



fodese
p

Fondo de desarrollo de la educación superior
Vinculado al Ministerio de Educación Nacional

**PLAN DE SEGURIDAD Y PRIVACIDAD
DE LA INFORMACIÓN – FODESEP 2022**

| | | | | |
|--|--|-----------------------------|--|----------------------|
| PROCESO: GESTIÓN DE CALIDAD | Fecha elaboración: 26/01/2022 | Fecha actualización: | Versión: 1 | Página 1 de 7 |
| Plan de Seguridad y Privacidad de la Información 2022 | Elaborado por: Carlos Andres Silva Moreno Profesional 3 Tecnología | | Aprobado por: Comité Institucional de Gestión y Desempeño | |
| Responsable: Carlos Andres Silva Moreno Profesional 3 Tecnología | Revisado por Gloria Eugenia Mendoza Luna, secretaria general (E) | | Código: GC-FM-012 | |

**PLAN DE SEGURIDAD Y PRIVACIDAD
DE LA INFORMACIÓN – FODESEP**

1. Introducción

El Plan de Seguridad y Privacidad de la Información del Fondo de Desarrollo de la Educación Superior FODESEP, busca aplicar los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, establecidos en los componentes de Gobierno Digital, el cual cuenta con dos componentes; TIC PARA EL ESTADO y TIC PARA LA SOCIEDAD, a su vez se tienen tres habilitadores transversales, en el cual está la Seguridad de la información, busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información –MSPI.

2. Definiciones

Para el FODESEP es muy importante dar la definición de diferentes términos técnicos, que a su vez permite que el plan de seguridad y privacidad sea más claro e incluyente.

- **INTEGRIDAD:** La información y sus métodos de procesamiento deben ser completos y exactos.
- **DISPONIBILIDAD:** La información y los servicios deben estar disponibles en el momento que sea requerido.
- **CONFIDENCIALIDAD:** La información debe ser accesible sólo a aquellas personas autorizadas.
- **CLASIFICACIÓN DE INFORMACIÓN:** Es la clasificación que se debe dar en función de los requisitos legales, valor, criticidad, y susceptibilidad a divulgación o modificaciones no autorizadas.
- **ACTIVOS DE INFORMACIÓN:** Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- **AVISO DE PRIVACIDAD:** Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.
- **IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN:** Es un código para ordenar y localizar los activos de información dentro del FODESEP.

| | | | | |
|--|--|-----------------------------|--|----------------------|
| PROCESO: GESTIÓN DE CALIDAD | Fecha elaboración: 26/01/2022 | Fecha actualización: | Versión: 1 | Página 2 de 7 |
| Plan de Seguridad y Privacidad de la Información 2022 | Elaborado por: Carlos Andres Silva Moreno Profesional 3 Tecnología | | Aprobado por: Comité Institucional de Gestión y Desempeño | |
| Responsable: Carlos Andres Silva Moreno Profesional 3 Tecnología | Revisado por Gloria Eugenia Mendoza Luna, secretaria general (E) | | Código: GC-FM-012 | |

- **CONTROL:** Los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **INFORMACIÓN CLASIFICADA:** Es aquella información que estando en poder o custodia de un sujeto, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado de manera motivada y por escrito, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados estipulados en el artículo 18 de la Ley 1712 de 2014 y su acceso pudiere causar un daño a los siguientes derechos: a) El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado; b) El derecho de toda persona a la vida, la salud o la seguridad; c) Los secretos comerciales, industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la Ley 1474 de 2011. d) Estas excepciones tienen una duración ilimitada y no deberán aplicarse cuando la persona natural o jurídica ha consentido en la revelación de sus datos personales o privados o bien cuando es claro que la información fue entregada como parte de aquella información que debe estar bajo el régimen de publicidad aplicable. (Artículo 6, literal c y 18 Ley 1712 de 2014).
- **INFORMACIÓN PÚBLICA RESERVADA:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía de manera motivada y por escrito, por daño a intereses públicos y bajo el cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. Se podrá negar el acceso a esta información cuando concurra una de las siguientes circunstancias y siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional: a) La defensa y seguridad nacional b) La seguridad pública c) Las relaciones internacionales. d) La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso e) El debido proceso y la igualdad de las partes en los procesos judiciales f) La administración efectiva de la justicia g) Los derechos de la infancia y la adolescencia h) La estabilidad macroeconómica y financiera del país i) La salud pública.
Se exceptúan también los documentos que contengan las opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos. (Artículo 6, literal d y artículo 19 Ley 1712 de 2014).
- **TRANSFERENCIA:** La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.
- **DATO PERSONAL:** Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley.

