PLAN DE TRATAMIENTO DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, INSTITUTO DE DESARROLLO URBANO VIVIENDA Y GESTIÓN TERRITORIAL DE CHÌA - 2020

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.

Objetivo y alcance del documento.

El presente documento describe en forma macro el plan actividades enfocado en la gestión de riesgos de seguridad de la información en el IDUVI

Marco en el que se desarrolla este plan. La entidad en este momento se encuentra en la etapa inicial de una nueva administración.

Como antecedentes, tenemos que la entidad ha dado importantes avances en la gestión riesgos, identificando las vulnerabilidades y asociándolas a amenazas, de manera que los riesgos sean evaluados, calificados y priorizados para determinar la importancia de su tratamiento.

A continuación se presenta una vista general de la matriz de riesgo de seguridad de la información del IDUVI.

1. Mapa de calor. La siguiente es la distribución del riesgo residual, como se aprecia prácticamente todos los riesgos están ubicados en el nivel mayor y catastrofico.

			IMPACTO				
			INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO
			1	2	3	4	5
PROBABILIDAD	Raro	1	(1) ZONA DE RIESGO BAJA Asumir el riesgo	(2) ZONA DE RIESGO BAJA Asumir el riesgo	(3) ZONA DE RIESGO MODERADA Asumir o Reducir el Riesgo	(4) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(5) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo
	Improbable	2	(2) ZONA DE RIESGO BAJA Asumir el riesgo	(4) ZONA DE RIESGO BAJA Asumir el riesgo	(6) ZONA DE RIESGO MODERADA Asumir o Reducir el Riesgo	(8) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(10) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo
	Posible	3	(3) ZONA DE RIESGO BAJA Asumir el riesgo	(6) ZONA DE RIESGO MODERADA Asumir o Reducir el Riesgo	(9) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(12) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo	(15) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo
	Probable	4	(4) ZONA DE RIESGO MODERADA Asumir o Reducir el Riesgo	(8) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(12) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(16) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo	(20) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo
	Casi seguro	5	(5) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(10) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(15) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo	(20) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo	(25) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo

Amenazas más representativas. Las siguientes son las amenazas más representativas que aparecen en la matriz de riesgo.

DIRECCIÓN: Calle 12 No. 6 – 121
Teléfono: 8844398 - 8844708
E-Mail: contactenos@iduvichia.gov.co
Página Web: www.iduvichia.gov.co

Abuso de derechos de usuario.
Acceso a red y/o sistemas de información por usuario no autorizado.
Perdida de suministro de energía.
Uso inadecuado de los recursos.
Exposición de datos y/o documentos.

En cuanto a los criterios parar calificar la probabilidad, se tomaron los niveles establecidos por el DAFP, en su guía para la administración del riesgo y el diseño de controles en entidades públicas (versión 4 octubre de 2018), la cual se muestra a continuación:

CRITERIOS DE VALORACIÓN PROBABILIDAD		
Nivel	**HIPOTÉTICA**	**EXPOSICIÓN**
Casi seguro	Ocurre en la mayoría de las circunstancias o se tiene la suficiente información para determinar una frecuencia muy alta.	Constantemente se presentan situaciones de exposición, que normalmente conllevan a la materialización del riesgo.
Probable	Probablemente ocurre la mayoría de las veces o se tiene la suficiente información para determinar una frecuencia alta.	A menudo se presentan situaciones de exposición, que pueden conllevar a la materialización del riesgo varias veces en la entidad.
Posible	Alguna posibilidad de que el evento ocurra o no se tiene la información suficiente para determinar su ocurrencia.	Algunas veces se presentan situaciones de exposición, de las cuales es posible que conlleven a la materialización del riesgo alguna vez.
Improbable	Puede ocurrir en circunstancias ocasionales o existe la suficiente información para determinar una frecuencia baja.	Ocasionalmente se presentan situaciones de exposición, de las cuales no se espera que conlleve a la materialización del riesgo, aunque puede ser concebible.
Raro	Puede ocurrir en circunstancias excepcionales o existe toda la información para determinar una frecuencia muy baja.	Eventualmente se presentan situaciones de exposición que pueden conllevar a la materialización del riesgo.

