UNIVERSIDAD DE LA FRONTERA
SECRETARÍA GENERAL
DECRETACIÓN

Aprueba Reglamento Técnico de Seguridad de la Información y Ciberseguridad de la Universidad de La Frontera.

TEMUCO, **03 de marzo de 2023**

RESOLUCION **EXENTA 0607/2023**

VISTO:

- Ley N°21.094, Ley sobre Universidades del Estado.
- DFL Nºs 17 de 1981 del MINEDUC que crea la Universidad de La Frontera.
- DFL N°156 de 1981 del MINEDUC que aprueba Estatuto de la Universidad de La Frontera.
- D.S. N°132 de 2022, que aprueba nombramiento del Sr. Rector de la Universidad de La Frontera.
- D.U. Nº 036 de 2007, que crea Asignación de Docencia para el Personal Administrativo de la Universidad de La Frontera.
- D.U. Nº314 de 2010 que aprueba nombramiento de Secretario General de la Universidad de La Frontera, y

CONSIDERANDO:

1. Que, por Resolución Exenta N°2394 de fecha 14 de junio de 2011, se aprobó Reglamento de Normas de Seguridad Informática de la Universidad de La Frontera, el cual tuvo por objeto su aplicación a todas las personas que hacen uso de recursos informáticos y de comunicaciones de la Universidad de La Frontera.

2. Que, la Universidad de La Frontera elabora el presente Reglamento técnico de Seguridad de la Información y Ciberseguridad, según lo dispuesto en la norma NCH-ISO27002:2013, ISO 27002:2022 y en el Decreto Supremo N°83 de 2005, del Ministerio Secretaría General de la Presidencia, que aprueba la Norma Técnica para los órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos, donde se indica que deberá cumplir con las condiciones previstas en la Norma NCh2777, la cual es reemplazada por el Artículo 2° de la Resolución 1535 Exenta del Ministerio de Economía por la Norma NCh-ISO 27002.Of2009 Tecnología de la información – Códigos de prácticas para la gestión de la seguridad de la información, encontrándose dicha norma “No Vigente” (inn.cl), y siendo reemplazada por la norma NCh-ISO27002:2013 Tecnologías de la información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información. En esta se indica en el capítulo 5 “Política de Seguridad de la Información” que dispone:

“La necesidad de contar con políticas internas para la seguridad de la información varía entre las organizaciones. Las políticas internas son especialmente útiles en organizaciones de mayor tamaño y complejidad, donde aquellos que definen y aprueban los niveles ampliados de control se segregan de los que implementan los controles o en situaciones donde una política se aplica a varias personas o funciones distintas de la organización. Las políticas para la seguridad de la información se pueden emitir en un documento de política de seguridad de la información único o como un conjunto de documentos individuales pero relacionados”.

3. Que, el Vicerrector de Administración y Finanzas, don Jorge Petit-Breuilh Sepúlveda, en Ord. N°020/3010 de fecha 28 de febrero de 2023, solicita aprobar Reglamento Técnico de Seguridad de la Información y Ciberseguridad de la Universidad de La Frontera.

4. Que, la Dirección Jurídica de la Universidad de La Frontera otorgó visto bueno a la presente solicitud.

R E S U E L V O

APRUEBASE Reglamento Técnico de Seguridad de la Información y Ciberseguridad de la Universidad de La Frontera.

TITULO I.
DISPOSICIONES GENERALES

ARTÍCULO 1°: Seguridad de la información y Ciberseguridad. La seguridad de la información corresponde al conjunto de principios: confidencialidad, integridad y disponibilidad, que aseguran la preservación de la información, un activo esencial para el funcionamiento de la Universidad de La Frontera. Así también, la ciberseguridad es técnicas o herramientas que velan por la seguridad de los usuarios que comparten información de la Universidad en internet o entre sistemas que transitan por dicha red.

ARTÍCULO 2º: Objetivo general. El presente reglamento tiene por objeto establecer medidas para resguardar la seguridad de la información abordando riesgos y oportunidades, enfocadas en la mejora continua y asegurando la confidencialidad, integridad y disponibilidad de la información.

ARTÍCULO 3º: Objetivos específicos. Son objetivos específicos del presente reglamento los siguientes:

1. Establecer un catastro de los activos de información de la Universidad de La Frontera, junto a los estándares asociados a estos.
2. Definir las medidas esenciales de seguridad de la información y ciberseguridad de la Universidad para prevenir efectos no deseados y disminuir la probabilidad de amenazas que afecten la confidencialidad, integridad y disponibilidad de la información.
3. Promover la necesidad de la seguridad de la información y ciberseguridad a nivel institucional destacando la difusión, comunicación y comprensión de las responsabilidades de la comunidad universitaria.
4. Especificar los lineamientos para la elaboración de estándares relacionados a seguridad de la información de la Universidad de la Frontera.
5. Efectuar la evaluación, seguimiento y análisis de los eventos vinculados a la seguridad de la información y que generen impacto en el quehacer institucional con mirada en la mejora continua.

ARTÍCULO 4º: Alcance.

1. Este reglamento se aplica a todas las personas que hagan uso de los recursos y sistemas informáticos y de comunicaciones de la Universidad de La Frontera, considerando la normativa vigente en el ámbito de seguridad de la información y ciberseguridad.

2. Los recursos y sistemas informáticos comprenderán como mínimo:

    a. Equipamiento e infraestructura de la red de datos y de telecomunicaciones de la Universidad.
    b. Los servidores institucionales.
    c. Las plataformas de software instaladas para proporcionar servicios a la comunidad.
    d. Los sistemas informáticos desarrollados internamente, o sistemas externos y/o software debidamente licenciados.
    e. Todo el equipamiento de propiedad de la Universidad de La Frontera, lo que incluye equipos computacionales, periféricos computacionales y todo otro equipamiento tecnológico conectado a la red corporativa. Entre otros se incluyen: computadores, impresoras, proyectores, cámaras, etc.

ARTÍCULO 5º: Glosario. Se incluyen las siguientes siglas y abreviaturas técnicas, cuyo significado se detalla a continuación:

Sigla o abreviatura	Descripción
1. Cortafuegos	Un cortafuegos es una tecnología que funciona como una barrera entre internet u otras redes públicas y nuestra computadora.
2. CSIRT	“Computer Security Incident Response Team”, traducido como “Equipo de Respuesta a Incidentes de Seguridad Informática”.
3. DAM	“Digital Asset Management” o "Gestión de Activos Digitales" es una plataforma para que las empresas gestionen activos digitales durante su ciclo de vida: desde su creación hasta su publicación y almacenamiento .
4. EDR	“Endpoint Detection Response”, es un sistema de protección de los equipos e infraestructuras de la organización, que combina el antivirus tradicional junto con herramientas de monitorización e inteligencia artificial para ofrecer una respuesta rápida y eficiente ante los riesgos y las amenazas más complejas.
5. HTTPS	“Hyper Text Transfer Protocol Secure” o “Protocolo Seguro de Transferencia de Hipertexto”, hace referencia al protocolo bajo el que se envían los datos entre un navegador y un sitio web. Al ser un protocolo seguro, todas las comunicaciones entre el navegador y el sitio web están encriptadas.
6. IDS	“Intrusion Detection System” o “Sistema de Detección de Intrusiones”, es una aplicación usada para detectar accesos no autorizados a un computador o a una red.
7. IPS	“Intrusion Prevention System” o “Sistema de Prevención de Intrusiones”, es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva.
8. LOG	En informática, se usa el término “registro”, “log” o “historial de log” para referirse a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular.
9. Malware	Término que se utiliza para describir software malintencionado que se ha diseñado para ocasionar daños o realizar acciones no deseadas en un sistema informático.
10. Networking	En tecnologías, el concepto de networking aplica a las redes de cómputo para vincular dos o más dispositivos informáticos con el propósito de compartir datos.
11. Off-line	Término empleado para hacer referencia a todo aquello que tiene lugar fuera de Internet, cuando no se está conectado a la red.
12. Ransomware	Es un tipo de código malicioso que impide la utilización de los equipos o sistemas que infecta, una de las principales características es que se solicita un “rescate” a cambio de dinero para desbloquear equipos, descifrar archivos modificados y devolver la información sustraída.
13. SLA	“Service Level Agreement”, traducido como “Acuerdo de Nivel de Servicio”, se trata de un acuerdo, habitualmente anexo a un contrato de prestación de servicios tecnológicos, que define el nivel de servicio que se espera de un proveedor cuando implementa soluciones avanzadas de infraestructura tecnológica, Habitualmente en este acuerdo se definen los tiempos de respuesta y resolución de problemas que el equipo de soporte del proveedor proporciona a los clientes.
14. SMTP	“Simple Mail Transfer Protocol”, traducido como “Protocolo simple de transferencia de correo”, es un protocolo que permite que los correos sean enviados.
15. SPAM	Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.
16. TI	Tecnologías de Información.

