RESOLUCIÓN RECTORAL No. 011 DE 2025

(11 de abril de 2025)

POR LA CUAL SE ADOPTA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA FUNDACIÓN UNIVERSITARIA CEIPA

El Rector de la Fundación Universitaria CEIPA, en uso de sus facultades estatutarias, en especial las conferidas en el artículo 28 del Estatuto General, y

CONSIDERANDO:

1. La seguridad de la información es un componente esencial para el cumplimiento del principio rector institucional, en el marco de la transformación digital y la confianza de los actores internos y externos.

2. Es deber de la Institución proteger la confidencialidad, integridad y disponibilidad de la información académica, administrativa y personal que administra, conforme a la Ley 1581 de 2012 y demás normas que regulan la protección de datos personales y la seguridad de la información.

3. Que la Fundación Universitaria CEIPA ha formulado una Política de Seguridad y Privacidad de la Información, la cual establece los principios, medidas, roles y procedimientos para garantizar el adecuado manejo de la información y la protección de los sistemas tecnológicos institucionales.

4. Que dicha política ha sido elaborada y validada por las instancias técnicas y requiere su adopción formal mediante acto administrativo rectoral.

RESUELVE:

ARTÍCULO PRIMERO. Adoptar la Política de Seguridad y Privacidad de la Información de la Fundación Universitaria CEIPA, la cual se anexa a la presente resolución y hace parte integral de la misma.

ARTÍCULO SEGUNDO. La política adoptada será de obligatorio cumplimiento para todos los miembros de la comunidad institucional, incluidos estudiantes, profesores, colaboradores administrativos, contratistas, proveedores y terceros que accedan o gestionen información institucional, quienes deberán cumplir las disposiciones establecidas en ella.

ARTÍCULO TERCERO. La Dirección de Tecnología, en coordinación con el Comité de Seguridad de la Información, será responsable de su divulgación, implementación, monitoreo, actualización y cumplimiento.

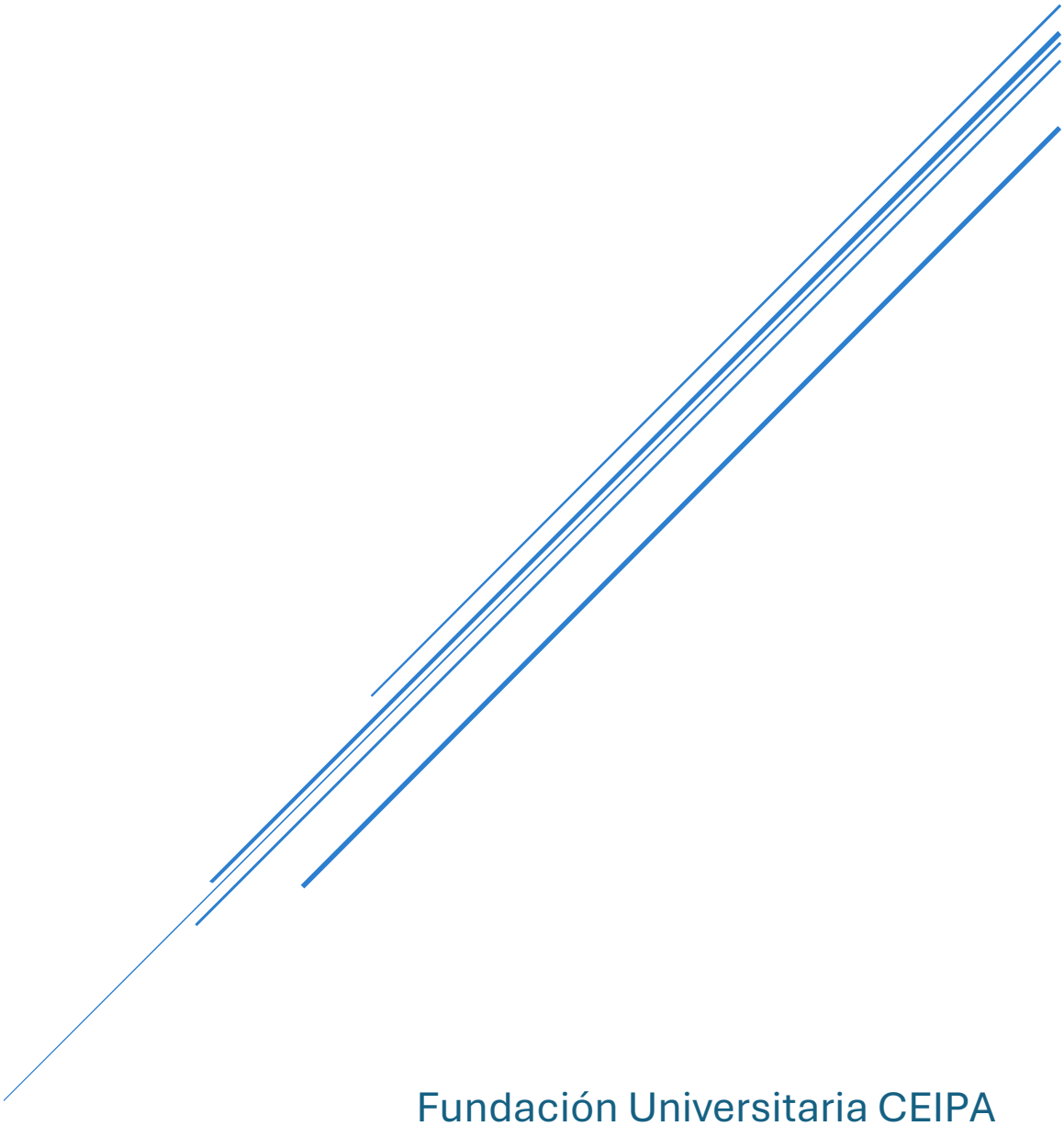
ARTÍCULO CUARTO. La presente resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE Y CÚMPLASE

Dado en Sabaneta, a los once (11) días del mes de abril de 2025.

DIEGO MAURICIO MAZO CUERVO
Rector

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



Fundación Universitaria CEIPA
Política de Seguridad

Tabla de contenido

I. Introducción

La **Fundación Universitaria CEIPA** reconoce la importancia fundamental de la **seguridad de la información** en el entorno académico y administrativo, tanto para la protección de datos sensibles como para garantizar la confianza de nuestros estudiantes, colaboradores, proveedores y otras partes interesadas. Dado el contexto actual de crecimiento digital, innovación tecnológica y el incremento de riesgos cibernéticos, la Institución considera esencial la implementación de políticas robustas que aseguren la **confidencialidad**, **integridad** y **disponibilidad** de la información que se maneja dentro de sus sistemas y plataformas tecnológicas.

Por ello, la **Política de Seguridad y Privacidad de la Información** es un documento clave que guía todas las acciones y decisiones relacionadas con el manejo, uso y protección de la información dentro de la Institución. Esta política se basa en el compromiso de CEIPA para cumplir con las normativas nacionales e internacionales sobre **protección de datos personales**, y **seguridad de la información**, brindando a sus miembros un entorno seguro y confiable.

La seguridad de la información no solo se refiere a la protección de datos críticos y confidenciales, sino también a la creación de una cultura organizacional que entienda la importancia de cuidar los recursos informáticos de manera responsable y efectiva. En este contexto, la política tiene como propósito **establecer principios claros** sobre el manejo de los datos, el uso de los sistemas tecnológicos, la protección de la privacidad y las medidas a seguir en caso de incidentes de seguridad.

A través de esta política, la Institución establece las directrices necesarias para que todos los usuarios de sus sistemas informáticos, incluidos estudiantes, colaboradores, proveedores y otros terceros, sean conscientes de sus responsabilidades y cumplan con los procedimientos de seguridad que garantizan que la información sea tratada adecuadamente. Asimismo, se detallan las medidas de protección, los controles de acceso, la clasificación de la información, la retención de datos y los procedimientos para manejar incidentes de seguridad, con el fin de mantener la integridad y privacidad de los datos en todo momento.

De esta manera, la **Fundación Universitaria CEIPA** reitera su compromiso de proporcionar un entorno académico y administrativo seguro, facilitando el acceso a la información necesaria mientras protege los datos sensibles de manera eficiente y conforme a la legislación aplicable.

El cumplimiento de esta política es obligatorio para todos los miembros de la comunidad educativa y laboral de la Institución, quienes deberán adherirse a los

principios establecidos y colaborar en la ejecución de las medidas de seguridad definidas para preservar la protección de la información.

II. Propósito

El **propósito** de la **Política de Seguridad y Privacidad de la Información** de la **Fundación Universitaria CEIPA** es establecer un marco integral y coherente para garantizar que toda la información manejada por la Institución, en sus diferentes formatos (digital, física, etc.), se gestione de manera segura y confidencial, respetando los principios de integridad, disponibilidad y privacidad. Esta política tiene como objetivo principal proteger tanto la información sensible como la infraestructura tecnológica de la Fundación, a través de una serie de directrices y medidas concretas que deben ser cumplidas por todos los usuarios y actores involucrados.

Objetivos Específicos del Propósito:

1. **Establecer Directrices Claras de Manejo de Información:** La política proporciona pautas detalladas para la clasificación, almacenamiento, uso, acceso, y transferencia de datos dentro de la Fundación Universitaria CEIPA, asegurando que cada tipo de información reciba el nivel adecuado de protección según su sensibilidad.

2. **Garantizar la Protección de la Información Sensible:** La política tiene como objetivo principal proteger la información sensible de la Institución, incluyendo datos personales de estudiantes y colaboradores, registros académicos, información financiera y cualquier otro dato confidencial. Estas directrices aseguran que todos los recursos informáticos estén protegidos contra accesos no autorizados, pérdida, daño, alteración o destrucción.

3. **Cumplimiento Normativo:** Asegurar que la Fundación cumpla con las leyes y regulaciones locales e internacionales sobre privacidad y protección de datos (como la Ley 1581 de 2012 en Colombia y el Reglamento General de Protección de Datos - GDPR en la Unión Europea, si aplica). Esto incluye la aplicación de procedimientos y controles de seguridad necesarios para evitar violaciones de privacidad y sanciones legales.

4. **Establecer Protocolos para la Gestión de la Información:** La política define procedimientos para la retención, archivado y destrucción de la información una vez que ya no sea necesaria, cumpliendo con los plazos legales y de

normativa interna. Este aspecto incluye directrices claras para la eliminación segura de la información tanto en formato digital como físico, evitando riesgos de exposición o recuperación no autorizada.

