PLAN DE TRATAMIENTO DE RIESGOS 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.

La política nacional de seguridad digital pretende apoyar a las entidades del gobierno en las definiciones de cumplimiento, las recomendaciones y las mejores prácticas internacionales en gestión de riesgos de seguridad digital emitidas a nivel mundial y recientemente por la organización para la cooperación y el desarrollo económicos (OCDE).

A través del documento CONPES 3854 del 11 de abril de 2016 se estableció la política nacional de seguridad digital que tiene por objetivo:

"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. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el País".

El IDUVI reconociendo la información como un activo, se alinea a las definiciones y lineamientos de la gestión de riesgos, mediante la aplicación de procedimientos y controles requeridos para la protección de la información, en particular los establecidos por el Ministerio de Tecnologías de la Información.

La entidad para dar cumplimiento de esta iniciativa presenta este documento para conocimiento de la ciudadanía, órganos de control y demás partes interesadas.

En relación con lo anterior, en este documento se presenta el Plan a seguir para tratar los riesgos que se identifiquen en los procesos que se especifican a continuación:

Planeación Institucional
Mejoramiento Continuo.
Atención al Ciudadano y Comunicaciones.

Gestión inmobiliaria.
Habitabilidad.
Espacio Público.
Gestión Humana.
Gestión Jurídica.
Gestión Financiera.
Contratación.
Gestión TICS.
Gestión Documental.
Gestión de Recursos Físicos
Gestión Social
Evaluación Independiente.

2. OBJETIVO

Gestionar las acciones pertinentes que permitan identificar y tratar los riesgos de seguridad de la información asociados a los procesos que hacen parte del alcance del Sistema de gestión de calidad de la entidad.

3. ALCANCE

El alcance del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información abarca todos los procesos y actividades que forman parte del Sistema de Gestión de Calidad (SGC) de la entidad, en relación con la seguridad de la información y la protección de la privacidad. Este plan se centrará en la identificación, evaluación y tratamiento de los riesgos asociados a la información.

4. RESPONSABLES

La responsabilidad para la ejecución de este plan de tratamiento de riesgos es compartida entre los líderes de los procesos que hacen parte del alcance del Sistema de Gestion de Calidad, el líder de TICS y Planeación.

5. MARCO LEGAL

El Instituto de Desarrollo Urbano, Vivienda y Gestión Territorial de Chía, como entidad del estado, atiende los lineamientos, resoluciones, decretos y leyes que enmarcan los aspectos de seguridad de la información y seguridad digital. Los aplicables a este plan de seguridad de la información, se relacionan a continuación:

- 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.”
- Decreto 1008 de 2018 “"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".
- Resolución 1519 del 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”
- Resolución número 00500 de marzo 10 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”
- Anexo 3, Resolución MinTIC 1519 del 2020, Condiciones mínimas técnicas y de seguridad digital. Seguridad Web. MinTIC – Viceministerio de Transformación Digital. Dirección de Gobierno Digital. Diciembre 2020
- Anexo 1. Modelo de seguridad y privacidad de la información, febrero 2021, Ministerio de Tecnología de la Información y las comunicaciones.

- Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas.

6. MARCO CONCEPTUAL

Con el fin de preservar los pilares de seguridad de la información que son: confidencialidad, disponibilidad e integridad, las entidades públicas han identificado la necesidad de priorizar la criticidad de sus activos de información para definir unas amenazas, vulnerabilidades y consecuencias que producto de una valoración permiten establecer un conjunto de controles para mitigar la materialización de los riesgos de seguridad de la información asociados a dichos activos.

En relación con lo anterior, las entidades públicas definen la adopción de una metodología de riesgos de seguridad de la información, de acuerdo con lo dispuesto en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" en su versión 5 de 2020 en la cual se encuentran los lineamientos para la gestión de los riesgos de seguridad de la información.

Por otro lado, si bien las entidades públicas identifican sus riesgos de seguridad de la información de acuerdo a su contexto organizacional que incluye estructura organizativa, actividades misionales, los activos de información de su responsabilidad, entre otros aspectos, es necesario que las entidades implementen los controles de seguridad de la información y para ello estipulen un plan que permita tratar los riesgos de seguridad mediante el establecimiento de un plan que aborde el tratamiento de estos riesgos en tiempos específicos de acuerdo a la criticidad del activo o su importancia para la operación.

7. EJECUCIÓN DEL PLAN

6.1 ESTRATEGIAS

Las estrategias planteadas para ejecutar el plan de tratamiento de riesgos son las siguientes:

1. Actualización de los riesgos de seguridad de la información establecidos por los procesos dentro del alcance del SGC de acuerdo con la metodología de riesgos de seguridad de la información vigente en la entidad y identificar vulnerabilidades.

3. Determinar la efectividad de los controles establecidos por los procesos dentro del alcance del SGC, con el fin de establecer la pertinencia de los controles existentes o la necesidad de implementar nuevos controles para el tratamiento de los riesgos de seguridad de la información.

6.2 INDICADORES Y METAS

A continuación, se describe el indicador y la meta del Plan de tratamiento de riesgos de seguridad de la información.

