LOS LIBERTADORES
FUNDACIÓN UNIVERSITARIA

Política Institucional de
Seguridad de la Información

LOS LIBERTADORES
FUNDACIÓN UNIVERSITARIA

Política institucional de
Seguridad de la Información

DICIEMBRE 01 DE 2017

Consejo Superior

Juan Manuel Linares Venegas
Presidente del Claustro

Lucía del Pilar Bohórquez A.
Rectora

Javier Daza Piragauta
Representante de la comunidad profesoral

Antonio Jacanamijoy
Representante de la comunidad estudiantil

Andrés Fernando Reyes Torres
Miembro del Consejo Superior

María Paula Linares Venegas
Miembro del Consejo Superior

Martha Sandino de Oliveros
Miembro del Consejo Superior

Sonia Arciniegas Betancourt
Miembro del Consejo Superior

María Angélica Cortes Montejo
Secretaria General

Apoyo Técnico

Hector Cruz
Gerente de Tecnología

Consejo Académico

Lucia del Pilar Bohórquez Avendaño
Rectora

Orlando Salinas Gómez
Vicerrector Académico

Jorge Eduardo Corrales Amaya
Decano Facultad de Ciencias Administrativas

Olga Patricia Sánchez Rubio
Decana Facultad de Ciencias de la Comunicación

Martha Lorena Martínez Correal
Decana Facultad de Ciencias de la Educación

Álvaro Luis Mercado Suárez
Decano Facultad de Ciencias Económicas y Contables

John Jairo Morales Alzate
Decano Facultad de Derecho Ciencias Políticas y Relaciones Internacionales

Edwin Yair Oliveros Ariza
Decano Facultad de Psicología

Adriana Cecilia Páez Pino
Decana Facultad Ingeniería

Hernán Jurado Duque
Representante de la comunidad profesoral

María Angélica Cortes Montejo
Secretaria General

ACUERDO DEL CONSEJO SUPERIOR No. 37 DEL 01 DE DICIEMBRE DEL AÑO 2017 POR EL CUAL SE APRUEBA LA POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN DE LA FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES Y SE REGLAMENTA SU ORGANIZACIÓN

EL CONSEJO SUPERIOR DE LA FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES EN EJERCICIO DE SUS ATRIBUCIONES LEGALES Y ESTATUTARIAS:

CONSIDERANDO QUE

a. El derecho de las Instituciones de Educación Superior para darse y modificar sus propios reglamentos, adoptar el régimen de estudiantes y profesores, está consagrado en el Artículo 1.1.1.1., en su numeral 5 y el Artículo 2.2.2.2 del Decreto Único Reglamentario del Sector Educación 1075 de 2015, y ratifica la autonomía universitaria consagrada en el artículo 69 de la Constitución Política de Colombia.

b. La aplicación de la Política de Seguridad de la Información se rige de acuerdo con las siguientes normativas:

- Constitución política de Colombia 1991, Artículo 15
- Ley 527 de 1999
- Ley 1273 de 2009
- Ley estatutaria 1581 de 2012
- Ley 1712 de 2014
- Decreto 1377 de 2013
- Norma técnica NTC-ISO-IEC colombiana 27001:2013
- Acuerdo 40 de 2006 del Consejo Superior.
- Acuerdo 18 de 2016 del Consejo Superior.
- Proyecto Educativo Institucional (PEIL)
- Plan de Desarrollo Libertador 2016-2020 Calidad académica para el desarrollo sostenible.

c. El Consejo Superior de la fundación universitaria Los Libertadores aprobó en sesión del 24 de octubre de 2016 su Código de Buen Gobierno Libertador y en él se orienta el quehacer institucional a todos los miembros de la comunidad educativa libertadora en la apropiación de los valores fundacionales Libertad, Orden y Justicia y el fortalecimiento de una cultura organizacional basada en la transparencia, la ética, la integridad,

la planeación, la sostenibilidad, la estrategia y la eficiencia. En ese contexto, se establecen los lineamientos que debe seguir la Fundación Universitaria Los Libertadores para garantizar una adecuada administración de los activos de información de los procesos que forman parte del SGSI. Por lo anterior, el Consejo Superior

ACUERDA:

Artículo 1. Aprobar la Política de Seguridad de la Información de la Fundación Universitaria Los Libertadores, con sujeción a las disposiciones legales, reglamentarias y estatutarias.