17. TIC	Tecnologías de Información y Comunicación.
18. WAF	“Web Application Firewall” o “Cortafuegos de Aplicaciones Web” es un tipo de cortafuegos que supervisa, filtra o bloquea el tráfico hacia y desde una aplicación web.
19. XDR	“Extended Detection and Response”, es la tecnología más avanzada de ciberseguridad, que permite la detección y respuesta a incidentes de seguridad en todas las capas del entorno de TI (que pueden incluir puntos finales, redes y usuarios).

TITULO II.
DE LA ORGANIZACIÓN INTERNA

ARTÍCULO 6º: Roles y responsabilidades. La Universidad de La Frontera establece los siguientes roles mínimos obligatorios vinculados a la importancia de la seguridad de la información.

Rol	**Responsabilidad**
1. Alta dirección	a. Velar por la existencia de un plan formal de difusión de este reglamento y los estándares que lo sucedan o se relacionen con este. b. Establecer un estándar de traspaso de información cuando existan cambios de personas en cargos. c. Propiciar la existencia de estándares vinculados a la seguridad de la información y ciberseguridad que permitan la continuidad del quehacer institucional.
2. Dirección de Informática	La Dirección de Informática o unidad que la suceda en la Universidad de La Frontera, es la responsable de: a. Coordinar y supervisar la implementación y difusión del cumplimiento del presente reglamento. b. Promover la difusión de los estándares vinculados a la seguridad de la información y ciberseguridad. c. Coordinar y dirigir el Comité de Seguridad de la Información.
3. Encargado/oficial de seguridad de la información	a. Plantear y desarrollar inicialmente los estándares de seguridad, control de implementación y velar por la correcta aplicación. b. Coordinar la respuesta de incidentes de seguridad de la información. c. Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y externos con el fin de mantenerse actualizado en términos de seguridad de la información. d. Participar del Comité de Seguridad de la Información, asumiendo el rol estratégico y técnico que la organización requiera para estas materias. e. Proponer procedimientos de manipulación del procesamiento del documento electrónico, es decir: copiado; almacenamiento; transmisión por correo electrónico y sistemas protocolizados de transmisión de datos digitales; y destrucción. f. Cooperar en la formulación del plan de contingencia o su

	homólogo para asegurar la continuidad de operaciones críticas.
4. Comité de Seguridad de la Información	Estará conformado por representantes de la administración central y de cada facultad, y será dirigido por la Directora o Director de Informática o unidad que la suceda en la Universidad de La Frontera. Entre las funciones se encuentran las siguientes: a. Asesorar a la Universidad de La Frontera en materias de seguridad de la información. b. Analizar, proponer y validar los estándares de seguridad de la información de la Universidad de La Frontera, supervisando el estado de implementación del presente reglamento. c. Revisar e identificar periódicamente los requisitos legales, estatutarios, regulatorios y contractuales vinculados a la seguridad de la información y proponer mejoras continuas, que permitan alcanzar estándares superiores de calidad en la operación de los sistemas, redes, equipamiento, servicios, etc. d. Proponer y revisar planes de renovación anual del equipamiento corporativo, tanto a nivel de servidores y equipos de comunicaciones, como de estaciones de trabajo y otros equipos. e. Reunirse al menos una vez al año.
5. Estudiantes, académicas, académicos, funcionarias y funcionarios.	a. Velar por el cumplimiento del presente reglamento. b. Informar cualquier evento o actividad que atente contra los principios de la seguridad de la información de la Universidad de La Frontera. c. Participar en las acciones de capacitación en línea o presencial en relación a todas las materias de Ciberseguridad y Seguridad de la Información.

La Universidad deberá revisar y asignar los roles y responsabilidades de la Seguridad de la Información según los estándares vinculados al presente reglamento.

ARTÍCULO 7º: Segregación de Tareas. Se entiende como segregación de tareas o funciones la separación de áreas o procesos de alta responsabilidad, con la finalidad de disminuir los riesgos. Cada función de TI deberá tener una segregación de roles documentada y especificada en los organigramas y documentos, especialmente en los Planes de Emergencia o equivalente que la organización desarrolle en el futuro, de acuerdo con el Reglamento de la Seguridad de la Información.

A su vez la Universidad deberá crear un estándar que cubra y especifique la segregación de deberes, cómo llegan las decisiones con respecto a tal segregación, quién tiene la autoridad para tomar estas decisiones y el seguimiento regular de las actividades y los registros de Auditoría. El control de estos procesos deberá estar debidamente documentado y controlado por medio de un calendario de auditorías aprobados por la más alta autoridad de la Universidad.

ARTÍCULO 8º: Uso de recursos. Las y los integrantes de la comunidad universitaria y usuarios que utilicen los recursos de tecnologías de información y comunicación que la Universidad de La Frontera provea, será para el cumplimiento del quehacer institucional, ajustando su uso a lo dispuesto en la legislación vigente, y a las normas de la Universidad, quedando prohibido cualquier uso privado y/ o comercial no autorizado por este reglamento o por la Dirección de Informática o unidad que la suceda.

Toda autorización de acceso a los recursos es exclusiva del usuario al que le fue asignada y no es transferible por éste a otros usuarios. Por lo mismo, cada usuario es responsable del buen uso de estos.

Es responsabilidad del usuario el respaldo periódico de la información que maneja, la que debe ser respaldada institucionalmente, ya sea en el espacio virtual institucional o en dispositivos mantenidos en dependencias de la Universidad. Además, el usuario deberá velar por mantener en lo posible limpio su escritorio electrónico y físico, adoptando todas las medidas que sean necesarias para mantener la confidencialidad de la información que maneja.

TITULO III.
DE LA SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

ARTÍCULO 9º: Antes del empleo.

1. Investigación de antecedentes: La Universidad, por medio de la Vicerrectoría de Administración y Finanzas, Dirección de Recursos Humanos o unidad que la suceda, deberá implementar mecanismos de investigación de antecedentes del personal a contratar de forma que se cumplan como mínimo las siguientes indicaciones:
   a. La evaluación previa al empleo toma en cuenta las leyes y regulaciones relevantes de privacidad y empleo.
   b. Regular la selección, en caso de que sea ejecutada por un tercero, revisando el proceso y si estos son acordes a los requerimientos en seguridad de la información y ciberseguridad.
   c. Se deberá hacer contacto de referencias y una verificación de antecedentes, dejando evidencia de estas acciones.
   d. Para los roles críticos deberán existir procesos de selección mejorados.

2. Términos y condiciones del empleo. La Universidad, por medio de la Vicerrectoría de Administración y Finanzas, Dirección de Recursos Humanos o unidad que la suceda, deberá tener las siguientes condiciones mínimas habilitadas en lo relacionado a términos y condiciones del empleo:
   a. Definir claramente los términos y condiciones del empleo.
   b. Distinguir entre profesionales de la seguridad de la información, administradores de redes, de sistemas TI, los puestos directivos, los auditores y los trabajadores en general. E indicar las responsabilidades específicas relacionadas con el riesgo y la seguridad de la información de acuerdo con la naturaleza de los roles.
   c. Mantener registros para probar que los trabajadores entendieron, reconocieron y aceptaron sus obligaciones de seguridad de la información.

ARTÍCULO 10º: Durante el Empleo.

1. **Responsabilidades de gestión:** La Universidad deberá en forma anual crear un programa de concienciación relacionado con la Seguridad de la Información y Ciberseguridad destinado exclusivamente a la alta dirección, decanos y puestos estratégicos. Esta capacitación además deberá contener los aspectos relevantes sobre las posturas, estrategias y estándares de seguridad de la organización haciendo hincapié en la responsabilidad de gestión de estas materias y las variables jurídicas especificadas en las leyes, ya sea del territorio nacional como de otras variables presentes en el mundo.

   Este programa de concienciación deberá tener un registro de los participantes e identificación de los tópicos y materias tratadas en cada ciclo. La Universidad deberá nombrar al área más competente para el desarrollo de esta actividad.

