CONSEJO SUPERIOR

ACUERDO No. 13
(Agosto 01 de 2024)

Por el cual se expide la Política de Seguridad de la Información de la Fundación Universitaria Konrad Lorenz

El Consejo Superior de la FUNDACIÓN UNIVERSITARIA KONRAD LORENZ, en uso de sus facultades legales y estatutarias y

CONSIDERANDO

Que, de acuerdo con lo establecido en el artículo 28 de los Estatutos de la Fundación, son funciones del Consejo Superior, entre otras, lo estipulado en el numeral 2, *"Velar porque la marcha de la Institución esté acorde con las disposiciones legales vigentes y sus propios estatutos"*, y en el numeral 4, *"Formular y evaluar periódicamente las políticas y objetivos de la Fundación"*.

Que mediante el Acuerdo No. 23 del 5 de octubre de 2021 se integraron, actualizaron y reconocieron, como Política, los lineamientos y acciones asociados a la Gestión de la Información y de las Comunicaciones Internas en la Fundación Universitaria Konrad Lorenz y, según se dispone en el numeral 1) del artículo segundo, la Institución *"reconoce en la información y en las comunicaciones un recurso valioso para el desarrollo de la Misión, del Proyecto Educativo Institucional, de los objetivos institucionales y de los frentes estratégicos en el marco del Horizonte Institucional de Largo Plazo, del Plan de Desarrollo Institucional y de los planes de acción"*.

Que, de conformidad con lo dispuesto en el numeral 7) del artículo segundo de la Política de Gestión de la Información y de las Comunicaciones Internas, la Institución considera que *"la seguridad es un elemento fundamental en los requerimientos de los aplicativos y estándares relacionados con el manejo de los datos y de la información; adopta las medidas necesarias para la seguridad electrónica en la protección y custodia de la información y en la preservación de los datos bajo la política de habeas data"*, asimismo, el numeral 8) del artículo segundo de la Política,

determina que la Institución *"contará con un Plan de Seguridad de la Información, el cual será actualizado anualmente. Este plan incluirá los análisis sobre amenazas y vulnerabilidades y se implementará en forma de reglamentos, estándares y procedimientos de seguridad en conjunto con las inversiones apropiadas en servicios, personal, software y hardware"*.

Que mediante el Acuerdo No. 12 del 26 de junio de 2019 se expidió el Código de Ética y Buen Gobierno de la Fundación Universitaria Konrad Lorenz, que determina en el capítulo 9° el uso de los equipos de cómputo, sistemas electrónicos y de acceso, correos y comunicación electrónica; en el capítulo 10° la información confidencial y reservada; y en el capítulo 11° los aspectos éticos de la propiedad intelectual.

Que mediante el Acuerdo No. 04 de 2022, el Consejo Superior expidió el Plan de Desarrollo Institucional para el período 2022-20230 en el que se define, dentro del 5° eje estratégico "*Transformación Digital y de la Gestión*", el objetivo estratégico 6 de "*Convertir la tecnología y la ciencia de datos en factores claves para la toma de decisiones y para la transformación digital de la Institución, fortaleciendo la seguridad y el gobierno de la información, y la gestión institucional con el fin de aumentar la efectividad de sus procesos y servicios*".

Que para la Fundación Universitaria Konrad Lorenz resulta fundamental y necesario identificar y tratar los riesgos con el fin de proteger sus activos de información, entendidos estos como cualquier elemento que contenga, genere, adquiera, gestione y/o procese información y que tiene valor para uno o más procesos de la organización y por tanto debe protegerse[1].

En virtud de lo anterior, la Fundación Universitaria Konrad Lorenz expide la presente Política de Gestión de la Información con el propósito de proteger la integridad, confidencialidad y disponibilidad de la información en la Institución.

ACUERDA

ARTÍCULO PRIMERO. Objetivos de la Política. Son objetivos de la Política de Seguridad de la Información, los siguientes:

[1] https://www.iso.org/standard/27001

1. Definir, implementar, mantener y mejorar los controles, lineamientos y procedimientos que deben ser adoptados y apropiados con el fin de garantizar que los riesgos a los que están expuestos los activos de información y la información generada dentro de los procesos institucionales, sean tratados de acuerdo con metodologías y estándares reconocidos.
2. Asegurar que los controles, lineamientos y procedimientos relacionados con la Seguridad de la Información se adapten a la normativa interna y la legislación vigente, se encuentren alineados con el Proyecto Educativo Institucional, la Misión, Visión y principios institucionales, y respondan de manera dinámica a los cambios en las personas, los procesos y la tecnología.
3. Establecer una cultura de seguridad de la información que promueva en la comunidad universitaria de la Fundación Universitaria Konrad Lorenz el compromiso constante con la protección de la información.

