PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN INDER VALLEDUPAR VIGENCIA 2022

Contenido

COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de del Instituto de Deporte, Recreación y Actividad Física - INDER Valledupar, se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI); así mismo, se compromete a revisar el avance de la implementación del SGSI de manera periódica y también garantizará los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

INTRODUCCIÓN

El MinTic – Ministerio de las Tecnologías y las comunicaciones, como entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones es consecuente que las entidades públicas están cada vez más expuestas a sufrir incidentes de seguridad digital, lo cual, puede afectar su funcionamiento repercutiendo en la prestación de los servicios a la ciudadanía. Razón por la cual el ministerio como entidad encargada de diseñar, adoptar y promover políticas, planes, programas y proyectos en el uso y apropiación de las TIC, establece lineamientos con el objetivo de generar confianza en el uso del entorno digital, garantizando el máximo aprovechamiento de las tecnologías de la información y las comunicaciones.

Para el Instituto de Deporte, Recreación y Actividad Física - INDER Valledupar, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados, además, el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital, de igual manera el Decreto 2106 de 2019, Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública, en el parágrafo del artículo 16 indica que (…)

Las entidades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones. (…) Teniendo en cuenta lo anterior, se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, implementando el Plan de Seguridad y Privacidad de la Información.

OBJETIVOS

OBJETIVO GENERAL

Establecer los lineamientos definidos por la Alta Dirección del Instituto de Deporte, Recreación y Actividad Física - INDER Valledupar, para la seguridad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información, las políticas de Seguridad Digital y Gobierno Digital y demás requisitos de ley y las necesidades de las partes interesadas.

OBJETIVO ESPECÍFICOS

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.

PROPÓSITOS

- Proporcionar a los sujetos obligados mecanismos, lineamientos e instrumentos de implementación claros que les permitan adoptar, implementar y apropiar el MSPI con mayor facilidad.
- Aportar en el desarrollo e implementación de la estrategia de seguridad digital de las Entidades.
- Establecer procedimientos de seguridad que permitan a las Entidades apropiar el habilitador de seguridad en la política de Gobierno Digital.
- Institucionalizar la seguridad y privacidad de la información en los procesos y procedimientos de las Entidades.
- Mediante la implementación eficiente, eficaz y efectiva del MSPI, se busca contribuir al incremento de la transparencia en la gestión pública.
- Contribuir en el desarrollo y ejecución del plan estratégico institucional, de cada entidad, a través del plan de seguridad y privacidad de la información

DEFINICIÓN

A los efectos de la presente guía se deberán atender las siguientes definiciones:

1. Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
2. Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
3. Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).
4. Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
5. Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
6. Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
7. Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
8. Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo **el** Tratamiento de datos personales (Ley 1581 de 2012, art 3)
9. Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
10. Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
11. Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
12. Control: Las políticas, 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. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
13. Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están

bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sinde los mismos (Ley 1712 de 2014, art 6)

14. Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
15. Datos Personales Públicos: 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. (Decreto 1377 de 2013, art 3)
16. Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
17. Datos Personales Mixtos: Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.
18. Datos Personales Sensibles: 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. (Decreto 1377 de 2013, art 3)
19. Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
20. Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)
21. Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
22. Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, 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, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
23. 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 por daño a

intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

24. Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.
25. Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.
26. Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
27. Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
28. Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
29. Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
30. Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
31. Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).
32. Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
33. Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
34. Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
35. Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
36. Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
37. Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).
38. Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

39. Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

MARCO JURÍDICO

Conforme con lo establecido en la normatividad vigente el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la Entidad:

1. Constitución Política de Colombia. Artículos 15, 209 y 269.
2. Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
3. Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
4. Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
5. Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
6. 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.
7. Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
8. Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
9. Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
10. Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
11. Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
12. Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
13. CONPES 3854 de 2016. Política Nacional de Seguridad digital.
14. Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
15. Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
16. Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad

digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

17. Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario

ALCANCE

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del Instituto de Deporte, Recreación y Actividad Física INDER Valledupar, con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de Instituto de Deporte, Recreación y Actividad Física – INDER Valledupar

Ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- INDER protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- INDER protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- INDER protegerá su información de las amenazas originadas por parte del personal.
- INDER protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- INDER controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- INDER implementará control de acceso a la información, sistemas y recursos de red.
- INDER garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- INDER garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- INDER garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- INDER garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

