POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

1. INTRODUCCIÓN.....2
2. OBJETIVO POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN UNICAFAM.....2
3. TÉRMINOS Y DEFINICIONES 2
4. RESPONSABILIDADES 4
5. GENERALIDADES 6
5.1. Política De Seguridad De La Información 6
5.2. Objetivos de Seguridad de la información 7
5.3. Gestión de riesgos de seguridad de la información 7
5.4. Seguridad relacionada con el recurso humano 7
5.5. Uso aceptable de los activos 8
5.6. Control de acceso a la información y los sistemas 9
5.7. Seguridad física y del entorno 9
5.8. Recursos e infraestructura física para el procesamiento de información 10
5.9. Seguridad de las operaciones y las comunicaciones 10
5.10. Adquisición, desarrollo y mantenimiento de sistemas de información 10
5.11. Gestión de incidentes de seguridad de la información 10
5.12. Incidentes de seguridad que involucren datos personales 11
5.13. Continuidad de negocio 11
5.14. Mejora Continua 12
5.15. Violaciones a las Políticas de Seguridad de la Información 12
6. REVISION Y APROBACION DE LA POLÍTICA.....13

1. INTRODUCCIÓN

La Universidad reconoce la importancia de proteger la información y los datos sensibles de sus estudiantes, docentes, personal administrativo y demás partes interesadas. Este documento establece las directrices y procedimientos necesarios para asegurar la confidencialidad, integridad y disponibilidad de la información que manejamos en nuestra institución.

2. OBJETIVO POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN UNICAFAM

A través de la implementación de medidas preventivas y correctivas, buscamos mitigar los riesgos asociados a posibles amenazas, cumplir con las normativas legales vigentes, fomentar una cultura de seguridad entre todos los miembros de nuestra comunidad universitaria y la mejora continua en las prácticas de seguridad con el fin de garantizar el desarrollo óptimo de las actividades académicas, administrativas y de investigación. Esta política promueve la responsabilidad compartida en el manejo de la información, asegurando que todos los activos de información en nuestra institución estén protegidos contra accesos no autorizados, alteraciones o destrucción.

3. TÉRMINOS Y DEFINICIONES

Amenaza: Cualquier circunstancia, evento, acción o condición que pueda causar daño o afectar negativamente la confidencialidad, integridad o disponibilidad de los activos de información de una organización.

Ciberseguridad: Es la protección de la infraestructura tecnológica, realizando tratamiento de las amenazas que ponen en riesgo la información que se procesa, se almacena o se transporta por medios digitales y sistemas que se encuentran interconectados.

Cifrado: Proceso de codificación de información sensible para evitar que esta llegue a personas no autorizadas.

Confidencialidad: Protección de la información para garantizar que solo las personas autorizadas puedan acceder a ella. Su objetivo es prevenir que los datos sensibles o críticos sean divulgados, accedidos o visualizados por individuos no autorizados.

Control: Es una medida, práctica, política o tecnología implementada para reducir, mitigar o eliminar riesgos asociados a amenazas que puedan afectar la confidencialidad, integridad o disponibilidad de la información. Los controles ayudan a garantizar que los activos de información estén protegidos frente a accesos no autorizados, alteraciones o destrucción

Disponibilidad: Principio referente a garantizar que los sistemas de información y los datos estén listos para su uso cuando se necesiten. Capacidad de permanecer accesible en el sitio, en el momento y en la forma en que los usuarios que estén autorizados lo requieran.

Evento: Cualquier ocurrencia o cambio en el estado de un sistema, red o servicio que tiene relevancia para la seguridad. Un evento no siempre indica una amenaza o un incidente, pero puede ser un indicador o precursor de un problema de seguridad

Incidente: Cualquier evento o serie de eventos que comprometen o amenazan la confidencialidad, integridad o disponibilidad de la información, los sistemas o los activos de una organización. Un incidente generalmente implica la materialización de un riesgo que afecta negativamente la seguridad de la información, y requiere una respuesta inmediata para mitigar el daño y restaurar la normalidad.

Incidente de seguridad en datos personales: Cualquier evento que compromete la confidencialidad, integridad o disponibilidad de los datos personales almacenados o procesados por una organización. Este tipo de incidente puede resultar en la divulgación no autorizada, modificación, pérdida, o destrucción de datos personales, lo que puede generar consecuencias legales y reputacionales para la organización, así como daños a los individuos afectados.