5. **Promover una Cultura de Seguridad en la Institución:** El propósito también incluye fomentar una cultura de seguridad y privacidad entre todos los usuarios de los sistemas informáticos de la Institución. A través de la formación continua, sensibilización y la creación de conciencia sobre las amenazas de seguridad, los usuarios estarán mejor preparados para gestionar la información de manera responsable y proteger los activos de la Fundación.
6. **Clarificar las Responsabilidades de los Usuarios:** La política proporciona un marco claro de responsabilidades para todos los usuarios (estudiantes, profesores, colaboradores, proveedores y otros terceros) que accedan a los sistemas informáticos de la Institución. Cada usuario deberá cumplir con las normas establecidas sobre acceso, uso y protección de los datos, lo cual se detalla en los procedimientos internos de la Fundación.
7. **Prevenir Incidentes de Seguridad:** La política establece procedimientos de auditoría, monitoreo y gestión de incidentes para detectar, prevenir y responder a posibles violaciones de seguridad de la información. Esto incluye protocolos de comunicación interna para la notificación de incidentes, así como las acciones correctivas y preventivas que se tomarán.
8. **Asegurar la Disponibilidad de la Información:** Además de la confidencialidad e integridad de los datos, la política busca garantizar la **disponibilidad** de la información cuando sea necesario, mediante controles de acceso adecuados y mecanismos de respaldo que permitan la recuperación ante desastres o situaciones imprevistas.

Elementos Clave que Apoya el Propósito de la Política:

- **Clasificación y Manejo de Información:** Se establecen directrices claras para categorizar la información según su nivel de sensibilidad, desde datos públicos hasta información crítica que requiere las más estrictas medidas de protección.
- **Protección y Seguridad de los Sistemas:** La política define las medidas de protección necesarias para evitar el acceso no autorizado a los sistemas tecnológicos, incluyendo el uso de contraseñas seguras, autenticación de dos factores, y medidas de encriptación.

- **Capacitación y Sensibilización:** Como parte de la implementación, se lleva a cabo la capacitación continua para todos los usuarios en cuanto a las buenas prácticas de seguridad, el manejo adecuado de la información y cómo evitar vulnerabilidades comunes, como ataques de phishing o malware.
- **Monitoreo y Auditoría:** La política también prevé un sistema de monitoreo continuo para detectar accesos no autorizados o actividades sospechosas dentro de los sistemas. Esto incluye la auditoría de logs de acceso y el análisis de incidentes.

III. Audiencia

La **Política de Seguridad y Privacidad de la Información** de la **Fundación Universitaria CEIPA** tiene un alcance amplio y es aplicable a todos los individuos y entidades que interactúan con los sistemas, redes, bases de datos y otros recursos informáticos de la Institución. Esto incluye tanto a los usuarios internos como externos que manejan información confidencial, académica, administrativa o personal, garantizando así una protección integral de los datos en todos los niveles de la organización. Las siguientes categorías de personas son las principales audiencias de esta política:

1. Estudiantes

Los estudiantes son usuarios clave de los sistemas informáticos de la Institución, ya que interactúan con plataformas de aprendizaje, registros académicos, aplicaciones de gestión y almacenamiento de datos personales. Los estudiantes deben seguir las normas y directrices establecidas para asegurar la protección de su información personal, la integridad de su desempeño académico y la privacidad de sus interacciones dentro de los sistemas tecnológicos.

- **Accesos autorizados**: Acceden a información académica (calificaciones, historial académico) y administrativa (horarios, pagos, solicitudes).
- **Responsabilidades**: Respetar la privacidad de otros estudiantes y no acceder a información no autorizada.
- **Formación y sensibilización**: Recibirán capacitación periódica en cuanto a seguridad y privacidad de la información, incluida la importancia de proteger sus credenciales de acceso y los datos sensibles que gestionan en las plataformas de la Institución.

2. Colaboradores (profesores, administrativos, personal de soporte)

Este grupo es crucial para la operación diaria de la Institución, ya que tienen acceso tanto a información personal de estudiantes como a datos académicos, administrativos y financieros de la Institución. Los colaboradores incluyen tanto a personal docente como no docente, y están involucrados en la creación, procesamiento y almacenamiento de información crítica.

- **Accesos autorizados**: Los profesores tienen acceso a los registros académicos de los estudiantes y a las herramientas de enseñanza y evaluación. El personal administrativo puede acceder a bases de datos académicas y financieras. El personal de soporte técnico tiene acceso a los sistemas de infraestructura y servidores.
- **Responsabilidades**: Además de seguir las políticas de acceso y uso de información, los colaboradores deben garantizar la protección de los datos que manejan y reportar incidentes de seguridad. Están sujetos a restricciones de acceso de acuerdo con su rol específico dentro de la Institución.
- **Formación y sensibilización**: Deben recibir formación continua en seguridad de la información y cumplimiento de políticas internas sobre privacidad y protección de datos.

3. Proveedores y Contratistas

Los proveedores y contratistas externos que tienen acceso a sistemas o recursos informáticos de la Institución, ya sea para ofrecer servicios tecnológicos, consultoría o materiales, también deben cumplir con las políticas de seguridad de la información. Esto es crucial para garantizar que los datos de la Institución se manejen con el mismo nivel de protección que recibirían si fueran gestionados internamente.

- **Accesos autorizados**: Dependiendo del contrato y los servicios prestados, los proveedores y contratistas pueden tener acceso a sistemas específicos de la Institución, bases de datos, o incluso a información confidencial relacionada con proyectos, actividades administrativas, o investigación.
- **Responsabilidades**: Deben firmar acuerdos de confidencialidad y cumplir con los protocolos de seguridad establecidos por la Institución, incluyendo el uso de medidas de protección de datos como cifrado y autenticación fuerte.
- **Formación y sensibilización**: Aunque son externos, los proveedores y contratistas deben ser informados sobre las expectativas de seguridad y

privacidad de la información, y ser capacitados en las mejores prácticas para el manejo de datos sensibles.

4. Cualquier Otra Persona o Entidad que Utilice los Recursos Informáticos de la Institución

Este grupo incluye a individuos o entidades que no pertenecen directamente a la Fundación Universitaria CEIPA, pero que tienen acceso ocasional o específico a los sistemas y recursos tecnológicos de la Institución. Esto puede incluir visitantes, auditores, socios académicos o empresas colaboradoras que no son contratistas formales, pero que requieren acceso a información o infraestructura tecnológica de la Institución.

- **Accesos autorizados**: El acceso se limita a los recursos específicos para los que han sido autorizados, como por ejemplo acceso a plataformas de colaboración, sistemas de evaluación externa, auditorías de seguridad, o servicios temporales de TI.
- **Responsabilidades**: Aunque el acceso es limitado, estas personas y entidades deben cumplir con las políticas de seguridad de la información, incluidas las normas de protección de datos personales y la no divulgación de información sensible.
- **Formación y sensibilización**: Dependiendo del acceso y del tipo de relación, se les informará de manera puntual sobre las prácticas y protocolos de seguridad aplicables durante el tiempo en que tengan acceso a los sistemas.

Resumen de Responsabilidades Comunes para Toda la Audiencia

Aunque las responsabilidades pueden variar dependiendo del rol y el nivel de acceso a la información, todos los usuarios de los sistemas tecnológicos de la Institución deben cumplir con las siguientes normas básicas:

- **Proteger las credenciales de acceso**: Las contraseñas y las claves de acceso deben ser gestionadas de manera segura, no compartiéndolas con otras personas ni dejándolas accesibles de forma no segura.
- **Respetar los límites de acceso**: Solo se debe acceder a la información que sea necesaria para llevar a cabo las tareas o funciones asignadas.

- **Cumplir con las políticas de seguridad y privacidad**: Todos los usuarios deben adherirse a las políticas de seguridad, privacidad y protección de la información y asistir a las capacitaciones relacionadas.
- **Reportar incidentes**: Cualquier incidente relacionado con la seguridad de la información, como intentos de acceso no autorizado, robo de datos, vulnerabilidades detectadas, debe ser reportado inmediatamente a las autoridades competentes de la Institución.

IV. Glosario

1. **Amenaza**: Posible evento o acción que puede comprometer la seguridad de la información, como ataques cibernéticos, errores humanos o fallos tecnológicos.
2. **Autenticación Multifactor (MFA)**: Método que refuerza la seguridad del acceso a un sistema exigiendo dos o más credenciales distintas, como una contraseña y un código de verificación enviado por SMS o una aplicación de autenticación."
3. **Backup (Copia de Seguridad)**: Proceso de almacenamiento de información en un medio secundario para su recuperación en caso de pérdida de datos o fallos en los sistemas.
4. **Cifrado**: Técnica de protección de datos que transforma la información en un formato ilegible sin la clave de descifrado correspondiente.
5. **Control de Acceso**: Conjunto de políticas y medidas para regular y restringir el acceso a la información según el nivel de autorización del usuario.
6. **Gestión de Incidentes**: Conjunto de procedimientos establecidos para detectar, responder y mitigar eventos de seguridad que comprometan la confidencialidad, integridad o disponibilidad de la información.
7. **Ingeniería Social**: Técnica de manipulación psicológica utilizada por atacantes para obtener información confidencial mediante engaños o suplantación de identidad.
8. **Malware**: Programa malicioso diseñado para dañar, alterar o acceder sin autorización a sistemas informáticos.

9. **Phishing**: Método de fraude cibernético en el que los atacantes intentan obtener información sensible haciéndose pasar por entidades legítimas mediante correos electrónicos, mensajes o sitios web falsificados.
10. **Política de Seguridad de la Información**: Conjunto de directrices y normas establecidas por una organización para proteger su información y sistemas contra amenazas y riesgos.
11. **Respaldo de Información**: Procedimiento de copia y almacenamiento de datos críticos en ubicaciones seguras para garantizar su disponibilidad en caso de incidentes.
12. **Vulnerabilidad**: Debilidad en un sistema de información que puede ser explotada por amenazas para comprometer la seguridad de los datos.
13. **Inteligencia Artificial Generativa:** Tecnología que utiliza modelos avanzados de aprendizaje automático para crear contenido original, como textos, imágenes, o videos, y que puede ser usada maliciosamente en ciberataques, como phishing automatizado o manipulación de datos.
14. **IoT (Internet de las Cosas):** Conjunto de dispositivos interconectados que recopilan, transmiten y reciben datos a través de Internet. Aunque mejora la operatividad, presenta vulnerabilidades de seguridad que pueden ser explotadas para ataques cibernéticos.
15. **Deepfake:** Técnica de inteligencia artificial que utiliza redes neuronales para alterar imágenes, audios o videos, creando falsificaciones realistas utilizadas frecuentemente para desinformación o suplantación de identidad.

