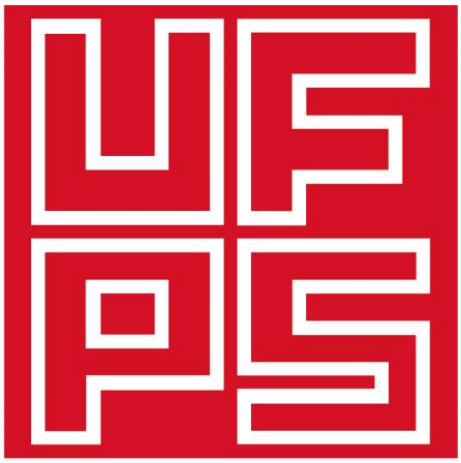
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN V.1



Universidad Francisco de Paula Santander

Ocaña - Colombia

Vigilada Mineducación

www.ufpso.edu.co

Universidad Francisco de Paula Santander
Ocaña - Colombia
Vigilada Mineducación
NIT. 800 163 130 - 0

O-DP-OPL-0052
1.02.00.00 21,03

Ocaña, 1 de abril de 2024

Magister
ANTÓN GARCÍA BARRETO
Jefe de División de Sistemas
Universidad Francisco de Paula Santander Ocaña

Asunto: Confirmación de Aprobación

Cordial saludo:

Me permito informarle que el COMITÉ INSTITUCIONAL DE GESTION Y DESEMPEÑO según consta en *el Acta 0002 del 20 de marzo de 2024*, APROBO el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información presentados por el Jefe de División de Sistemas el día 20 de marzo de 2024.

Por lo tanto, se solicita continuar con el trámite respectivo.

Cordialmente,

Original firmado en la oficina.
THOMAS E GUERRERO B
Secretario Comité Institucional de Gestión y Desempeño

Copia: anton@ufpso.edu.co
teguerrerob@ufpso.edu.co
cxtovaro@ufpso.edu.co
divisionsistemas@ufpso.edu.co
acpenarandag@ufpso.edu.co

Transcriptor: Lisbeth Maryure Gallardo Ropero

Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
Línea gratuita nacional: 01 8000 121 022 - PBX: (+57) (7) 569 00 88
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
SC-CER102673

CONTENIDO

1. PRESENTACIÓN 4
2. INTRODUCCIÓN 5
3. OBJETIVO 7
OBJETIVOS ESPECÍFICOS 7
4. ALCANCE 8
5. NORMATIVIDAD 9
6. DEFINICIONES 11
7. ESTRATEGIAS 15
8. RESPONSABILIDADES 16
9. EVALUACIÓN Y MEJORA CONTINUA 17
10. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 18
11. CONCLUSIÓN 20

1. PRESENTACIÓN

La información de la Universidad Francisco de Paula Santander Ocaña se ha reconocido como un activo valioso, y a medida que los sistemas de información apoyan cada vez más los procesos de la Universidad, en especial los procesos misionales, se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. Es así, que la seguridad de la información se convierte en prioridad, encaminando todos los esfuerzos para la preservación, aseguramiento y cumplimiento de medidas y procedimientos para protegerla, fundamentados en los tres principios de la seguridad informática: Confidencialidad, integridad y disponibilidad.

La implementación de la seguridad y privacidad de la Información en la Institución es una necesidad para ofrecer servicios de calidad, basados en un adecuado tratamiento de la información, aplicando normas para la protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información. El componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se administra tenga controles de seguridad y privacidad, de tal manera que la interacción de información con el ciudadano, otras entidades y las empresas privadas sean confiables.

Es así, como la Institución presenta el siguiente documento como una herramienta que le permitirá establecer los lineamientos y contar con una guía para la protección de la información a su cargo. En este, se define un portafolio de proyectos o actividades que tienen por objetivo lograr la implementación y mejoramientos continuo en materia de gestión y seguridad de la información.

2. INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones –MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. Una de las estrategias lideradas por este ministerio es la de Gobierno Digital, la cual tiene como objetivo garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, eficiente y más transparente, y que en su componente de seguridad y privacidad de la información, suministra el Modelo de Seguridad y Privacidad de la Información –MSPI, que a su vez promueve la preservación de la confidencialidad e integridad de los datos, permitiendo garantizar su privacidad mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas, basado en la guía del Modelo de Seguridad y Privacidad de la Información (MSPI) aprobada por el MinTIC, para iniciar el proceso de implementación del Plan de Seguridad y Privacidad de la Información, el cual sugieren cinco etapas para llevar acabo el ciclo de funcionamiento del modelo de operación: Etapa diagnostica, etapa planificación, implementación, evaluación de desempeño y mejora continua.

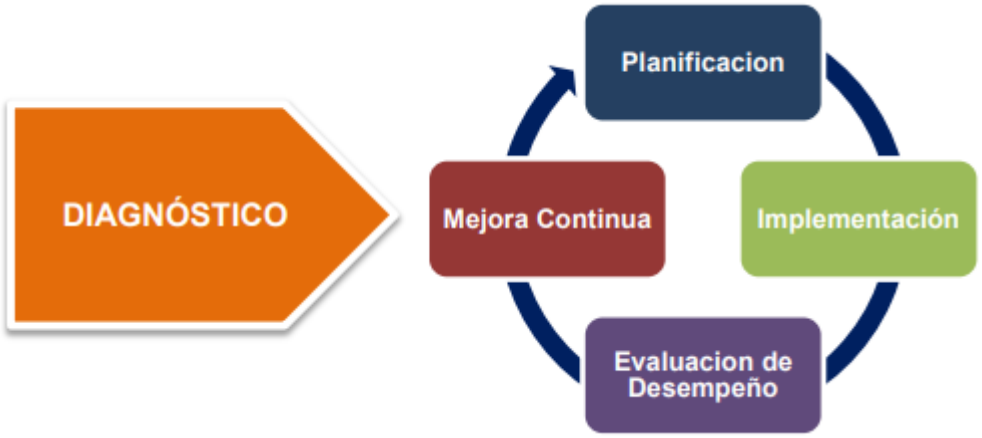


Figura 1. Fuente MINTIC, Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

La Universidad Francisco de Paula Santander seccional Ocaña define el Plan de Seguridad y Privacidad de la Información, con el objetivo de fortalecer la integridad, confidencialidad y disponibilidad de los activos de información, reduciendo así los riesgos a los que la universidad está expuesta. Este plan se basa en las estrategias de seguridad digital definidas en el Modelo de Seguridad y Privacidad de la Información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia.

Acorde a la resolución 500 de 2021 y alineado a las actividades descritas dentro del MPSI, la UFPS Ocaña define estrategias específicas o ejes que contribuyen a la

protección de la información y mitiguen los posibles riesgos asociados a daños; los ejes establecidos para tal fin son: liderazgo de seguridad de la información, gestión de riesgos, concientización, implementación de controles y gestión de incidentes. En donde para cada eje se definen proyectos y productos esperados a los cuales se les asignará un presupuesto aproximado, se les establecerá un cronograma de actividades y por último se les realizará seguimiento si es que estos son aprobados por la alta dirección.

Es importante señalar, que la UFPS seccional Ocaña al finalizar cada vigencia, realizará la actualización del cronograma, incorporando el estado del avance de los proyectos formulados, si se cumplieron o se plantean aplazamientos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la Universidad. Con esto se requiere enfatizar, que la Institución trabaja en el fortalecimiento de la seguridad de la información, al reconocer que es uno de los recursos de mayor valor, y debe ser debidamente protegida frente a las innumerables amenazas a las que se encuentra expuesta, garantizando la protección y la privacidad de los datos de los ciudadanos y funcionarios de la Universidad, todo esto acorde con lo expresado en la legislación colombiana.

Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
Línea gratuita nacional: 01 8000 121 022 - PBX: (+57) (7) 569 00 88
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co

3. OBJETIVO

Establecer el Plan de seguridad y privacidad de la Información de la Universidad Francisco de Paula Santander seccional Ocaña, que fortalezca la integridad, confidencialidad y disponibilidad de los activos de información, con el fin de reducir los riesgos a los que la Universidad está expuesta, a partir de la implementación de las estrategias de seguridad digital teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información emanado por el MinTIC.