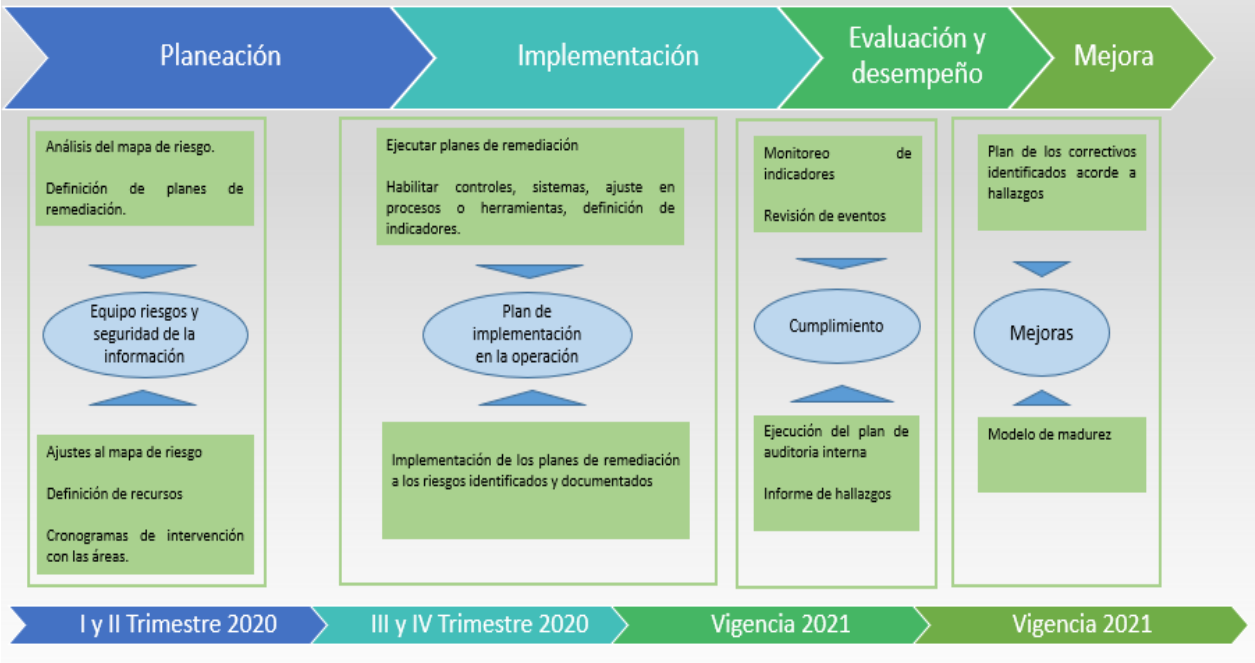
2. Controles sugeridos en los planes de mitigación para tener un nivel aceptable de riesgo.

Conforme a lo establecido en la guía 7 de MinTIC de Gestión de Riesgo, la mitigación de riesgo requerirá la adopción de controles y en forma preliminar el IDUVI identifica controles

susceptibles de implementar los cuales serán tenidos en cuenta en las mesas de trabajo a adelantar con los líderes de proceso. En el Anexo A se relacionan los controles asociados a los riesgos identificados.

3. Actividades para realizar en la vigencia 2020.

Conforme al contexto, antecedentes y estado actual de la entidad en cuanto a gestión de riesgos, el siguiente gráfico muestra las actividades a adelantar y los periodos estimados para la realización de éstas;



Este plan preliminar está sujeto tanto en tiempos como en actividades a los cronogramas y prioridades que la entidad defina en la implementación.

ANEXO A
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
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

DIRECCIÓN: Calle 12 No. 6 – 121
Teléfono: 8844398 - 8844708
E-Mail: contactenos@iduvichia.gov.co
Página Web: www.iduvichia.gov.co

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
		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.
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.

DIRECCIÓN: Calle 12 No. 6 – 121
Teléfono: 8844398 - 8844708
E-Mail: contactenos@iduvichia.gov.co
Página Web: www.iduvichia.gov.co

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
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 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

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
		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. 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.

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
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.
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.

DIRECCIÓN: Calle 12 No. 6 – 121
Teléfono: 8844398 - 8844708
E-Mail: contactenos@iduvichia.gov.co
Página Web: www.iduvichia.gov.co

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
		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.
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.

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
		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 atencion 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 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.

DIRECCIÓN: Calle 12 No. 6 – 121
Teléfono: 8844398 - 8844708
E-Mail: contactenos@iduvichia.gov.co
Página Web: www.iduvichia.gov.co

CONTROLES SUGERIDOS PARA EL DESARROLLO DE LOS PLANES DE MITIGACIÓN		
RIESGO		CONTROL
		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 pagina web, sistema de gestión documental, administrar los servidores y demás sistemas de información.

Área de Gestión de Tecnologías de la información
Instituto de Desarrollo Urbano Vivienda y Gestión Territorial de Chía