PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Seguridad y Privacidad de la Información
Dimensión: Diagnóstico de Seguridad y Privacidad

Gobierno Digital
Ministerio de las Tecnologías de la Información y Comunicaciones

Alcaldía de Oiba

2018

Contenido

Histórico

VERSIÓN	FECHA	AUTOR
1	01-06-2018	Secretaría General y de Gobierno

Introducción

La información es parte primordial en el cumplimiento de los objetivos de una organización, por lo tanto resguardar todo tipo de información es una necesidad ante cualquier posible alteración, mal uso, pérdida entre otros muchos eventos. Es así que la administración de los potenciales riesgos es una estrategia metodológica y sistemática que garantizará alcanzar los objetivos de la Organización.

1. Objetivos

El objetivo principal de este plan busca establecer la clara metodología para hacer una administración a la medida de los potenciales riesgos por medio de la identificación, manejo y seguimiento de los mismos.

Como objetivos específicos se formularon:

- Acceder a información consistente, confiable y real para realizar una correcta toma de decisiones
- Hacer participes y responsables a los funcionarios de la entidad de la magnitud y relevancia de mantener información confiable
- Generar un ambiente de autogestión con relación a la integridad y seguridad de la información

2. Definiciones

- **Acceso a la información pública:** El acceso a la información pública es un derecho fundamental, reconocido por la Convención Americana de Derechos Humanos en su artículo 13, el cual recalca la obligación de los Estados de brindar a los ciudadanos acceso a la información que está en su poder.
- **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.

- **Activo de información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.
- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO/IEC 27000)
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Datos Abiertos:** Son los datos que se encuentran en formatos estandár e interoperables que facilitan su acceso y reutilización (Ley 1712 de 2014, art 6)
- **Datos personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos personales públicos:** Son los relativos al estado civil de las personas, profesión u oficio y calidad de comerciante o servidor público (Decreto 1377 de 2013, art 3)
- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.
- **Riesgo de corrupción:** posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
- **Riesgo institucional:** Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.

Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.

Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.

Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.

- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.
- **Seguridad de la información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** 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).[1]

1 Definiciones tomadas del Plan de Tratamiento de Riesgos e Seguridad de la información de FODESEP y Plan de tratamiento de Riesgos de Seguridad y Privacidad de la información INFOTEP

3. Roles y responsabilidades

- Alta Dirección: Es el grupo de funcionarios de la entidad que aprueban las diferentes políticas y directrices con relación a las TIC. En este caso particular aprobarán o establecido para la administración del riesgo.
- Responsables por procesos: Son las personas encargadas de identificar, analizar y valorar los riesgos en la entidad por lo menos una vez al año.
- Funcionarios: Se encargan llevar a cabo los controles y ejecutar acciones para la administración de los riesgos identificados.
- Control interno: Realiza la evaluación y seguimiento a la política, procedimientos y controles.

4. Política de administración del riesgo

La política del riesgo cubre las acciones pertinentes para la implementación y mantenimiento del proceso de la Administración del Riesgo, por lo tanto los servidores de la entidad se comprometen a:

1. Cumplir las normas establecidas con la administración del riesgo, presentadas en este plan
2. Propender por un ambiente de administración de los riesgos a nivel general en la entidad, comunicando los beneficios y efectos negativos de la no aplicación de este plan de tratamiento
3. Realizar un análisis continuo de los potenciales riesgos de acuerdo a la aplicación de las metodologías desarrolladas
4. Mantener control y reportar los eventos de riesgo, consultando posibles cambios en la actualización de la clasificación de riesgo
5. Llevar a cabo la implementación de planes de contingencia y transmitir propuestas a la alta dirección, las cuales permitan una mejora continua la gestión de las actividades

5. Etapas para el tratamiento del riesgo

Las etapas que componen este Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información son:

- Establecimiento del contexto
- Identificación
- Análisis
- Valoración
- Manejo
- Seguimiento

6. Contexto externo

El contexto externo es ese ambiente en el cual la organización busca alcanzar sus objetivos, para este caso es el ambiente externo es el que la alcaldía no puede controlar, y entenderlo es importante porque se lograría garantizar que los objetivos y las preocupaciones de las partes involucradas externas se toman en consideración al desarrollar criterios del riesgo.