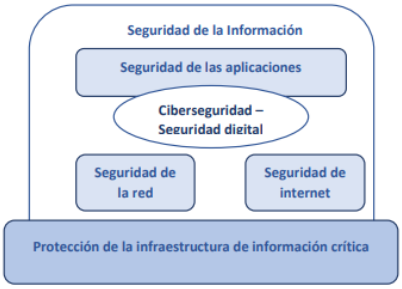
PROCESO DE IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto de Deporte, Recreación y Actividad Física – INDER Valledupar, adopta el proceso de Seguridad y Privacidad de la Información garantizando continuamente la seguridad y privacidad de la información, seguridad digital y continuidad de las operaciones de los servicios, por medio de políticas, programas, lineamiento, estrategia y actividades.

Teniendo en cuenta lo anterior, el MinTIC elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI y define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de los sujetos obligados un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. Por ello, los sujetos obligados deben abordar las siguientes fases:

1. Diagnóstico: Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.
2. Planificación: Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.
3. Operación: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.
4. Evaluación de desempeño: Determinar el sistema y forma de evaluación de la adopción del modelo.
5. Mejoramiento Continuo: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición

Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas.



Relación entre la ciberseguridad y otros ámbitos de la seguridad

Ciclo del Modelo de Seguridad y Privacidad de la Información

Imagen: resol 500 de 2021 anexo 2

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición del Instituto de Deporte, Recreación y Actividad Física – INDER Valledupar, con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

FASE 1 DIAGNOSTICO

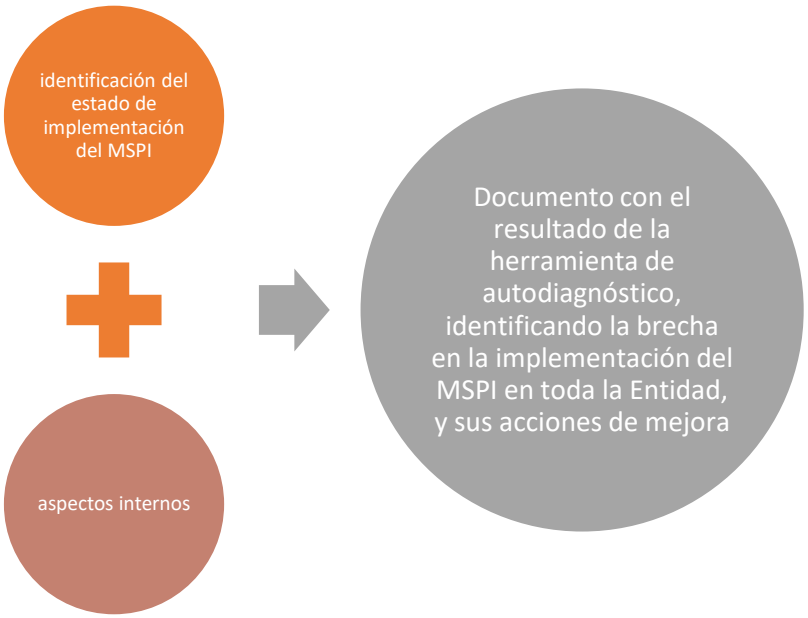
Esta fase de diagnóstico permite a los sujetos obligados establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe realizar un "Diagnóstico" utilizando el "instrumento de evaluación MSPI" con el que se identifica de forma

específica los controles implementados y faltantes y así tener insumos fundamentales para la fase de planificación.

Este autodiagnóstico se debe realizar antes de iniciar la fase de planificación, y actualizarlo posterior al término de la fase de evaluación de desempeño, esto con el fin de identificar los avances en la implementación del Modelo en la entidad, el resultado que se obtenga posterior a la fase de evaluación de desempeño será incluido como un insumo, en la fase de mejoramiento continuo

Propósito:

Identificar el nivel de madurez de seguridad y privacidad de la información en que se encuentra la Entidad, como punto de partida para la implementación del MSPI



Entradas recomendadas	Salida
Para la identificación del estado de implementación del MSPI, se debe utilizar la herramienta de autodiagnóstico del MSPI	Documento con el resultado de la herramienta de autodiagnóstico, identificando la brecha en la implementación del MSPI en toda la Entidad, y sus acciones de mejora
Revisar aspectos internos tales como el talento humano, procesos y procedimientos, estructura organizacional, cadena de servicio, recursos disponibles, cultura organizacional, entre otros.	

