación, servidores y equipos computacionales, como también aplicando mecanismos de protección de acceso sobre las aplicaciones y la información de la institución, tratando de evitar en todo momento que se pueda ver afectada por el acceso o la manipulación no autorizada.

II.11.- SEGURIDAD EN LA ADQUISICIÓN, DESARROLLO Y MANTENCIÓN DE SISTEMAS DE INFORMACIÓN

La Universidad de Valparaíso cuenta con sistemas de información que dan soporte a los procesos internos, con lo cual permite entregar una mayor calidad y seguridad en la ejecución de las actividades y optimizar el uso de los recursos informáticos, Sin embargo, la incorporación de nuevas tecnologías también incorpora riesgos que son propios de esta, por lo mismo la institución mantiene mecanismos que permiten controlar estos riesgos a través de normativas y estándares de seguridad, metodologías y procesos formales para el desarrollo de sistemas de información, implementación de controles criptográficos, así como también actividades de aseguramiento de software y adquisición de recursos tecnológicos.

Por otra parte, los sistemas de información que se encuentran en producción cuentan con medidas de control que permiten resguardar adecuadamente los archivos de sistema y la información sobre la cual se realiza tratamiento, las normativas y herramientas de gestión de cambios y de configuración. Estas son acciones que ayudan al cumplimiento de esta política y al logro de los objetivos de la institución.

II.11.1.- DESARROLLO Y OBJETIVOS INFORMÁTICOS DE LA UNIVERSIDAD DE VALPARAÍSO

El desarrollo tecnológico de la Universidad de Valparaíso deberá contribuir de forma consistente y segura a mejorar los procesos académicos y administrativos presentes en el plan estratégico vigente, y de esta manera aumentar su eficacia, transferencia oportuna de información para la toma de decisiones y mejora de procesos, en beneficio directo de los miembros de la comunidad universitaria y usuarios/as de los servicios.

La Unidad de Modernización y Gestión de Procesos será la encargada de levantar, mejorar y documentar procesos de la Universidad de Valparaíso, así como también ejecutar proyectos tecnológicos, con el fin de actualizar y mejorar dichos procesos.

El Departamento de Tecnologías de Información y Comunicación (DTIC) es el único responsable de la asesoría, desarrollo y/o provisión de aplicaciones, redes de comunicación y sistemas computacionales institucionales, y de la implementación de estos, los que serán utilizados como herramientas de apoyo para los procesos administrativos y académicos en la Universidad de Valparaíso.

Los sistemas de información y comunicación institucionales existentes o a ser desarrollados deberán cumplir estrictamente con la compatibilidad e integración, con el fin de mantener la consistencia de la información entre los diferentes sistemas institucionales.

II.11.2.- USO ADECUADO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD DE VALPARAÍSO

Los sistemas de información y comunicación, y todo recurso tecnológico de la Universidad de Valparaíso, deberán estar ajustados y estandarizados de acuerdo con los procesos institucionales definidos en el plan estratégico vigente.

Todo activo de información y/o recursos tecnológicos provisto por la Universidad de Valparaíso deben tener como propósitos los siguientes:

- Docencia.
- Investigación.
- Extensión.
- Administración.
- Difusión y promoción institucional.
- Atención de usuarios/as.
- Seguridad de la información y ciberseguridad.

Además, todo activo de información y/o recursos tecnológicos provistos por la Universidad de Valparaíso deben cumplir con los lineamientos establecidos por el Departamento de Tecnologías de Información y Comunicación (DTIC).

II.11.3.- DESARROLLO, ADQUISICIÓN E INSTALACIÓN DE APLICACIONES Y SISTEMAS COMPUTACIONALES

Cada unidad académica o administrativa de la Universidad de Valparaíso deberá solicitar el desarrollo de un nuevo sistema de información de acuerdo con los procesos y procedimientos definidos por la Unidad de Modernización y Gestión de Procesos perteneciente a la Dirección General de Modernización y Transformación Digital.

La adquisición de nuevo hardware institucional será responsabilidad del Departamento de Tecnologías de Información y Comunicación (DTIC), quienes determinarán si es necesaria su adquisición en el caso de que el existente esté obsoleto y/o no funcione adecuadamente con la tecnología actual.