OBJETIVOS ESPECÍFICOS

- Garantizar la integridad de la información académica, administrativa y de investigación de la Universidad Francisco de Paula Santander Seccional Ocaña.
- Proteger la confidencialidad de los datos sensibles de estudiantes, profesores, personal administrativo y demás partes interesadas.
- Asegurar la disponibilidad de los sistemas y servicios de información críticos para el funcionamiento de la universidad.
- Cumplir con las normativas y regulaciones vigentes en materia de seguridad y privacidad de la información.

4. ALCANCE

El presente documento establece el alcance del Plan de Seguridad y Privacidad de la Información para la Universidad Francisco de Paula Santander seccional Ocaña, con el objetivo de fortalecer la integridad, confidencialidad y disponibilidad de los activos de información. Este plan busca reducir los riesgos a los que la Universidad está expuesta mediante la implementación de estrategias de seguridad digital, en consonancia con el Modelo de Seguridad y Privacidad de la Información emanado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

El alcance de este plan incluye:

- Evaluación de Riesgos: Identificar y analizar los riesgos relacionados con la seguridad y privacidad de la información en la Universidad, teniendo en cuenta las amenazas internas y externas.
- Diseño de Políticas y Procedimientos: El desarrollo de políticas y procedimientos específicos que regulen la adecuada gestión de la información y consideren aspectos como el acceso, clasificación, almacenamiento y transmisión de datos.
- Implementar controles de seguridad: Implementación de medidas técnicas y organizativas para proteger los recursos de información, tales como firewalls, cifrado de datos, autenticación multifactor y capacitación del personal en seguridad informática.
- Monitoreo y Gestión de Incidentes: Establecer mecanismos para la detección temprana de incidentes de seguridad y respuesta y recuperación ante posibles violaciones de seguridad o datos.
- Sensibilización y Formación: Realizar actividades de sensibilización y formación en toda la comunidad universitaria para promover una cultura de seguridad de la información y fomentar las mejores prácticas en la gestión de datos.
- Revisión y Mejora Continua: Establecer un proceso de revisión periódica del plan de seguridad y privacidad de la información con el objetivo de identificar áreas de mejora y actualizar las medidas de seguridad en respuesta a cambios en el entorno técnico y regulatorio.

El alcance de este plan se extiende a todos los activos de información de la Universidad Francisco de Paula Santander seccional Ocaña, así como a todos los miembros de la comunidad universitaria que interactúan con dicha información, incluyendo estudiantes, docentes, administrativos y personal contratista.

5. NORMATIVIDAD

1. Directiva Presidencial 02, de febrero 24 de 2022: Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC).
2. Decreto 338 de marzo 8 de 2022: Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
3. Resolución 746 de 2022: Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021.
4. Decreto 767 de 2022: Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
5. Directiva Presidencial 03 de 2021: Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos
6. Resolución 500 de 2021: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
7. Resolución 1519 de 2020: Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
8. Conpes 3995 de 2020: Política Nacional De Confianza y Seguridad Digital.
9. Resolución 0312 de 2019: Por la cual se adopta el Modelo Integrado de Planeación y Gestión (MIPG) para las entidades del orden nacional, territorial y de los órganos autónomos e independientes. Esta resolución establece lineamientos para la implementación de planes de seguridad y privacidad de la información en las entidades públicas, con el fin de garantizar la protección de los activos de información.
10. Resolución 2140 de 2017: Por la cual adopta el Modelo Integrado de Planeación y Gestión y se crean algunas instancias administrativas al interior del Ministerio de Ambiente y Desarrollo Sostenible y del Fondo Nacional Ambiental, y se dictan otras disposiciones.
11. Conpes 3854 de 2016: Política Nacional de Seguridad Digital. Busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia.
12. Decreto 103 de 2015: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

13. Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
14. Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Este decreto establece los procedimientos para la protección de los datos personales, incluyendo aspectos como la recolección, almacenamiento, uso, circulación y supresión de dicha información.
15. Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales en Colombia. Esta ley establece los principios, deberes y derechos en materia de protección de datos personales, los cuales deben ser considerados en el manejo de la información por parte de la Universidad.
16. Guía de Buenas Prácticas para la Seguridad de la Información en Colombia: Documento elaborado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), que proporciona lineamientos y recomendaciones para la gestión de la seguridad de la información en organizaciones públicas y privadas en el país.
17. Modelo de Seguridad y Privacidad de la Información del MinTIC: Marco de referencia que establece los lineamientos y estándares para la implementación de medidas de seguridad de la información en entidades públicas y privadas en Colombia, con el fin de proteger la integridad, confidencialidad y disponibilidad de los activos de información.
18. Constitución Política de Colombia 1991: Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.