2. **Concienciación, educación y capacitación en seguridad de la Información:** La Universidad deberá implementar un programa de concienciación en Seguridad de la Información transversal a todo el personal interno, contratistas y estudiantes de forma que se cumplan como mínimo los siguientes requisitos:

   a. Concienciación exclusiva para los profesionales de seguridad de la información y otros con funciones y responsabilidades específicas identificadas explícitamente.

b. La concienciación en materias de seguridad de la información deberá ser obligatoria al inicio del contrato de las personas o ingreso a la Universidad.
b. Se deberán implementar acciones de seguimiento de estas capacitaciones con sus reforzamientos semestrales considerando los riesgos de la información en evolución.
c. Se deberá contar con un plan de comunicación que incluya folletos, correos electrónicos, gestión de aprendizaje en línea, cuestionarios, concursos, videos u otros métodos pertinentes.
d. Estas capacitaciones deberán cubrir los requisitos legales, reglamentarios, contractuales, políticos, responsabilidad personal, responsabilidades generales, puntos de contacto y otros recursos que la organización considere pertinentes.

3. **Procedimiento disciplinario.** La Universidad deberá implementar, por medio de sus unidades especializadas, un procedimiento disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial por parte de los estudiantes, académicas, académicos, funcionarias y funcionarios, teniendo como principal insumo la legislación vigente en materia. Asimismo, se deberá informar a los estudiantes, académicas, académicos, funcionarias y funcionarios sobre cómo se ejecuta este proceso disciplinario, las expectativas de la organización y sus derechos. Así también esto deberá estar completamente cubierto por contratos y acuerdos, capacitación inicial y conocimiento continuo.

ARTÍCULO 11º: Finalización del empleo o cambio de puesto de trabajo. La Universidad, por medio de la Dirección de Recursos Humanos o unidad que la suceda, deberá implementar un estándar que regule la revisión, normativas, directrices y registros relacionados con la Seguridad de la Información para los funcionarios que se mueven lateral o verticalmente dentro de la organización, donde se deberán además considerar las promociones, cambio de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias y desvinculaciones. Se deberá para todo efecto considerar la recuperación de los activos de información (documentos, datos, sistemas), las llaves, la eliminación de los derechos de acceso físicos y digitales y todo los que la organización considere necesario para resguardar la Seguridad de la Información y la Ciberseguridad.

TITULO IV.
DE LOS ESTÁNDARES

ARTÍCULO 12º: Estándar. Para fines generales, a continuación, se llamará “estándar” a cualquier política, proceso, procedimiento, norma, lineamientos, protocolo u otro documento que se deba crear a partir del presente reglamento.

La Universidad de La Frontera deberá contar con los estándares listados o sus respectivos homólogos que se indican en los artículos siguientes.

ARTÍCULO 13º: Plan de contingencias informáticas.
Deberá ser estructurado de manera clara y ordenada con las funciones y responsabilidades del personal.

Deberá definir las actividades ante desastres, alertas y advertencias de incidentes, los distintos niveles de alertas, mecanismos, comunicación ante incidentes, y la lista de contacto para las autoridades reguladoras u otras autoridades y organismos que podrán ser contactados en caso de consulta, incidentes y emergencias. Indicando quien es el responsable de contactar a las autoridades y en qué punto del incidente/evento se realiza este contacto y cómo, además, indicar quién es el responsable de la mantención actualizada de este listado y con qué periodicidad se actualiza. Contacto con otros grupos de interés en caso de incidentes, CSIRT de Gobierno u otros.

Se deberá incorporar planes y entrenamientos de estos, y activos junto a su clasificación que resguardan este plan.

ARTÍCULO 14º: Gestión de proyectos.
1. La Universidad deberá a través de su Dirección de Informática o unidad que la suceda, incorporar el análisis del requisito de adquisición de sistemas y software, identificando y abordando los riesgos de la seguridad de la información, incorporando todos los tipos de

proyectos, nuevos desarrollos, cambios, mejoras de los sistemas, aplicaciones y procesos existentes. Siendo responsabilidad de la Unidad que lidera y/o coordina el proyecto solicitar y respetar la validación técnica de la Dirección de Informática.

2. Deberán existir métricas de calidad y seguridad para los proyectos donde se manipule información, ya sea en forma de bases de datos o en documentos, la cual sea sensible para la organización.

ARTÍCULO 15º: Gestión de activos.

1. Se deberá identificar, elaborar y mantener un inventario de activos de información con los siguientes campos o ítems mínimos: Datos digitales, información impresa, software, infraestructura, servicios de información y proveedores de servicios, seguridad física, relaciones comerciales; y con respecto a las personas, quién es el dueño del inventario, etiquetado de los activos.
2. Se deberán especificar algunas consideraciones administrativas en estándares que regulen estas acciones, tales como: mantención del inventario en una condición razonablemente completa, precisa y actualizada; propietario de riesgo y responsable técnico del activo; asignación de la propiedad poco después de crear o adquirir los activos críticos; codificación y etiquetado de los activos; cómo se informan los incidentes de seguridad de la información que los afectan; recuperación de los activos tras una baja o despido, identificando todos los factores de riesgos que estas acciones suponen en la práctica, abordando los casos en que los activos no se devuelvan o no se puedan recuperar en caso de robo o extravió, poniendo especial énfasis en las cuentas de acceso a las plataformas que pudieran tener estos activos.

ARTÍCULO 16º: Clasificación de la información. La Universidad deberá establecer:

1. Estándares para la clasificación de la información, amparada bajo las obligaciones legales o contractuales donde se desenvuelva la organización, contemplando los requisitos de confidencialidad, integridad y disponibilidad de todas sus plataformas. Al igual que en otras obligaciones de la Seguridad de la Información, las personas contratadas deberán conocer los requisitos de seguridad correspondientes para el manejo de materiales clasificados.
2. El etiquetado de la información tanto en forma física como electrónica, garantizando el correcto etiquetado por medio de controles o auditorías permanentes, permitiendo solo a personal autorizado el acceso a información clasificada relevante. Así también, se deberá garantizar y auditar los ingresos a la información más sensible por medio de algún procedimiento autorizado y definido.
3. Un protocolo de auditoría que permita revisar en forma periódica si la clasificación de los activos es adecuada a su condición, regulando además el método de etiquetado, su transferencia cuando se realice, su almacenamiento, el manejo de los medios extraíbles, la eliminación de los medios electrónicos de acuerdo con la ley, su forma de divulgación e intercambio con terceros.

ARTÍCULO 17º: Manipulación de los soportes. La Universidad deberá establecer.

1. Estándar que incluya el control por medio de un registro, de la lista completa de los medios extraíbles que se consideren críticos, los cuales deberán estar debidamente etiquetados y clasificados, además, la forma de almacenamiento y los controles apropiados para mantener la confidencialidad de los datos almacenados.
2. Estándar específico que regule y controle de acuerdo con las obligaciones contractuales, legales o reglamentarias, la eliminación de los medios físicos y lógicos, donde se deberá especificar que cada aprobación de cada etapa deberá ser documentada y registrada, validando los datos que aún deberán conservarse, verificación de borrado efectivo y los periodos de retención que obligan las leyes vigentes o contratos específicos para determinados datos.
3. Regulación con un estándar específico del transporte de los soportes físicos que indique los aspectos en relación con la confiabilidad de los medios de transportes o servicios a utilizar, mecanismos de cifrado adecuados durante el período de transferencia y la validación segura de recepción por el destinatario.

ARTÍCULO 18º: Seguridad de las operaciones. La Universidad deberá implementar:

1. Un estándar que regule y documente los procedimientos operacionales de la Infraestructura y Sistemas TI, donde se incluyan las directrices de seguridad, procesos razonablemente seguros y bien controlados, roles y responsabilidades bien definidos,

consideraciones en relación a los cambios, configuraciones, versiones, capacidades, incidentes, copias de seguridad, restauración y sus validaciones y revisiones rutinarias y documentadas.