ARTÍCULO SEGUNDO. Alcance. La presente Política es aplicable a estudiantes, docentes, personal administrativo, proveedores, contratistas y cualquier persona natural o jurídica que, en razón de sus funciones, actividades o vínculo con la Institución, tenga acceso permanente o temporal a activos de información.

ARTÍCULO TERCERO. Definiciones. Las definiciones concernientes a la presente Política se encuentran en el *Glosario del Sistema de Gestión de Seguridad de la Información (SGSI)*, que puede ser consultado en este enlace.

ARTÍCULO CUARTO. Declaración. La Política de Seguridad de la Información de la Fundación Universitaria Konrad Lorenz está formulada con base en los principios institucionales de integridad, buena fe, cumplimiento, respeto, transparencia y excelencia; se alinea con los objetivos estratégicos de la Institución y está orientada a la prevención de eventos que puedan afectar la integridad, confidencialidad y disponibilidad de la información.

ARTÍCULO QUINTO. Objetivos de Seguridad de la Información. Son objetivos de la seguridad de la información:

1. Implementar políticas, controles y procedimientos de seguridad de la información adecuados a los niveles de riesgo identificados para los activos de información de la Institución.
2. Gestionar constantemente los riesgos de seguridad de la información de manera que se mantengan dentro de los niveles de aceptación definidos por el Comité de Seguridad de la Información.
3. Establecer y mantener una cultura institucional de seguridad de la información que propenda por la apropiación, adopción, cumplimiento y mejora continua de las políticas, lineamientos, controles y procedimientos relativos a la seguridad de la información.
4. Gestionar efectivamente los incidentes de seguridad de la información en un ambiente de cooperación entre las dependencias de la Institución, buscando el apoyo de las autoridades en lo concerniente a la seguridad de la información.

ARTÍCULO SEXTO. Seguridad de la información relativa al talento humano. La Dirección del Departamento de Talento Humano de la Institución, en coordinación con el Oficial o Líder de Seguridad de la Información, establecerán estrategias y mecanismos para:

a) Asegurar que las personas vinculadas a la Fundación Universitaria Konrad Lorenz conozcan, apropien y cumplan con las responsabilidades de acuerdo con los roles asignados en el marco del Sistema de Gestión de Seguridad de la Información.
b) Incorporar, en todos los contratos laborales, cláusulas de confidencialidad y de no divulgación de la información, así como cláusulas de cumplimiento de las políticas, controles, lineamientos y procedimientos de seguridad de la información.
c) Establecer planes de formación y capacitación para las personas vinculadas a la Institución, destinados a fortalecer las competencias en seguridad de la información y a medir su grado de adopción y apropiación.

ARTÍCULO SÉPTIMO. Gestión de activos de información. La Institución adopta las siguientes acciones para la gestión de activos de información:

a) Establecer los mecanismos y procedimientos para la identificación, clasificación, valoración, responsabilidad, propiedad y custodia de los activos de información para todos los procesos institucionales.

b) Implementar los mecanismos para etiquetar activos de información facilitando que se identifique el nivel de criticidad en términos de integridad, confidencialidad y disponibilidad.

ARTÍCULO OCTAVO. Gestión de control de accesos. La Institución implementa las siguientes acciones para la gestión de control de accesos:

a) Establecer, documentar, revisar y mantener actualizadas las matrices de roles y perfiles para el acceso a las plataformas y los servicios tecnológicos que soportan los procesos institucionales.
b) Asegurar la implementación de métodos de identificación, autenticación y autorización para el acceso a plataformas y servicios tecnológicos entregados a estudiantes, docentes, personal administrativo y personas naturales o jurídicas que tengan algún vínculo con la Institución, para el desarrollo de sus funciones y/o actividades.
c) Las credenciales, medios y dispositivos de autenticación entregados a los usuarios para el acceso a las plataformas, los servicios tecnológicos y los activos de información son de carácter personal e intransferible y cada usuario es responsable de su uso y custodia.

ARTÍCULO NOVENO. Criptografía. Se deben establecer los mecanismos, procedimientos y herramientas tecnológicas que permitan la implementación de controles criptográficos con el fin de proteger la confidencialidad e integridad de la información. Los administradores de los activos de información, en coordinación con el Oficial o Líder de Seguridad de la Información, determinarán la información y circunstancias en las que tales controles deben ser implementados.