6. DEFINICIONES

- Activos de información: Pueden incluir datos personales de estudiantes, docentes, administrativos y contratistas, registros académicos, información financiera, investigaciones, propiedad intelectual, sistemas informáticos y cualquier otro recurso o registro que sea importante para el funcionamiento y la reputación de la Universidad Francisco de Paula Santander seccional Ocaña.

- Amenaza: Una situación externa que está fuera del control de la empresa y que puede afectar las operaciones.

- Análisis de Riesgos: La etapa en la gestión de riesgos donde la probabilidad y el impacto de un riesgo se determinan antes de que se establezcan los controles.

- Aceptar riesgo: Una opción de gestión que acepta la pérdida residual esperada si el riesgo ocurre.

- Auditoría de seguridad de la información: Es un proceso sistemático para evaluar la efectividad de los controles de seguridad de la información y garantizar el cumplimiento de las políticas y procedimientos establecidos. Las auditorías pueden incluir la revisión de registros de seguridad, pruebas de penetración, evaluaciones de vulnerabilidades y revisión de políticas y procedimientos.

- Causa: Los medios, circunstancias y/o factores que crean el riesgo.

- Calificación del riesgo: evaluación de la probabilidad de que se produzca un riesgo y el posible impacto de su realización.

- Compartir o transferir riesgos: Opciones de gestión que determinan la transferencia o reparto de pérdidas resultantes de la realización de riesgos con otras organizaciones a través de figuras como subcontratación, seguros y ubicaciones alternativas.

- Confidencialidad de la información: En el contexto de la Universidad, la confidencialidad de la información se refiere a proteger los datos sensibles o privados de acceso no autorizado. Esto puede incluir información personal de los estudiantes, docentes, administrativos y contratistas registros académicos, resultados de investigaciones en curso y cualquier otra información que deba mantenerse privada para proteger la privacidad y los derechos de las personas involucradas.

- Consecuencia: El probable impacto si el riesgo ocurre.

- Contexto estratégico: son condiciones internas y ambientales que pueden crear oportunidades o crear eventos que afecten negativamente el logro de la misión y los objetivos de una institución.

- Control: Acción o conjunto de acciones diseñadas para minimizar la probabilidad de que ocurra un riesgo o los efectos causados por su realización.

- Control Preventivo: Una medida o grupo de medidas que elimina o reduce una fuente de riesgo. El objetivo es reducir la probabilidad de que ocurra un riesgo.

- Control correctivo: Medida o conjunto de medidas para eliminar o reducir las consecuencias de un riesgo. El objetivo es reducir el alcance del impacto del riesgo.

- Controles de seguridad de la información: Son medidas técnicas y organizativas diseñadas para proteger los activos de información contra amenazas y riesgos. Estos controles pueden incluir medidas físicas, como el control de acceso a las instalaciones, así como medidas lógicas, como la encriptación de datos, la autenticación de usuarios y la implementación de firewalls y sistemas de detección de intrusiones.

- Debilidades: Condiciones internas que una empresa puede controlar y que pueden afectar sus operaciones.

- Disponibilidad de la información: La disponibilidad de la información garantiza que los datos estén accesibles y utilizables cuando sea necesario por parte de los usuarios autorizados. Esto implica prevenir interrupciones no planificadas en los sistemas o servicios que podrían causar la inaccesibilidad de la información, asegurando que los recursos tecnológicos y los procedimientos operativos estén diseñados para mantener la continuidad del acceso a la información crítica.