Integridad: Propiedad que garantiza que los datos y la información no sean alterados o modificados de manera no autorizada, ya sea durante su almacenamiento, procesamiento o transmisión. Asegura que la información se mantenga exacta, completa y confiable, y que cualquier cambio en ella sea realizado solo por personas autorizadas y de manera controlada.

ISO 27001: Es una norma internacional publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). El objetivo de la norma es garantizar que las organizaciones gestionen de manera eficaz los riesgos de seguridad de la información, protegiendo la confidencialidad, integridad y disponibilidad de los datos.

Manual de Seguridad de la Información: Documento formal que describe las políticas, procedimientos, directrices y controles que una organización ha implementado para proteger la confidencialidad, integridad y disponibilidad de su información. Este manual sirve como una guía integral para la gestión de la seguridad de la información dentro de la organización y asegura que los empleados y partes interesadas sigan prácticas seguras en el manejo de los datos.

Riesgo: Posibilidad de que ocurra un evento o condición que pueda causar un daño a la confidencialidad, integridad o disponibilidad de la información o los sistemas. En otras palabras, es una combinación de la probabilidad de que ocurra una amenaza y el impacto potencial que tendría si esa amenaza se materializara.

Seguridad de la Información: Protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar la materialización de los riesgos. Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de la Fundación y de los servicios que presta.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Vulnerabilidad: Se define como una debilidad o fallo en un sistema, proceso, o control que puede ser explotado por una amenaza para comprometer la confidencialidad, integridad o disponibilidad de la información. Las vulnerabilidades pueden existir en software, hardware, procedimientos operativos, o incluso en el comportamiento humano, y representan un punto débil que puede ser atacado o explotado por actores maliciosos o errores no intencionados.

4. RESPONSABILIDADES

4.1 Consejo Superior Universitario:

- ✓ Deberá aprobar la Política General de Seguridad de la Información.
- ✓ Aprobará las modificaciones si las hubiese, en la Política General de la Seguridad de la información.
- ✓ Solicitará en períodos establecidos informes sobre el estado del Sistema de Gestión de Seguridad de la Información, del manejo de incidentes y de su mejora continua.

4.2 Comité de Seguridad de la Información (CSI)

La Fundación Universitaria Cafam, creará e implementará un Comité de Seguridad de la Información (CSI) que permitirá el logro de los objetivos y la minimización de los riesgos del componente de TI. El Comité estará encargado de monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de la información. Este comité estará conformado por el Rector, el Gerente Administrativo y Financiero, El Vicerrector, el jefe de Tecnologías, el Oficial de Seguridad de la Información de CAFAM como invitado, un representante del área jurídica, uno del área académica y otro del área administrativa. Las responsabilidades del comité son:

- ✓ Establecerá directrices para la gestión de la seguridad de la información.
- ✓ Discutirá y aprobará cualquier decisión relacionada con seguridad de información.
- ✓ Supervisará el cumplimiento de la política.
- ✓ Promoverá una cultura de seguridad de la información
- ✓ Revisará y presentará al CSU las propuestas de actualización de la política.
- ✓ Evaluará los incidentes de seguridad, coordinará su respuesta y establecerá planes de contingencia.
- ✓ Identificará amenazas y vulnerabilidades que puedan afectar la información de la organización, así como proponer estrategias de mitigación de riesgos.
- ✓ Identificará leyes y regulaciones cuando se adquieran controles criptográficos, licencias, herramientas de auditoría, grabaciones de conversaciones y otros que sean regulados.
- ✓ Supervisará que la estrategia de seguridad de información se cumpla acorde a las definiciones y los objetivos de la Fundación.
- ✓ Asegurará los recursos necesarios para implementación y mantenimiento de la estrategia de seguridad de información
- ✓ Desarrollará y gestionará la estrategia de seguridad de la información de la Fundación.
- ✓ Identificará y gestionará los riesgos de seguridad de la información.

- ✓ Desarrollará, implementará y supervisar las políticas de ciberseguridad alineadas con la misión y visión de la Fundación.
- ✓ Fomentará la concientización de todos los empleados en ciberseguridad.
- ✓ Se emitirán informes semestrales sobre la gestión del Comité de Seguridad de la Información (CSI), y se programarán reuniones trimestrales para revisar avances, decisiones estratégicas y acciones pendientes.

