PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INSTITUTO DE DESARROLLO URBANO, VIVIENDA Y GESTIÓN TERRITORIAL DE CHÍA – IDUVI

SUBGERENCIA ADMINISTRATIVA Y FINANCIERA

CHÍA, CUNDINAMARCA
Fecha (enero/2025)

Carrera 8 No 14 - 20 Oficinas 301-307
TEL: 3173791170
contactenos@iduvichia.gov.co
www.iduvichia.gov.co

CONTENIDO

1. INTRODUCCIÓN. 3
2. OBJETIVO 3
2.1 OBJETIVOS ESPECÍFICOS 3
3. ALCANCE DEL DOCUMENTO. 4
4. PROCESO DE REFERENCIA 4
5. DEFINICIONES 4
6. MARCO LEGAL 5
7. EJECUCIÓN DEL PLAN 8
7.1 ESTRATEGIAS 8
7.2 IDENTIFICACIÓN DE OPORTUNIDADES Y NECESIDADES DE TI PARA LA SEGURIDAD DE LA INFORMACIÓN 8
7.3 PROYECTOS 10

1. INTRODUCCIÓN.

La seguridad y privacidad de la información es un aspecto transversal en las labores misionales y de apoyo en cualquier entidad, dado que continuamente se deben ejecutar mecanismos que permitan evitar la pérdida de integridad, confidencialidad y disponibilidad de la información en cualquier formato en la que ésta se recoja, procese y se disponga a la ciudadanía o a las diferentes partes interesadas. Conforme a lo anterior, se presenta en este documento el Plan de Seguridad y Privacidad de la información para la vigencia del año 2025 - 2027, en el cual se relacionan los objetivos, metas, estrategias e indicadores de cumplimiento de todas las actividades planeadas a ejecutar durante el año en conjunto con funcionarios y contratistas de persona natural y jurídico de la entidad y de esta manera ir aumentando el nivel de madurez de seguridad y privacidad de la información.

2. OBJETIVO

Adoptar e implementar los lineamientos del Modelo de Seguridad y Privacidad de la Información y la Estrategia de seguridad digital conforme a lo establecido por el Ministerio de las TICS con el fin de fortalecer la integridad, confidencialidad y disponibilidad de los activos de información del IDUVI y el tratamiento de sus riesgos

2.1 OBJETIVOS ESPECÍFICOS

- Definir y comunicar la Estrategia de seguridad de la información y seguridad digital.
- Definir y establecer las necesidades del IDUVI para la implementación del Sistema de Gestión de Seguridad de la Información y seguridad digital.
- Incrementar el nivel de madurez en la gestión de la seguridad de la información y seguridad digital.
- Priorizar los proyectos a implementar para la correcta implementación del Sistema de Gestión de Seguridad de la Información - SGSI y seguridad digital.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información y seguridad digital.

3. ALCANCE DEL DOCUMENTO.

El presente documento describe el plan de seguridad y privacidad, enmarcados en los objetivos, procesos, procedimientos de IDUVI, formulado con el fin de dar continuidad al proceso que busca asegurar la confidencialidad, integridad y disponibilidad de los componentes de información en la operación actual.

4. PROCESO DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- ISO/IEC 27001

5. DEFINICIONES

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Modelo de Seguridad y Privacidad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Riesgo de seguridad de la información: 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.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de gestión de seguridad de la información

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

6. MARCO LEGAL

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", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

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".

Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).

Ley 1273 de 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.

Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas.

Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se

dictan otras disposiciones.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC, se crea la agencia Nacional de espectro y se dictan otras disposiciones.

Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

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.

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.

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

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.

Decreto 0884 de 2012. Por el cual se reglamenta parcialmente la Ley 1221 del 2008.

Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de

2014 y se dictan otras disposiciones.

Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases deDatos. Artículos 25 y 26.

Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.

Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.

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 materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

Directiva 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

CONPES 3854 de 2016. Política Nacional de Seguridad Digital.

ISO 22301: Norma desarrollada por ISO que especifica los requisitos para un sistema de gestión encargado de proteger a una empresa de incidentes que provoquen una interrupción en la actividad, reducir la probabilidad de que se produzcan y garantizar la recuperación de la empresa.

ISO 27001: establece los requisitos para una gestión eficaz de los riesgos que pueden afectar a la confidencialidad, la integridad y la disponibilidad de la información.

7. EJECUCIÓN DEL PLAN

7.1 ESTRATEGIAS

- Gestión de riesgos de seguridad de la información. Esta es una actividad que tiene como punto de partida la matriz de riesgos de seguridad de la información, La actividad inicial de este frente es la revisión detallada de la matriz entregada y la identificación de los posibles controles a implementar, posteriormente las actividades resultantes serán socializadas con los líderes de proceso con el fin de obtener el consenso, aprobación y compromiso con el plan que se defina.
- Revisar, actualizar y socializar en caso de ser requerido la matriz de activos de información, esquemas de publicación, e índice de información clasificada y reservada con el fin de que los todos los procesos actualicen dichas matrices.
- Generar campañas de comunicación y sensibilización para fomentar la cultura organizacional de seguridad de la información al funcionariado, contratistas y demás colaboradores del IDUVI, a través de los canales de comunicación establecidos en la entidad.
- Elaborar un diagnóstico de seguridad y privacidad de la información, construido a través de autodiagnóstico del MSPI.