| | | | | |
|--|--|-----------------------------|--|----------------------|
| PROCESO: GESTIÓN DE CALIDAD | Fecha elaboración: 26/01/2022 | Fecha actualización: | Versión: 1 | Página 3 de 7 |
| Plan de Seguridad y Privacidad de la Información 2022 | Elaborado por: Carlos Andres Silva Moreno Profesional 3 Tecnología | | Aprobado por: Comité Institucional de Gestión y Desempeño | |
| Responsable: Carlos Andres Silva Moreno Profesional 3 Tecnología | Revisado por Gloria Eugenia Mendoza Luna, secretaria general (E) | | Código: GC-FM-012 | |

- **DATO PÚBLICO:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **DATO PRIVADO:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- **DATO SEMIPRIVADO:** Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.
- **DATO SENSIBLE:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
- **DOCUMENTO EN CONSTRUCCIÓN:** Es aquella información preliminar o no definitiva. (artículo 6, literal k Ley 1712 de 2014).

3. Objetivos

3.1. Objetivo General

Efectuar diversas actividades para la identificación de activos y riesgos de información ligados a los diferentes procesos que el FODESEP tiene dentro del modelo organizacional, con el fin de que se puedan medir los riesgos inherentes y residuales de la entidad.

3.2. Objetivos Específicos

- Actualizar la política de seguridad y privacidad de la información.
- Aplicar la política de seguridad y privacidad de la información del FODESEP.
- Realizar capacitación sobre la política de seguridad y privacidad de la información, a todos los funcionarios del FODESEP.
- Adecuar perfiles de riesgo con la implementación del ERP o del software de crédito y cartera.
- Ajustar los protocolos de seguridad a los requerimientos de la Superintendencia de Economía Solidaria.
- Diagnosticar el modelo de seguridad y privacidad en el FODESEP.

4. ALCANCE

| | | | | |
|--|--|-----------------------------|--|----------------------|
| PROCESO: GESTIÓN DE CALIDAD | Fecha elaboración: 26/01/2022 | Fecha actualización: | Versión: 1 | Página 4 de 7 |
| Plan de Seguridad y Privacidad de la Información 2022 | Elaborado por: Carlos Andres Silva Moreno Profesional 3 Tecnología | | Aprobado por: Comité Institucional de Gestión y Desempeño | |
| Responsable: Carlos Andres Silva Moreno Profesional 3 Tecnología | Revisado por Gloria Eugenia Mendoza Luna, secretaria general (E) | | Código: GC-FM-012 | |

| | | |
|---|--|----------------------|
|  | PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022 | Código: GC-FM-012 |
| | | Versión: 1 |
| | | Vigencia: Junio 2016 |

Que sea aplicado en todos los procesos del FODESEP y de cumplimiento por parte de todos los funcionarios, contratistas, practicantes y proveedores.

5. Responsables

Para que la administración del riesgo tenga un éxito, se debe contar con la participación activa de los directivos, funcionarios y contratistas; por esto, es preciso identificar los actores que intervienen:

- **COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO:** Sus integrantes son quienes aprueban las directrices para la seguridad y privacidad de la información de la entidad. La alta dirección es la responsable del fortalecimiento de la política de privacidad de la información.
- **Proceso Administración del Sistema Integrado de Gestión:** Sus integrantes son quienes Generan la metodología para la administración de la seguridad de la información de la Entidad, coordina, lidera, capacita y asesora en su aplicación.
- **Responsables de los procesos:** Son los encargados de Identificar, analizar, evaluar y valorar los riesgos de la entidad al menos una vez al año, (responsable de cada proceso).
- **Funcionarios y contratistas:** Deben ejecutar los controles y acciones definidas para garantizar la privacidad y seguridad de la información.
- **Control Interno:** El profesional de control interno es quien debe realizar la evaluación y seguimiento a la política, los procedimientos y los controles propios de la seguridad y privacidad de la información.

6. CICLO DE OPERACIÓN DEL MSPI

Para efectuar y ejecutar la implementación del Modelo de Seguridad y Privacidad de la Información en el FODESEP, se adopta la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos y directrices emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, a través de sus diferentes decretos, resoluciones y/o leyes emitidas.