CAPITULO I
DISPOSICIONES GENERALES

Artículo 2. Definiciones

Activo de información: Información representada en registros de tipo físico o digital que tienen valor para la Fundación.
Amenaza: Evento que puede ser la causa de un hecho que comprometa la confidencialidad, integridad o disponibilidad de algún activo de información de la Fundación.
Análisis de riesgo: Diagnóstico para identificar los riesgos de los mecanismos de protección de los activos de información con el fin de optimizar dichos mecanismos y facilitar su monitoreo.
Confidencialidad: Garantía que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
Continuidad: Conjunto de actividades que permitan garantizar la operación cotidiana de la Fundación Universitaria Los Libertadores
Control: Medida utilizada para garantizar la confidencialidad, integridad y disponibilidad de un activo de la información.
Custodio de la información: Cargo o grupo de trabajo encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
Disponibilidad: Garantizar que el personal autorizado podrá acceder a la información cuando lo requieran.
Efectividad: Capacidad de lograr el resultado esperado.
Eficiencia: Capacidad de conseguir un objetivo deseado con el menor gasto posible de recursos.
Evaluación del riesgo: Determina el valor de los activos de información, identifica las amenazas aplicables y las vulnerabilidades que existen (o pueden existir), identifica los controles existentes y sus efectos en

el riesgo identificado, determina los efectos potenciales y finalmente prioriza los riesgos derivados y los ordena contra el conjunto de criterios de valoración del riesgo en el contexto establecido.

Gestión de activos: Conjunto de actividades que consisten en la clasificación de los activos identificados, gestión de riesgo y seguimiento de los controles aplicados con el fin de garantizar la confidencialidad, integridad y confidencialidad de los activos de información que forman parte del SGSI.

Gestión de incidentes: Conjunto de actividades y recursos con los que se manejan los eventos que afectan la confidencialidad, integridad y disponibilidad de la información de La Fundación.

Gestión de vulnerabilidades: Conjunto de actividades que consiste en detectar y controlar el riesgo generado por las vulnerabilidades mediante el uso de controles.

Hardware: Elementos físicos de la infraestructura informática de La Fundación. Ejemplo: computador, servidor, switch, router, teclado, pantalla.

Incidente de seguridad de la información: Evento no deseado o inesperado con una probabilidad significativa de comprometer operaciones de negocio, divulgación de datos confidenciales o de uso interno de la Fundación o datos personales de los cuales la Fundación es responsable, tal que desencadene en repercusiones sobre aspectos financieros, operativos o en su reputación. Ejemplos de incidentes de seguridad de la información son: Pérdida de servicio en equipos, instalaciones o conexiones, incumplimiento de las políticas o directrices referentes a seguridad de la información, ataques de Phishing, infecciones de código malicioso (virus, malware, etc.), entre otros.

Impacto: Grado en que se ve afectado un activo de información e incluso la Institución por la materialización de un riesgo.

Información: Datos relacionados que tienen significado para la Fundación. Estos datos pueden presentarse en formato digital o en documentos físicos.

Integridad: Propiedad o atributo de la información que indica que la información no debe tener modificaciones por parte de personas o procesos que no cuenten con la debida autorización.

Medio removible: Componente extraíble de hardware utilizado para el almacenamiento de información. Por ejemplo, cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB.

Phishing: Técnica utilizada para obtener información confidencial (nombres de usuario, contraseñas, etc.) mediante el envío de comunicaciones electrónicas aparentemente confiables.