Complementos a la Política

- **Roles y Responsabilidades Detalladas**: Especificación de las funciones clave dentro del marco de seguridad, asegurando que cada usuario, colaborador y proveedor comprenda su papel en la protección de la información.
- **Actualización Periódica de la Política**: Definición de un ciclo de revisión continuo para asegurar que la política esté alineada con las normativas vigentes y los avances tecnológicos.
- **Gestión de Riesgos**: Inclusión de metodologías para la identificación, evaluación y mitigación de riesgos relacionados con la seguridad de la información.

V. Política General de Seguridad y Privacidad de la Información

La **Fundación Universitaria CEIPA** reconoce la importancia de proteger la **información sensible**, **garantizar la privacidad** de los **datos personales** y asegurar la **protección de los sistemas informáticos** para cumplir con su misión educativa y administrativa de manera eficiente. Esta política general de seguridad y privacidad busca establecer las bases para el manejo seguro de la información en todas las áreas de la Institución, garantizando que todos los datos sean tratados de acuerdo con los principios fundamentales de **confidencialidad**, **integridad** y **disponibilidad**.

1. Principios Fundamentales

La política se basa en tres principios clave que guiarán el manejo de la información dentro de la Institución:

- **Confidencialidad**: La información debe ser accesible solo a las personas o entidades autorizadas para acceder a ella. Esto incluye la protección de datos personales y académicos de los estudiantes, así como los registros administrativos y financieros.
- **Integridad**: La información debe ser precisa, completa y actualizada. Se deben tomar medidas para evitar alteraciones no autorizadas o errores que puedan comprometer la veracidad de los datos. Cualquier cambio en los datos debe estar registrado y ser verificable.
- **Disponibilidad**: La información debe estar disponible para los usuarios autorizados cuando lo necesiten, asegurando que los sistemas informáticos y de almacenamiento sean fiables y accesibles en todo momento. En caso de fallos o incidentes, debe existir un plan de contingencia para restaurar el acceso.

Además, La política incorpora un conjunto adicional de directrices éticas fundamentales, que complementan los principios clave de confidencialidad, integridad y disponibilidad. Estas directrices refuerzan el compromiso de la Institución con el manejo responsable de la información. Los principios éticos son:

- **Transparencia:** La Institución se compromete a ser abierta sobre cómo se recopila, almacena, utiliza y comparte la información de los usuarios. Esto incluye proporcionar información clara y comprensible sobre las políticas de privacidad y los procedimientos relacionados con la seguridad de los datos.

- **Uso Responsable:** Los datos recopilados por la Institución solo serán utilizados para los fines previstos y legítimos. Cualquier uso adicional debe contar con el consentimiento explícito de las partes interesadas, respetando los derechos de privacidad y evitando la explotación de la información para propósitos no autorizados.
- **Protección Equitativa:** Se garantizará que todos los datos sean tratados con el mismo nivel de respeto y cuidado, independientemente de su origen o propietario, promoviendo un trato justo para todas las partes involucradas.
- **Integridad Ética:** La Institución adoptará un enfoque ético en todas las actividades relacionadas con la seguridad y privacidad de la información, asegurando que cualquier decisión o acción esté alineada con los valores y principios de la Fundación Universitaria CEIPA.

2. Alcance de la Política

Esta política se aplica a todos los usuarios de la Institución, incluidos:

- **Colaboradores (empleados)**: Todo el personal que tiene acceso a sistemas, bases de datos o cualquier tipo de información institucional.
- **Estudiantes**: Usuarios que interactúan con los sistemas académicos y administrativos.
- **Proveedores y terceros**: Empresas externas que manejan o procesan información en nombre de la Institución.
- **Visitantes**: Personas que, aunque no sean usuarios regulares, acceden a sistemas o recursos específicos de la Institución.

3. Objetivos de la Política

Los objetivos principales de la Política General de Seguridad y Privacidad de la Información son:

- **Proteger la información sensible**: Evitar el acceso no autorizado a información confidencial y asegurar que los datos personales de estudiantes, colaboradores y otras partes sean tratados de acuerdo con las normativas legales de privacidad y protección de datos.
- **Garantizar la protección de los sistemas informáticos**: Implementar medidas de seguridad física, lógica y técnica para proteger los servidores, bases de datos, aplicaciones y redes internas contra amenazas cibernéticas.

- **Cumplir con las normativas y leyes aplicables**: Asegurar que la Institución cumpla con las regulaciones nacionales e internacionales en cuanto a privacidad de datos (como la Ley de Protección de Datos Personales o leyes de seguridad cibernética).
- **Fomentar una cultura de seguridad**: Sensibilizar a todos los usuarios sobre la importancia de la seguridad de la información y la privacidad, promoviendo buenas prácticas de ciberseguridad.

4. Medidas de Seguridad

La Institución tomará una serie de medidas técnicas, organizacionales y procedimentales para asegurar que la información sea manejada de manera segura y conforme a los principios de confidencialidad, integridad y disponibilidad. Algunas de las medidas clave incluyen:

- **Control de acceso a la información**: El acceso a la información será gestionado mediante políticas de control de acceso basadas en el principio de "mínimos privilegios". Solo se concederá acceso a la información necesaria para realizar las funciones laborales, y se emplearán tecnologías como contraseñas seguras, autenticación multifactor y sistemas de gestión de identidades.
- **Protección de datos personales**: Los datos personales de estudiantes, colaboradores y otras personas serán tratados conforme a las leyes de privacidad, implementando mecanismos de encriptación y almacenamiento seguro de información personal sensible. Solo personal autorizado podrá acceder a estos datos.
- **Cifrado de la información**: Toda la información crítica y confidencial será cifrada tanto en tránsito (cuando se envía a través de la red) como en reposo (cuando se almacena en los servidores de la Institución). Esto garantizará que, incluso si los datos son interceptados, no puedan ser leídos ni utilizados.
- **Monitoreo y auditoría**: Se implementarán sistemas de monitoreo continuo para detectar accesos no autorizados y otros comportamientos sospechosos. Se mantendrán registros detallados de acceso a los sistemas y auditorías periódicas para garantizar que las políticas de seguridad estén siendo cumplidas.
- **Protección contra amenazas externas**: Se implementarán firewalls, sistemas de detección de intrusos (IDS), antivirus y otros mecanismos para proteger las

redes y sistemas informáticos de ataques cibernéticos externos, como malware, phishing, ransomware, etc. Además de las herramientas tradicionales de seguridad, la institución reforzará la protección frente a amenazas emergentes como:

  - **Inteligencia Artificial Generativa**: Prevención contra intentos de phishing automatizados.
  - **Dispositivos IoT (Internet de las Cosas)**: Monitoreo de redes para detectar accesos sospechosos.
  - **Deepfakes**: Validación de identidad en procesos administrativos importantes.

- **Protección contra pérdida de datos**: La Institución implementará estrategias de respaldo de datos periódicas para asegurar la recuperación de la información en caso de fallos técnicos, ataques cibernéticos o desastres naturales. Además, se garantizará que los procedimientos de recuperación ante desastres estén bien definidos.

5. Roles y Responsabilidades

- **La alta dirección** de la Fundación Universitaria CEIPA tiene la responsabilidad de asegurar que esta política sea adoptada y aplicada de manera efectiva en toda la Institución. Esto incluye proporcionar los recursos necesarios, establecer directrices claras y asegurar que todos los miembros de la organización reciban capacitación adecuada en cuanto a seguridad y privacidad.
- **Usuarios (colaboradores, estudiantes, proveedores)**: Los usuarios de la Institución tienen la responsabilidad de seguir las políticas, procedimientos y directrices relacionadas con la seguridad de la información. Esto incluye no compartir contraseñas, reportar incidentes de seguridad y no acceder a información no autorizada.
- **Departamento de TI**: El personal encargado de los sistemas informáticos tiene la responsabilidad de implementar y mantener las medidas de seguridad tecnológicas (como firewalls, sistemas de autenticación, etc.), además de gestionar las políticas de control de acceso y los mecanismos de auditoría.
- **Comité de Seguridad de la Información**: Un equipo encargado de revisar, actualizar y mantener las políticas de seguridad y privacidad de la información.

Este comité también se encargará de la coordinación de la capacitación y sensibilización en toda la Institución.

6. Cumplimiento de la Política

El incumplimiento de la **Política General de Seguridad y Privacidad de la Información** puede resultar en consecuencias disciplinarias que van desde amonestaciones hasta la suspensión o terminación del contrato, dependiendo de la gravedad de la infracción.

Además, la Institución podrá tomar acciones legales contra aquellos que comprometan la seguridad de la información o violen la privacidad de los datos personales, de acuerdo con las normativas vigentes. Algunos ejemplos:

- **Incumplimientos leves**: Amonestación verbal o escrita (ejemplo: compartir credenciales de acceso).
- **Incumplimientos graves**: Suspensión temporal del acceso a los sistemas (ejemplo: descarga de software malicioso).
- **Incumplimientos críticos**: Terminación del contrato y posible denuncia legal (ejemplo: acceso no autorizado o filtración de datos personales).

7. Actualización y Revisión de la Política

La **Política General de Seguridad y Privacidad de la Información** será revisada y actualizada regularmente para garantizar que se mantenga alineada con las mejores prácticas, avances tecnológicos y cambios regulatorios. La alta dirección evaluará anualmente el estado de la seguridad de la información y la efectividad de los controles implementados.

VI. Clasificación de la Información

La **clasificación de la información** es un proceso esencial para garantizar que todos los datos, documentos y registros de la **Fundación Universitaria CEIPA** sean tratados de acuerdo con su **sensibilidad** y **valor**, y que se implementen medidas de seguridad adecuadas para cada categoría. Esta clasificación ayuda a la Institución a manejar la información de forma eficiente, asegurando que la protección y el acceso a los datos sean proporcionales al riesgo y la importancia de la información.

A continuación, se detallan las categorías de clasificación de la información utilizadas por la Institución, y los procedimientos para su manejo:

1. Información Pública

La **información pública** es aquella que no tiene restricciones de acceso y puede ser compartida libremente sin representar ningún riesgo para la Institución o sus miembros. Este tipo de información no requiere medidas de seguridad adicionales y es accesible a cualquier persona o entidad, dentro y fuera de la Institución.