Dado lo anterior, se definen las siguientes fases de implementación del MSPI: 1. Diagnosticar 2. Planear 3. Hacer 4. Verificar 5. Actuar

| | | | | |
|--|--|-----------------------------|--|----------------------|
| PROCESO: GESTIÓN DE CALIDAD | Fecha elaboración: 26/01/2022 | Fecha actualización: | Versión: 1 | Página 5 de 7 |
| Plan de Seguridad y Privacidad de la Información 2022 | Elaborado por: Carlos Andres Silva Moreno Profesional 3 Tecnología | | Aprobado por: Comité Institucional de Gestión y Desempeño | |
| Responsable: Carlos Andres Silva Moreno Profesional 3 Tecnología | Revisado por Gloria Eugenia Mendoza Luna, secretaria general (E) | | Código: GC-FM-012 | |



Ilustración 1 Ciclo de operación Modelo de Seguridad y Privacidad de la Información

Fuente: <http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html>

7. Cronograma.

- Archivo Adjunto Excel.

8. Seguimiento Y Evaluación

Al término de cada ítem se efectuará una reunión con el comité de gestión es quien hace el seguimiento, con el fin de presentar el informe del avance del proyecto y a su evaluar todos los pasos que se han ido realizado.

| | | | | |
|--|--|-----------------------------|--|----------------------|
| PROCESO: GESTIÓN DE CALIDAD | Fecha elaboración: 26/01/2022 | Fecha actualización: | Versión: 1 | Página 6 de 7 |
| Plan de Seguridad y Privacidad de la Información 2022 | Elaborado por: Carlos Andres Silva Moreno Profesional 3 Tecnología | | Aprobado por: Comité Institucional de Gestión y Desempeño | |
| Responsable: Carlos Andres Silva Moreno Profesional 3 Tecnología | Revisado por Gloria Eugenia Mendoza Luna, secretaria general (E) | | Código: GC-FM-012 | |

| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - FODESEP 2022 | | | | | | | | | | | | | | | |
|--|---|-----------------------------|--|-------|---------|-------|-------|------|-------|-------|--------|------------|---------|-----------|-----------|
| COMPONENTE | ACTIVIDADES | RESPONSABLE | META / ENTREGABLE | Enero | Febrero | Marzo | Abril | Mayo | Junio | Julio | Agosto | Septiembre | Octubre | Noviembre | Diciembre |
| Planeación Sistema de Gestión de Seguridad de la Información: Documentación, procedimientos y requerimientos pertinentes a la seguridad de la información, establecidos por El Ministerio de las Tecnologías de la Información y las Telecomunicaciones y el Ministerio de Educación Nacional. (El alcance del MSPi permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad) | Mantenimiento de la plataforma | Profesional 3 de Tecnología | Contratos de soporte | | | | | | | | | | | | |
| | Revisar los procedimientos del proceso de informática y tecnología y socializarlos. | Profesional 3 de Tecnología | Socializar los Procedimientos revisados | | | | | | | | | | | | |
| | Diagnosticar los riesgos en seguridad y privacidad de la información. | Profesional 3 de Tecnología | Mapa de riesgos de gestión actualizado | | | | | | | | | | | | |
| | Diagnostico para la transición de IPv4 a IPv6. | Profesional 3 de Tecnología | Contrato de Diagnostico | | | | | | | | | | | | |
| Implementación Sistema de Gestión de Seguridad de la Información: Implementar y operar la política, controles, procesos y procedimientos del Subsistema de Seguridad y Privacidad de la Información. (Esta fase le permitirá a la Entidad, llevar a cabo la implementación de la planificación realizada en la fase anterior del MSPi) | Aplicar la política de seguridad y privacidad de la información | Profesional 3 de Tecnología | Asistencia a capacitación de buen uso de la política de seguridad y privacidad de la información | | | | | | | | | | | | |
| | Realizar mantenimiento a la Plataforma tecnológica en funcionamiento | Profesional 3 de Tecnología | Reporte de incidentes, fichas técnicas e informes finales de los contratos de soporte | | | | | | | | | | | | |
| | Realizar la actualización a los procedimientos del proceso de informática y tecnología y socializarlos. | Profesional 3 de Tecnología | Procedimientos actualizados, publicados y socializados en el sistema de gestión de calidad. | | | | | | | | | | | | |

| | | | | |
|--|--|-----------------------------|--|----------------------|
| PROCESO: GESTIÓN DE CALIDAD | Fecha elaboración: 26/01/2022 | Fecha actualización: | Versión: 1 | Página 7 de 7 |
| Plan de Seguridad y Privacidad de la Información 2022 | Elaborado por: Carlos Andres Silva Moreno Profesional 3 Tecnología | | Aprobado por: Comité Institucional de Gestión y Desempeño | |
| Responsable: Carlos Andres Silva Moreno Profesional 3 Tecnología | Revisado por Gloria Eugenia Mendoza Luna, secretaria general (E) | | Código: GC-FM-012 | |