FASE 2. PLANIFICACIÓN

Para el desarrollo de esta fase se debe utilizar los resultados de la fase anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información con el objetivo de que la Entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI

Los documentos que se deben generar en esta fase son:

1. Alcance MSPI
2. Acto administrativo con las funciones de seguridad y privacidad de la información.
3. Política de seguridad y privacidad de la información.
4. Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información
5. Procedimiento de inventario y Clasificación de la Información e infraestructura crítica
6. Metodología de inventario y clasificación de la información e infraestructura crítica
7. Procedimiento de gestión de riesgos de seguridad de la información
8. Plan de tratamiento de riesgos de seguridad de la información
9. Declaración de aplicabilidad
10. Manual de políticas de Seguridad de la Información
11. Plan de capacitación, sensibilización y comunicación de seguridad de la información

.

Contexto

Comprensión de la organización y de su contexto

Propósito:

Conocer en detalle las características de la Entidad y su entorno, que permitan implementar el Modelo de Seguridad y Privacidad adaptado a las condiciones específicas de cada Entidad

Entradas recomendadas	Salida
Para establecer el contexto de la Entidad debe tener en cuenta los aspectos relacionados en el Manual Operativo MIPG	Documentos obligatorios: Contexto de la entidad (Política de Planeación Institucional)
Modelo estratégico, modelo de procesos, modelo de servicios y modelo organizacional siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.	

Necesidades y expectativas de los interesados

Propósito:

Conocer las expectativas que se tiene respecto a la implementación del modelo de seguridad y privacidad de la información, para asegurar que el modelo garantizará su cumplimiento

Entradas recomendadas	Salida
Comprensión de la organización y de su contexto	Documentos obligatorios: Partes interesadas. (Política de Planeación Institucional).
Plan Nacional de Desarrollo.	
Política de Gobierno Digital.	
Entrevistas con los líderes de procesos de la Entidad.	
Listado de entidades de orden nacional o territorial que se relacionan directamente el cumplimiento misional de la Entidad.	
Listado de proveedores de la Entidad.	
Listado de operadores de la Entidad.	
Normatividad que le aplique a la Entidad de acuerdo con funcionalidad respectivamente	

Definición del alcance del MSPI

Propósito:

Identificar qué información (generada o utilizada en los procesos de la Entidad) será protegida mediante la adopción del MSPI.

Entradas recomendadas	Salida
Comprensión de la organización y de su contexto (numeral 0)7.1.1 Comprensión de la organización y de su contexto	Alcance del MSPI, (Este alcance puede estar integrado al Manual del Sistema Integrado de Gestión
Necesidades y expectativas de los interesados	
Modelo de procesos, modelo organizacional, modelo de servicios y catálogo de servicios tecnológicos; siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.	
Entrevistas con los líderes de procesos de la Entidad.	

Presupuesto disponible para implementar el MSPI.	
Listado de las sedes físicas donde opera la Entidad.	

Liderazgo

Liderazgo y Compromiso

Garantizar el liderazgo y el compromiso del comité institucional de gestión y desempeño o quien haga sus veces para conseguir los objetivos definidos para la implementación del MSPI.

Entradas recomendadas	Salida
Definición del alcance del MSPI	Evidencia en el acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información.
Modelo de procesos y modelo organizacional articulado con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.	
Modelo de procesos y modelo organizacional articulado con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.	
Necesidades y expectativas de los interesados	

Roles y responsabilidades

Propósito:

Hay que asegurar que los funcionarios de la Entidad conozcan qué se espera de ellos, cuál es su impacto en la seguridad de la información y de qué manera contribuyen con la adopción del MSPI.

Entradas recomendadas	Salida
Modelo de procesos, y modelo organizacional, desarrollados para la Arquitectura Misional de la Entidad, siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.	Roles y responsabilidades
Modelo de procesos y modelo organizacional articulado con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.	

Modelo de procesos y modelo organizacional articulado con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.	
Necesidades y expectativas de los interesados	

Planificación

Identificación de activos de información e infraestructura critica

Propósito:

Estructurar una metodología que permita identificar y clasificar los activos de información

Entradas recomendadas	Salida
Modelo de procesos, y modelo organizacional, desarrollados para la Arquitectura Misional de la Entidad, siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.	Procedimiento de inventario y clasificación de la información.
Guía para la Gestión y Clasificación de Activos de Información	Documento metodológico de inventario y clasificación de la información.