- **Ejemplos de información pública**:
    - Publicaciones académicas y científicas.
    - Comunicados oficiales y boletines informativos.
    - Información sobre eventos públicos organizados por la Institución.
    - Resultados de investigación que no contienen datos sensibles.
    - Información general sobre programas académicos, requisitos de inscripción, horarios, etc.
- **Manejo de la información pública**:
    - **Distribución abierta**: La información pública puede ser distribuida a través de canales accesibles, como el sitio web institucional, redes sociales, o publicaciones en medios.
    - **No requiere protección adicional**: No se aplican restricciones de acceso ni mecanismos de cifrado para la protección de esta información.

2. Información Interna

La **información interna** es aquella que es relevante para las operaciones diarias de la Institución, pero que no contiene datos sensibles que puedan causar un daño directo si se divulgan sin autorización. Este tipo de información debe ser controlada y compartida solo dentro de la comunidad interna de la Institución, pero no necesariamente está sujeta a una protección estricta.

- **Ejemplos de información interna**:
    - Políticas internas, manuales operativos, y procedimientos administrativos.
    - Informes de gestión interna, planes de trabajo y proyectos en curso.

    - Comunicaciones internas entre departamentos o colaboradores que no contengan información confidencial.
    - Estadísticas institucionales generales, informes de actividades académicas no sensibles.
    - Documentos de planificación estratégica sin datos críticos.
- **Manejo de la información interna**:
    - **Acceso controlado**: El acceso a esta información será restringido a los colaboradores y miembros autorizados de la Institución.
    - **Protección básica**: Aunque no requiere niveles altos de protección, la información interna debe ser almacenada en sistemas seguros, con protección por contraseñas y políticas de acceso basado en roles.
    - **Divulgación limitada**: No debe ser compartida con entidades externas, a menos que haya una justificación válida para ello.

3. Información Confidencial

La **información confidencial** contiene datos que requieren protección debido a su **sensibilidad** o **privacidad**, y cuyo acceso no autorizado podría afectar negativamente a la Institución, a sus miembros o a sus relaciones externas. Esta información debe ser tratada con un alto nivel de seguridad, y su divulgación debe estar estrictamente controlada.

- **Ejemplos de información confidencial**:
    - Registros académicos de los estudiantes, incluyendo calificaciones, matrículas y evaluaciones.
    - Información personal de estudiantes y colaboradores, como identificaciones, datos de contacto, historiales médicos, etc.
    - Información financiera sensible, como presupuestos detallados, transacciones financieras y detalles bancarios.
    - Contratos laborales y documentación personal de los empleados.
    - Datos de investigación que puedan contener información privada o propiedad intelectual aún no publicada.
- **Manejo de la información confidencial**:

- **Acceso restringido**: Solo los individuos que necesiten esta información para desempeñar sus funciones podrán acceder a ella, previa autorización.
- **Medidas de seguridad avanzadas**: La información confidencial será almacenada y transmitida utilizando **protocolos de cifrado** y **sistemas de control de acceso estrictos**, con auditorías regulares de acceso y uso.
- **Contratos de confidencialidad**: Los colaboradores y usuarios que manejen este tipo de información deberán firmar acuerdos de confidencialidad (NDA, por sus siglas en inglés) para asegurar su compromiso con la protección de estos datos.

4. Información Crítica

La **información crítica** es aquella cuya **compromiso** o **pérdida** podría tener un **impacto negativo significativo** en las operaciones de la Institución, en su reputación o en la seguridad de sus miembros. Este tipo de información es extremadamente sensible y debe estar bajo un control de seguridad extremadamente riguroso.

- **Ejemplos de información crítica**:
  - **Credenciales de acceso** a sistemas informáticos, contraseñas, claves de autenticación, tokens de seguridad, y demás datos que permiten el acceso a los sistemas sensibles.
  - **Información de infraestructura tecnológica**, como configuraciones de servidores, bases de datos clave, y redes internas.
  - **Planes de contingencia** y documentación sobre la continuidad del negocio, que contienen detalles sobre la respuesta ante incidentes de seguridad.
  - **Datos de acceso a sistemas de pago y plataformas de recursos financieros**, como información sobre plataformas de pago, sistemas de administración de finanzas o redes bancarias utilizadas.
- **Manejo de la información crítica**:
  - **Control de acceso estricto**: Solo un número limitado de usuarios de alto nivel (como administradores de sistemas y personal de TI autorizado) tendrán acceso a esta información, y el acceso será **registrado y auditado** regularmente.

- **Cifrado completo**: Toda la información crítica debe ser cifrada tanto en tránsito como en reposo. Esto incluye el uso de protocolos avanzados de cifrado y tecnologías de protección como autenticación multifactorial (MFA).
- **Monitoreo constante**: Los sistemas que contienen información crítica deben ser monitoreados en tiempo real mediante soluciones de seguridad como sistemas de detección de intrusos (IDS) y registros de auditoría para detectar accesos no autorizados.
- **Copia de seguridad y redundancia**: La información crítica debe ser respaldada y almacenada en sistemas redundantes, garantizando su disponibilidad incluso en caso de un desastre o incidente de seguridad.

Políticas de Seguridad por Categoría de Información

Cada categoría de información será manejada con una política de seguridad específica, que establecerá medidas de protección basadas en su nivel de sensibilidad. Estas políticas se deben aplicar en todas las etapas del ciclo de vida de la información, desde su creación hasta su destrucción, y serán revisadas regularmente para asegurar su adecuación.

Política de Acceso a la Información

- **Información pública**: **Acceso libre**; disponible para todo el público.
- **Información interna**: **Acceso restringido** dentro de la Institución, basado en roles y necesidades de acceso.
- **Información confidencial**: **Acceso altamente controlado**, solo para personal autorizado, con cifrado de la información y control de acceso riguroso.
- **Información crítica**: **Acceso limitado** a personal esencial, con cifrado, autenticación avanzada y monitoreo constante.

Política de Protección de la Información

- **Información pública**: **Sin medidas de protección estrictas**.
- **Información interna**: **Protección básica** mediante contraseñas y accesos controlados.

- **Información confidencial**: **Protección avanzada**, incluyendo cifrado y medidas de seguridad como autenticación multifactor.
- **Información crítica**: **Protección máxima**, con cifrado de extremo a extremo, autenticación estricta y monitoreo constante.

Política de Retención y Destrucción de la Información

- **Información pública**: Puede ser **eliminada** cuando ya no sea relevante o cuando la Institución decida discontinuarla.
- **Información interna**: Retención según los requerimientos internos de la Institución, pero no más allá de lo necesario para las operaciones.
- **Información confidencial**: **Retención por plazos definidos** por la ley, y destrucción segura una vez finalizada su utilidad.
- **Información crítica**: **Retención mínima** y destrucción inmediata una vez que ya no sea necesaria, siguiendo procedimientos de destrucción segura.

VII. Retención de la Información

La **retención de la información** es un aspecto fundamental para garantizar que la **Fundación Universitaria CEIPA** cumpla con los requisitos legales, normativos y operativos relacionados con la gestión de la información. Esta práctica no solo asegura la conformidad con las leyes aplicables, sino que también contribuye a una gestión eficiente de los datos, protegiendo tanto los intereses de los usuarios como los de la institución. La información debe ser mantenida durante el tiempo necesario para cumplir con los fines previstos y con las normativas legales pertinentes, evitando la retención innecesaria de datos que pueda implicar riesgos adicionales, como la exposición de datos personales.

Indicadores de Éxito y Mediciones

Para garantizar la efectividad de las políticas de retención de la información, se establecerán métricas de éxito que permitan evaluar su cumplimiento y optimizar las prácticas de gestión. Los indicadores definidos son:

Resolución de incidentes de seguridad: Al menos el 90% de los incidentes relacionados con la retención de datos deberán ser resueltos en menos de 24 horas, garantizando la protección y continuidad de las operaciones institucionales.

Cumplimiento en las capacitaciones: Más del 80% de los usuarios involucrados en la gestión de información deberán completar exitosamente las capacitaciones anuales en seguridad de datos y normativa de retención.

Evaluación periódica: Se realizarán revisiones trimestrales de los procedimientos de retención para garantizar el cumplimiento con las normativas legales y las políticas internas, identificando posibles áreas de mejora.

Los procedimientos de retención se regirán por las siguientes directrices:

1. Plazos de Retención

Los plazos de retención son establecidos con base en las regulaciones legales, normativas internas y la naturaleza de la información. Los tiempos de retención pueden variar dependiendo del tipo de información, y se establecen de la siguiente manera:

- **Información académica y administrativa de los estudiantes**:
    - **Plazo de retención**: La información académica y administrativa, que incluye expedientes académicos, actas de calificación, matrículas, evaluaciones, entre otros documentos, se mantendrá durante el tiempo requerido por la legislación educativa vigente y las normativas locales o internacionales aplicables. Generalmente, la legislación exige que se conserven al menos **10 años** después de la finalización de los estudios o de la última actualización del expediente académico. En algunos casos, los documentos pueden ser retenidos durante un período más largo si es necesario para fines legales o contractuales, como para la emisión de certificados de estudios en el futuro.
- **Información relacionada con recursos humanos**:
    - **Plazo de retención**: Los documentos laborales, como contratos, nóminas, documentos de ingreso, de salida, certificaciones, y otros relacionados con el personal, se conservarán conforme a las **leyes laborales nacionales e internacionales**. En general, esta documentación se debe conservar durante al menos **5 años** después de la finalización de la relación laboral, aunque algunos documentos específicos pueden requerir plazos más largos, dependiendo de las regulaciones locales.
- **Registros financieros y contables**:

- **Plazo de retención**: La información financiera y contable, que incluye registros de ingresos, egresos, balances, libros contables, facturación, y otros documentos fiscales, debe ser retenida durante un periodo mínimo de **5 años**. Este plazo puede extenderse si lo requiere la normativa fiscal vigente o los procedimientos de auditoría interna. Además, la legislación tributaria puede exigir la conservación de ciertos documentos durante **más de 5 años** en función de la naturaleza de los registros o de posibles auditorías fiscales.

- **Datos de comunicaciones y correo electrónico**:
  - **Plazo de retención**: Los correos electrónicos y otros registros de comunicación interna o externa, especialmente aquellos que contienen información relevante para las operaciones institucionales o que podrían tener implicaciones legales, se deben conservar según las directrices establecidas por la política interna de la institución. El plazo puede ser de **1 a 3 años**, dependiendo de la importancia y naturaleza de la comunicación.