Tanto empleados, estudiantes, proveedores y todas las áreas de la Fundación son responsables de mantener la seguridad de información, especialmente:

- **ÁREA DE TECNOLOGÍAS.** Es responsable de la seguridad de tecnología y la innovación en pro de la seguridad informática y de información. Es el responsable de desarrollar la estrategia tecnológica de la empresa y alinearla a la estrategia de seguridad de información, sus funciones principales son:

  - ✓ Planificar y desarrollar la estrategia TI de la Fundación junto al Gerente Administrativo y Financiero.
  - ✓ Investigar y desarrollar nuevos avances y tendencias tecnológicas.
  - ✓ Gestionar los proyectos tecnológicos de seguridad de información.
  - ✓ Garantizar la seguridad tecnológica.
  - ✓ Gestionará riesgos, controles e incidentes de seguridad relacionados con tecnología.

- **OFICIAL DE SEGURIDAD DE LA INFORMACIÓN.** Responsable del desarrollo, implementación y gestión de toda la seguridad de la Fundación, tanto física como digital. Sus responsabilidades son:
  - ✓ Desarrollará procedimientos, guías, lineamientos y demás normativa interna en relación con seguridad de información.
  - ✓ Asegurará que los procesos de TI estén bien planificados para cumplir los objetivos de la empresa.
  - ✓ Estudiará el modelo de negocio de la empresa para comprender los riesgos de seguridad.
  - ✓ Definirá y ejecutará el plan de capacitación y concientización en seguridad de información a través del área de Talento Humano.
  - ✓ Realizará evaluaciones periódicas acerca de la efectividad de la política y propondrá las modificaciones que sean necesarias para asegurar la protección de información y los activos que se relacionan con ella en la Fundación Universitaria Cafam.
  - ✓ Liderará los ejercicios periódicos de identificación y gestión de riesgos, acorde con las directrices en esta materia.

- **EMPLEADOS, DIRECTIVOS Y JEFES DE UNIDAD ACADÉMICA Y ADMINISTRATIVA**
  - ✓ Realizarán periódicamente el análisis y gestión de riesgos a los activos de información a su cargo.
  - ✓ Definirán, actualizarán e implementarán los controles que prevengan la ocurrencia de riesgos en los activos de información a su cargo.

- ✓ Observarán, reportarán y tomarán acciones ante la ocurrencia de eventos e incidentes, debilidades y el uso inadecuado de los activos de información de la Fundación Universitaria Cafam, de acuerdo con el procedimiento de gestión de incidentes establecido.

Estas responsabilidades no solo competen a la disposición de los distintos intereses que persigue la Fundación, sino también se encuentran en consonancia con las obligaciones legales y éticas que conciernen al buen funcionamiento y privacidad de la Información de la Fundación Universitaria Cafam.

5. GENERALIDADES

5.1. Política de Seguridad de la Información

La Política de Seguridad de la Información tiene como finalidad establecer lineamientos para facilitar la protección de los activos de información de la Fundación Universitaria Cafam, así como el adecuado uso de los recursos y gestión del riesgo, proteger la información de todas las amenazas internas o externas bien sean deliberadas, accidentales o naturales. Esta política busca asegurar los siguientes principios, de acuerdo con las buenas prácticas y estándares como ISO/IEC 27001:

5.1.1. **Confidencialidad**: Protegeremos la información sensible y reservada de la organización de la divulgación o acceso no autorizado.

5.1.2. **Integridad**: Mantendremos la precisión y la probidad de la información y los activos de la Fundación a través de controles adecuados.

5.1.3. **Disponibilidad**: Garantizaremos que la información y los sistemas críticos estén disponibles para su uso cuando sea necesario.

5.1.4. **Cumplimiento legal y normativo**: Cumpliremos con todas las leyes, regulaciones y requisitos aplicables relacionados con la seguridad de la información.

5.1.5. Compromiso con el cumplimiento de los requisitos aplicables relacionados con la seguridad de la información.

5.1.6. Cumplimiento de las obligaciones contractuales con nuestros empleados, miembros de la comunidad de la Fundación Universitaria Cafam y demás grupos de interés (clientes, proveedores, etc.).

5.1.7. Entrenamiento, generación de cultura y conciencia a todos los estudiantes, docentes, empleados, graduados, contratistas, clientes y proveedores en seguridad de la información y demás grupos de interés.

5.2. Objetivos de seguridad de la información

5.2.1. Preservar la confidencialidad, integridad y disponibilidad de la información en la Fundación Universitaria Cafam.

5.2.2 Mantener la confianza de los grupos de interés (estudiantes, profesores, directivos, personal administrativo, contratistas, proveedores, entes reguladores) en cuanto a la seguridad de la información.