Valoración de los riesgos de seguridad de la información

Propósito:

Estructurar una metodología que permita gestionar los riesgos de seguridad y privacidad de la información.

Entradas recomendadas	Salida
Directorio de servicios de componentes de información, de acuerdo con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.	Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité de coordinación de control interno.
Inventario de activos de información de la Entidad	
Proceso de valoración de riesgos de la seguridad de la información definido por medio de:	

Plan de tratamiento de los riesgos de seguridad de la información

Propósito:

Estructurar una metodología que permita definir las acciones que debe seguir la Entidad para poder gestionar los riesgos de seguridad y privacidad de la información

Entradas recomendadas	Salida
Inventario de activos de información de la Entidad.	Plan de tratamiento de riesgos, aprobado por los dueños de los riesgos y el comité institucional de gestión y desempeño
Valoración de los riesgos de seguridad de la información	

Soporte

Propósito:

Determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del MSPI.

Entradas recomendadas	Salida
Definición del alcance del MSPI	Incluir dentro de los proyectos de inversión de la Entidad aquellas actividades relacionadas con la adopción de MSPI de acuerdo con el alcance establecido.
Política de seguridad y privacidad de la información	
Roles y responsabilidades	
Plan de tratamiento de los riesgos de seguridad de la información	

Competencia, toma de conciencia y comunicación

Propósito:

Funcionarios estén al tanto de la política de seguridad y privacidad, cuál es su rol en el cumplimiento del MSPI, beneficios y consecuencias de no poner en práctica las reglas definidas en el modelo (desde el punto de vista de seguridad y privacidad de la información).

Entradas recomendadas	Salida

Manual de funciones de la Entidad.	Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital. Este se puede incluir en el Plan Institucional de Capacitaciones - PIC.
Plan de capacitación Institucional.	Plan de comunicaciones del modelo de seguridad y privacidad de la información.

FASE 3: OPERACIÓN

Planificación e implementación

Implementar los planes y controles para lograr los objetivos del MSPI

Entradas recomendadas	Salida
Valoración de los riesgos de seguridad de la información	Plan de implementación de controles de seguridad y privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable
Plan de tratamiento de los riesgos de seguridad de la información	Evidencia de la implementación de los controles de seguridad y privacidad de la información.

FASE 4: EVALUACIÓN DE DESEMPEÑO

Seguimiento, medición, análisis y evaluación

Propósito:

Evaluar el desempeño de seguridad de la información y la eficacia del MSPI.

Entradas recomendadas	Salida
Documento con los resultados de la valoración de los riesgos	Hoja de vida de indicadoress, los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el decreto 612 de 2018.
Documento con los resultados del tratamiento de riesgos de seguridad de la información	Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.
Resultado de la implementación de controles	

Auditoría Interna

Entradas recomendadas	Salida

Todos los documentos producto de las salidas de las fases anteriores del MSPI.	Resultados de las auditorías internas
El informe de los resultados de las evaluaciones independientes, seguimientos y auditorías.	No conformidades de las auditorías internas.
Informes y compromisos adquiridos en los comités institucional de gestión y desempeño.	Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información, este plan debe estar aprobado por el Comité de Coordinación de Control Interno.
El informe de los incidentes de seguridad y privacidad de la información reportados y la solución de estos.	
Informe sobre los cambios (legales, procesos, reglamentarios, regulatorios, tecnológicos, ambientales, o aquellos en el marco del contexto de la organización) en la Entidad.	
Indicadores definidos y aprobados para la evaluación del MSPI.	

Revisión por la dirección

Propósito:

Revisar el MSPI de la Entidad, por parte de la alta dirección (comité de gestión institucional), en los intervalos planificados, que permita determinar su conveniencia, adecuación y eficacia.

Entradas recomendadas	Salida
Todos los documentos del MSPI deberán ser aprobados, incluyendo los actos administrativos que se necesiten para constituirlos al interior de la Entidad.	Revisión a la implementación
Documento con los resultados del tratamiento de riesgos de seguridad de la información	Acta y documento de Revisión por la Dirección.
	Compromisos de la Revisión por la Dirección.

FASE 5: MEJORAMIENTO CONTINUO

Mejora

Propósito:

Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos.