2. Un estándar de gestión de cambios donde existan los registros documentados en relación con la gestión de los cambios, sus planificaciones, evaluaciones de riesgos potenciales asociados a los cambios y las autorizaciones por la administración.
3. Un estándar de control de la gestión de capacidades, sus registros, SLA, seguimiento de las métricas relevantes, niveles de alerta crítico, planificaciones hacia adelante y prioridades especialmente en lo relacionado a servicios críticos. Se deberá considerar para esta gestión los análisis de riesgos relacionados con la gestión de las capacidades y las decisiones de implementación futura.
4. Un estándar que permita segregar los entornos TI, que tengan como mínimo las siguientes obligaciones o consideraciones:
   a. Consideraciones para tomar en relación con la seguridad de cada ambiente y sus controles de aislamiento.
   b. Accesos diferenciados de perfiles de usuario para cada uno de los entornos, además, la revisión periódica de los usuarios y perfiles asignados.
   c. Autorizaciones a la gestión del cambio y migración de software, datos, metadatos y configuraciones entre entornos en cualquier dirección.
   d. Consideraciones de riesgos de la información y los aspectos de seguridad que incluya el cumplimiento de privacidad si los datos personales se mueven a entornos menos seguros.
   e. Identificación de los responsables de garantizar que el software nuevo/modificado no interrumpa las operaciones de otros sistemas o redes.

ARTÍCULO 19º: Protección contra código malicioso. La Universidad, deberá implementar estándares asociados a controles de software malicioso, que contengan como mínimo las siguientes indicaciones:

1. Utilizar listas blancas y negras para controlar el uso de software autorizado.
2. Controles antivirus en todos los dispositivos relevantes.
3. Controles por XDR y EDR para toda la plataforma relevante.
4. Actualizaciones automáticas para los Antivirus, Antimalware y XDR/EDR.
5. Protocolo de alertas accionables tras una detección.
6. Protocolo de gestión de vulnerabilidades técnicas.
7. Capacitación y concienciación apropiada que cubra la detección, el informe y la resolución de Malware para usuarios, rectoría, decanos, profesores, investigadores y especialistas de soporte.
8. Protocolo de escalamiento para incidentes graves.
9. Segregación escalonada de las redes de la Universidad, con objeto de evitar propagación masiva de Malware.

Será responsabilidad del Comité de Seguridad de la Información establecer los criterios para definir qué dispositivos y plataformas serán consideradas como relevantes.

ARTÍCULO 20º: Copias de seguridad. La Universidad deberá implementar un estándar que regule las copias de seguridad de la información de acuerdo con la siguiente pauta mínima:

1. Mandato basado en el riesgo preciso y completo de copias de seguridad cuyo estándar de retención y frecuencia reflejen la necesidad de la organización.
2. Las copias de seguridad deberán cubrir los datos y metadatos, sistemas y programas de aplicación y los parámetros de configuración de copias de seguridad para todos los sistemas, incluyendo servidores, computadores de escritorio, portátiles y todo equipo que pertenece al inventario de activos y que sea considerado sensible.
3. Ubicación adecuada de almacenamiento protegido contra desastres físicos y accesos.
4. Mantención de las copias en off-line para evitar propagación de Malware catastrófica.
5. Pruebas regulares de las copias de seguridad para garantizar sus restauraciones.
6. Clara adherencia a principios de confidencialidad, integridad y disponibilidad.

ARTÍCULO 21º: Registro de actividad y supervisión.

1. La Universidad, deberá implementar un estándar que regule el registro de eventos de acuerdo con el siguiente estándar mínimo:

a. Establecer un monitoreo y registro de manera consistente y segura de todos los sistemas claves, incluido el registro de eventos.
b. Responsabilidades de revisión y seguimiento de los eventos informados.
c. Establecimiento de periodos de retención de eventos.
d. Determinación de proceso para revisar y responder adecuadamente a las alertas de seguridad.
e. Revisión de todos los parámetros principales como cambios en los ID de usuarios, actividades privilegiadas de los sistemas, intentos de acceso exitosos y fallidos, instalaciones de software y otros.

2. La Universidad deberá implementar un estándar que proteja la información de los registros, los cuales se deberán almacenar en un formato seguro o mecanismo de control no-editable. Además, los accesos a estos registros deberán estar controlados y monitoreados, verificando los volúmenes en forma periódica para que los registros no fallen en su compilación de información. Así también se deberá establecer cómo se harán las copias de seguridad de estos y bajo qué periodicidad, y los responsables identificados para la administración de accesos privilegiados al análisis de eventos.
3. La Universidad implementar un estándar que regule los procesos de cambios horarios en los servidores, sistemas, bases de datos y otras arquitecturas TI relevantes para la organización. El método de sincronización deberá cumplir con los requisitos de seguridad, legales, regulatorios, comerciales, contractuales y operacionales que la organización deba cumplir. Su implementación deberá abarcar todos los ambientes, sistemas de monitoreo, sistemas de alertas o entornos TI que la organización considere relevantes.

ARTÍCULO 22º: Control de software en explotación. La Universidad deberá implementar un estándar que regule la instalación de software, donde se deberá asegurar que todo el software instalado es probado, aprobado, permitido y mantenido para su uso en producción. Así también, deberá existir algún estándar que permita identificar si en la plataforma se tiene software sin soporte, adoptando controles para evitar instalaciones sin autorización, excepto por administradores capacitados y autorizados, los cuales también deberán adoptar normas de control de cambio y aprobaciones adecuadas.

ARTÍCULO 23º: Sobre el uso del Software.
En los equipos computacionales, de telecomunicaciones y en dispositivos basados en sistemas computacionales, únicamente se permitirá la instalación de software con licenciamiento apropiado.

El uso de todo nuevo software que se requiera utilizar y se encuentre debidamente licenciado, deberá ser aprobado por la Dirección de Informática o unidad que la suceda, con el fin de corroborar que éste no dañe el buen rendimiento de la red de telecomunicaciones institucional, de las plataformas o del propio equipo computacional.

ARTÍCULO 24º: Gestión de vulnerabilidad técnica.
1. La Universidad deberá implementar un estándar de gestión de vulnerabilidades técnicas, la cual deberá contener como mínimo las siguientes indicaciones:
   a. Deberá definir la forma como se deberán escanear los sistemas para detectar vulnerabilidades en forma automática.
   b. Deberá definir la respuesta de la organización ante vulnerabilidades técnicas descubiertas en equipos, servidores, aplicaciones, dispositivos de red y otros componentes.
   c. Deberá definir procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes.
   d. Deberá definir la forma de realizar la evaluación integral de riesgos de los sistemas TIC y su priorización.
   e. Deberá definir la forma de evaluar los parches por su aplicabilidad y riesgos antes de ser implementados.
2. La Universidad deberá implementar un estándar que regule que la instalación de software en los sistemas esté limitada a personal autorizado, con los privilegios adecuados y que idealmente estos privilegios estén divididos en categorías y que permitan instalar tipos de sistemas específicos.
3. La Universidad deberá implementar un estándar que regule los controles de auditoría de sistemas de información, detallando el programa anual y los procedimientos para realizar

estas auditorías. Se deberá considerar especialmente los riesgos de interrupciones en los procesos relevantes de la Universidad que puedan afectar la continuidad de los servicios. El alcance de estas auditorías deberá estar especificado y coordinado con la administración u otros grupos de interés relevantes de la Universidad. Las herramientas de auditoría de sistemas deberán estar controladas para evitar el uso y acceso no autorizado.

ARTÍCULO 25º: Seguridad de las comunicaciones.

1. La Universidad deberá implementar un estándar que regule los controles de red de acuerdo con las siguientes indicaciones mínimas:
   a. Deberá existir una separación de la administración de las operaciones de sistemas y la de infraestructuras de red.
   b. Deberá existir un mecanismo de autentificación razonablemente seguro para todos los accesos a la red de la organización.
   c. Deberá existir limitantes al acceso de personas autorizadas a aplicaciones/servicios legítimos.
   d. La autenticación de inicio de sesión deberá ser obligatoria.
   e. Deberá existir una segmentación de red adecuada a la realidad de la organización.
   f. Deberá existir un mecanismo que permita controlar los puertos y servicios utilizados para funciones de administración de sistemas.
   g. Deberá existir un protocolo de revisión de parches y actualizaciones del equipamiento de networking y los dispositivos asociados.
2. La Universidad deberá implementar un estándar que gestione, clasifique y proteja los servicios de red en forma adecuada, describiendo la forma del monitoreo, los derechos a auditar los servicios de red gestionados por terceros (contratos, SLA, requisitos de informe de gestión), mecanismos de cifrado de red y forma de auditar las configuraciones y LOG de cortafuegos IDS/IPS/WAF/DAM.
3. La Universidad deberá implementar un estándar que regule la segregación de sus redes, detallando la segmentación que existe, los niveles de confianza, dominios, forma de monitorear y controlar la segregación, segmentación de la red inalámbrica de la red física, control de la red de invitados o red de alumnos si existe y protocolos de incidentes de seguridad de redes.

ARTÍCULO 26º: Intercambio de información.