5.2.3. Determinar y gestionar los riesgos, a través de la adopción de controles y la supervisión efectiva, y las oportunidades que puedan afectar la seguridad de la información e impactar a la Fundación Universitaria Cafam.

5.2.4. Incentivar la cultura de seguridad de la información en la Fundación Universitaria Cafam y que ésta permita generar un valor agregado en todos los procesos de la Fundación.

5.2.5. Ser competitivos y un referente en la educación por medio de plataformas digitales seguras que generen confianza a nuestros estudiantes y clientes.

5.3. Gestión de riesgos de seguridad de la información

La Fundación Universitaria Cafam promueve una cultura para la gestión del riesgo en seguridad de la información mediante el establecimiento, formalización e implementación de una metodología para la valoración y tratamiento del riesgo.

Todos los activos de información dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) deben ser evaluados al menos una vez al año y/o cuando hay cambios significativos en la Fundación, en especial por los líderes de proceso, para determinar en conjunto con el Comité de Seguridad de la Información, o quien haga sus veces, los controles mínimos requeridos para reducir y mantener el riesgo a un nivel aceptable.

La ejecución, desarrollo e implementación de los controles requeridos para minimizar los riesgos será responsabilidad de los líderes de proceso (propietario), con el apoyo de las diferentes áreas competentes de la Fundación.

La evaluación de riesgos se realizará según se define en la metodología de gestión de riesgos establecida en la Fundación. Es importante aclarar que siempre se debe estar gestionando los riesgos que se hayan identificado.

5.4. Seguridad relacionada con el recurso humano

Toda la comunidad de la Fundación Universitaria Cafam incluyendo graduados y terceros que tengan acceso o hagan uso de los recursos de la Fundación deben cumplir con las políticas, procedimientos y directrices de seguridad de información de la Fundación, los cuales están publicados en la página web de la Institución. El área de talento humano tiene las siguientes responsabilidades mínimas en términos de seguridad de la información:

5.4.1. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran en función de la seguridad de la información.

5.4.2. Definir junto con el Gerente Administrativo y Financiero, la estrategia de verificación de antecedentes de los candidatos a una vacante de acuerdo con los requisitos de negocio, la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

5.4.3. Incluir en los acuerdos contractuales con empleados y contratistas las responsabilidades en cuanto a seguridad de la información sus principios de confidencialidad, integridad y disponibilidad definidos por el Gerente Administrativo y Financiero.

5.4.4. Asegurar que los empleados y contratistas sean capacitados y evaluados respecto a la importancia y responsabilidades de seguridad de la información, estas capacitaciones se realizarán de forma periódica.

5.4.5. Aplicar las definiciones en cuanto a las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo definidos por el Gerente Administrativo y Financiero.

5.5. Uso de los activos de información

La Fundación Universitaria Cafam establecerá procedimientos para el acceso y uso de los activos de información, en cabeza del Gerente Administrativo y Financiero, con el objetivo que sean cumplidas por los usuarios, tales como:

5.5.1. Identificación de los activos organizacionales y definición de responsabilidades de protección apropiada.

5.5.2. Autenticación para su uso.

5.5.3. Lista de recursos a los que los usuarios tienen acceso.

5.5.4. Dispositivos etiquetados con información del propietario.

5.5.5. Lista de productos aprobados por la Fundación.

5.5.6. Ubicación de las tecnologías en la red.

5.5.7. Desconexión automática de sesiones de tecnologías de acceso remoto.

5.5.8. Acceso remoto a proveedores sólo cuando este acceso es estrictamente requerido.

5.5.9. Desarrollo e implementación de procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la Fundación.

5.5.10. Prevención de divulgación, modificación, retiro o destrucción de información.

5.6. Control de acceso a la información y los sistemas

Los controles para el acceso a la información de la Fundación Universitaria Cafam deben ser definidos de acuerdo con su clasificación.

Los estudiantes, docentes, empleados y terceros deben acceder únicamente a la información que es necesaria para el desarrollo de sus funciones o responsabilidades con base a las definiciones del principio de confidencialidad y disponibilidad.

La Fundación Universitaria Cafam cuenta con un procedimiento de administración de usuarios para asignar o cancelar los derechos de acceso para todos los sistemas y servicios. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. Los responsables de los activos de información deben revisar los derechos de acceso de los usuarios con una frecuencia regular.

