Plan de tratamiento de Riesgos de la Seguridad y Privacidad de la Información

TABLA DE CONTENIDO

INTRODUCCIÓN

El presente Plan de Tratamiento de Riesgos se elabora con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno digital en el Eje Temático de la Estrategia en seguridad y privacidad de la información, el cual busca proteger los datos de los ciudadanos garantizando la seguridad de la información dado que la Personería de Madrid Cundinamarca baja la figura de entidad de carácter público y de servicio de la comunidad en pro de los derechos humanos se encuentra en constante intercambio de información con la comunidad, con entidades públicas y privadas. La información que se recibe de entidades y personas es el insumo principal para el desarrollo de varias de las funciones y con base en ella se toman decisiones y se ejecutan acciones que pueden derivar en la generación de comunicados, resoluciones, per, oficios etc. Esta información puede ser de carácter público para conocimiento de la ciudadanía en general o puede tratarse de investigaciones de alta confidencialidad dentro del desarrollo de sus procesos misionales. Por lo anterior, es de suma importancia identificar claramente el tipo de información que se está procesando para determinar los riesgos a los que está expuesta con el fin de protegerla debidamente. De igual manera el Modelo de Seguridad y Privacidad de la Información – MSPI, de la Política de Gobierno Digital de MINTIC, establece metas, resultados y entregables correspondientes a cada una de las fases de implementación del SGSI en sus fases de Planificación e Implementación, las cuales deben ser tenidas en cuenta.

La Personería Municipal de Madrid, decide entonces vincular el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos para el logro de los objetivos de mantener la información de la Entidad confidencial, íntegra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

OBJETIVOS

Tratar y monitorear los riesgos asociados a los procesos existentes de la Personería Municipal de Madrid con el fin de proteger los activos de información, el manejo de medios, el control de acceso y la gestión de los usuarios.

Objetivos Específicos

- Establecer el plan de trabajo y cronograma para adelantar las actividades correspondientes a la identificación, valoración y tratamiento de riesgos de seguridad de la información durante la vigencia 2021.

- Elaborar un plan de trabajo para la implementación del plan de tratamiento de riesgo de seguridad y privacidad de la información.

- Fortalecer el sistema de gestión de riesgos de la Entidad incorporando controles y medidas de seguridad de la información que estén acordes al entorno operativo de la Entidad.

- Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad de la información, y su mitigación.

TÉRMINOS Y DEFINICIONES

Administración del riesgo: Conjunto de elementos de control que al interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización.

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros

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

Criterios de riesgo: Términos de referencia frente a los cuales la importancia de un riesgo es evaluada.

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

Evaluación de riesgo: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Reducción del riesgo: Acciones que se toman para disminuir la probabilidad de las consecuencias negativas, o ambas, asociadas con un riesgo.

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información.

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

SGSI: Sistema de Gestión de Seguridad de la Información.

ESTABLECIMIENTO DEL CONTEXTO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la Personería Municipal de Madrid Cundinamarca, se toma referencia la metodología PHVA (Planear, Hacer, Verificar y Actuar) en acuerdo con esto, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la Entidad y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Entidad.

CRITERIOS DE EVALUACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN:

La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso de información en la Personería Municipal de Madrid Cundinamarca.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- Los requisitos legales y reglamentarios.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la Personería Municipal de Madrid.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la Personería Municipal
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la entidad.

CRITERIOS DE IMPACTO:

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la Entidad, causados por un evento de seguridad de la información considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.
- Operaciones deterioradas (afectación a partes internas o terceras partes)

VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Los riesgos se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la Personería Municipal de Madrid, esta fase consta de las siguientes etapas:

El objetivo de este paso es generar una lista completa de los riesgos sobre la base de los acontecimientos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar la consecución de los objetivos de la Entidad.

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

- Análisis del riesgo
- Identificación de los riesgos
- Estimación del riesgo
- Evaluación del riesgo

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los riesgos previamente mencionados:

Deliberadas (D), fortuito (F) o ambientales (A).