1. La Universidad deberá implementar un estándar que regule los procesos de intercambio de información entre entidades internas y otras organizaciones externas, sujetándose a las leyes actuales, estableciendo canales seguros y regulados de transferencia, considerando siempre el aumento de las medidas de seguridad cuando la información sea de carácter sensible. La condición anterior además deberá establecer algún mecanismo de cadena de custodia digital para la transferencia de datos.
2. La Universidad deberá implementar un estándar que regule la mensajería electrónica, con el objetivo de cubrir los controles de seguridad adecuados (cifrado, autenticación, confidencialidad y la irrenunciabilidad de mensajes).
3. La Universidad deberá implementar un estándar donde sea obligatorio los acuerdos de confidencialidad, tanto en información confidencial y no confidencial, especialmente cuando la información física o electrónica es sensible para la organización. Esta normativa deberá especificar quiénes deberán aprobar y firmar estos acuerdos y las sanciones adecuadas y acciones esperadas en caso de incumplimiento.

ARTÍCULO 27º: Adquisición, desarrollo y mantenimiento de los sistemas de información.

1. La Universidad deberá implementar un estándar que regule los registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software. Se deberá considerar los análisis de riesgos, requisitos funcionales y técnicos, arquitectura de seguridad, las pruebas de seguridad y la certificación de sistemas y desarrollo. Todo lo anterior, deberá ser obligatorio para todos los nuevos desarrollos y cambios en los sistemas existentes, actualizaciones de sistema operativo/aplicaciones. Así también, se deberá especificar los alcances de seguridad y de arquitecturas para los softwares comerciales que la organización adquiera.
2. La Universidad deberá implementar un estándar que regule las aplicaciones web de comercio electrónico, de cara hacia los distintos servicios que por estos medios se ejecutan. Se deberá verificar los aspectos de seguridad como: control de acceso y

autentificación de usuarios, integridad de datos y la disponibilidad del servicio. Además, deberán estar especificados controles de validación de datos de entrada, validación de procesamiento, encriptación, autentificación de mensaje e irrenunciabilidad, forzado de https, monitoreo de los sitios por medio de un EDR/XDR y la forma de analizar y documentar las amenazas rutinarias con su gestión de incidentes y cambios para tratarlos.

3. La Universidad deberá implementar un estándar que indique la forma de almacenar en un entorno interno seguro las transacciones que se realizan por las aplicaciones expuestas a internet. Para lo anterior se deberá considerar la protección de la información mediante el uso de protocolos seguros, cifrados, firma electrónica y otras medidas de seguridad que la organización considere. Todo lo anterior deberá cumplir con todos los requisitos legales, regulatorios y de cumplimiento que la organización deba cumplir.
4. La Universidad deberá implementar un estándar que regule la protección de los datos de prueba especificando los mecanismos para proteger estos datos, como la seudonimización, enmascaramiento, datos falsos, borrado u otros mecanismos de comprobada eficiencia. Además, deberá especificarse el mecanismo de verificación y aprobación para el uso de datos no protegidos para pruebas y dejar evidencia documentada de estas actividades.
5. La Universidad a través de su Dirección de Informática o unidad que la suceda implementará un estándar especificando que el acceso a las Bases de Datos Institucional es restringido y según los criterios de la Dirección de Informática.

ARTÍCULO 28º: Continuidad de la seguridad de información.

1. La Universidad deberá implementar un estándar que especifique las siguientes condiciones mínimas para establecer la planificación de la continuidad de la seguridad de la información:
   a. Mecanismo que permita determinar los requisitos de continuidad del quehacer institucional.
   b. Se deberá diseñar e implementar un plan de continuidad del negocio o de los servicios de la Universidad.
   c. Se deberá regular e implementar el diseño adecuado de alta disponibilidad para sistemas de TI, redes y procesos críticos.
   d. Se deberá tener identificado el impacto potencial de los incidentes.
   e. Se deberá hacer un calendario de evaluación semestral de los planes de continuidad.
   f. Se deberá implementar un calendario periódico de ensayos de continuidad.
2. La Universidad deberá implementar un estándar que establezca la continuidad de la seguridad de la información detallando los siguientes aspectos mínimos:
   a. Definición de plazos para restaurar los servicios tras una interrupción.
   b. Definición de la identificación y el acuerdo de responsabilidades, la identificación de las pérdidas aceptables, la implementación de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares.
   c. Definición de planes para la gestión de crisis donde estén reguladas las responsabilidades y los roles.
   d. Controles de seguridad adecuados en los sitios de recuperación de desastres remotos.
3. La Universidad deberá implementar un estándar que permita establecer un método de pruebas del plan de continuidad, las frecuencias con que se realizan estas pruebas, sus evidencias y sus resultados. Además, se deberán documentar las deficiencias detectadas y cómo se han remediado.

TITULO V.
DE LA GESTIÓN DE ACCESO

ARTÍCULO 29º: Del derecho de acceso a través de red fija o inalámbrica.

El acceso a través de red fija o través de redes inalámbricas a Internet como a los sitios web de la Universidad de La Frontera mediante los recursos informáticos institucionales es un derecho que se reconoce a sus funcionarios y estudiantes, bajo las condiciones definidas en este reglamento y determinadas por la Dirección de Informática o unidad que la suceda.

ARTÍCULO 30º: Servicio de Red Privada Virtual (VPN).
Podrán ser usuarios del servicio de Red Privada Virtual (VPN) quienes la requieran para el desarrollo de su quehacer en la Universidad de La Frontera, para lo cual utilizarán la infraestructura de la red de la Universidad de La Frontera para acceder y/o intercambiar información, cumpliendo los objetivos generales de la red y utilizándola eficientemente, con el fin de evitar en la medida de lo posible la congestión de la misma, la interrupción de los servicios de red o del equipamiento de la infraestructura conectada.
Cuando se demuestre el incumplimiento de alguna de las normas en el uso del servicio de Red Privada Virtual, la Dirección de Informática, o unidad que la suceda, podrá suspender temporal o definitivamente el servicio al usuario, sin perjuicio de las responsabilidades que eventualmente puedan generarse.

ARTÍCULO 31º: Claves de Acceso.
1. La autorización para el acceso a plataformas institucionales y servicios en red de la Universidad de La Frontera para todo nuevo usuario, deberá ser gestionada por cada unidad ante la Dirección de Informática o unidad que la suceda.
2. Cada usuario contará con una identidad (nombre de usuario), la que le permitirá el acceso a las plataformas institucionales y servicios en red de la Universidad de La Frontera, en función de su perfil de usuario. Dicha identidad tendrá asociada una contraseña confidencial, que el usuario deberá cautelar.
3. Todas las acciones realizadas con un nombre de usuario serán responsabilidad del usuario titular de dicha identidad, salvo sustracción de identidad, no atribuible a su negligencia.
4. La Universidad deberá implementar un estándar de “información secreta de autenticación de los usuarios” que permita regular, de acuerdo con las buenas prácticas, la gestión de autentificación en todos los sistemas, en la red o en otros accesos de la organización. Las condiciones de esta gestión deberán tener como mínimo lo siguiente:
    a. Implementar controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas en el primer uso, autentificación de múltiples factores, datos biométricos u otros métodos avanzados.
    b. Verificar rutinariamente si existen contraseñas débiles.
    c. Utilizar mecanismos de comprobación de identidad de los usuarios antes de proporcionarles contraseñas temporales nuevas.
    d. Transmitir información de contraseñas solamente por medios seguros.
    e. Establecer contraseñas temporales suficientemente fuertes.
    f. Cambiar todas las contraseñas por defecto de los fabricantes.
    g. Instruir al personal el uso del software adecuado de protección de contraseñas.
    h. Instruir y verificar que el almacenamiento de las contraseñas de los sistemas, dispositivos y aplicaciones estén cifrados con un algoritmo de alto estándar.
5. La Universidad deberá implementar un estándar que establezca cómo proceder con las claves entregadas por organismos externos para la institución, considerando las situaciones derivadas de traspasos y cambios de cargos y personas.

ARTÍCULO 32º: Del acceso a plataformas institucionales y servicios en red.
La autorización para el acceso a plataformas institucionales y servicios en red de la Universidad de La Frontera, será gestionada ante la Dirección de Informática o unidad que la suceda, por la unidad correspondiente y deberá contar con la autorización del jefe de ésta. El identificador concedido expira cuando la unidad correspondiente solicite a la Dirección de Informática o unidad que la suceda, la suspensión de acceso para dicho identificador del usuario, o cuando se compruebe un uso indebido. Será obligación de cada jefatura informar la baja de los usuarios de su área que cesen en su función, para que sea dado de baja el permiso de acceso existente.