El acceso a la información por parte de terceros debe concederse solamente para las funciones requeridas y con los mecanismos que aseguren, tanto la identidad de quienes realizan el acceso como la confidencialidad, integridad y disponibilidad de la información.

5.7. Seguridad física y del entorno

Toda área o equipo informático donde se procesa información de la Fundación Universitaria Cafam debe cumplir con las directrices funcionales y procedimientos de seguridad física y del entorno establecidos por la Fundación directamente o a través de la compañía de seguridad que tenga contratada, con el fin de evitar el acceso a personas no autorizadas, daño e interferencia a los recursos e infraestructura de información.

Los empleados que trabajan en las modalidades teletrabajo, trabajo en casa o cualquier esquema en el cual se desarrollen actividades por fuera de las instalaciones de la Fundación Universitaria Cafam, realizarán todas las actividades tendientes a garantizar que personas no autorizadas accedan a los equipos o la información contenida en ellos.

5.8. Recursos e infraestructura física para el procesamiento de información

En cualquier recurso o infraestructura física donde se realice procesamiento de la información de la Fundación Universitaria Cafam, se deben cumplir todas las políticas, procedimientos y directrices de seguridad de la información, que garanticen la confidencialidad, integridad, y disponibilidad de la información.

El administrador de cada plataforma es responsable de mantener e implementar los procedimientos y estándares en el ambiente correspondiente, con el apoyo de la Oficina de Tecnologías.

5.9. Seguridad de las operaciones y las comunicaciones

La Fundación Universitaria Cafam, en cabeza del jefe de tecnologías, o quien a haga sus veces, debe asegurar el correcto funcionamiento de la infraestructura tecnológica que realiza el procesamiento de información, garantizar operaciones correctas y seguras y debe hacer seguimiento al uso de recursos tecnológicos, realizar los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema. Para lo cual definirá los procedimientos, guías e instructivos necesarios.

5.10. Adquisición, desarrollo y mantenimiento de sistemas de información

La Fundación Universitaria Cafam en cabeza del jefe de tecnologías, o quien a haga sus veces, debe asegurar la correcta adquisición, desarrollo y mantenimiento de los sistemas de información, garantizando la seguridad de la información en cada una de las etapas, para lo cual definirá los procedimientos, guías e instructivos necesarios.

5.11. Gestión de incidentes de seguridad de la información

La Fundación en cabeza del Gobierno de seguridad, definirá el procedimiento de gestión de incidentes de seguridad de la información para comunicar, dar respuesta, monitorear y establecer la causa raíz de los incidentes, dicho procedimiento está compuesto por:

5.11.1. Roles y responsabilidades.

5.11.2. Estrategias de comunicación y canales apropiados.

5.11.3. Procedimiento de respuesta a incidentes.

5.11.4. Requerimientos legales y notificación a las Autoridades.

5.11.5. Procedimiento de recuperación.

5.11.6. Procesos de respaldo de información (backup).

5.11.7. Recolección y análisis de evidencia.

El procedimiento de gestión de incidentes de seguridad de la información se revisa por lo menos una vez al año y se realizan las mejoras pertinentes de acuerdo con las lecciones aprendidas tanto de los incidentes simulados como de los reales.

5.12. Incidentes de seguridad que involucren datos personales

Estos incidentes deben ser reportados por parte del Oficial de Datos Personales o quien haga sus veces, a la Superintendencia de Industria y Comercio dentro de los 15 días hábiles siguientes a su conocimiento. Requiere la adopción de todas las medidas que evidencien la diligencia de la Fundación para evitar o mitigar el daño que pueda causar a la privacidad de los titulares en los términos de la Ley, la Política de Tratamiento de Datos y del Manual de Seguridad de la Información de la Fundación Universitaria Cafam vigente. El Oficial de Datos Personales o quien haga sus veces, debe llevar una bitácora exacta y soportada de su gestión.

Cuando se observen afectaciones sustanciales a los titulares debe considerarse la comunicación de estas y la adopción de medidas de seguimiento y monitoreo para evitar efectos que puedan afectar a los titulares de los datos.

5.13. Continuidad de negocio

La Fundación Universitaria Cafam, debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres. Además, establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación.

Debido a que cualquier interrupción en los procesos de la Fundación puede afectar su operación, es responsabilidad de sus directivas aprobar estrategias, soluciones y planes de continuidad de negocio que cubran las actividades esenciales y críticas de la Fundación Universitaria Cafam.