- **Información de propiedad intelectual y contratos**:
  - **Plazo de retención**: Los contratos, acuerdos de confidencialidad, licencias y otros documentos relacionados con la propiedad intelectual y la investigación deben ser retenidos según los plazos establecidos en la legislación vigente sobre propiedad intelectual, así como en los acuerdos contractuales. En muchos casos, estos documentos deben mantenerse durante **mínimo 5 años** después de la finalización o cancelación del contrato, aunque pueden ser retenidos durante un período mayor si es necesario para la protección de los derechos de propiedad intelectual o para la resolución de posibles disputas legales.

2. Revisión Periódica

Para garantizar la **gestión adecuada de la información**, la institución llevará a cabo **revisiones periódicas** de los datos almacenados para determinar si es necesario mantenerlos, archivarlos o proceder con su eliminación. Este proceso incluye:

- **Revisión de la relevancia y necesidad de la información**:
  - Se evaluará regularmente la **relevancia continua** de la información almacenada. Algunos datos pueden volverse obsoletos o irrelevantes con el tiempo, por lo que se debe verificar si la retención sigue siendo

necesaria para cumplir con fines operativos, educativos, legales o contractuales.

- **Evaluación de la conformidad con las normativas**:
    - La institución debe asegurarse de que los plazos de retención de la información estén alineados con las regulaciones legales y políticas internas actualizadas. En caso de cambios en la legislación, los plazos de retención podrían ajustarse en consecuencia.
- **Auditorías y controles de acceso**:
    - Durante la revisión periódica, también se realizará una **auditoría de acceso** para verificar que solo el personal autorizado tenga acceso a la información sensible. Esto incluye revisar los registros de acceso y actividades para detectar accesos no autorizados o usos indebidos.
- **Procedimiento de archivado**:
    - Para aquellos documentos que deben ser conservados más allá de su período de uso regular pero que no requieren acceso frecuente, se debe implementar un **procedimiento de archivado** para asegurar que la información esté organizada y sea fácilmente recuperable cuando sea necesario, sin ocupar espacio innecesario en los sistemas operativos activos.

3. Destrucción de la Información

Una vez que los datos hayan cumplido su ciclo de vida útil y hayan superado el plazo de retención establecido, serán destruidos de manera segura. La **destrucción de la información** se llevará a cabo siguiendo procedimientos adecuados que garanticen que los datos no puedan ser recuperados o mal utilizados. Los métodos de destrucción incluyen:

- **Borrado seguro de discos y dispositivos**:
    - Para la **información electrónica**, se utilizarán herramientas de borrado seguro de discos, que aseguren que los datos sean **irrecuperables**. Esto puede incluir el uso de software especializado que sobrescribe los datos varias veces, evitando su restauración a través de métodos de recuperación.
- **Destrucción física de documentos**:

    - Los documentos en **formato físico** que contienen información confidencial serán destruidos mediante **trituración segura**. Las trituradoras utilizadas deben cumplir con los estándares internacionales de destrucción de datos, asegurando que los documentos sean irreconocibles y no puedan ser reconstruidos.

- **Destrucción de dispositivos y soportes de almacenamiento**:
    - Los dispositivos de almacenamiento, como discos duros, cintas, tarjetas de memoria o dispositivos portátiles, serán destruidos o desmagnetizados de forma que no pueda recuperarse la información almacenada. En caso de que la destrucción no sea físicamente posible, se recurrirá al **cifrado** completo antes de proceder con la eliminación.
- **Proceso documentado**:
    - Todo el proceso de destrucción de la información será **documentado** para asegurar que se cumpla con las políticas y que no se haya retenido información innecesaria. Esto incluirá la fecha y el método de destrucción, así como la identificación de la persona o el equipo responsable.
- **Destrucción de información de terceros**:
    - Cuando la información que debe ser destruida pertenece a **terceros** (como proveedores o colaboradores externos), se asegurará que estos sigan los mismos procedimientos de destrucción segura. Se establecerán **acuerdos contractuales** que garanticen que la destrucción de la información por parte de terceros se haga conforme a los mismos estándares de seguridad y privacidad de la institución.

4. Excepciones a la Destrucción de la Información

En algunos casos, puede haber **excepciones** a la destrucción de la información, como:

- **Requisitos legales o contractuales**: Si existe un requerimiento legal o contractual que exija la conservación de ciertos documentos más allá del plazo habitual, la información será **retenida** durante el tiempo necesario para cumplir con dicha obligación.
- **Investigaciones en curso**: Si la información está involucrada en **investigaciones o litigios**, no se procederá a su destrucción hasta que la

situación esté resuelta, o hasta que se determine que la destrucción no afectaría el proceso.

VIII. Fases de Implementación de Políticas de Seguridad de la Información

1. Planeación: Análisis de riesgos, identificación de activos clave y planificación de medidas de seguridad adecuadas

La fase de **planeación** es crucial porque establece las bases para la implementación efectiva de las políticas de seguridad de la información. En esta etapa, se lleva a cabo un análisis profundo de los riesgos y se planifican las medidas adecuadas para mitigar dichos riesgos. Los principales componentes de esta fase incluyen:

- **Análisis de riesgos**: Se identifican y evalúan los posibles riesgos a los que la información y los sistemas de la institución podrían estar expuestos. Esto incluye amenazas internas y externas, como ataques cibernéticos, fallas del sistema, pérdida de datos y accesos no autorizados. Se realiza una evaluación de impacto para determinar el daño potencial que cada riesgo podría causar en términos de privacidad, integridad y disponibilidad de la información.
- **Identificación de activos clave**: Se realiza un inventario completo de todos los activos de información esenciales para la institución, tales como bases de datos, sistemas de gestión académica, correos electrónicos institucionales, aplicaciones, equipos y redes. Cada activo se clasifica según su importancia para las operaciones de la institución y se determina su nivel de protección necesario.
- **Gestión de cambios tecnológicos:**
    - **Evaluación de nuevas tecnologías:** Antes de implementar nuevos sistemas o herramientas, se debe realizar un análisis exhaustivo de sus riesgos y beneficios. Este proceso incluye pruebas de compatibilidad, impacto en la seguridad de la información, y cumplimiento normativo.
    - **Plan de migración:** Para la transición a nuevas tecnologías, se desarrollará un plan detallado que asegure la continuidad operativa. Este incluirá medidas para minimizar interrupciones, garantizar la

integridad de los datos y capacitar al personal en el uso de las nuevas herramientas.

    - **Monitoreo de obsolescencia tecnológica:** Identificar equipos, sistemas o aplicaciones que hayan alcanzado el final de su ciclo de vida útil y planificar su reemplazo oportuno para evitar brechas de seguridad.

- **Planificación de medidas de seguridad**: Basándose en los resultados del análisis de riesgos y la identificación de activos clave, se diseñan medidas de seguridad específicas. Estas incluyen políticas de control de acceso, protección de datos, medidas de recuperación ante desastres, estrategias de encriptación y el establecimiento de reglas sobre el uso de dispositivos móviles y portátiles. Además, se define un plan de respuesta ante incidentes que detalle cómo actuar en caso de brechas de seguridad.
- **Definición de objetivos claros**: Se establecen objetivos de seguridad concretos, medibles y alineados con los requisitos regulatorios y las necesidades de la institución. Los objetivos podrían incluir la reducción de riesgos específicos, la mejora de la protección de datos personales, la prevención de accesos no autorizados o la mejora de la disponibilidad de los servicios clave.

2. Implementación: Ejecución de medidas de protección, control de acceso y gestión de información de acuerdo con los lineamientos de la política

La fase de **implementación** consiste en llevar a cabo las acciones que fueron planificadas en la fase anterior. Esta etapa implica la ejecución de las medidas de protección establecidas, la configuración de los sistemas, la capacitación de los usuarios y la integración de las políticas de seguridad en las operaciones diarias de la institución. Los elementos clave de esta fase son:

- **Ejecución de medidas de protección**: Las políticas de seguridad diseñadas se implementan en los sistemas tecnológicos de la institución. Esto incluye la instalación de software de seguridad, como antivirus, firewalls y herramientas de cifrado, así como la configuración de sistemas de autenticación y control de acceso. La infraestructura tecnológica se ajusta para garantizar que se cumpla con los requisitos establecidos en la fase de planeación.
- **Control de acceso**: Se establece un sistema robusto de control de acceso para garantizar que solo los usuarios autorizados puedan acceder a información y

sistemas sensibles. Esto incluye la implementación de políticas de contraseñas seguras, la autenticación multifactor (MFA), y la asignación de privilegios según el rol de cada usuario. Se configurarán permisos de acceso a la información y se implementarán mecanismos de monitoreo para detectar intentos de acceso no autorizado.

- **Gestión de la información**: Se adoptan medidas de protección para asegurar que la información esté disponible, íntegra y confidencial. Esto incluye la clasificación de la información según su sensibilidad, el cifrado de datos sensibles tanto en reposo como en tránsito, y la implementación de procesos para la **retención de la información** de acuerdo con las políticas de la institución y las regulaciones externas. Asimismo, se garantizará la correcta gestión de copias de seguridad (backups) y la creación de procedimientos claros para la recuperación ante incidentes.
- **Capacitación de usuarios**: Se implementan programas de capacitación y sensibilización sobre seguridad de la información para todos los usuarios, asegurando que todos entiendan las políticas y prácticas de seguridad de la institución. Esto incluye la formación sobre el uso adecuado de los sistemas, el manejo seguro de la información y la identificación de amenazas.

3. Monitoreo y auditoría: Supervisión continua de la seguridad de la información, registro de accesos y revisión de auditorías para detectar incidentes

La fase de **monitoreo y auditoría** es fundamental para asegurar que las políticas de seguridad se estén aplicando correctamente y para detectar de manera temprana cualquier incidente de seguridad. Los principales componentes de esta fase incluyen:

- **Monitoreo continuo**: Se implementan herramientas de monitoreo para supervisar en tiempo real el estado de los sistemas y las redes de la institución. Esto incluye la detección de comportamientos anómalos, como accesos no autorizados, uso indebido de la red, y la identificación de vulnerabilidades que puedan ser explotadas. El monitoreo también abarca la actividad de los usuarios, como intentos fallidos de inicio de sesión y cambios en la configuración de los sistemas.
- **Registro de accesos**: Se establece un sistema de **registro de auditoría** para registrar todas las actividades relevantes de los usuarios, administradores y sistemas. Esto incluye el acceso a información confidencial, el uso de

aplicaciones y las modificaciones en los sistemas. Estos registros permiten realizar un seguimiento detallado de las acciones realizadas, facilitando la detección y análisis de incidentes de seguridad.