Propietario de un activo de información: Parte designada por la entidad (un cargo, proceso o grupo de trabajo) que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se

clasifican adecuadamente. También se encargan de definir y revisar periódicamente las restricciones y clasificaciones del acceso. El propietario decide sobre la finalidad, contenido y uso del activo de información y es responsable de la seguridad del activo.

Riesgo: Es una combinación de los efectos que pueden seguir a la ocurrencia de un evento no deseado y de la probabilidad de la ocurrencia del evento. La evaluación del riesgo describe cualitativamente el riesgo y permite a los gerentes priorizar los riesgos de acuerdo a su percepción de la gravedad u otros criterios establecidos.

Registros de auditoría (logs): Registro histórico de las actividades generadas en un sistema o una aplicación. Se utilizan para rastrear, detectar, auditar y analizar comportamientos no esperados.

RPO (Recovery Point Objective – Punto de recuperación objetivo): Punto de referencia anterior al que debe ser restaurada la información usada por un proceso de negocio después de una interrupción, para lograr su reanudación. Se debe definir su pérdida máxima de información (DRII).

RTO (Recovery Time Objective – Tiempo de recuperación objetivo): Periodo de tiempo inmediatamente posterior a la ocurrencia de un evento de interrupción dentro del cual deben reanudarse o recuperarse: la entrega de productos o servicios, las actividades críticas, y los recursos. El RTO debe ser menor al tiempo en el que los impactos financieros y operacionales identificados en el BIA sean inaceptables (DRII).

Seguridad de la información: Es la preservación de la confidencialidad, integridad y disponibilidad de los activos de información a través de la gestión de riesgos.

Seguridad informática: Implementación y mantenimiento de herramientas y controles a nivel de hardware, software y decisiones organizacionales para garantizar la seguridad de la infraestructura tecnológica.

SGSI: Sistema de Gestión de Seguridad de la Información

Sistema de información: Componente de software desarrollado por la Fundación o por un fabricante externo que requiere la interacción de uno o más activos de información para efectuar sus tareas.

Software malicioso: Programa que tiene como objetivo infiltrarse o dañar la infraestructura tecnológica. Los objetivos más comunes son los sistemas operativos, redes de datos o los sistemas de información.

Tercero: Persona jurídica o natural que tienen relaciones contractuales o de otro tipo con la Fundación y que no son empleados, profesores, estudiantes o egresados. Ejemplo: Proveedores, contratistas y consultores.

Vulnerabilidad: Debilidad frente a una amenaza. Generalmente responde a la ausencia o deficiencia de controles que permiten que una amenaza materialice un riesgo.

CAPITULO II
MARCO INSTITUCIONAL DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Artículo 3. Alcance. La Política de Seguridad de la Información aplica para todos los activos de información de la Fundación Universitaria Los Libertadores.

Desde el punto de vista de la responsabilidad esta Política aplica para directivos, administrativos, practicantes y terceros (contratistas y/o proveedores de La Fundación) y debe ser de conocimiento de los estudiantes y profesores.

La Fundación está encargada de facilitar los recursos humanos, técnicos, financieros y demás necesarios para llevar a cabo la implantación y mantenimiento de estas políticas.

Artículo 4. Criterios Orientadores. La Política de Seguridad de la Información se orienta por los criterios de planificación, gestión del riesgo, responsabilidad, corresponsabilidad, prevención y cumplimiento. Estos criterios permiten que la política se articule con las actividades cotidianas de la Fundación.

Artículo 5. Responsabilidad Todo Colaborador administrativo, académico y tercero que tenga acceso a los activos de información de la Fundación debe conocer, aceptar de manera expresa y cumplir con las disposiciones de esta Política. Además, debe utilizar la información sólo para los fines permitidos por la Ley, la Fundación o los titulares de los datos personales, según el caso, y garantizar la reserva y confidencialidad de la misma cuando no sea de carácter público y, por lo tanto, abstenerse de suministrarla a personas no autorizadas.

Es responsabilidad del Grupo de Seguridad de la Información supervisar el cumplimiento de la Política, evaluar periódicamente la aplicabilidad de los controles y fomentar una cultura de seguridad de la información para todas las partes involucradas.