Entradas recomendadas	Salida

Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.	Plan anual de mejora del MSPI
Resultados de auditorías y revisiones independientes al MSPI.	Acta y documento de Revisión por la Dirección.
	Compromisos de la Revisión por la Dirección.

GUÍA - ROLES Y RESPONSABILIDADES

Definición de roles y responsabilidades

INDER, como sujetos obligados deben definir internamente las responsabilidades para ejecutar las actividades específicas de seguridad de la información designando al equipo que corresponda.

El mayor aporte que genera una definición de roles es que se tendrán establecidas las tareas que realizará cada uno de los miembros del equipo del MSPI, dejando un campo muy pequeño a que se presenten imprecisiones con referencia a las responsabilidades que cada integrante tiene.

Partiendo de este punto, la entidad tendrá asegurado que cada actividad establecida dentro de la etapa de planeación del MSPI, tenga un responsable claro y de igual forma que cada uno de los miembros del equipo responsable de la ejecución entiendan claramente sus roles y responsabilidades.

Identificación de los responsables

En primer lugar, se genera la necesidad de vincular de forma más efectiva al personal de alto nivel que estará vinculado al proceso de desarrollo del MSPI en las entidades para que el apoyo se vaya garantizando desde el principio de la planeación del proyecto debe ir marcando un punto de partida de éxito con la implementación del modelo de gestión de seguridad de la información planteado para la entidad.

Los representantes de alto nivel de la entidad deben identificar y establecer, sin perjuicio de lo establecido en la Ley 489 de 1998, en el menor tiempo posible organizar el grupo de trabajo responsable para implementar el Modelo de seguridad de la información en las entidades del Estado, definiendo el perfil y rol de conformidad con lo establecido en su documento de política.

Teniendo en cuenta lo anterior, la implementación del MSPI, debe dar a conocer el perfil y responsabilidades de cada integrante.

A continuación, se proponen las siguientes actividades asociadas a la seguridad y privacidad de la información:

Responsable de Seguridad de la Información para la entidad

El responsable de Seguridad de la información será el líder de la implementación del Modelo de seguridad y privacidad de la información en la Entidad y velará por el cumplimiento de las siguientes actividades:

1. Fomentar la implementación de la Política de Gobierno Digital
2. Asesorar a la Entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información para la entidad de conformidad con la regulación vigente.
3. Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la entidad.
4. Realizar la estimación, planificación y cronograma de la implementación del MSPI.
5. Liderar la implementación y hacer seguimiento a las tareas y cronograma definido.
6. Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI.
7. Realizar el acompañamiento a los procesos y /o proyectos en materia de seguridad y privacidad de la información.
8. Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.
9. Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información.
10. Definir e implementar en coordinación con las dependencias de la Entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y contratistas.
11. Apoyar a los procesos de la Entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información.
12. Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad.
13. Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de la información.
14. Poner en conocimiento de las dependencias con competencia funcional, cuando se detecten irregularidades, incidentes o prácticas que atentes contra la seguridad y privacidad de la información de acuerdo con la normativa vigente.

Comité Institucional de Gestión y Desempeño Institucional – Comité de Seguridad y privacidad de la información

1. Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades: o Aprobación seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarios para la implementación interna de las políticas de seguridad y privacidad de la información.

- socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad.
- Aprobar acciones y mejores prácticas que en la implementación del MSPI.
- Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.

2. Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

Oficina asesora Jurídica

1. Brindar asesoría a los procesos de la Entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
2. Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
3. Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los sujetos obligados, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.
4. Representar a la Entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información.
5. Apoyar y asesorar a los procesos en la elaboración del Índice de Información

Gestión del Talento Humano

1. Controlar y salvaguardar la información de datos personales del personal de planta de la Entidad, en concordancia con la normatividad vigente.
2. Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.