7.2 IDENTIFICACIÓN DE OPORTUNIDADES Y NECESIDADES DE TI PARA LA SEGURIDAD DE LA INFORMACIÓN

En el ejercicio de planeación de la estrategia seguridad de la información, se ha llevado a cabo la identificación de oportunidades y necesidades de TI en diferentes áreas del Instituto de Desarrollo Urbano, Vivienda y Gestión Territorial, y su alineación con la estrategia institucional, y que se registran en la siguiente tabla:

TABLA OPORTUNIDADES Y NECESIDADES DE SEGURIDAD DE TI IDENTIFICADAS

No	Oportunidad / Necesidad de TI	Estado Actual	Descripción
1	**Sistemas de seguridad**	Firewall Fortinet FortiGate 100E obsoleto, sin suscripción activa	En cuanto a seguridad ciberseguridad, la Entidad deberá contar con un firewall actualizado para garantizar la seguridad informática, detección de amenazas y mitigar los ataques externos a la red e infraestructura tecnológica de la entidad
2	**Sistema de antivirus**	Sistema de protección de antivirus Microsoft Defender Antivirus, dicha aplicación está integrada en el sistema operativo Windows	software antivirus por suscripción para proteger y detectar amenazas tanto a los servidores como los equipos de los funcionarios.
4	**Sistemas de backup**	Las copias de seguridad realizan directamente en los servidores y en medios externos	Sistema de respaldo de la información en caso de desastres o pérdida parcial. Para esto, se deberá definir la periodicidad que se tendrá en cuanto a los respaldos y a los tipos de respaldo que se requieren por parte del IDUVI. Es importante respaldar la información que se tiene a nivel de los sistemas de almacenamiento (SAN), así como de las configuraciones de hardware y software de los diferentes sistemas, pruebas en las copias de seguridad, de las configuraciones tanto de aplicaciones como de servidores y de los datos.
6	**Plan de Capacitaciones**	Las capacitaciones que se realizan están establecidas en el plan de capacitaciones de la entidad.	Capacitaciones a los funcionarios de la entidad en temas relacionados con seguridad y privacidad de la información, ciberseguridad.
7	**Datacenter Secundario en caso de desastres**	La entidad no cuenta con un datacenter secundario para la continuidad de negocio.	Teniendo en cuenta el criterio de Tier (alta disponibilidad y los beneficios de un modelo integral de servicio), idealmente se debería integrar la prestación de todos los servicios, para lo cual, la Entidad deberá centralizar los servicios de datos en un solo

			espacio. La infraestructura de cada datacenter deberá contar con sistemas de control de acceso físico y seguridad perimetral, sistemas de detección y extinción de incendios, sistema eléctrico con autonomía (sistema de adecuación eléctrica independiente para la red de servidores, sistema de redundancias N+1 para UPS, sistema de control de condiciones ambientales y el cableado estructurado (por lo menos categoría 6a), adicionalmente debe permitir que el servicio no se vea afectado debido a detenciones por operaciones de mantenimiento básicas.

7.3 PROYECTOS

Se define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

Proyecto No. 1: Implementar el Modelo de Seguridad y Privacidad de la Información	
Descripción Proyecto	Ejecutar las acciones orientadas a la implementación del Modelo de seguridad y privacidad de la información, orientadas a garantizar la disponibilidad, confidencialidad e integridad de la información, y para realizar monitoreo y acciones de mejora al cumplimiento de los lineamientos de la política de gobierno digital en la materia.

¿Para qué?	Fortalecer la gestión de seguridad y privacidad de lainformación de la entidad, enmarcados en la implementación de un 100% del Modelo de Seguridad y Privacidad de la Información, basado en la identificación y valoración de los riesgos asociados, propendiendo por la protección de la confidencialidad, integridad y disponibilidad de la Información Con el fin de implementar la estrategia de seguridad digital para la entidad, alineado las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021
¿Por qué?	Es deber del IDUVI y con el apoyo de seguridad de la información garantizar la confiabilidad, disponibilidad e integridad de los activos de información de la Entidad, en cumplimiento del marco normativo vigente y la Política Nacional de Confianza y Seguridad Digital (CONPES 3995 de 2020).
¿Cómo?	Con la definición e implementación de políticas, procedimientos, directrices, normas y leyes, con el fin de asegurar la información del IDUVI, la ejecución de proyectos de adquisición y de herramientas o de implementación de normas o buenas prácticas y actividades inherentes al modelo de seguridad de la información que nos ayudará a minimizar las brechas de seguridad.
Ejes de Transformación Digital	• Seguridad y confianza digital • Infraestructura de datos • Transformación digital pública
Áreas funcionales beneficiarias del Proyecto.	Todas las áreas
Responsable	Profesionales Seguridad de la Información
Línea de tiempo del proyecto	Vigencia 2025 a 2027
Indicador	(Número total de tareas realizadas / Número total de tareas planeadas) X 100
Meta del Indicador	100% de cumplimiento del plan de trabajo para la vigencia