Nombre indicador	**Porcentaje de riesgos identificados en los procesos**
Objetivo	Gestionar el levantamiento y tratamiento de los riesgos de los procesos
Tipo de indicador	Eficiencia
Meta	Evaluar los riesgos identificados donde al menos el 90% se encuentren por encima de un nivel aceptable para la entidad.
Formulación	Número total de riesgos categorizados en nivel aceptable / Número total de riesgos identificados
Frecuencia de medición	Anual
Registro	Documento administrativo

Nombre indicador	**Eventos e Incidentes de seguridad de la información gestionados por el personal responsable dentro del IDUVI**
Objetivo	Gestionar los eventos e incidentes de seguridad de la información, fortaleciendo la capacidad del IDUVI para hacer frente a las amenazas y ataques informáticos.

Tipo de indicador	Eficiencia
Meta	Evaluar la eficiencia de la gestión de eventos e incidentes de seguridad de la información en donde al menos el 80% de los eventos e incidentes identificados se gestionen de acuerdo con los tiempos y rutas establecidas por el IDUVI
Formulación	Numero de eventos e incidentes de seguridad gestionados / Numero de eventos e incidentes de seguridad identificados
Frecuencia de medición	Trimestral
Registro	Documento administrativo

6.3 CONTROLES DE LOS RIESGOS

Controles sugeridos en los planes de mitigación para tener un nivel aceptable de riesgo.

CONTROLES SUGERIDOS PARA MITIGACIÓN DEL RIESGO

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
1	Datos, documentos y/o mensajes de correo electrónico tomados sin autorización.	Uso Aceptable de los Activos. Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información Toma de conciencia, educación y formación de la Seguridad de la Información. Todos los funcionarios y contratistas de la entidad y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
2	Red de la entidad contaminada por programas informáticos malintencionados.	Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
3	Información catalogada como pública reservada divulgada sin autorización.	Manejo de Activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información que debe adoptar la entidad. Protección de registros. Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio. Toma de conciencia, educación y formación de la Seguridad de la Información. Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
4	Información conocida, producida y/o procesada por la entidad expuesta a pérdida o fuga de información.	Disposición segura o reutilización de equipos. Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o rehúso. Equipos sin supervisión de los usuarios. Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.
5	Cuentas de usuario sustraídas con fines de suplantación de identidad.	Sistema de Gestión de Contraseñas. los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
6	Requisitos de trazabilidad y soporte incumplidos en los registros de auditoria de los sistemas de información.	Registro de eventos. Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
7	Recursos físicos, documentales y/o tecnológicos soportes de la gestión incinerados de manera accidental.	Protección de registros. Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
8	'Datos, documentos y/o mensajes de correo electrónico modificados, dañados o eliminados sin autorización.	Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares. Restricción de acceso a información. El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso. Gestión de Cambios. Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
9	Servicios de TIC interrumpidos por daños o desactualizaciones del firewall o los sistemas operativos.	Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. Gestión de incidentes y mejoras en la seguridad de la información. Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.
10	Tiempos de respuesta excedidos en la solución de incidentes de seguridad.	Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. Informe de eventos de seguridad de la información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
		apropiados tan pronto como sea posible. Informe de debilidades de seguridad de la información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información. Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados. Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros. Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
11	Índices de disponibilidad de los servicios TIC otorgados por debajo de los requeridos para la operación.	Mantener el nivel de servicio acordados de seguridad de la información y de prestación del servicio con las áreas usuarias Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
		Seguimiento y revisión de los servicios de los proveedores. Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
12	Sistemas de información, sistemas operativos y/o plataformas tecnológicas operados de manera limitada o deficiente.	Gestión de Capacidad. Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
13	Autenticaciones de usuario sobre los sistemas de información, servicios en línea y/o sistemas operativos suplantados por terceras personas.	Registro y cancelación del registro de usuarios. Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso. Suministro de acceso de usuarios. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios. Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. Gestión de información de autenticación secreta de usuarios. La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
14	Comunicaciones electrónicas interceptadas antes de que lleguen a su destino.	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
15	Activos de información alojados en puestos de trabajo dañados o deteriorados de forma total o parcial.	Clasificación de la Información. Objetivo. Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización. Clasificación de la Información. La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. Etiquetado de la Información. Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización. Manejo de Activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la entidad
16	Funcionarios con conocimientos y/o experiencia especifica perdidos por jubilación, enfermedad, retiro voluntario o involuntario.	Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
17	Procesos del datacenter interrumpidos ante el fallo de cualquiera de sus componentes vitales (climatización, suministro eléctrico, infraestructura física)	Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado. Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
18	Equipos de procesamiento de información crítica accedidos, dañados o interferidos con un propósito específico.	Perímetro de Seguridad Física. Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. Controles Físicos de entrada. Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. Seguridad de oficinas, salones e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones. Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. Trabajo en áreas seguras. Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras. Áreas de atención al ciudadano. Se deben controlar los puntos de acceso tales como áreas atención en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado. Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.
19	'Disrupciones en el datacenter causados por acontecimientos planificados e imprevistos.	Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan. Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
		desastres naturales, ataques maliciosos o accidentes.
20	Sistemas detección y extinción temprana insuficientes, ineficientes o en malas condiciones para el resguardo de los componentes del datacenter.	Perímetro de Seguridad Física. Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. Controles Físicos de entrada. Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. Seguridad de oficinas, salones e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones. Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. Trabajo en áreas seguras. Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
21	Inadecuada administración de los distintos sistemas de información y demás elementos que comprenden el área de tecnologías de la información	El funcionario a Cargo de administrar los sistemas de información y demás elementos que comprenden el área de tecnologías de información de la entidad, deberá ser una persona apta y con experiencia para el manejo de dichas funciones relacionadas como lo son página web, sistema de gestión documental, administrar los servidores y demás sistemas de información.

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

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