- **Revisión de auditorías**: Los registros de auditoría son revisados regularmente para identificar patrones de acceso sospechosos o cualquier actividad que pueda indicar un incidente de seguridad. Esta revisión ayuda a detectar vulnerabilidades antes de que se conviertan en amenazas reales. Además, se generan informes de auditoría periódicos que se presentan a la alta dirección para su análisis.
- **Detección de incidentes de seguridad**: Se implementan sistemas automáticos de alerta que notifican a los equipos de seguridad sobre cualquier actividad sospechosa. Las alertas pueden incluir intentos de acceso no autorizado, malware detectado o violaciones de políticas de seguridad. Esta información es crucial para una respuesta rápida ante incidentes.

4. Revisión continua: Evaluación periódica de las políticas y procedimientos para adaptarlos a nuevos riesgos o cambios regulatorios

La **revisión continua** es una fase crítica para garantizar que las políticas y medidas de seguridad sigan siendo efectivas a lo largo del tiempo, especialmente en un entorno tecnológico y normativo que está en constante cambio. Los aspectos clave de esta fase incluyen:

- **Evaluación periódica**: Se programan revisiones periódicas de las políticas de seguridad y los procedimientos implementados para evaluar su efectividad. Esto incluye realizar auditorías internas y externas, revisar incidentes previos, y analizar las lecciones aprendidas para mejorar las políticas. También se evalúa el cumplimiento con las regulaciones locales e internacionales sobre protección de datos y privacidad.
- **Adaptación a nuevos riesgos**: A medida que emergen nuevas amenazas cibernéticas y cambian las condiciones tecnológicas, las políticas de seguridad deben ser ajustadas para hacer frente a esos riesgos. Por ejemplo, si surgen nuevas vulnerabilidades en el software utilizado por la institución, se deben actualizar las políticas y los controles de seguridad para mitigar el riesgo.
- **Cumplimiento de normativas**: Los cambios regulatorios, como nuevas leyes de protección de datos o requisitos específicos para la seguridad de la

información, deben ser monitoreados y las políticas deben ajustarse para garantizar el cumplimiento continuo. La alta dirección y los responsables de seguridad trabajan estrechamente con el departamento legal para asegurarse de que todas las regulaciones se cumplan de manera adecuada.

- **Mejora continua**: Con base en los resultados de las evaluaciones periódicas, se identifican áreas de mejora y se ajustan las políticas, procedimientos y controles para optimizar la seguridad de la información. Esto incluye la incorporación de nuevas tecnologías, herramientas de seguridad y mejores prácticas que ayuden a mitigar los riesgos de manera más eficiente.
- **Planes de contingencia específicos:** Se desarrollarán planes detallados para la continuidad del negocio en áreas críticas como sistemas académicos, pagos, comunicaciones internas, y gestión de datos. Estos planes incluirán acciones específicas para minimizar interrupciones y asegurar que los servicios esenciales sigan operativos durante emergencias.
- **Simulacros regulares:** La institución implementará simulacros periódicos para probar la eficacia de los planes de contingencia y la capacidad de respuesta ante incidentes. Estos simulacros involucrarán a todos los departamentos, evaluando tiempos de recuperación, coordinación interdepartamental, y la adecuación de los recursos disponibles.
- **Redundancia en sistemas críticos:** Para garantizar la disponibilidad de información clave, se adoptará la estrategia de redundancia, que incluye respaldos en sistemas alternativos y el uso de tecnología basada en la nube para proteger datos y operaciones esenciales.
- **Evaluación de la resiliencia organizacional:** Se realizarán auditorías específicas para medir la capacidad de recuperación de la institución frente a incidentes, revisando el desempeño de los simulacros y los resultados de las estrategias de contingencia implementadas.
- **Mejoras derivadas de simulacros e incidentes:** Basándose en los aprendizajes obtenidos de simulacros y revisiones post-incidentes, los planes de contingencia y los procedimientos serán ajustados continuamente para adaptarse a nuevos riesgos o cambios en el entorno tecnológico y normativo.

IX. Políticas Específicas Recomendadas para la Implementación de Controles de Seguridad de la Información

1. Control de acceso

El control de acceso es uno de los pilares fundamentales para garantizar la seguridad de los sistemas de información. A continuación, se detallan las medidas y recomendaciones clave para su implementación efectiva:

- **Autenticación robusta de usuarios**: La autenticación es el primer nivel de protección contra el acceso no autorizado. Se deben implementar contraseñas fuertes, que deben cumplir con criterios mínimos de complejidad, como longitud mínima de 8 caracteres, la inclusión de al menos una letra mayúscula, una letra minúscula, un número y un carácter especial. Se recomienda el uso de **autenticación de dos factores (2FA)** para garantizar una capa adicional de seguridad. Esto puede incluir el uso de aplicaciones de autenticación (como Google Authenticator o Microsoft Authenticator) o la validación mediante un mensaje SMS o correo electrónico.
- **Asignación de privilegios según roles**: La asignación de privilegios debe basarse en el principio de **mínimo privilegio**, lo que significa que cada usuario debe tener acceso únicamente a los sistemas y recursos necesarios para realizar su trabajo. Esto se debe gestionar a través de **roles y perfiles de acceso** definidos de acuerdo con las responsabilidades del usuario (por ejemplo, usuario regular, administrador, supervisor, etc.). Además, deben implementarse políticas para realizar revisiones periódicas de los accesos y roles, asegurando que los permisos asignados sigan siendo apropiados.
- **Control de acceso físico**: El acceso físico a los sistemas y equipos debe ser restringido a personal autorizado, con medidas como **tarjetas de identificación**, **biometría**, o sistemas de **códigos de acceso**. Los dispositivos físicos, como servidores y estaciones de trabajo, deben estar en áreas seguras y protegidas, y los accesos deben ser registrados y monitoreados.
- **Monitoreo y control continuo**: La implementación de sistemas de monitoreo en tiempo real es crucial para detectar intentos de acceso no autorizado o comportamientos sospechosos. Se debe contar con herramientas que registren y generen alertas sobre cualquier actividad de acceso inusual.

2. Gestión de activos

La gestión adecuada de los activos de información es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información institucional. Las siguientes acciones son clave para su protección:

- **Identificación de activos críticos**: Todos los activos de información (servidores, bases de datos, aplicaciones, redes, dispositivos de almacenamiento, etc.) deben ser debidamente identificados y clasificados en función de su importancia para la organización. Estos activos deben ser catalogados en un inventario completo y actualizado, que incluya la ubicación física de los equipos y los datos que contienen.
- **Protección de activos**: Los activos críticos deben ser protegidos mediante controles específicos. Esto incluye:
    - **Cifrado de datos**: Tanto los datos en reposo (almacenados en discos duros o servidores) como los datos en tránsito (enviados a través de la red) deben estar cifrados utilizando estándares de cifrado modernos (como AES-256) para proteger la información contra accesos no autorizados.
    - **Control de acceso**: Solo el personal autorizado debe tener acceso a los activos críticos. Debe garantizarse que se implementen medidas de control de acceso físico y lógico adecuadas.
    - **Protección contra malware**: Todos los sistemas que almacenan o procesan información crítica deben tener un software antivirus y antimalware actualizado, que se actualice automáticamente para protegerse contra nuevas amenazas.
- **Ciclo de vida de los activos**: Cada activo debe contar con un plan de gestión que abarque desde su adquisición hasta su disposición. Esto incluye la **actualización regular** de los activos (como parches de seguridad) y la **eliminación segura** de equipos y medios de almacenamiento obsoletos o que ya no sean necesarios.

3. Auditoría y monitoreo

La auditoría y monitoreo continuo son fundamentales para detectar y prevenir incidentes de seguridad, garantizando una respuesta temprana ante posibles amenazas. Las siguientes acciones son clave:

- **Identificación de amenazas emergentes:** Incorporar el monitoreo y análisis de nuevas amenazas en ciberseguridad, tales como:
    - **Inteligencia artificial generativa:** Uso de algoritmos avanzados para generar ataques personalizados, como phishing automatizado y creación de malware adaptativo.
    - **Dispositivos IoT (Internet de las cosas):** Supervisar vulnerabilidades en dispositivos conectados que podrían ser explotados como puntos de entrada para ataques.
    - **Técnicas de deepfake:** Analizar riesgos asociados con la manipulación de datos e identidades mediante tecnología de deep learning.
- **Monitoreo especializado:** Implementar herramientas que permitan la detección proactiva de estas amenazas, generando alertas automáticas y priorizando eventos de alta criticidad. Esto incluye el uso de sistemas avanzados de detección de intrusos (IDS) y análisis de comportamiento de red.
- **Capacitación para identificar amenazas:** Formar al personal en la detección temprana de señales relacionadas con nuevas técnicas de ataque, como correos fraudulentos sofisticados o tráfico anómalo generado por dispositivos IoT comprometidos.
- **Revisión periódica de registros:** Asegurar que los informes de auditoría incluyan indicadores de actividad sospechosa relacionados con estas amenazas emergentes, proporcionando información clave para ajustar los controles de seguridad de manera preventiva.

- **Registro detallado de actividades**: Se deben generar y almacenar registros de todas las actividades de los usuarios en los sistemas críticos, incluidos los intentos de acceso, las modificaciones en los archivos y bases de datos, y las transacciones realizadas. Los registros deben incluir:

    - **Fecha y hora exacta** de las acciones realizadas.

    - **Identificación del usuario** que realizó la acción.

    - **Detalles de la acción** (por ejemplo, acceso, modificación, eliminación, etc.).

- **Monitoreo en tiempo real**: Se deben implementar sistemas de **monitoreo en tiempo real** para detectar patrones de actividad sospechosos o inusuales que puedan indicar un incidente de seguridad (como intentos de acceso no autorizado o picos en el uso de recursos). Las herramientas de monitoreo deben generar alertas automáticas que sean analizadas por personal de TI o de seguridad.

- **Revisión periódica de auditorías**: Los registros y logs generados deben ser revisados de manera periódica para identificar tendencias o incidentes que hayan pasado desapercibidos. Además, los registros deben almacenarse de manera segura y tener un periodo de retención determinado, acorde con las normativas legales.
- **Auditorías internas y externas**: Se deben realizar auditorías periódicas internas y externas para evaluar la efectividad de los controles de seguridad implementados y asegurarse de que se cumplan las políticas de seguridad. Esto incluye auditorías de acceso, auditorías de uso de la red y auditorías de sistemas.