ARTÍCULO DÉCIMO. Gestión de la seguridad física y del entorno. Las instalaciones de la Fundación Universitaria Konrad Lorenz deben contar con controles de restricción de acceso físico con el fin de evitar accesos no autorizados que amenacen los activos de información. Asimismo, estos controles deben incluir mecanismos para evitar acciones intencionales o no intencionales que deriven en daño o pérdida de los activos de información, para lo cual la Institución debe:

a) Implementar procedimientos que faciliten el control en el ingreso, retiro y traslado de los activos de información desde y hacia las instalaciones de la Institución.
b) Las áreas de procesamiento de información y aquellas donde se almacenen activos de información en formato físico o digital deben contar con mecanismos de control de acceso y monitoreo que permitan evidenciar que únicamente el personal autorizado tenga acceso.

ARTÍCULO DÉCIMO PRIMERO. Gestión de seguridad de las operaciones. Con el fin de preservar la seguridad de la información dentro de las operaciones institucionales, se establecen las siguientes medidas:

a) Implementar controles de ciberseguridad orientados a asegurar las plataformas y los servicios tecnológicos en pro de evitar la materialización de riesgos derivados de ciberataques.
b) Velar por que las plataformas, herramientas y servicios tecnológicos entregados a la comunidad universitaria sean utilizados exclusivamente para las actividades propias de cada rol y función.
c) Los cambios en las plataformas, herramientas y servicios tecnológicos deben hacerse bajo procedimientos documentados, asegurando que los cambios sean evaluados, autorizados y planificados. La planeación de los cambios debe incluir planes de "rollback" o vuelta atrás en caso de ser necesario.
d) Generar políticas y procedimientos de respaldo y recuperación de información para minimizar el riesgo por daño, pérdida o destrucción.
e) Medir y evaluar la capacidad de las plataformas, herramientas y servicios tecnológicos, además de optimizar y proyectar el crecimiento en la demanda de estas para evitar indisponibilidad derivada de la pérdida de capacidad.
f) Los sistemas de información que soportan los procesos misionales, así como los sistemas de información considerados críticos para la operación de la Institución deben contar con ambientes separados de pruebas, desarrollo y producción. Asimismo, implementar controles para evitar la introducción de código malicioso, no probado o no autorizado en cualquiera de estos ambientes.
g) Implementar herramientas tecnológicas que estén en capacidad de anticipar la ocurrencia de ciberataques o la introducción de códigos maliciosos.
h) Realizar periódicamente pruebas de detección de vulnerabilidades y hacking ético con el objetivo de detectar y evaluar posibles brechas de seguridad. Los resultados

de estos ejercicios deben derivar en planes de acción para implementar acciones de mejora e incrementar la seguridad de las plataformas, herramientas y servicios tecnológicos.

i) Mantener un registro de los eventos y logs en las plataformas tecnológicas para correlacionar eventos y facilitar la detección y análisis de posibles incidentes de seguridad de la información.
j) Los sistemas operativos, software y aplicaciones deben ser probados antes de ser puestos en producción. Se deben adoptar procedimientos de pruebas para asegurar la compatibilidad con las plataformas, herramientas y servicios tecnológicos existentes para prevenir interrupciones o degradaciones en su funcionalidad.
k) La instalación de software en los equipos de cómputo, servidores y demás componentes de las plataformas tecnológicas debe estar restringida a los miembros del equipo de la Dirección de Desarrollo Tecnológico e Innovación y a los terceros o proveedores que tal instancia autorice.
l) Realizar periódicamente auditorias técnicas sobre las plataformas, herramientas y servicios tecnológicos con el propósito de detectar de manera proactiva y corregir inconsistencias en los privilegios de acceso, así como en la confiabilidad y capacidad.