Cada unidad académica y administrativa de la Universidad de Valparaíso podrá contar con una persona responsable de instalar las aplicaciones que requiere para desarrollar sus funciones. Dicho responsable deberá estar previamente capacitado/a y deberá trabajar en forma coordinada con el Departamento de Tecnologías de Información y Comunicación (DTIC) y el Departamento de Ciberseguridad.

II.12.- GESTIÓN DE INCIDENTES DE SEGURIDAD

La retroalimentación de parte de las personas y entidades es la base para mejorar los controles de la institución, por lo mismo se desarrollan canales de comunicación para la notificación de eventos, debilidades y oportunidades de mejora en la seguridad de la información y en cómo también se establecen equipos de respuesta frente a eventuales incidentes que puedan afectar la seguridad de la información y la ciberseguridad, considerando el análisis y aprendizaje de los efectos generados por dichas situaciones e implementando mecanismos que permitan prevenir o detectar su ocurrencia, además de minimizar su impacto y/o probabilidad, apoyando la mejora continua del SGSI.

Toda sospecha, vulnerabilidad o incidente de ciberseguridad detectado por la comunidad universitaria debe ser informado al Departamento de Ciberseguridad, mediante los canales de comunicación oficiales.

Por otro lado, el Departamento de Ciberseguridad de la Universidad de Valparaíso debe informar a la Agencia nacional de Ciberseguridad (ANCI) todo incidente de seguridad de la información, en particular de ciberseguridad, de acuerdo con lo indicado en el Decreto N° 295 “Aprueba reglamento de reporte de incidentes de ciberseguridad de la ley N° 21.633” del 24 de septiembre de 2024.

Se establecerá un procedimiento de gestión de incidentes para detectar, informar y responder a incidentes de seguridad de la información y ciberseguridad.

II.13.- GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD OPERACIONAL

La operación educativa, la información financiera-contable y la tecnología/innovación son la cadena de valor de la Universidad de Valparaíso, por lo mismo se deben implementar los mecanismos necesarios para mantener su continuidad operacional frente a situaciones que pudieran afectar prioritariamente su disponibilidad, donde la infraestructura, la tecnología, los procesos, las personas y la información son la base fundamental sobre la cual se centran los planes de continuidad operacional, los que a través de la gestión de riesgos, el análisis de impacto, el desarrollo de estrategias y los planes de contingencia y recuperación permiten garantizar razonablemente la operación de los productos estratégicos de la institución.

II.13.1.- PROTECCIÓN CONTRA AMENAZAS

II.13.1.1. GESTIÓN DE RIESGOS

La Universidad de Valparaíso llevará a cabo evaluaciones de riesgos y tomará medidas para mitigar amenazas.

II.13.1.2. PREVENCIÓN DE AMENAZAS

Se deben implementar controles técnicos, como *firewalls*, antivirus y detección de intrusiones, para prevenir amenazas cibernéticas.

II.13.1.3.- CONCIENTIZACIÓN Y FORMACIÓN

La Universidad de Valparaíso proporcionará campañas de concientización en seguridad de la información y ciberseguridad para aumentar la conciencia digital y promover buenas prácticas de seguridad.

II.14.- SANCIONES

El incumplimiento de la política general de Seguridad de la Información y Ciberseguridad, políticas específicas, procedimientos o instructivos asociados al Sistema de Gestión de Seguridad de la Información, ya sea por parte de los/as funcionarios/as de planta, suplente, contrata, reemplazos, personal a honorarios, académicos/as, directivos/as, estudiantes, titulados/as y graduados/as, proveedores/as de servicios y personal externo que utilicen los recursos tecnológicos y sistemas de información de la Universidad de Valparaíso, sea cual fuere su nivel jerárquico y su calidad contractual, puede resultar en la aplicación de sanciones administrativas, acciones disciplinarias, civiles o penales, en conformidad con lo establecido en la legislación vigente y en los procedimientos internos de la Universidad de Valparaíso.

Es deber de todos/as los/as funcionarios/as de planta, suplente, contrata, reemplazos, personal a honorarios, académicos/as, directivos/as, estudiantes, titulados/as y graduados/as, proveedores/as de servicios y personal externo, informar a la brevedad a su jefatura directa si se tiene conocimiento del incumplimiento de la normativa vigente en esta materia. Esta información deberá canalizarse al Departamento de Ciberseguridad, a través de los medios de comunicación oficiales de la Universidad de Valparaíso.