CAPITULO III
OBJETIVOS DE LA POLÍTICA

Artículo 6. Objetivo General. Orientar y dar lineamientos de seguridad de la información sobre los activos de la Fundación, con el fin de garantizar que los riesgos son identificados, valorados y administrados de una forma estructurada, repetible, eficiente y adaptada a los cambios

que se produzcan en el entorno, en las tecnologías de información.

Artículo 7. Objetivos Específicos. La Fundación Universitaria Los Libertadores establece los siguientes objetivos de seguridad de la información:

- Definir, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información.
- Velar por la confidencialidad, integridad y disponibilidad de la información de manera que esté protegida de acuerdo con las necesidades organizacionales, incluyendo los datos personales que por su naturaleza debe manejar la Fundación.
- Garantizar la continuidad de las operaciones críticas de la Fundación frente a incidentes que puedan resultar en interrupción o afectación.
- Mantener la confianza de estudiantes, personal administrativo, profesores, contratistas, proveedores y entes reguladores en cuanto a seguridad de la información.
- Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas en cuanto a seguridad de la información.
- Fortalecer la cultura de seguridad de la información en toda la comunidad académica, como medida para proteger la información como un activo crítico.

Artículo 8. Revisión de la Política de Seguridad. El Grupo de Seguridad de la Información se encargará de revisar el presente documento como mínimo una vez al año, cada vez que se presenten cambios significativos en la estrategia de la Fundación, el contexto organizacional o el entorno tecnológico.

Artículo 9. Divulgación de la Política de Seguridad**.** Es tarea del Grupo de Seguridad de la Información coordinar a través del Oficial de Seguridad la divulgación de la Política de Seguridad a la totalidad de los colaboradores, estudiantes, profesores y terceros que tengan acceso a los activos de información de la Fundación, cada vez que se realice una actualización.

Artículo 10. Organización de la seguridad de la información. La Fundación garantiza el apoyo al SGSI por medio de la creación del Grupo de Seguridad de la Información, el cual es liderado por la Dirección de Auditoría y Riesgo. El detalle de la composición y las funciones del Grupo se encuentra en el Manual del Sistema de Gestión de Seguridad de la Información.

CAPITULO IV
ESTRATEGIAS

Artículo 11. Gestión de activos de información. Los activos de información de la Fundación deben ser identificados y clasificados de acuerdo con su grado de criticidad. Así mismo, deben tener un propietario designado, quien tiene la responsabilidad de garantizar que se clasifican adecuadamente, revisar las restricciones de acceso y la seguridad del activo.

Todos los miembros de la comunidad de la Fundación tienen la responsabilidad de proteger y usar adecuadamente los activos de información.

Los activos de información deben categorizarse según la siguiente clasificación:

- Confidencial: Información que puede ser conocida y utilizada por personas autorizadas de la Fundación, pero no puede ser divulgada sin autorización del propietario.
- De uso interno: Información que puede ser utilizada por empleados de la Institución y entidades con la debida autorización del propietario.
- Pública: Información conocida y utilizada por cualquier persona.

El etiquetado, manejo, procesamiento, almacenamiento y comunicación de todos los activos de información se dará de acuerdo con la clasificación asignada.

Artículo 12. Seguridad de la información y recursos humanos.
La Fundación incorpora elementos de seguridad de la información en su relación con los colaboradores administrativos y profesores antes, durante y después de la relación contractual, de acuerdo con el nivel de riesgo identificado.

Todos los colaboradores y estudiantes deben conocer y dar cumplimiento a la política de seguridad.

Así mismo, con el fin de propender por una cultura sólida en seguridad de la información, la Fundación define y ejecuta periódicamente programas de sensibilización y capacitación en seguridad de la información de acuerdo con las necesidades identificadas.