ARTÍCULO DÉCIMO SEGUNDO. Gestión de seguridad en las comunicaciones. La Institución establece las siguientes acciones para la gestión de la seguridad en las comunicaciones internas y externas:

a) La gestión de redes internas y externas debe contar con procedimientos definidos, documentados y aprobados que permitan identificar las responsabilidades asociadas con su administración y operación.
b) Mantener el registro de las actividades ejecutadas sobre las redes tanto internas como externas de la Institución con el fin de detectar y prevenir acciones no autorizadas y establecer acciones de mejora.
c) Los servicios de red, tanto internos como externos provistos por la Institución o por un tercero, deben contar con acuerdos de niveles de servicio (ANS) que aseguren la disponibilidad y la calidad de estos. Se deben realizar auditorías periódicas a los servicios de red para identificar y evaluar posibles riesgos.
d) Establecer controles para asegurar que únicamente las personas autorizadas tengan acceso a los servicios de red con los privilegios asignados.

e) Contar con segmentación y separación de redes con el objetivo de proteger las plataformas tecnológicas de accesos no autorizados o ciberataques.
f) Asegurar que el intercambio de información confidencial cuente con controles que permitan alcanzar niveles de protección adecuados.

ARTÍCULO DÉCIMO TERCERO. Adquisición, desarrollo y mantenimiento de los sistemas de información. En el proceso de instalación y mantenimiento de sistemas de información, se abordan las siguientes acciones:

a) Establecer, implementar y mantener procedimientos, mecanismos y controles adecuados que garanticen la seguridad de las plataformas, herramientas y servicios tecnológicos a lo largo de su ciclo de vida.
b) Las operaciones transaccionales entre sistemas de información deben contar con controles que garanticen la protección de los datos.
c) Adoptar metodologías, estándares y reglas de seguridad aplicables a los procesos de desarrollo de software, así como durante su ciclo de vida y garantizar que los desarrollos de software subcontratados cuenten con tales lineamientos.

ARTÍCULO DÉCIMO CUARTO. Relación con proveedores. Se adoptan las siguientes acciones de seguridad de la información con contratistas, proveedores o terceros vinculados con la Institución:

a) Los contratos con proveedores de servicios los cuales tengan acceso a los activos de información, a la plataformas, herramientas y servicios tecnológicos de la Institución, deben incluir clausulas específicas en seguridad de la información.
b) Realizar evaluaciones periódicas que evidencien el cumplimiento de los proveedores en cuanto a las políticas de seguridad de la información aplicables.

ARTÍCULO DÉCIMO QUINTO. Gestión de incidentes de seguridad de la información. Los incidentes de seguridad de la información deben ser tratados y gestionados mediante un procedimiento único, centralizado, documentado y aprobado que facilite su reporte, clasificación, análisis, evaluación, respuesta y tratamiento.

a) Establecer los mecanismos, procedimientos y planes de fortalecimiento de competencias para que los miembros de la comunidad universitaria puedan

identificar y reportar incidentes, conductas y/o acciones de riesgo que comprometan la seguridad de la información.

b) Identificar las autoridades competentes y los mecanismos para el reporte de incidentes de seguridad de la información que impliquen vulneración de la normativa aplicable.

PARÁGRAFO. La Institución puede implementar el uso de nuevas tecnologías para la detección temprana de amenazas, prever riesgos potenciales, automatizar respuestas a incidentes, mejorar la toma de decisiones estratégicas y garantizar la protección de la información.

ARTÍCULO DÉCIMO SEXTO. Seguridad de la información en la gestión de continuidad de las operaciones. La Institución adopta las siguientes medidas para preservar la continuidad en la operación:

a) Establecer, documentar e implementar planes de recuperación de los servicios críticos que puedan verse comprometidos ante un evento que implique la interrupción de las operaciones de la Fundación Universitaria Konrad Lorenz.
b) Efectuar controles, herramientas, métodos y procedimientos necesarios para garantizar que los componentes de la infraestructura tecnológica sean monitoreados con el objetivo de detectar de manera preventiva eventos que puedan impactar la disponibilidad y la capacidad de los servicios tecnológicos.
c) Diseñar, socializar y actualizar las matrices de riesgos de la Fundación Universitaria Konrad Lorenz, con los respectivos controles de cambios que permitan salvaguardar la seguridad de la información.

ARTÍCULO DÉCIMO SÉPTIMO. Cumplimiento de aspectos legales y contractuales. La Institución articula, en coordinación con la Secretaría General, el establecimiento de los mecanismos y procedimientos para cumplir con la legislación aplicable, la normativa interna y los requisitos contractuales relativos a aspectos de seguridad de la información.

ARTÍCULO DÉCIMO OCTAVO. Revisiones al Sistema de Gestión de Seguridad de la Información - SGSI. El SGSI debe ser auditado periódicamente por el Comité de Seguridad de la Información mediante auditorías planificadas o, en los casos en que se presenten cambios importantes en la legislación, la normativa interna o los procesos asociados a la

seguridad de la información. El cumplimiento de las políticas, controles y procedimientos que se implementen a partir de la aprobación de la presente Política debe ser revisado como mínimo una vez al año para identificar e implementar acciones preventivas, correctivas y de mejora, a partir de la exposición de indicadores sobre la seguridad de la información en la Institución.