Tratándose de las redes inalámbricas, su acceso es solo previa autorización de la Dirección de Informática o unidad que la suceda, e instalación y conexión de puntos de acceso correspondientes. Los usuarios habilitados, bajo ningún concepto, podrán trasladar equipos de puntos de acceso inalámbrico a otros espacios o zonas de los edificios, ni conectarlos a otros puntos de la red corporativa.

Los usuarios internos de la red inalámbrica de la Universidad dispondrán de una cuenta de usuario y contraseña para conectarse al servicio de red inalámbrica corporativa. Por su parte, los usuarios externos de la misma (visitantes temporales, asistentes a congresos, jornadas, etc.) podrán disponer de credenciales temporales, las que serán solicitadas a la Dirección de

Informática o unidad que la suceda por parte de la unidad que recibe al usuario u organiza la actividad.

ARTÍCULO 33º: Control de acceso a los sistemas y aplicaciones.

1. La Universidad, por medio de su Dirección de Informática o unidad que a suceda, deberá establecer un estándar que asegure la confidencialidad de las credenciales de autentificación, con su respectivo proceso de cambio de contraseña en caso de ser comprometida.
2. La Universidad, por medio de su Dirección de Informática o unidad que a suceda, deberá establecer un estándar que permita controlar los accesos de todos los sistemas en forma adecuada e identificar a los usuarios en forma individual, indicando cómo se definen, autorizan, asignan, revisan, gestionan y retiran los derechos de acceso, los permisos y las reglas asociadas.
3. La Universidad, por medio de su Dirección de Informática o unidad que a suceda, deberá implementar un estándar de inicio seguro de sesión sobre todos los sistemas, acceso a red u otros aplicativos que controle la organización. Este deberá contener como mínimo lo siguiente:
   a. Pantalla de inicio con advertencia en el proceso de inicio de sesión para disuadir el acceso no autorizado.
   b. Autentificación doble factor sobre todos los accesos.
   c. Información de inicio de sesión validada una vez imputadas las credenciales.
   d. Alertas de contraseñas no validadas.
   e. Registros de inicio de sesión exitosos.
   f. Transmisión de contraseñas de modo seguro mediante el uso de cifrado.
4. La Universidad deberá implementar un estándar de gestión de contraseñas de acuerdo con estándares de la organización, detallando la longitud mínima, evitando la reutilización de un número específico de contraseñas, detallando las reglas de complejidad, cambio forzado en el primer inicio, ocultamiento de la contraseña durante la imputación y su forma de transmisión. Todo esto además deberá estar validado por lo menos una vez al año por medio de una auditoría interna documentada.
5. La Universidad deberá implementar un estándar que regule los aspectos relacionados con los servicios privilegiados de los sistemas, con registro de acceso a ellos, bajo qué condiciones y con qué fines se otorgan, verificación de las necesidades de acceder para otorgar el acceso según roles y responsabilidades. Además, deberá existir un proceso auditable de aprobación y cada instancia de su uso deberá estar registrada.
6. La Universidad implementar un estándar que permita controlar el código fuente de los sistemas de la organización, bajo un entorno seguro, con accesos adecuados, control de versiones, monitoreo, registro y control de los repositorios. También deberá existir una forma regulada para modificar estos códigos, su publicación y la revisión constante de los registros de accesos y cambios.

TITULO VI.
DE LA CRIPTOGRAFÍA

ARTÍCULO 34º: Estándares de controles Criptográficos. La Universidad, por medio de su Dirección de Informática o unidad que la suceda, deberá:

1. Implementar un estándar de uso de controles criptográficos detallando lo siguiente como mínimo:
   a. Los casos en los que la información deberá ser protegida a través de criptografía.
   b. Normas que deberán aplicarse para la aplicación efectiva.
   c. Proceso basado en riesgo para determinar y especificar la protección requerida.
   d. Uso de cifrado para información almacenada o transferida.
   e. Los efectos de cifrado en la inspección de contenidos de software.
   f. Cumplimiento de las leyes y normativas aplicables.
2. La Universidad, por medio de su Dirección de Informática o unidad que la suceda, deberá implementar un estándar donde se especifique el ciclo de vida completo de la gestión de claves, reglas de cambio/actualización, copias de respaldo de las claves, registro de actividades y sus auditorías para los privilegios elevados.
3. La Universidad, por medio de su Dirección de Informática o unidad que la suceda, deberá implementar un estándar que regule los controles criptográficos relacionados con

importación/exportación de este material y que además cumplan con los requisitos legales y reglamentarios.

TITULO VII.
DE LA SEGURIDAD FÍSICA Y DEL ENTORNO

ARTÍCULO 35º: Estándares de controles de seguridad física y entorno.

1. La Universidad, por medio de su Dirección de Informática y Dirección de Infraestructura y Servicios, o unidades que las sucedan, deberá implementar un estándar que defina los perímetros de seguridad físicos (edificios, oficinas, redes, armarios de red, archivos, salas de datos u otras instalaciones sensibles), determinando que la construcción de estas zonas sea la adecuada para la seguridad, protegiéndola de accesos externos no autorizados, implementando idealmente mecanismos de controles de accesos regulados y cámaras de vigilancia con grabación de imágenes. Así también se deberá regular para las zonas más sensibles los registros de acceso por medio de alguna bitácora y el acompañamiento de las visitas autorizadas. Todo esto deberá tener un protocolo de auditoría semestral.
2. La Universidad, por medio de su Dirección de Informática o unidad que la suceda, deberá:
   a. Implementar un estándar de seguridad para el emplazamiento y protección de los equipos, que cumpla como mínimo las siguientes condiciones:
      i. Las pantallas de los equipos de trabajo, las impresoras y los teclados deberán estar ubicados o protegidos para evitar la visualización no autorizada.
      ii. Los equipos deberán estar protegidos de riesgos de amenazas físicas y medio ambientales.
      iii. Las instalaciones de red y eléctricas de los equipos deberán estar protegidas y acordes a las normas establecidas para la seguridad de las personas.
   b. Un estándar que regule y controle las instalaciones de suministro eléctrico y de aires acondicionados en caso de que tenga salas de servidores o equipos de comunicaciones críticos dentro de la organización, revisando que los suministros eléctricos sean los adecuados y suficientes, con las protecciones que correspondan para los equipos y las personas. Además, se deberá regular su mantención y registro de estas revisiones por personal especializado.
   c. Un estándar que regule la instalación del cableado de red dentro de la organización, no sólo en lo relacionado a sus estructuras de calidad de transmisión, sino que a las normas de emisión en caso de incendios. Se deberá además establecer que el cableado de red deberá estar separado del cableado eléctrico, de acuerdo con las normas, a objeto de evitar interferencias. El acceso a los nodos de red deberá estar regulado y controlado y no pueden existir puntos de red o accesos a equipos de comunicaciones desatendidos.
   d. Un estándar que regule el mantenimiento de los equipos por personal calificado, estableciendo un calendario de estas actividades de forma anual. Se deberá considerar para lo anterior a todo el equipamiento existente en el inventario de activos que tenga la organización. Así también, se deberá considerar el protocolo de reutilización o eliminación segura de los equipos, registrando en forma adecuada todos los medios que se eliminan. Junto a lo anterior, se deberá considerar el protocolo de equipo desatendido, definiendo los tiempos de inactividad adecuada a los riesgos de acceso físico no autorizados, protegiendo los bloqueos de pantalla con contraseña. Este procedimiento, además, deberá considerar la retirada de activos de propiedad de la Universidad, regulando las aprobaciones o autorizaciones documentadas para entrega o traslados.

TITULO VIII.
DE LA SEGURIDAD CON PROVEEDORES

ARTÍCULO 36º: De la relación con proveedores. La Universidad deberá regular las relaciones con los proveedores que involucran servicios de TI, ya sea en nube, logística, servicios públicos, recursos humanos, médicos, financieros, legales y otros servicios subcontratados de alto riesgo estableciendo algunos puntos mínimos:

1. Arreglos de gestión de relaciones, incluyendo el riesgo de información y los aspectos de seguridad, las métricas, el rendimiento, problemas y rutas de escalamiento.