II.15.- GLOSARIO DE TÉRMINOS

Término	Definición
Activos de información	Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución, cualquiera sea el formato que la contenga y los equipos y sistemas que la soporten. Por ejemplo: dispositivos móviles, tarjetas de accesos, software, equipamiento computacional, personal, edificios, infraestructura tecnológica y física.
Amenaza	Causa potencial de un incidente no deseado por el cual puede resultar dañado o afectado un sistema u organización. Ejemplos: terremotos, inundaciones, sabotajes, amenazas de bombas, negligencias humanas, cortes eléctricos, fallas en sala de servidores, entre otras.
BCP	(Business Continuity Plan) Plan de continuidad del negocio: es el plan de la institución ideado para recuperar el funcionamiento de sus funciones críticas ante eventos o incidentes graves. Este plan abarca a toda la Universidad de Valparaíso, y debe estar construido para ser eficiente en tiempos, esfuerzos y recursos.
Confidencialidad	La información debe estar protegida de accesos no autorizados. Por lo tanto, debe ser accesible solo por aquellos que tengan la autorización. Los/as funcionarios/as, directivos/as, estudiantes, personal a honorarios y proveedores/as de servicios deben proteger la información confidencial y no divulgarla sin autorización.
Criptografía	Es el conjunto de técnicas utilizadas para cifrar la información, pero que a la vez permite que esta sea utilizable o legible solo por las personas o elementos autorizados.
Custodio de activo de información	Es quien, sin ser el/la dueño/a del activo de información, tiene responsabilidades sobre su integridad, confidencialidad o disponibilidad. Un ejemplo es: el Departamento de Tecnologías de la Información y Comunicación (DTIC) es el custodio de FIN700, no es el propietario, pero tiene la responsabilidad de velar que el sistema esté disponible y que el/la proveedor/a cumpla con mantener la disponibilidad del servicio.
Disponibilidad	La información y los sistemas críticos deben estar disponibles y funcionales cuando se necesiten. Se deben implementar medidas de respaldo y recuperación ante desastres.
Documento electrónico	Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.
DRP (Disaster Recovery Plan) Plan de recuperación ante desastres	Es un conjunto de acciones ordenadas e ideadas para devolver la disponibilidad de las operaciones tecnológicas que dan soporte a las operaciones críticas del negocio. Al igual que el BCP, este plan debe estar construido para ser eficiente en tiempos, esfuerzos y recursos. Conceptualmente se puede decir que el DRP es parte del BCP.
Dueños/as de los datos	Se refiere a la unidad/dirección que maneja datos institucionales, contenidos tanto en medios tradicionales como en sistemas informáticos a que pertenecen los/as usuarios/as que son funcionarios/as de la institución, en la calidad contractual que sea.

Estación de trabajo	Equipo computacional conectado a una red de computadores que facilita a los/as usuarios/as el acceso a los servidores y periféricos de la red.
Evaluación del riesgo	Proceso consistente en la comparación de los niveles de riesgo encontrados contra los criterios de riesgo prestablecidos (si es que han sido establecidos por la dirección) considerando el balance entre los beneficios potenciales y resultados adversos, para posteriormente ordenar y priorizar mediante un ranking los riesgos analizados.
Gestión del riesgo	Proceso definido para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto al alcance de los objetivos de la organización. Es un proceso iterativo que debe contribuir a la mejora organizacional a través del perfeccionamiento de los procesos.
Incidente de seguridad	Cualquier evento o situación que comprometa la disponibilidad, integridad y confidencialidad de la información, o bien afecte a la plataforma tecnológica, proceso y aplicativos que la contienen, impidiendo acceder a esta en forma oportuna. En general, es una transgresión de una política, estándar o procedimiento de seguridad, que no permite prestar los servicios institucionales por medios informáticos o tradicionales. Ejemplos de incidentes: acceso no autorizado, robo de contraseñas, robo de información, denegación de servicio en internet, un malware actuando en los equipos institucionales o un phishing que ataca a los/as usuarios/as institucionales.
Integridad	La información debe ser precisa, confiable actualizada y ser veraz, sin modificaciones o alteraciones no autorizadas o corruptas. Se deben tomar medidas para prevenir alteraciones no autorizadas de la información.
Política de seguridad	Conjunto de normas o buenas prácticas, declaradas y aplicadas por la institución, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto.
Proceso	Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un fin determinado.
Programa malicioso	Es un tipo de *software* que tiene como objetivo infiltrarse o dañar un equipo. También se denominan *malware.*
Propietario/a de activo de información	Es el/la dueño/a del proceso en el cual el activo de información es utilizado o generado. Por ejemplo, el/la director/a de la DGDP es el/la propietario/a del activo de información “nómina de sueldos”.
Restricción del acceso	Acción consistente en la delimitación de acceso a los/as funcionarios/as, personar a honorarios y terceras partes a determinados recursos físicos y lógicos.
Riesgo	Es la contingencia de un daño a un activo de información. A su vez, contingencia significa que el daño se puede materializar en cualquier momento o no suceder nunca.
Sanción	Consecuencia jurídica de naturaleza administrativa, civil o penal derivada del incumplimiento de un deber.
Seguridad de la información	Proceso encargado de asegurar y proteger los recursos de un sistema de información para que sean utilizados de la manera que