Entregables Asociados	Documento Modelo de Seguridad y Privacidad de la Información. Resultados del plan de ejecución de auditorías y revisiones al MSPI.
Presupuesto Estimado:	Por Establecer

Proyecto No. 2: Implementación de acciones para la continuidad de la seguridad de la información de infraestructura y servicios de tecnología de la información	
Descripción Proyecto	Implementación de acciones para la continuidad de la seguridad de la información, de infraestructura y servicios de tecnologías de la información
¿Para qué?	La Entidad no cuenta con un plan de continuidad de tecnología de la información, que le permita determinar las actividades a ejecutar y los mecanismos de recuperación de los servicios de Tecnologías de la Información en eventos disruptivos (desastres, fallas de seguridad, pérdida del servicio y disponibilidad del servicio) La Entidad no cuenta con un sitio alterno de procesamiento de información (Datacenter Secundario) que le permita recuperar los servicios críticos de Tecnologías de la Información en caso de una falla crítica y/o un evento catastrófico.

¿Por qué?	Contar con la continuidad de la seguridad de la información, de la infraestructura y servicios de tecnologías de la información, disminuye la posibilidad de ocurrencia de incidentes disruptivos y, en caso de producirse, la Entidad estar preparada para responder en forma adecuada y oportuna, de esa manera se reduce de manera significativa un daño potencial que pueda ser ocasionado. Contar con la continuidad de servicios de tecnologías de la información ayuda a la Entidad a establecer procedimientos que deben seguir en caso de un desastre o materialización de un riesgo y reconocer los servicios que como negocio tendrán que restablecerse de manera oportuna para garantizar la operación y atención a los grupos de valor. De esta forma la organización podrá reducir el impacto de un desastre o cualquier evento disruptivos y fortalecer la respuesta ante un evento de este tipo, garantizando así menores pérdidas que pudieran ser humanas, materiales y económicas La Entidad debe tener la capacidad de discernir entre sus operaciones de misión crítica y no crítica, además de saber cuánto les cuesta y cuál es el impacto en sus operaciones ante una contingencia, ya sea debido a un fenómeno natural o por causa de una falla humana. El IDUVI requiere llevar a cabo el desarrollo e implementar un plan de continuidad de seguridad de la información, de la infraestructura y servicios de tecnologías de la información, que le permitan garantizar que sus servicios misionales estarán siempre disponibles para sus grupos de valor.

¿Cómo?	3. Evaluar riesgos y amenazas - Identificar amenazas potenciales: Considerar amenazas naturales, tecnológicas, humanas y otras que puedan afectar la continuidad del negocio. - Evaluar la probabilidad y el impacto: Calificar cada amenaza en términos de probabilidad de ocurrencia e impacto en el IDUVI. - Desarrollar estrategias de mitigación: Crear estrategias para reducir la probabilidad y/o el impacto de cada riesgo identificado. 4. Desarrollar estrategias de continuidad - Definir estrategias de recuperación: Desarrollar planes detallados para la recuperación de cada proceso crítico, incluyendo la recuperación de datos y sistemas de TI. - Establecer sitios alternos: Identificar y preparar ubicaciones alternativas donde el IDUVI pueda operar en caso de una interrupción en la ubicación principal. - Garantizar la disponibilidad de recursos: Asegurar que se disponga de los recursos necesarios (personal, tecnología, infraestructura) en las ubicaciones alternativas. 5. Desarrollar el plan de continuidad del negocio - Documentar el BCP (Business Continuity Plan): Redactar un documento claro y comprensible que incluya todos los procedimientos y pasos necesarios
Ejes de Transformación Digital	• Seguridad y confianza digital • Infraestructura de datos • Transformación digital pública
Áreas funcionales beneficiarias del Proyecto.	• Todas las áreas
Responsable	Profesionales Seguridad de la Información
Línea de tiempo del proyecto	Vigencias 2025 a 2027

Indicador	100% de cumplimiento del plan de trabajo para la vigencia
Meta del Indicador	(Número total de tareas realizadas / Número total de tareas planeadas) X 100
Entregables Asociados	Plan de continuidad de los procesos críticos del IDUVI Análisis de Impacto BIA Diagnóstico de Plan de Recuperación de Desastres de TI – DRP. Seguimiento y actualización del plan de Continuidad del Negocio y plan de Recuperación desastres
Presupuesto Estimado:	Por establecer

Versión	Fecha de Versión	Descripción del Cambio
2	31 enero 2025	

Elaboró: Diego Andres Chibuque Lamprea – Prof Universitario
Revisó: Nancy Janeth Agudelo Moreno – Subgerente Administrativa y financiera