Artículo 13. Control de acceso. El acceso a la información, los sistemas y redes de La Fundación, incluyendo recursos como carpetas compartidas, se otorgará con base en el principio de "necesidad de saber", es decir, con una justificación de la Institución. Se deben seguir los procedimientos establecidos para la gestión de usuarios y contraseñas, velando siempre por mantener los accesos mínimos requeridos.

Cada miembro de la comunidad académica y demás personas a quienes se asignen permisos para el acceso a la información debe mantener confidenciales e intransferibles sus credenciales de acceso.

Los escritorios o puestos de trabajo de los colaboradores y contratistas deben mantenerse limpios y sin documentos fuera del horario de trabajo o en ausencia prolongada del sitio.

Artículo 14. Cifrado. La elaboración y actualización de la política relacionada con el uso de controles criptográficos debe ser consecuente con una evaluación de riesgos previa, la cual ayudará a determinar el nivel de protección que debe recibir la información.

Artículo 15. Seguridad física y del entorno.

Áreas Seguras: Es responsabilidad de los líderes de los procesos identificar las áreas usadas para almacenar y procesar información confidencial y de uso interno. Como se encuentra estipulado en la Política de Seguridad Física.

Los equipos de procesamiento de información, así como sus elementos de soporte, deben contar con medidas de protección de acuerdo con la sensibilidad del activo.

Artículo 16. Seguridad en las operaciones

- Documentación de los sistemas: Debe existir documentación para los procedimientos operativos y estar disponible para todos los individuos con una necesidad legítima de conocerlos. La Gerencia de Tecnología es responsable del mantenimiento de esta documentación.

- Gestión de cambios: Todo cambio que tenga o pueda tener algún tipo de influencia sobre los sistemas de información o la infraestructura tecnológica que lo soporta, debe ser sometido a análisis y aprobación por un proceso formal de control de cambio.

• Gestión de la capacidad: Para cada sistema de información de la Fundación, la Gerencia de Tecnología deberá determinar regularmente el nivel de utilización de sus recursos, así como la respectiva demanda. Esta información permitirá establecer proyecciones sobre la capacidad de los recursos del sistema.

• Separación de los ambientes de desarrollo, pruebas y producción: Todo sistema en producción debe tener por lo menos un ambiente de desarrollo que permita probar cualquier cambio y reducir el riesgo de acceso no autorizado. Deben existir mecanismos que garanticen el control de acceso a los ambientes de desarrollo y producción.

• Protección ante software malicioso: Se debe contar con mecanismos de detección de código malicioso en la infraestructura tecnológica de la Fundación.

El Oficial de Seguridad de la Información debe realizar campañas de divulgación con el objetivo de informar a los usuarios acerca de medios de prevención y protección ante software malicioso.

Copias de seguridad: Toda información de la Fundación debe ser respaldada por copias de seguridad tomadas de acuerdo con los requerimientos aplicables, tanto legales como organizacionales. Estos tiempos deben estar alineados con el RPO y RTO de cada sistema de información, de acuerdo con el análisis de impacto. Así mismo, los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.

• Seguimiento: La Fundación ha establecido mecanismos para detectar actividades no autorizadas en los sistemas de información, como la activación de los registros de auditoría (logs).

Los repositorios o almacenamientos donde se guarden los registros deberán estar protegidos contra accesos no autorizados y/o alteraciones.
Las actividades de usuarios operadores y administradores en los sistemas de procesamiento de información o sus componentes, están condicionadas a monitoreo.
Debe acordarse una fuente segura para la sincronización de todos los relojes de sistemas que controlen accesos o generen registros de auditoría.

• Control de software operacional: Todo software que se ejecute en los equipos de cómputo de la Fundación debe originarse de fuentes confiables, para evitar alteraciones no autorizadas. La Gerencia de Tecnología es responsable de verificar las fuentes del software antes de proceder con la instalación.

• Gestión de vulnerabilidades técnicas: Se deberá mantener una constante revisión de las vulnerabilidades técnicas que son detectadas por la comunidad de seguridad de la información que tengan relación con el software utilizado por la Fundación.