Se deben incluir controles para identificar y reducir riesgos, limitar las consecuencias de los diferentes incidentes y por último asegurar la recuperación inmediata de las operaciones esenciales.

Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Como parte fundamental del soporte a la Fundación, todos los sistemas de información deben poseer estrategias, soluciones y planes de contingencia con los recursos necesarios que aseguren la continuidad de los procesos académicos, así como el conocimiento de los Planes de Continuidad de Negocio (BCP) de los proveedores que prestan servicios críticos a la Universidad.

5.14. Mejora Continua

La Fundación debe implementar un proceso sistemático y cíclico para perfeccionar el SGSI, esto implica la identificación de áreas de oportunidad, la implementación de cambios y la evaluación constante para optimizar la seguridad de la información. Este proceso se logra mediante la aplicación del ciclo PDCA (Planificar, Hacer, Verificar, Actuar), el cual guía la implementación, operación, evaluación y mejora del sistema. Para la Planificación se definirán los objetivos de seguridad de la información, se identificarán y se evaluarán los riesgos, se establecerán políticas, procedimientos y controles y se planificarán acciones correctivas y preventivas. Para el ciclo del Hacer, se debe implementar el SGSI de acuerdo con los controles y políticas planificadas, se capacitará a todo el personal (estudiantes, docentes, empleados, graduados o terceros) en buenas prácticas de seguridad y se deberán ejecutar proyectos de seguridad como actualizaciones de software e implementaciones de herramientas SIEM. En la parte de Verificar se debe monitorear y medir la efectividad de los controles implementados, se deberán realizar auditorías internas y revisiones para evaluar el desempeño del SGSI y se realizará el análisis de incidentes y no conformidades y tomar acciones correctivas. Para el último ciclo, Actuar, se implementarán acciones de mejora basadas en los hallazgos de auditoría, análisis de incidentes y revisiones; si es necesario se actualizarán la política de seguridad de la información y los procedimientos y se deberá documentar y comunicar las mejoras a todas las partes interesadas.

La mejora continua en un Sistema de Gestión de Seguridad de la Información no es un proceso de una sola vez, sino un compromiso permanente para proteger los activos de información de la Fundación frente a un panorama de amenazas en constante evolución. Aplicar el ciclo PDCA asegura que el SGSI sea dinámico y se mantenga en línea con las mejores prácticas y necesidades del negocio.

5.15. Violaciones a las Políticas de Seguridad de la Información

Cualquier situación que evidencie la violación a las políticas de seguridad de la información por parte de los estudiantes, docentes, empleados, graduados o terceros que tengan relación directa o indirecta en el manejo de la infraestructura tecnológica y sistemas de información de la Fundación Universitaria Cafam podrá resultar en un proceso que deberá ser iniciado por parte del líder de proceso, jefe inmediato o responsable del tercero, con base a las evidencias recopiladas las cuales pueden incluir, mas no estar limitadas a:

5.15.1. Acción de tipo disciplinario por parte del área que la Fundación ha dispuesto para el efecto según los lineamientos establecidos por el código sustantivo del trabajo, el reglamento estudiantil, reglamento docente o reglamento interno de trabajo según el rol del implicado, las cláusulas especiales que se establezcan con los empleados en sus contratos laborales y/o todo aquello que según las leyes colombianas definan como acciones disciplinarias patronales.

5.15.2. Suspensión o acceso restringido a las áreas de procesamiento de la información.

5.15.3. Terminación del contrato de trabajo o relación comercial (basados en las disposiciones emitidas por las leyes colombianas en materia laboral y el reglamento interno de trabajo).

5.15.4. Demanda de tipo civil o penal como resultado de las acciones de tipo disciplinario.

5.15.5. Asunción de consecuencias legales derivadas de la investigación que adelante la autoridad.

6. REVISIÓN Y APROBACIÓN DE LA POLÍTICA

Esta política será revisada por el Gerente Administrativo y Financiero o quien haga sus veces mínimo cada doce (12) meses; con el fin de asegurar su vigencia y cumplimiento deberá actualizarse en el mismo periodo previo concepto del Comité de Seguridad de la Información de la Fundación Universitaria Cafam y aprobación del Consejo Superior Universitario. También se encuentra dispuesta a modificaciones ante cambios en la estructura organizacional para la administración de la seguridad de la información, siempre y cuando cuente con la revisión del Comité de Seguridad de la Información de la Fundación Universitaria Cafam y aprobación del Consejo Superior Universitario.