TIPO	AMENAZA	ORIGEN
Daño Físico	Fuego	F, D, A
Daño Físico	Agua	F, D, A
Eventos naturales	Fenómenos climáticos, sísmicos	F
Fallas técnicas	Fallas del equipo Mal funcionamiento del equipo Saturación del sistema de información Mal funcionamiento del software Incumplimiento en el mantenimiento del sistema de información	F,D
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	F,D,A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida Espionaje remoto	D

Acciones no autorizadas	Uso no autorizado del equipo Copia fraudulenta del software	F,D
Revisiones programadas	Ausencia de esquemas de reemplazo periódico	F,D
Dirigidas por el humano	Piratería Ingeniería social Crimen por computador Acto fraudulento Ataques contra el sistema DDoS Penetración en el sistema Ventaja de defensa Hurto de información Asalto a un empleado Chantaje	D
Compromiso de las funciones	Error en el uso o abuso de derechos Falsificación de derechos	D
Soporte Himano	Mantenimiento insuficiente Falta de cuidado en la disposición final Copia no controlada	F,D
Recursos de La institución	Almacenamiento sin proteccion	D

IDENTIFICACIÓN DE LAS VULNERABILIDADES.

Se deben identificar vulnerabilidades (debilidades) de acuerdo con los siguientes tipos:

TIPO	VULNERABILIDAD
SOFTWARE	Ausencia de registros de auditoría Asignación errada de los derechos de acceso Interfaz de usuario compleja Ausencia de documentación Fechas incorrectas Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección Software nuevo o inmaduro

HARDWARE	Fallas del equipo Mal funcionamiento del equipo Saturación del sistema de información Mal funcionamiento del software Incumplimiento en el mantenimiento del sistema de información
RED	Ausencia de pruebas de envío o recepción de mensajes Líneas de comunicación sin protección Conexión deficiente de cableado Tráfico sensible sin protección Punto único de falla WIFI no responde Intermitencia de servicios de terceros
Lugar	Uso inadecuado de los controles de acceso a las instalaciones Áreas susceptibles a inundación Red eléctrica inestable Ausencia de protección en puertas o ventanas

Se sugiere realizar este análisis con el funcionario encargado de la Oficina o funcionario a quien se presenta la falla de este modo por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos establecidos.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas de información, costos de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, daños personales, entre otros.

ANÁLISIS DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

El objetivo del Análisis de Riesgos es identificar y valorar los riesgos a los cuales están expuestos los procesos y los flujos de información, para identificar y seleccionar los controles apropiados de seguridad. El análisis está basado en los flujos de información de cada uno de los procesos y los requerimientos de seguridad, tomando en cuenta los controles existentes.

los riesgos identificados de acuerdo con los niveles para la estimación de los riesgos que deberán ser tomados del documento.

PROBABILIDADES			
Concepto	Valor	Descripción	Frecuencia
Raro	1	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 2 meses.
Improbable	2	Es muy poco factible que el evento se presente	Al menos de 1 vez en los últimos 2 meses.
Posible	3	El evento podría ocurrir en cualquier momento	Al menos 1 vez en los últimos 2 meses.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos 1 vez en los últimos 2 meses.
Casi Certeza	5	Se espera que ocurra en la mayoría de las circunstancias	Más de 1 vez los últimos 2 meses.

IMPACTO		
Concepto	Valor	Descripción
Insignificante	1	La materialización del riesgo puede ser controlado por los participantes del proceso, y no afecta los objetivos del proceso.
Menor	3	La materialización del riesgo ocasiona pequeñas demoras en el cumplimiento de las actividades del proceso, y no afecta significativamente el cumplimiento de los objetivos de la Entidad. Tiene un bajo impacto en los procesos de otras áreas de la Entidad.
Moderado	5	La materialización del riesgo demora el cumplimiento de los objetivos del proceso, y tiene un impacto moderado en los procesos de otras áreas de la Entidad. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus actividades, impidiendo la continuidad del desarrollo en forma habitual.
Mayor	7	La materialización del riesgo retrasa el cumplimiento de los objetivos de la Entidad y tiene un impacto significativo en la imagen pública.
Catastrófico	11	La materialización del riesgo imposibilita el cumplimiento de los objetivos de la Entidad, tiene un impacto catastrófico en la imagen pública de la Entidad y puede incurrir en sanciones , multas u otra obligación legal.

Al definir los criterios de riesgo, se tendrán en cuenta:

•La naturaleza, los tipos de causas y consecuencias que pueden ocurrir y cómo se van a medir.

•La manera de definir la probabilidad de ocurrencia de un evento.

•La forma de determinar el nivel de riesgo.

•Niveles de riesgo aceptable para la organización.