4. Gestión de incidentes

La gestión adecuada de incidentes de seguridad es esencial para minimizar los impactos negativos en la seguridad de la información. Las políticas de gestión de incidentes deben establecer los siguientes pasos:

- **Establecimiento de un equipo de respuesta a incidentes (IRT)**: Se debe formar un equipo especializado para responder a incidentes de seguridad. Este equipo debe contar con personal capacitado en la gestión de incidentes, incluyendo roles específicos para la **detección**, **respuesta** y **recuperación** ante incidentes.
- **Protocolos claros de notificación**: Todos los empleados, estudiantes y proveedores deben ser instruidos sobre cómo notificar inmediatamente cualquier incidente de seguridad o actividad sospechosa. Esto incluye la creación de una línea de comunicación directa con el equipo de TI o el equipo de seguridad. Adicionalmente se establece lo siguiente:
    - Se utilizarán plantillas estándar para notificar incidentes menores y mayores, asegurando que toda la información relevante sea comunicada de manera rápida y precisa.
    - Ejemplo de notificación de incidente menor:
        - Asunto: Notificación de Incidente Menor
        - Cuerpo del Mensaje: "Se informa que el día [fecha] se detectó un incidente menor relacionado con [descripción breve]. El equipo técnico ya ha tomado las medidas necesarias para resolverlo. Si tiene preguntas o necesita más detalles, por favor contacte a [responsable]."

    - Ejemplo de notificación de incidente mayor
        - Asunto: Alerta: Incidente de Seguridad Mayor Detectado
        - Cuerpo del Mensaje: "El día [fecha], se identificó un incidente de seguridad mayor que afecta [descripción del área o sistema afectado]. Actualmente, el Equipo de Respuesta a Incidentes (IRT) está trabajando para mitigar el impacto y restaurar la normalidad. Mantendremos informada a la comunidad con actualizaciones periódicas. Para consultas, contacte a [responsable]."
- **Lineamientos de comunicación:**
    - Garantizar que los responsables de comunicación interna transmitan los mensajes según la gravedad del incidente, utilizando los canales oficiales como correo institucional, tablones digitales o plataformas de colaboración interna.
    - Asegurar que las notificaciones sean claras, breves y contengan
        - Descripción del incidente.
        - Estado actual (resuelto, en mitigación, investigando).
        - Impacto estimado.
        - Contactos de soporte o responsables.
- **Actualizaciones periódicas:**
    - Para incidentes en curso, emitir actualizaciones periódicas hasta su resolución, proporcionando detalles adicionales cuando sea relevante.
    - Las actualizaciones se enviarán cada [intervalo de tiempo], dependiendo de la naturaleza y el impacto del incidente.
- **Lecciones aprendidas:**
    - Al cierre del incidente, se compartirá un reporte final con las partes interesadas que incluya las acciones tomadas, impacto mitigado y recomendaciones para prevenir incidentes futuros.
- **Evaluación de incidentes**: Una vez notificado un incidente, debe realizarse una **evaluación rápida** para determinar su gravedad y el impacto potencial en la organización. Se debe clasificar el incidente según su naturaleza (por ejemplo,

acceso no autorizado, pérdida de datos, ataque de malware, etc.) y su impacto (bajo, medio, alto).

- **Resolución y mitigación**: Dependiendo de la naturaleza del incidente, se deben tomar medidas correctivas para **mitigar el daño** y **restaurar la operación** normal lo más rápido posible. Esto puede incluir la **desconexión** de sistemas comprometidos, el bloqueo de cuentas de usuario, la restauración de datos desde copias de seguridad, etc.
- **Documentación y reporte**: Todos los incidentes deben ser documentados de manera detallada, incluyendo el análisis, las decisiones tomadas, las acciones correctivas implementadas y cualquier lección aprendida. Esto ayudará a mejorar las medidas de seguridad y a evitar futuros incidentes similares.
- **Revisión post-incidente**: Después de la resolución de un incidente, se debe realizar una **revisión post-incidente** para evaluar la respuesta y determinar si se debe ajustar alguna política, procedimiento o tecnología para prevenir incidentes similares en el futuro.

X. Responsables y Responsabilidades

1. Alta Dirección

La alta dirección de la Fundación Universitaria CEIPA tiene la responsabilidad última de garantizar que la seguridad de la información sea una prioridad estratégica dentro de la Institución. Las responsabilidades clave de la alta dirección incluyen:

- **Compromiso con la seguridad de la información**: Asegurar que la seguridad de la información sea considerada una prioridad organizacional. La alta dirección debe demostrar liderazgo activo, promoviendo la importancia de la seguridad de la información dentro de la Institución y garantizando el cumplimiento de las políticas establecidas.
- **Asignación de recursos**: Garantizar que la Fundación Universitaria CEIPA disponga de los recursos financieros, humanos y tecnológicos necesarios para implementar las medidas de seguridad de la información de forma efectiva. Esto incluye la asignación de presupuesto para la formación, actualización de infraestructuras y el mantenimiento de sistemas seguros.

- **Cumplimiento de normativas y regulaciones**: Asegurar que la Institución cumpla con todas las normativas legales y regulatorias relacionadas con la seguridad de la información, la privacidad de los datos y la protección de la información personal y confidencial.
- **Evaluación y gestión de riesgos**: Aprobar la evaluación periódica de riesgos relacionada con la seguridad de la información y asegurar que se implementen las medidas adecuadas para mitigar dichos riesgos. La alta dirección debe revisar las auditorías y los informes de incidentes de seguridad.
- **Aprobación de políticas**: Aprobar la Política de Seguridad y Privacidad de la Información, así como las políticas asociadas, y asegurarse de que se implementen correctamente en toda la organización. De igual manera, la alta dirección debe fomentar la actualización continua de estas políticas en respuesta a cambios tecnológicos, amenazas emergentes o cambios regulatorios.
- **Cultura organizacional de seguridad**: Promover una cultura organizacional de seguridad a través de la sensibilización y capacitación continua en seguridad de la información, garantizando que todos los niveles de la organización comprendan sus responsabilidades y la importancia de proteger la información.
- **Gestión de incidentes de alto nivel**: En caso de incidentes de seguridad de alto impacto o brechas significativas en la seguridad, la alta dirección será responsable de la toma de decisiones clave, incluyendo la comunicación con las partes interesadas, la implementación de medidas correctivas y la supervisión de la respuesta.
- **Informe y rendición de cuentas**: Asegurar que la alta dirección reciba informes periódicos sobre el estado de la seguridad de la información, incluyendo las auditorías, incidentes, riesgos identificados y el progreso de la implementación de políticas.

2. Dirección de Tecnologías de la Información (TI)

- Implementar, monitorear y mantener las políticas y controles de seguridad de la información.
- Asegurar el cumplimiento de las políticas de seguridad dentro de todos los sistemas tecnológicos.

- Proporcionar asistencia técnica y capacitación continua a todos los usuarios en cuanto a las buenas prácticas de seguridad.

3. Comité de Seguridad de la Información

- Establecer las directrices específicas y las mejores prácticas en cuanto a la seguridad de la información.
- Realizar auditorías periódicas y análisis de riesgos.
- Desarrollar planes de acción frente a incidentes de seguridad y garantizar la capacitación constante del personal en seguridad de la información.

4. Usuarios (Estudiantes, Colaboradores, Proveedores)

- Cumplir con las políticas, procedimientos y controles definidos por la Fundación Universitaria CEIPA.
- Informar inmediatamente cualquier incidente de seguridad o violación de las políticas.
- Asegurar la protección de las credenciales de acceso y evitar el acceso no autorizado a los sistemas.

XI. Capacitación y Sensibilización en Seguridad de la Información

La **Fundación Universitaria CEIPA** reconoce que la seguridad de la información no solo depende de la infraestructura tecnológica, sino también de la conciencia y formación de sus usuarios. Por ello, se llevará a cabo un programa continuo de **capacitación y sensibilización** dirigido a todos los usuarios de la institución (colaboradores, estudiantes, proveedores, etc.) con el fin de promover buenas prácticas y prevenir incidentes relacionados con la seguridad de la información. Las actividades de capacitación estarán estructuradas en diferentes niveles, según el perfil y las responsabilidades de cada usuario. Los niveles son:

- **Directivos:** La capacitación para los directivos se enfocará en riesgos estratégicos, cumplimiento normativo y toma de decisiones informadas. Los temas incluirán:

    - Evaluación de riesgos en ciberseguridad desde una perspectiva organizacional.
    - Políticas de cumplimiento y regulaciones legales aplicables a la seguridad de datos.
    - Planificación estratégica para la continuidad del negocio y manejo de incidentes de alto impacto.
    - Supervisión de las auditorías de seguridad y análisis de incidentes para la mejora continua.
- **Personal Operativo:** Este nivel cubrirá las prácticas de seguridad aplicables al manejo cotidiano de información y sistemas tecnológicos. Los temas incluirán:
    - Uso seguro de contraseñas y autenticación multifactorial.
    - Identificación y prevención de correos fraudulentos (phishing) y archivos maliciosos.
    - Manejo adecuado de información confidencial y datos personales en sistemas internos.
    - Procedimientos de respuesta rápida ante incidentes menores en su área de trabajo.
- **Estudiantes y Terceros:** La capacitación para estudiantes y terceros tendrá un enfoque de concienciación y protección básica de datos. Los temas incluirán:
    - Buenas prácticas en el uso de plataformas académicas y correos institucionales.
    - Reconocimiento de amenazas comunes en ciberseguridad, como intentos de suplantación de identidad.
    - Protección de información personal en redes públicas y dispositivos no seguros.
    - Responsabilidades al interactuar con sistemas de la Institución y manejo ético de datos académicos.
- **Formato y Evaluación:** Cada nivel de capacitación será impartido a través de los siguientes formatos adaptados a las necesidades de los usuarios:
    - Seminarios presenciales y talleres específicos por área
    - Cursos en línea con módulos interactivos diseñados para cada nivel.
    - Simulacros prácticos de incidentes de seguridad según el nivel de responsabilidad.
    - Evaluaciones periódicas para medir la efectividad de la capacitación y hacer ajustes necesarios.