• Dispositivos móviles: Los dispositivos móviles son asignados a los colaboradores de La Fundación con una finalidad específica (bien sea académica, administrativa o de investigación), por lo cual sólo deben ser utilizados por los usuarios autorizados según su rol y para tal fin.

Además, los dispositivos móviles corporativos deben contar con software legalmente licenciado y mecanismos de protección adecuados para mitigar los riesgos identificados.

• Uso de correo electrónico, y mensajería Web: El uso del correo electrónico, servicio de mensajería Web y demás recursos que comprende (calendario, gestión de tareas, entre otros), es proporcionado para fines académicos para estudiantes y profesores, y para fines laborales para el caso de colaboradores y terceros. Todo colaborador, estudiante, profesor, contratista, etc., entiende y acepta que la cuenta que le asigna La Fundación es personal e intransferible y se compromete a salvaguardar la contraseña asignada, a cambiarla con frecuencia o cada vez que sea solicitado y a no compartirla con otros usuarios.

La Fundación se reserva el derecho de proveer este servicio directamente o mediante un proveedor, de establecer la ubicación física de la información y de hacer los cambios que considere pertinentes.

• Uso de Internet: La Fundación Universitaria los Libertadores provee acceso a Internet para los diferentes miembros de la comunidad académica con el objetivo de facilitar el logro de la misión institucional. En consecuencia, todos los usuarios deben acogerse a los lineamientos de esta política.

La Fundación se reserva el derecho de restringir el acceso a sitios que puedan afectar la productividad de la institución, la seguridad de su información o su personal.

Los usuarios deberán abstenerse de visitar sitios restringidos por la Fundación de manera directa o indirecta.

Así mismo, toda actividad relacionada con navegación en Internet puede ser registrada por la Fundación, quien podrá revelar cualquier acceso cuando una autoridad judicial así lo requiera.

- Uso de medios removibles (Memorias USB, discos externos, CDs, DVDs, tarjetas SD/mini SD/micro SD): El uso de medio removibles debe seguir el procedimiento definido para tal fin por la Gerencia de Tecnología.

- Manejo de incidentes de seguridad: Todo estudiante, colaborador y contratista debe reportar cualquier acto sospechoso o expuesto que pueda afectar la confidencialidad, integridad o disponibilidad de algún activo de información de La Fundación.

Artículo 17. Seguridad en las comunicaciones. Toda conexión hacia las redes de la institución, que provenga o pase a través de redes inseguras o desconocidas deberá contar con mecanismos de protección (ej. autenticación, cifrado y manejo de la integridad), de acuerdo con los riesgos identificados.

Todas las redes de la Fundación deben contar con mecanismos de segregación acordes a la sensibilidad de la información

Deben establecerse medidas que restrinjan el acceso a puertos remotos de diagnóstico o configuración, sin una autorización apropiada.

Artículo 18. Adquisición, desarrollo y mantenimiento de sistemas de información. El software utilizado puede ser adquirido a través de terceras partes bajo licencia o desarrollados por personal propio o por un tercero.

Todo sistema de información nuevo o cualquier modificación sobre uno existente debe incluir la identificación de requerimientos de seguridad en conjunto con los requerimientos funcionales.

Todo componente nuevo o que forme parte de un cambio en un sistema de información debe pasar previamente por un proceso de pruebas

que certifique su correcta operación antes de ser puesto en marcha.

Los datos de prueba deben ser protegidos de acuerdo con su sensibilidad, para evitar accesos no autorizados y fugas de información.

Artículo 19. Continuidad de las operaciones. Se debe definir e implementar un Plan de Continuidad de Negocio (BCP) donde se identifiquen las estrategias y planes de respuesta para afrontar eventos repentinos de interrupción sobre las actividades rutinarias de sus procesos de negocio, con base en el análisis de impacto al negocio (BIA). Este plan debe tener en cuenta los requerimientos de seguridad de la información cuando sucedan este tipo de situaciones y se deben documentar, implementar y mantener los controles para cubrir estos requerimientos.