- Estrategias de seguridad digital: Estas estrategias abarcan todas las acciones planificadas y medidas técnicas y organizativas implementadas para proteger los activos de información de la Universidad contra los riesgos de seguridad identificados. Esto puede incluir la implementación de firewalls, sistemas de detección de intrusiones, políticas de acceso y autenticación, capacitación del personal en seguridad informática y la elaboración de planes de respuesta a incidentes, entre otras medidas. El objetivo final es fortalecer la seguridad de la información y reducir la exposición de la Universidad a posibles amenazas y vulnerabilidades.

- Evaluación de Riesgos: Resultados de evaluación cuantitativa de probabilidad cruzada y de impacto para determinar áreas donde existen riesgos.

- Evitar el riesgo: Una opción de gestión que determina el desarrollo de medidas para prevenir la realización de un riesgo reforzando los controles identificados.

- Frecuencia: Ocurrencia de un evento. Se expresa como el número de veces que ocurre un evento dentro de un período de tiempo determinado.

- Gestión de riesgos: Es el proceso de identificar, evaluar y mitigar los riesgos potenciales para la seguridad de la información. Esto implica determinar las amenazas que podrían afectar los activos de información, evaluar la probabilidad y el impacto de estas amenazas, y luego implementar medidas para reducir o eliminar los riesgos identificados.

- Identificación de riesgos: La etapa de la gestión de riesgos donde se determinan los riesgos. Clasificados según sus causas (relacionadas con factores de riesgo externos e internos), consecuencias y tipo de riesgo definido.

- Impacto: medidas cuantitativas y cualitativas. Estimación de posibles impactos, realización de riesgos.

- Integridad de la información: La integridad de la información implica garantizar que los datos no hayan sido alterados de manera no autorizada durante su creación, almacenamiento, transmisión o procesamiento. Esto significa que la información debe permanecer completa, precisa y libre de modificaciones no autorizadas o corruptas que puedan afectar su exactitud o utilidad.

- Mapa de Riesgos: Documento que muestra sistemáticamente la evolución de las etapas de la gestión de riesgos.

- Materialización del riesgo: La ocurrencia de un riesgo identificado.

- Opciones de gestión: Cómo gestionar el riesgo después de la evaluación de los controles definidos (adoptar, reducir, evitar compartir o transferir los riesgos restantes).

- Plan de Seguridad y Privacidad de la Información: Este es un documento formal que describe las políticas, procedimientos, controles y recursos necesarios para proteger los activos de información de una organización, como la Universidad Francisco de Paula Santander seccional Ocaña. Este plan aborda aspectos clave de la seguridad y privacidad de la información, incluyendo la gestión de riesgos, la clasificación de datos, el control de acceso, la gestión de incidentes y la capacitación del personal.

- Políticas de seguridad de la información: Son declaraciones formales que establecen las reglas y directrices para proteger los activos de información de la

Universidad. Estas políticas pueden incluir la asignación de responsabilidades, la definición de los requisitos de seguridad, la gestión de contraseñas, el uso aceptable de la tecnología, entre otros aspectos relevantes para garantizar la seguridad y privacidad de los datos.

- Probabilidad: medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

- Procedimiento: conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.

- Proceso: conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

- Riesgos de seguridad de la información: Estos riesgos pueden incluir amenazas como el acceso no autorizado, el robo de datos, el malware, los errores humanos, los desastres naturales y otros eventos que podrían comprometer la integridad, confidencialidad o disponibilidad de la información. Identificar y evaluar estos riesgos es fundamental para implementar medidas de seguridad efectivas.

7. ESTRATEGIAS

1. Implementación de controles de acceso: Se establecerán políticas de acceso basadas en roles y privilegios para garantizar que únicamente el personal autorizado pueda acceder a la información pertinente a su labor.

2. Encriptación de datos: Se aplicará encriptación a los datos sensibles tanto en reposo como en tránsito, utilizando algoritmos robustos y certificados de seguridad reconocidos.

3. Actualización y parcheo de sistemas: Se establecerá un programa regular de actualización y parcheo de sistemas y aplicaciones para corregir vulnerabilidades conocidas y mitigar riesgos de seguridad.

4. Monitoreo y detección de amenazas: Se implementará un sistema de monitoreo continuo de la red y los sistemas de información para detectar y responder de manera proactiva a posibles amenazas y ataques cibernéticos.