1. Capacitación en el uso adecuado de los sistemas tecnológicos

La capacitación sobre el uso adecuado de los sistemas tecnológicos de la institución es un componente clave para garantizar que todos los usuarios manejen los sistemas de forma segura. La capacitación incluirá, entre otros temas:

- **Manejo seguro de contraseñas**: Los usuarios serán capacitados sobre la importancia de usar contraseñas robustas, cómo crear contraseñas seguras, y cómo mantenerlas de manera confidencial. Se les instruirá también en el uso de herramientas de gestión de contraseñas para evitar contraseñas débiles o reutilizadas.
- **Autenticación multifactor (MFA)**: Se proporcionará formación sobre el uso de sistemas de autenticación de múltiples factores, explicando cómo configurar y usar la autenticación en dos o más fases para acceder a sistemas y servicios críticos.
- **Uso seguro de aplicaciones y plataformas en línea**: La capacitación incluirá el uso adecuado y seguro de las plataformas tecnológicas utilizadas en la institución (sistemas de gestión académica, correo institucional, bases de datos, etc.). Esto incluye identificar y evitar comportamientos de riesgo, como hacer clic en enlaces sospechosos o descargar archivos de fuentes no verificadas.
- **Prácticas de seguridad en el manejo de correos electrónicos**: Se dará formación sobre cómo identificar correos electrónicos de phishing, adjuntos maliciosos, y enlaces sospechosos. Los usuarios aprenderán a verificar la autenticidad de las comunicaciones recibidas.
- **Uso adecuado de los dispositivos y redes institucionales**: Instrucción sobre cómo utilizar correctamente los dispositivos de la institución (computadoras, laptops, tablets, teléfonos móviles) de manera que se minimicen riesgos de seguridad. Se incluirá la importancia de **bloquear dispositivos** cuando no estén en uso y de **mantener actualizado el software** para evitar vulnerabilidades.

2. Sensibilización sobre la importancia de proteger los datos personales y académicos

Uno de los mayores activos de la Fundación Universitaria CEIPA son sus datos, tanto personales como académicos. La sensibilización de todos los usuarios sobre la importancia de proteger esta información es fundamental para cumplir con las

normativas de privacidad y proteger la confidencialidad de la comunidad educativa. La sensibilización incluirá:

- **Protección de la privacidad**: Se impartirán charlas y sesiones informativas sobre la importancia de proteger la información personal y académica de los estudiantes, profesores y personal administrativo. Los usuarios serán sensibilizados sobre los riesgos de la exposición indebida de datos personales, tanto dentro como fuera de la institución.
- **Cumplimiento de la normatividad**: Los usuarios serán informados sobre las leyes y regulaciones locales e internacionales relacionadas con la protección de datos personales, como la Ley 1581 de 2012 en Colombia y el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, entre otras. Se explicarán los derechos de los individuos sobre sus datos y las responsabilidades de la institución en cuanto a la protección de la privacidad.
- **Confidencialidad en el manejo de información académica**: Se brindará formación sobre la **confidencialidad** en el tratamiento de la información académica (notas, calificaciones, historiales académicos, etc.). Se destacará la importancia de no compartir esta información sin autorización expresa y de manejarla de forma adecuada en los sistemas de la institución.
- **Normas de privacidad en el uso de dispositivos móviles**: Se brindarán pautas para el uso de dispositivos móviles personales y dispositivos de la institución en lo que respecta a la protección de datos personales y académicos. Esto incluirá cómo evitar que la información confidencial sea expuesta a través de redes Wi-Fi públicas, el uso de aplicaciones no autorizadas, o el almacenamiento en dispositivos inseguros.

3. Actualización constante sobre nuevas amenazas y mejores prácticas en ciberseguridad

La **ciberseguridad** es un campo en constante evolución debido a las amenazas cada vez más sofisticadas. Para garantizar que los usuarios de la Fundación Universitaria CEIPA estén al tanto de los riesgos más recientes y de las mejores prácticas en seguridad, se llevará a cabo:

- **Entrenamiento sobre amenazas cibernéticas emergentes**: Se ofrecerán cursos y seminarios periódicos sobre nuevas amenazas de ciberseguridad, tales como ransomware, ataques de phishing, ataques de ingeniería social y

malware avanzado. Los usuarios serán capacitados para reconocer y protegerse ante estas amenazas.

- **Simulacros de incidentes de seguridad**: La institución organizará simulacros de incidentes de seguridad (como phishing o malware) para poner a prueba la respuesta de los usuarios ante ataques reales. Estos simulacros permitirán que los usuarios practiquen las mejores respuestas ante situaciones de riesgo y aprendan de manera práctica cómo mitigar incidentes.
- **Actualización continua de contenido educativo**: Los materiales de capacitación, como guías, videos, infografías y seminarios, serán actualizados regularmente para abordar las amenazas y vulnerabilidades emergentes. Esto incluye proporcionar información actualizada sobre **software de seguridad**, **pautas de navegación segura**, y el uso adecuado de **redes sociales**.
- **Charlas y talleres con expertos en seguridad**: Se organizarán eventos con expertos en ciberseguridad para compartir las mejores prácticas, herramientas y tecnologías emergentes en la protección de la información. Estas actividades brindarán a los usuarios la oportunidad de aprender directamente de profesionales del sector y mantenerse al día con las tendencias globales en seguridad.

4. Evaluación y seguimiento de la efectividad de la capacitación

Para garantizar que la capacitación y sensibilización en seguridad de la información sean efectivas, la institución llevará a cabo las siguientes acciones:

- **Evaluación periódica de conocimientos**: Los usuarios serán evaluados periódicamente mediante encuestas, cuestionarios y simulaciones para medir su comprensión de los temas tratados en las capacitaciones. Esto permitirá identificar áreas de mejora y ajustar el contenido de los programas de formación.
- **Análisis de incidentes**: El análisis de incidentes de seguridad reportados (por ejemplo, intentos de phishing exitosos o brechas de privacidad) se utilizará para ajustar y mejorar las estrategias de capacitación y sensibilización. Se revisarán las estadísticas y las causas subyacentes de los incidentes para identificar debilidades en los procesos de formación.
- **Feedback y retroalimentación de usuarios**: Se incentivará a los usuarios a proporcionar retroalimentación sobre las sesiones de capacitación y

sensibilización, lo cual permitirá a la institución mejorar constantemente la calidad de los programas y su efectividad en el refuerzo de buenas prácticas.

5. Formato de la capacitación

Las actividades de capacitación y sensibilización estarán disponibles en una variedad de formatos, que incluirán:

- **Sesiones presenciales**: Talleres y seminarios que se llevarán a cabo en las instalaciones de la institución.
- **Formación en línea**: Cursos en línea, módulos interactivos y webinars que permitirán a los usuarios capacitarse en su propio horario y ritmo.
- **Materiales de autoaprendizaje**: Guías, tutoriales y videos educativos que los usuarios podrán consultar de forma autónoma en cualquier momento.
- **Boletines informativos**: La institución enviará boletines informativos periódicos sobre nuevas amenazas y mejores prácticas en seguridad de la información, de forma que todos los miembros estén al tanto de cualquier cambio relevante.

XII. Modificaciones

La Fundación Universitaria CEIPA se reserva el derecho de actualizar, modificar o complementar esta política en cualquier momento con el fin de adaptarla a cambios normativos, mejoras en los procesos institucionales o nuevas necesidades operativas.

Las modificaciones serán notificadas a todos los usuarios a través de los canales oficiales de comunicación de la institución, garantizando que la información se entregue de manera clara, precisa y con la debida antelación. En caso de que los cambios impliquen ajustes significativos en los derechos y obligaciones de los usuarios, se proporcionará un período de transición razonable para su adopción.

Se recomienda a los usuarios revisar periódicamente esta política para estar informados sobre posibles actualizaciones y asegurarse de su cumplimiento.

Esta política de Seguridad y Privacidad de la Información proporciona las directrices necesarias para garantizar la protección de la información, el cumplimiento de las normativas vigentes y la continuidad de las actividades de la Fundación Universitaria

CEIPA, asegurando que todos los usuarios comprendan y asuman sus responsabilidades en el manejo seguro y adecuado de los recursos informáticos.

XIII. Políticas Específicas de Tecnologías de la Información (TI)

La Fundación Universitaria CEIPA ha establecido directrices específicas para el uso de la plataforma de TI con el fin de garantizar la seguridad de la información, la confidencialidad, la integridad y la disponibilidad de los recursos digitales. Estas políticas se aplican a todos los usuarios de la plataforma de TI de la Institución, incluidos estudiantes, egresados, profesores, colaboradores, contratistas, consultores, proveedores y clientes.

1. Acceso y Control de Acceso

- Cada usuario recibirá un identificador único que le permitirá acceder a los recursos y sistemas de información, según el perfil asignado.
- La Dirección de TI es responsable de actualizar y mantener esta política conforme a las mejores prácticas de seguridad.
- Se implementará la autenticación multifactor para accesos sensibles.
- Los usuarios deben cambiar sus contraseñas regularmente y seguir lineamientos de seguridad para su creación y gestión.

2. Uso Aceptable y Uso Prohibido

Se espera que los usuarios hagan un uso responsable de la plataforma de TI, lo que implica:

- Mantener la confidencialidad de sus credenciales de acceso.
- Usar software con licencia adquirida por la Institución.
- Proteger la información y evitar la instalación de software sin autorización.
- No acceder a sitios web con contenido ilegal o inadecuado.
- No usar recursos de TI para actividades personales o lucrativas sin autorización.

3. Uso de la Red e Internet

- Las redes institucionales están destinadas a actividades académicas y administrativas.
- El acceso a Internet debe realizarse a través de los canales seguros establecidos por la Institución.
- Se prohíbe el uso de herramientas que comprometan la seguridad de la red.
- Se monitoreará el uso de la red para prevenir accesos no autorizados.

4. Seguridad en el Correo Electrónico

- El correo institucional debe usarse para actividades académicas y laborales.
- Se prohíbe enviar correos masivos no autorizados o cadenas de mensajes.
- No se deben abrir enlaces o adjuntos de correos sospechosos.
- Se recomienda no utilizar el correo institucional para registros en sitios web externos.

5. Almacenamiento y Protección de la Información

- Toda información debe almacenarse en OneDrive o en carpetas de Teams.
- No se debe almacenar información en dispositivos personales o no autorizados.
- La Dirección de TI monitoreará el almacenamiento de datos para evitar fugas de información.
- Se prohibe la publicación de archivos ejecutables en espacios compartidos.

6. Control de Incidentes y Seguridad

- Todos los incidentes de seguridad deben reportarse de inmediato a la Dirección de TI.
- Se implementarán auditorías periódicas para evaluar la seguridad de los sistemas.
- Se aplicarán medidas correctivas ante cualquier vulnerabilidad detectada.
- Se restringirán medios de almacenamiento removibles para prevenir filtraciones.

7. Revisión y Cumplimiento

- Todos los usuarios deben cumplir con estas políticas para garantizar la seguridad de la información.
- El incumplimiento podrá acarrear sanciones disciplinarias o legales.
- Se realizarán capacitaciones periódicas en seguridad de la información