ARTÍCULO DÉCIMO NOVENO. Apropiación, adopción y divulgación del SGSI. A partir de la creación y puesta en marcha del Sistema de Gestión de Seguridad de la Información - SGSI, la Institución se orienta a:

a) Definir y establecer los mecanismos necesarios y suficientes que permitan a los integrantes de la comunidad universitaria de la Fundación Universitaria Konrad Lorenz apropiar y adoptar los lineamientos y controles de seguridad de la información con el propósito de minimizar la ocurrencia de eventos que pongan en riesgo la confidencialidad, integridad y disponibilidad de los activos de información de la Institución.
b) Establecer planes de formación orientados al fortalecimiento permanente de competencias en seguridad de la información para la comunidad universitaria de la Fundación Universitaria Konrad Lorenz.

ARTÍCULO VIGÉSIMO. Deberes y sanciones. Las personas que mantengan un vínculo permanente u ocasional, directo o indirecto con la Institución deben conocer y cumplir las disposiciones emanadas a partir de la aprobación de la presente Política. Los casos de incumplimiento de los controles en seguridad de la información serán evaluados por las instancias respectivas con el fin de establecer las acciones correspondientes.

ARTÍCULO VIGÉSIMO PRIMERO. Comité de Seguridad de la Información. El Comité de Seguridad de la Información está constituido por las siguientes personas:

a) El Rector, quien lo preside.
b) El Vicerrector Académico.
c) El Vicerrector Administrativo.
d) El Director de Desarrollo Tecnológico e Innovación.
e) El Director Administrativo y Financiero.
f) El Director del Departamento de Talento Humano.

g) El Oficial o Líder de Seguridad de la Información, quien ejerce la secretaría del Comité.

PARÁGRAFO. Podrán ser invitadas a las reuniones otras personas que, por su conocimiento o experiencia, se requiera su participación en el Comité.

ARTÍCULO VIGÉSIMO SEGUNDO. Funciones del Comité. El Comité de Seguridad de la Información es un órgano de control y gestión que tendrá a cargo las siguientes funciones:

a) Mantener el monitoreo y la evaluación permanente de los resultados del Sistema de Gestión de Seguridad - SGSI de la Fundación Universitaria Konrad Lorenz.
b) Mantener actualizada la matriz de riesgos de la Fundación Universitaria Konrad Lorenz a partir de la conceptualización que para tales efectos proponga el Oficial o Líder de Seguridad de la Información.
c) Liderar las acciones estratégicas orientadas al cumplimiento de los objetivos de seguridad de la información.
d) Garantizar que las directrices, lineamientos y políticas relacionadas con la seguridad de la información sean comunicadas a la comunidad universitaria y se establezcan los mecanismos pertinentes para su apropiación y adopción.
e) Asegurar la implementación eficaz del Sistema de Gestión de Seguridad de la Información - SGSI con los recursos económicos, técnicos y de formación pertinentes.
f) Designar un Oficial o Líder de Seguridad de la Información, como responsable de la definición, implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información en la Institución.
g) Efectuar la revisión anual del cumplimiento de los lineamientos, controles y procedimientos que se implementados a partir de la presente Política.

ARTÍCULO VIGÉSIMO TERCERO. El Comité de Seguridad de la Información se reunirá una vez cada trimestre de manera ordinaria y, extraordinariamente, cuando se convoque. El quórum para deliberar y adoptar decisiones válidas lo constituye la asistencia de al menos el 80% de sus integrantes; las decisiones se tomarán por mayoría simple de votos de los miembros presentes.

ARTÍCULO VIGÉSIMO CUARTO. Interpretación y Desarrollo. Corresponde al Rector, como máxima autoridad ejecutiva en el campo académico y administrativo, interpretar,

ampliar y desarrollar las disposiciones contenidas en el presente Acuerdo y decidir sobre los casos no contemplados en este, de conformidad con el espíritu y tradición que guía a la Fundación Universitaria Konrad Lorenz.

COMUNÍQUESE Y CÚMPLASE

Dado en Bogotá, D.C., al día 1° del mes de agosto de 2024.

LUIS FERNANDO FAJARDO FORERO
Vicepresidente Consejo Superior

LUISA MARÍA CASTELLANOS PINZÓN
Secretaria General