Control Interno

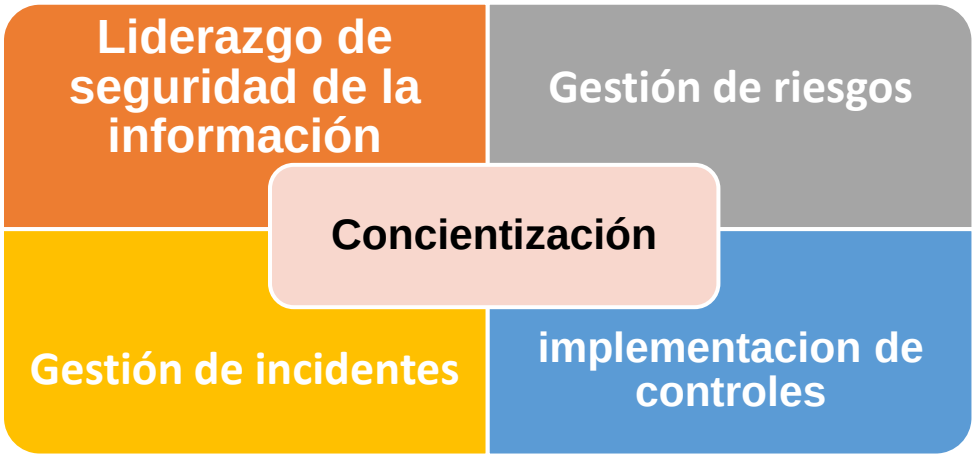
Dentro de la definición de responsables en cada uno de los Dominios entregados en el Marco de arquitectura Empresarial, está contemplado el papel del responsable de seguridad y privacidad de la información de la entidad, de esta forma se tienen las siguientes responsabilidades específicas de acuerdo con el Dominio:

DOMINIO	RESPONSABILIDADES
SERVICIOS TECNOLÓGICOS	-Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución.

	- Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. - Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. - Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias -Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. -Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
ESTRATEGIA TI	-Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.
GOBIERNO TI	-Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.
SISTEMAS DE INFORMACIÓN	-Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. - Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano.

	- Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. - Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. - Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
DE INFORMACIÓN	-Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. - Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.

ESTRATEGIAS



DESCRIPCIÓN DE LAS ESTRATEGIAS

• **Liderazgo de seguridad de la información**	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la políticas general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los jefes de las diferentes dependencias de la Entidad.
• **Gestión de riesgos**	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
• **Concientización**	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
• **Implementación de controles**	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad.
• **Gestión de incidentes**	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

Proyectos y productos

Por cada estrategia se define a modo general los proyectos a llevar a cabo y los productos esperados:

ESTRATEGIAS	PROYECTO	PRODUCTOS
Liderazgo de seguridad de la información	Desarrollar e implementar una política de seguridad Mejorar la coordinación entre el departamento de RRHH y el departamento TIC	
Gestión de riesgos	1. Identificar, valorar y clasificar los riesgos asociados a los activos de información	2. Matriz de riesgos de seguridad digital 3. Definir planes de tratamiento de riesgos
Concientización	1. Establecer desde el inicio de cada año la planeación de sensibilización para todo el año. 2. Realizar jornadas de sensibilización a todo el personal. 3. Realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializados en diferentes temas. 4. Medir el grado de sensibilización a toda la Entidad.	1. Plan de Sensibilización 2. Evidencias de las actividades desarrolladas 3. Certificaciones de cursos 4. Resultado de las encuestas de medición
Implementación de controles	1. Política de copias de seguridad 2. Clasificación de la información	
	1. Contar con una metodología de Gestión de Incidentes	2. Gestión de incidentes

ESTRATEGIAS	PROYECTO	PRODUCTOS
Gestión de incidentes		

METAS

2020		2021		2022	
Logro	**inversión**	**Logro**	**inversión**	**Logro**	**Inversión**
Construir los lineamientos técnicos e implementación de controles que se definan en el plan operacional de seguridad y privacidad de la información.	$	Implementar el 100% del Modelo de Seguridad y Privacidad de la Información y gestionar la auditoría interna de cumplimiento.	$	Mantener el funcionamiento del Modelo de seguridad y privacidad de la Información	$

CRONOGRAMA

Se define el cronograma de seguimiento a las diferentes actividades establecidas en el **plan de Seguridad y Privacidad de la información V1.0**, con la siguiente periodicidad:

1S		2S		1S		2S	
% Programado	**% Ejecutado**	**% Programado**	**% Ejecutado**	**% Programado**	**% Ejecutado**	**% Programado**	**% Ejecutado**
25		25		25		25	0

Nota: La distribución presupuestal y los responsables deben ir por actividad, atadas a actividades puntuales dentro del cronograma, no en las metas, ni con responsabilidades generales

NOMBRE	ELABORADO POR:	APROBADO POR:	VERSIÓN
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	JOSÉ LUIS PEÑARANDA TORO ING - ELECTRÓNICO	OFICINA PLANEACIÓN SILVIA OROZCO OSORIO	1.0