	se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, preservando la integridad, confidencialidad y disponibilidad.
Sistema informático	*Software* asociado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información o transferencia de información.
Sistema de comunicaciones electrónicas	Se refiere a todo medio o dispositivo que permite comunicarse. Entiéndase: correo electrónico, mensajería instantánea (WhatsApp, Telegram u otros), videoconferencia (Microsoft Teams, Zoom, u otros), telefonía fija y móvil, etc.
Teletrabajo	Si los servicios son prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones, o si tales servicios deben reportarse mediante estos medios. Válida mientras no exista una disposición legal que la sustituya o modifique en el contexto gubernamental.
Terceras partes	Persona u organismo ajeno a la relación directa establecida entre dos partes principales. Para estos efectos, se entenderá como terceras partes, entre otros/as, a los/as proveedores/as de servicios y de red, los/as proveedores/as de productos de software y servicios de información, outsourcing de instalaciones y operaciones, servicios de asesoría de seguridad y auditores/as externos/as.
Trabajo a distancia (remoto)	Aquel en el que el/la trabajador/a o funcionario/a presta sus servicios, total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos, instalaciones o dependencias de la institución. Válida mientras no exista una disposición legal que la sustituya o modifique en el contexto gubernamental.
Usuario/a	Persona que utiliza el sistema informático o los medios de la institución con independencia de su calidad contractual y la modalidad de trabajo (presencial, teletrabajo o trabajo a distancia).
SGSI	Sistema de Gestión de Seguridad de la Información, es el conjunto de políticas, procedimientos y controles implementados en la Universidad de Valparaíso para proteger los activos de información.

Fin de transcripción

II. Corresponderá al/la directora general de Desarrollo Institucional y Aseguramiento de la Calidad, a la Dirección General de Modernización y Transformación Digital y Departamento de Ciberseguridad, disponer de las medidas para su mejor implementación.

ANÓTESE, REGÍSTRESE Y COMUNÍQUESE.

OSVALDO CORRALES JORQUERA
RECTOR
UNIVERSIDAD DE VALPARAISO

OCJ/SNV/DME/jrb

Christian Hernan Corvalan Rivera Digitally signed by Christian Hernan Corvalan Rivera

María Soledad Narea Veas

Firmado digitalmente por Jeronimo Rojas Bugueño

Juan Pablo Jaña Núñez

Firmado digitalmente por Marco Antonio Azavena Vivar
Fecha: 2025.06.09 08:50:15 -04'00'

RECTORIA – SECRETARIA GENERAL- VICERRECTORIA DE GESTIÓN INSTITUCIONAL – FISCALÍA GENERAL- CONTRALORÍA - DIRECCIÓN GENERAL DE MODERNIZACIÓN Y TRANSFORMACIÓN DIGITAL - DEPARTAMENTO DE CIBERSEGURIDAD - OFICINA DE PARTES.

Página de Firmas - Oficios Internos

OSVALDO ENRIQUE CORRALES JORQUERA

Documento firmado digitalmente por:
OSVALDO ENRIQUE CORRALES JORQUERA
RUT: 12012272-K
El 13-06-2025 a las 17:54
Certificado Serial: a366ec0638244a24ad366ff04d0d7328
Emitido por: CA INT UNIVERSIDAD DE VALPARAISO FIRMA SIMPLE NO CERTIFICADA G1