Artículo 20. Relación con terceros. La Fundación debe identificar los riesgos de seguridad de la información relacionados con sus terceros, determinar las medidas apropiadas a adoptar y hacer el respectivo seguimiento de su adecuada implementación.

En caso de otorgársele acceso a información confidencial, de uso interno o a un activo de información tecnológico a un usuario externo, el mismo debe aceptar por escrito que conoce, entiende y acepta esta política de seguridad.

Artículo 21. Cumplimiento. Deben identificarse y documentarse las legislaciones, normativas y requerimientos contractuales asociados con la seguridad de la información.

Se deben definir e implementar procedimientos que garanticen el cumplimiento de los derechos de autor sobre el software que esté protegido por las regulaciones aplicables. En ellos debe mencionarse que únicamente se podrán utilizar aplicaciones con licencia de manera que no se infrinjan las leyes de Propiedad Intelectual.

Para proteger los registros de la Fundación, todos los colaboradores de la Fundación deben firmar un Compromiso de Confidencialidad.

El Grupo de Seguridad de la Información establecerá la gravedad de las infracciones a esta Política. El proceso investigativo y posible sanción seguirán lo establecido en el Reglamento Estudiantil, el Estatuto Profesoral o el Reglamento Interno de Trabajo, según corresponda. En caso de ser necesario, se contactará a las autoridades competentes.

CAPITULO V
ORGANIZACIÓN INSTITUCIONAL PARA LA EJECUCIÓN DE LA POLÍTICA

Artículo 22. Implementación de la política. Es responsabilidad de todos los miembros de la Institución, en el marco de sus competencias, velar por el cumplimiento de los principios, objetivos y estrategias definidos en esta política y la aplicación de los procedimientos definidos para tal fin.

Artículo 23. Seguimiento, evaluación y recomendaciones de actualización. Las recomendaciones de actualización de la Política de seguridad de la información al Consejo Superior es responsabilidad de la Rectoría y su seguimiento y evaluación deberá estar en el marco del Sistema Integrado de Gestión Institucional mediante indicadores que permitan la orientación y toma de decisiones informada.

Artículo 24. Coordinación para la ejecución de la política. La Gerencia de Tecnología es la dependencia responsable de coordinar la promoción, implementación, seguimiento y autoevaluación de la política de seguridad de la información con el concurso de todas las áreas misionales y de apoyo.

CAPITULO VI
DISPOSICIONES FINALES

Artículo 25. Vigencia. El presente Acuerdo rige a partir del primero de diciembre del año 2017 y deroga la Resolución 102 de 2008, por la cual se establece la Política de Seguridad Informática de la Institución, así como todas las demás normas que le sean contrarias.

Artículo 26. Interpretación. El Consejo Superior será el intérprete del presente Acuerdo y resolverá las ambigüedades y conflictos que se puedan presentar para su aplicación.

COMUNÍQUESE Y CÚMPLASE

Dado en Bogotá, D.C. al primer (01) día del
mes de diciembre de 2017

JUAN MANUEL LINARES VENEGAS
Presidente (e)

MARÍA ANGÉLICA CORTÉS MONTEJO
Secretaria General

Revisó: Lucía del Pilar Bohórquez Avendaño, Rectora
Héctor Cruz, Gerente de Tecnología

LOS LIBERTADORES

FUNDACIÓN UNIVERSITARIA

Bogotá
infopresencial@libertadores.edu.co
infovirtual@libertadores.edu.co
PBX: (+57) (1) 254 4750 ext. 4182-4183
(+57) (1) 329 9333 Opción 1
Carrera 16 No. 63A - 68

Cartagena
infocartagena@libertadores.edu.co
PBX: (+57) (5) 656 8534
(+57) (5) 656 0892
Móvil: (+57) 315 836 8864
Pie de la Popa - Calle 31 No. 19-51


UniLibertadores


UniLibertadores

Canal Libertador

www.ulibertadores.edu.co