2. Información y propiedad intelectual, junto a las obligaciones y limitaciones derivadas.
3. Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información.
4. Requisitos legales y normativos, como el cumplimiento certificado de la ISO 27001.
5. Identificación de controles físicos y lógicos.
6. Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalamiento, gestión de respuesta y aspectos de continuidad de servicios.
7. Habilitación de seguridad de los empleados y concienciación.
8. Derecho de Auditoría de seguridad por parte de la organización.

ARTÍCULO 37º: Estándares de la prestación de servicios con proveedores. La Universidad deberá implementar:

1. Un estándar en relación con los contratos o acuerdos formales con proveedores, que cubran como mínimo las siguientes condiciones:
   a. Gestión de las relaciones, incluyendo riesgos.
   b. Cláusulas de confidencialidad vinculantes.
   c. Descripción de la información que se maneja y el método para acceder a dicha información.
   d. Estructura de la clasificación de la información a usar.
   e. La inmediata notificación de incidentes de seguridad.
   f. Aspectos de continuidad de negocio.
   g. Subcontratación y restricciones en las relaciones con los proveedores.

2. La Universidad deberá implementar un estándar que permita los siguientes aspectos en relación con la cadena de suministros tecnológicos:
   a. Mecanismo de validación de los requisitos de seguridad de los productos adquiridos.
   b. Mecanismo para lograr una capacidad de recuperación cuando hay productos o servicios críticos que son suministrados por terceros.
   c. Mecanismo para rastrear el origen del producto o servicio.

3. La Universidad deberá implementar un estándar que regule la monitorización de servicios y los responsables de esta actividad. Junto a lo anterior, se deberán regular las reuniones las que deberán considerar los riesgos, incidentes, estándares, cumplimiento e informes de Auditoría. Cómo último punto se deberán considerar las cláusulas de penalización en el contrato relacionadas con el riesgo de información.

4. La Universidad deberá implementar un estándar que regule la gestión de cambios en la provisión de los servicios del proveedor, donde se especifique cómo se comunican los cambios en los servicios relacionados con la información, servicios adicionales o cambios en la forma que se prestan los servicios contratados. También cómo se comunican los cambios en los estándares y requerimientos legales de la organización y cómo se actualizan los acuerdos relacionados con los cambios.

TITULO IX.
DE LA DISPONIBILIDAD DE SERVICIOS

ARTÍCULO 38º: Identificación de requisitos de disponibilidad de servicios. La Universidad deberá implementar un estándar que permita identificar los requisitos de disponibilidad de servicios prestados por terceros, teniendo en cuenta la capacidad de recuperación, la capacidad de rendimiento, el balanceo de carga y otros factores que pudieran ser de importancia para estos aspectos. Además, se deberá considerar y tener identificados los servicios poco fiables, todo el inventario de activos, instalaciones, aplicaciones, enlaces, funciones y la organización en sí, determinando si los controles claves de seguridad de la información están implementados y son funcionales en los sitios de recuperación.

ARTÍCULO 39º: Cumplimiento de legislación y requisitos. La Universidad deberá implementar un estándar que regule la legislación aplicable y los requisitos contractuales contextualizados en el área TI, mediante un registro o base de datos que permita controlar el cumplimiento de las obligaciones, expectativas legales, reglamentarias y contractuales aplicables. Esta labor deberá tener una persona encargada, la cual deberá mantener, usar y

controlar este registro. Así también se deberán crear los controles adecuados que permitan hacer gestión sobre este proceso.

ARTÍCULO 40º: Derechos sobre propiedad intelectual. La Universidad deberá implementar un estándar que regule todas las materias relacionadas con la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento. Además, deberá considerar la inscripción y registro de los desarrollos propios de la Universidad, de sus académicos, académicas y estudiantes, cuando estos sean con aportes de la Institución o por medio de otras líneas de financiamiento estatal.

ARTÍCULO 41º: Protección de los registros de la organización. La Universidad deberá implementar un estándar en relación con estos aspectos, que considere como mínimo los siguientes ítems:

1. Clasificación, categorización, períodos de retención y medios de almacenamiento permitidos.
2. Almacenamiento o manipulación de las firmas digitales en forma segura.
3. Considerar la posibilidad de destrucción, falsificación y accesos no autorizados.
4. Verificación periódica de la integridad de los registros.
5. Utilización de medios de almacenamiento de larga duración para el almacenamiento a largo plazo.

ARTÍCULO 42º: Protección y privacidad de la información de carácter personal. La Universidad deberá implementar las siguientes acciones tendientes a cumplir con estos temas:

1. Se deberá habilitar un mecanismo de difusión para instruir al personal en el manejo de información de carácter personal.
2. Se deberá nombrar una persona responsable de privacidad en la organización, que cuente con las competencias necesarias en materias legales y de Seguridad de la Información, y que además tenga pleno control y conocimiento de la información de carácter personal que es recopilada, procesada y almacenada en la Universidad.
3. Generar los controles de gestión y auditoría sobre el acceso a información de carácter personal.
4. Identificar los niveles de acceso y roles (de las personas contratadas) que tienen acceso a estos activos.

TITULO X.
DEL CORREO ELECTRÓNICO

ARTÍCULO 43º: Definición del correo electrónico.
El correo electrónico es una herramienta para el intercambio de información y tiene como propósito ser utilizado como herramienta de apoyo a la gestión y de comunicación en general. No es un medio de difusión masiva e indiscriminada de información.

La Universidad proveerá gratuitamente de casilla de correo electrónico a todos los funcionarios y a estudiantes de pregrado y postgrado de la Universidad. Esta es personal e intransferible y de uso exclusivo para fines académicos y de sus funciones.

La Universidad podrá utilizar la dirección de correo para enviar a funcionarios y estudiantes información institucional y académica.

A través de la Dirección de Informática o unidad que la suceda se regulará las condiciones, frecuencia y oportunidad de uso de la correspondencia electrónica. Asimismo, cabe a ella aceptar o rechazar conexiones de correo electrónico desde cualquier dirección de correo electrónico o servidor externo.

En caso de producirse alguna anomalía o infracción en alguna cuenta de correo que afecte al buen funcionamiento del servicio de correo electrónico, se procederá a la cancelación preventiva del servicio.

ARTÍCULO 44º: Del uso del correo electrónico y mensajería instantánea.
El correo electrónico es un instrumento formal de la Universidad, que hace responsable al remitente de su contenido.

Los usuarios de correo electrónico, deberán abstenerse de abrir mensajes de dudosa procedencia y en caso de ser identificado deberá informar a la Dirección de Informática o unidad que la suceda. El usuario es el responsable de la administración de los mensajes, su contenido y los datos adjuntos. Deberá realizar la descarga de los mismos a fin de evitar la saturación de su casilla.

No se permite el envío de correo usando servidores SMTP externos.

Se podrá hacer uso del acceso de internet que se garantiza por la Universidad para recurrir a servicios de mensajería instantánea.

ARTÍCULO 45º: Del carácter privado de la correspondencia electrónica.
El contenido de los correos electrónicos es privado, salvo los casos en la legislación disponga su carácter público.

ARTÍCULO 46º: Prohibición de abuso en el correo electrónico. Se prohíbe toda conducta que constituya un abuso en el uso del correo electrónico el que se entiende como las diversas actividades que trascienden los objetivos habituales del servicio de correo y perjudican directa o indirectamente a los usuarios o que son contrarias a los fines para los cuales este fue creado. Estas actividades se pueden catalogar, a título ejemplar, en los siguientes grupos:

1. Abusivas por el contenido: Por lo mismo está prohibido enviar, almacenar o distribuir mensajes cuyo contenido atente contra las Leyes y Tratados Internacionales suscritos por Chile o promueva actuaciones contrarias a la ley.
2. Abusivas por el medio: Está prohibido la utilización de servidores de correo externos, estaciones de trabajo de usuario y en general cualquier recurso que no sea el dispuesto por la Universidad de La Frontera. También está prohibido habilitar servidores o levantar servicios de correo no acordados con la Dirección de Informática o unidad que la suceda, utilizando equipos o las redes de comunicaciones provistos por la Universidad.
3. Abusivas por no solicitadas: Queda prohibido brindar servicios que, de manera directa o indirecta, faciliten la proliferación de SPAM o "correo electrónico masivo no solicitado". También queda prohibido el enviar cadenas de cualquier tipo, hacer ofertas fraudulentas de compra o venta, así como también inducir cualquier tipo de fraude financiero, o enviar correo electrónico solicitando donaciones caritativas, peticiones de firmas o cualquier material relacionado.
4. Abusivas por su finalidad: Está prohibido el uso del correo electrónico para fines comerciales o de lucro personal. También se prohíbe el enviar mensajes de correo electrónico cuyo único propósito sea el de sobrecargar, paralizar o, de cualquier otro modo, perjudicar el normal uso de este servicio o los equipos informáticos de otros usuarios de Internet o acosar, amenazar o menoscabar a terceros.