5. Capacitación y concientización: Se llevarán a cabo programas de capacitación y concientización sobre seguridad de la información dirigidos al personal docente, administrativo y estudiantil, con el fin de promover buenas prácticas y prevenir incidentes de seguridad.

6. Respuesta a incidentes: Se establecerá un plan de respuesta a incidentes que incluya procedimientos claros para la gestión y mitigación de incidentes de seguridad, así como la notificación oportuna a las partes afectadas y las autoridades correspondientes.

8. RESPONSABILIDADES

El proceso de Sistema de Información, Telecomunicaciones y Tecnologías de la Universidad será la responsable de coordinar la implementación del Plan de MSPI y asegurar su cumplimiento.

Los responsables de cada área o dependencia serán los encargados de garantizar que se apliquen las políticas y controles establecidos en el plan dentro de sus respectivas áreas de competencia.

Todo el personal de la universidad deberá cumplir con las políticas y procedimientos definidos en el Plan de MSPI, así como participar activamente en las actividades de capacitación y concientización.

Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
Línea gratuita nacional: 01 8000 121 022 - PBX: (+57) (7) 569 00 88
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co

9. EVALUACIÓN Y MEJORA CONTINUA

Se realizarán evaluaciones periódicas del Plan de MSPI para identificar áreas de mejora y ajustar las estrategias de seguridad de acuerdo con las nuevas amenazas y tecnologías emergentes.

10. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Actividad	Tarea por desarrollar	Responsable	Fecha Inicio	Fecha Final
Actualización del inventario de activos de TI	Actualizar el inventario de activos de información de TI	SITT Procesos Institucionales	01/01/2024	31/12/2026
Gestión de incidentes de seguridad de la información	Gestionar los incidentes de seguridad de la información recopilando y analizando las evidencias para determinar la causa raíz, el alcance y el impacto del incidente.	SITT	01/01/2024	31/12/2026
Revisión del manual políticas de seguridad y privacidad de la información	Revisar el manual de políticas de seguridad y privacidad de la información para asegurar su relevancia y efectividad en la protección de los activos de información de la Universidad.	SITT	01/01/2024	31/12/2026
Implementación de los controles del anexo A de la norma ISO 27001:2022 (93 controles)	Realizar seguimiento a los controles establecidos de acuerdo con la norma ISO 27001:2022 que sean relevantes y aplicables a la Universidad.	SITT	01/01/2024	31/12/2026
Revisión y actualización del plan de continuidad y contingencia de TI	Actualizar el plan de continuidad y contingencia de la Universidad, identificando y evaluando los posibles escenarios de interrupción, como fallos de hardware, desastres naturales, ciberataques u otros eventos adversos.	SITT	01/01/2024	31/12/2026
Análisis de vulnerabilidades de plataforma tecnológica	Realizar escaneos regulares de la plataforma tecnológica de la Universidad para identificar posibles vulnerabilidades de seguridad, explorando activos de red, sistemas operativos, aplicaciones y otros componentes tecnológicos en busca de vulnerabilidades conocidas. Una vez identificadas, se evalúa el nivel de riesgo asociado a cada vulnerabilidad y se priorizan las acciones de corrección y mitigación necesarias.	SITT	01/01/2024	31/12/2026
Sensibilización, toma de conciencia, educación y	Realizar sensibilizaciones sobre seguridad de la información y	SITT	01/01/2024	31/12/2026

formación en la seguridad de la información	apoyar en el desarrollo de pruebas de ingeniería social para evaluar el nivel de conciencia en seguridad de la información de la comunidad académica.			

11. CONCLUSIÓN

El Plan de Seguridad y Privacidad de la Información de la Universidad Francisco de Paula Santander Seccional Ocaña tiene como objetivo principal proteger los activos de información de la institución, fortaleciendo la integridad, confidencialidad y disponibilidad de estos. Su implementación contribuirá a reducir los riesgos a los que la universidad está expuesta y a garantizar el cumplimiento de las normativas y regulaciones en materia de seguridad y privacidad de la información.

Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
Línea gratuita nacional: 01 8000 121 022 - PBX: (+57) (7) 569 00 88
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co