Las actividades realizadas para ejecutar el análisis de riesgos se realizan de acuerdo con el siguiente esquema:

•Definición de las áreas de la entidad que se incluirán dentro del alcance del proceso de gestión de riesgos de seguridad digital y ciberseguridad.

•Levantamiento de información relacionada con el proceso seleccionado.

•Consulta con personas claves dentro del proceso para conocer su percepción del riesgo al cual se encuentra expuesta la información.

•Ejecución de la evaluación de riesgos a los que se encuentra expuesto el proceso, por medio de valoración de hallazgos y evaluación de probabilidad de ocurrencia de amenazas y vulnerabilidades.

•Análisis y diagnóstico del nivel de riesgo para el proceso definido. Se llevará a cabo la elaboración del informe de resultados.

ACTIVIDADES PARA DESARROLLAR

Procesos o subprocesos y actividades en cumplimiento de las funciones. procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la Personería Municipal, procesos que contienen procesos secretos; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la Personería Municipal.

Información: información vital para la ejecución de la misión o funciones de la Personería Municipal; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas. Se debe tener en cuenta la información que se tramita en entidad de carácter personal de sus funcionarios y usuarios de la Personería Municipal.

De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

COSTO - BENEFICIO	OPCIÓN DE TRATAMIENTO
El nivel de riesgo está muy alejado del	**Evitar el riesgo**, su propósito es no

nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo.	**Transferir** o compartir el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	Retener o aceptar el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

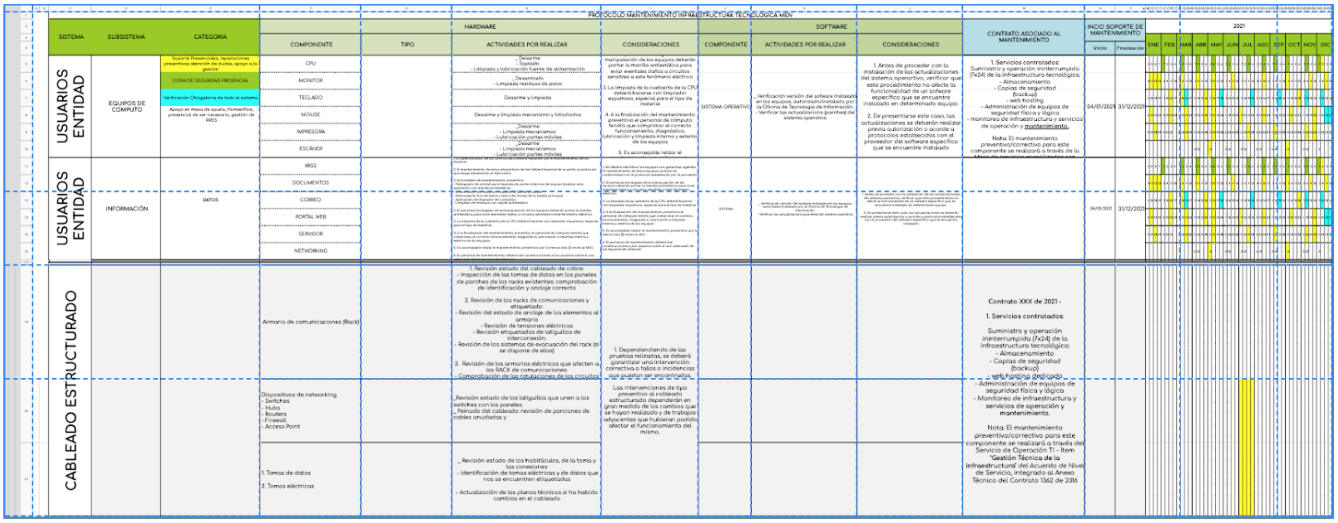
Los riesgos son dinámicos como la misma Entidad por tanto podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte:

1. Nuevos activos o modificaciones en el valor de los activos.
2. Nuevas amenazas.
3. Cambios o aparición de nuevas vulnerabilidades
4. Aumento de las consecuencias o impactos,
5. Incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

CRONOGRAMA

Visión General



Anexo *Archivo Cronológico 001

BIBLIOGRAFÍA

El presente documento define las medidas de seguridad identificadas para desarrollar e implementar al 31 de diciembre del 2020 el plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información Tomada de: https://goo.gl/S4r4Kk.