TITULO XI.
DE LA FIRMA ELECTRÓNICA

ARTÍCULO 47º: Uso de la Firma Electrónica.
Las claves de Firma Electrónica Simple proporcionadas internamente por la Universidad de La Frontera deberán ser solicitadas por cada académica, académico, funcionario o funcionaria a través del servicio de Intranet corporativa. El Secretario General de la Universidad es la autoridad competente en esta materia, quien evaluará la aceptación de creación de cada certificado de firma electrónica individual.

Cada usuario será responsable de su contraseña confidencial de Firma Electrónica Simple, la que es personal e intransferible. Asimismo, los usuarios de Firma Electrónica Avanzada, serán responsables del cuidado de los dispositivos externos (token o equivalente) que les sean asignados.

Todos los documentos electrónicos firmados electrónicamente serán responsabilidad del usuario titular de la firma electrónica.

El usuario deberá notificar inmediatamente a la Dirección de Informática o unidad que la suceda toda sospecha de vulnerabilidad en la seguridad de sus claves o la pérdida de dispositivos externos, para tomar las medidas pertinentes.

TITULO XII.
DE LAS AUDITORÍAS

ARTÍCULO 48º: **Auditorías:** Con el fin de velar por el correcto uso de los activos de información de su propiedad, la Universidad de La Frontera se reserva el derecho de auditar en todo momento y sin previo aviso, el cumplimiento de los estándares vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los activos de información. Además, se considerará la incorporación de auditorías de seguridad de la información en el plan de auditoría de la Universidad.

TITULO XIII.
DE LAS SANCIONES

ARTÍCULO 49º: **Sanciones.** El incumplimiento de este reglamento por parte del usuario y de los deberes y prohibiciones que se establecen, se entiende una falta a los deberes funcionarios y funcionarias o a los deberes de los estudiantes, que será sancionada conforme a la normativa vigente, según el caso, sin perjuicio de ser inhabilitado o desconectado de su conexión a la red por la Dirección de Informática o unidad que la suceda, caso en el cual solo se restituirán sus servicios una vez que se haya comprobado la solución a la causa de dicha medida.

En aquellas estaciones de trabajo que sean detectadas con problemas de seguridad, daño a lo instalado o intento de dañar otras estaciones de trabajo, serán intervenidas por la Dirección de Informática o unidad que la suceda y bloqueadas hasta que la situación sea corregida.

Una vez que se identifique una vulnerabilidad en la estación de trabajo, ésta perderá su calidad de objeto confiable, por lo tanto, conlleva la pérdida de los accesos con los que cuenta la estación en cuestión.

ARTÍCULO 50º: **Infracciones a las condiciones de uso.** Se consideran, entre otras, faltas a los deberes académicos, funcionarios o estudiantiles, cuya gravedad será apreciada en cada caso, las siguientes:

1. Violación de las políticas, normativas y reglamentos de la Universidad de La Frontera y de las Leyes del Estado de Chile y de los tratados internacionales vigentes, para el uso de la red y de Seguridad de la Información o Ciberseguridad.
2. Instalar, utilizar y/ o almacenar software sin licencia válida.
3. Re-venta de servicios utilizando la infraestructura de redes de la Universidad de La Frontera, tales como web hosting, servicios de correo, mensajería electrónica o conexiones a Internet.
4. Acceder o intentar acceder sin autorización a los sistemas y recursos informáticos de la Universidad de La Frontera, mediante el uso de herramientas intrusivas (hacking), descifrado de contraseñas, descubrimiento de vulnerabilidades o el uso de cualquier otro medio no permitido o ilegítimo.
5. Apropiarse o intentar apropiarse indebidamente de las claves de acceso de otros usuarios a sistemas y equipos.
6. Acceder, enviar y/o almacenar material pornográfico.
7. Provocar maliciosamente denegación o degradación de cualquier servicio de la red, dispositivos de comunicaciones, servidores, tanto internos de la Universidad de La Frontera como de entidades externas.
8. Sobre-utilizar la plataforma tecnológica en desmedro de otros integrantes de la Universidad, por ejemplo, utilización excesiva del ancho de banda o apropiarse mediante el uso de software de descarga Peer-to-Peer, del acceso a Internet o cualquier tramo de la red de la Universidad de La Frontera.
9. Conectar equipos de red activos o pasivos (por ejemplo: hubs, switches, routers, modems, firewalls, puntos de acceso inalámbrico, etc.) que previsiblemente afecten el correcto funcionamiento de la misma o comprometan su seguridad.
10. Realizar modificaciones en la infraestructura de la red actual (cambios de tendido de cables, ampliaciones, etc.), sin la aprobación de la Dirección de Informática o unidad que la suceda y de la Dirección de Infraestructura y Servicios.

11. Asignar direcciones IP sin autorización previa de la Dirección de Informática o unidad que la suceda.
12. Cargar en forma intencional o no avisar a la Dirección de Informática o unidad que la suceda de la existencia de archivos que contengan virus, caballos de Troya ("troyanos"), gusanos ("worms"), archivos dañinos o cualquier otro programa o software similar que pueda perjudicar el funcionamiento de los equipos, de la red o de propiedad de terceros o provocar que el recurso computacional realice funciones para las cuales no fue adquirido.
13. Monitorear tráfico de cualquier red, sistema o computador, como también hacer escaneo de puertos, sin autorización.
14. Suplantar, en un proceso informático, a cualquier miembro de la Comunidad Universitaria o ajeno a ella.
15. Utilizar y ceder a cualquier título de información contenida en bases de datos pertenecientes a la Universidad, sin estar habilitado para ello.
16. Revelar a terceros contraseñas de acceso o compartirlas con otros usuarios. Proporcionar accesos externos a la red universitaria no autorizados.
17. Abusar o hacer uso incorrecto de los recursos informáticos que la Universidad ha puesto a su disposición.
18. Incurrir en descarga, almacenamiento y distribución de material protegido con derechos de autor.

TITULO XIV.
DISPOSICIONES FINALES

ARTÍCULO 51º: **Revisión del reglamento.** La revisión del reglamento será realizada anualmente por el Comité de Seguridad de la Información, y su reevaluación periódica será cada 3 años, o si ocurren cambios significativos.

ARTÍCULO 52º: **Situación no contemplada.** Cualquier situación no contemplada en el presente Reglamento deberá ser resuelta por la Rectora o Rector, previo informe del Comité de Seguridad de la Información si así lo requiere.

Control de Legalidad
Dirección de Legalidad
Universidad de La Frontera

ANÓTESE Y COMUNÍQUESE

Secretario General TEMUCO

Firmado digitalmente por PLINIO DONOSOR DURÁN GARCÍA

PLINIO DURAN GARCIA
SECRETARIO GENERAL

RECTOR TEMUCO

Firmado digitalmente por Eduardo Rodolfo Alfredo Hebel Weiss

EDUARDO HEBEL WEISS
R E C T O R

Firmado digitalmente por Gustavo Becerra
Nombre de reconocimiento (DN): cn=Gustavo Becerra, o=UFRO, ou=UFRO, email=gustavo.becerra@ufrontera.cl, c=CL
Fecha: 2023.03.09 10:26:32 -03'00'

EHW/PDG/CMI/fhb

Contralor Universitario TEMUCO

ROBERTO CONTRERAS EDDINGER
CONTRALOR UNIVERSITARIO

Firmado digitalmente por Roberto David Contreras Eddinger
Motivo: TOMA DE RAZON CONTRALORIA UNIVERSIDAD DE LA FRONTERA
Ubicación: TEMUCO. CHILE
Fecha: 2023.03.09 12:14:19 -03'00'
Versión de Adobe Acrobat Reader: 2022.003.20322

Distribución:

- Rectoría
- Vicerrectoría Académica
- Vic. Administración y Finanzas
- Secretaría General
- Contraloría Universitaria
- Decanos de Facultad
- Vicedecanos de Facultad
- Directores de Instituto
- Centros de Excelencias
- Secretarios de Facultad
- Directores de Campus
- Directores de Pregrado
- Directores Administrativos
- Directores de Departamento
- Directores de Carrera
- Jefes de Sección
- Jefes de División
- Jefes de Oficina