6.1 Ambiente Social y Cultural

Las personas del municipio no tienen conciencia práctica sobre los métodos que podrían incrementar de forma real la seguridad de su información, lo que posiblitaría malas prácticas en el uso de alguno de los equipos puestos a dispoición por la entidad municipal. Lo anterior obliga a que la administración deje en los equipos a disposición de la comunidad con los más altos estándares de seguridad.

Por otra parte en términos de orden público, la entidad debe tener presente que puede existir la probabilidad de una irrupción en las istalaciones de la entidad y puedan correr riesgo los distintos equipos de la misma o el acceso al servicio de internet de la misma por temas de hurto o intercepción de señales.

6.2 Ambiente Político

Uno de los escenarios que se han de presentar es el cambio de gobierno y el mismo debe contar con el acceso de la información idonea e integra, para dar continuidad a los distintos procesos de la alcaldía.

La legislación actual fortalece e incluye más mecanismos que permiten la protección y conservación de la integridad de la información de la entidad.

Por último es necesario mantener presente las distintas políticas formuladas e implementadas dentro de este modelo de seguridad e integridad de la información, lo cual permite consolidar en el tiempo mejores prácticas de los usuarios hacia la entidad.

6.3 Ambiente Económico

En términos de liquídez existen factores como el alza de los servicios o productos tecnológicos y haga complejo el cumplir los objetivos del MSPI

La disponibilidad del capital para la implementación del Modelo de Seguridad y Privacidad de la Información, puede llegar a depender de recursos girados por la Nación, por lo tanto es recomendable por medio de la austeridad lograr alcanzar los objetivos con los recursos propios de la entidad o con fuentes de cofinancia a mediano plazo

6.4 Ambiente Tecnológico

Conforme avanza el tiempo el desarrollo y avance de tecnologías aumenta, logrando sistemas con mayor precisión y velocidad en el cálculo de información, sumando la velocidad de nevegación en la internet, por lo tanto el avance en estos temas exigirá conforme avance el tiempo una actualización de los equipos utilizados en la entidad, principalmente los que garantizan la seguridad de la información y evitan los ataques informáticos externos.

También se podrían encontrar con pertubación de radiación de tipo electromagnética, térmica e impulsos electromagnéticos los cuales desactivan y dejarían nulo algunos de los equipos electrónicos en la entidad.

6.5 Medio ambiental

Los equipos de la entidad podrían correr riesgos de tipo ambiental como incendios, diluvios, terremotos, entre otros semejantes, por lo tanto la entidad debe seleccionar espacios que puedan el daño por este tipo de catástrofes y claro está poder realizar copias de respaldos en servidores fuera de la entidad. A esto se le puede sumar el exceso de polvo, corrosión o congelamiento.

6.6 Ambiente Servicios a la Entidad

Dentro de los servicios esenciales de los que hace uso la administración podrían existir fallas en el sistema de suministro de agua o aire acondicionado, el cual les permite la refrigeración de los aparatos electrónicos. También puede existir una pérdida del suministro de energía y por último una falla en los equipos de comunicaciones de internet.

7. Contexto interno

Este contexto comprende el ambiente interno, donde comprende todo quello dentro de la organización que pueda tener influencia en la forma en que la organización gestionará el riesgo.

7.1 Integridad de la información

En este apartado pueden aparecer complicaciones como intercepción de señales, acceso y espionaje de forma remota, hurto de los documentos o secuestro de los mismos, hurto de equipos, obtención de equipos dados de baja, manipulación de software y hardware. Para lo anterior la alcaldía establece una serie de parámetros o políticas como el plan de manejo de residuos eléctricos o electrónicos para el caso especifico como la obtención de equipos dados de baja.

7.2 Fallas Técnicas y Acciones no Autorizadas

Dentro de las diversas fallas que podrían aparecer están las del equipo, saturaciones en los servidores o sistemas de información, errores en el software o aplicaciones maliciosas. Así mismo uno de las acciones no autorizadas podrían incluir el uso no autorizado del equipo, copia o uso fraudulento del software, malversación o corrupción de datos y el procesamiento ilegal de datos. Con relación a estas posibles fallas y acciones no autorizadas, la entidad ha tomado

medidas como el acceso al equipo con usuario y contraseña, o sistemas operativos como linux, que aumentan el nivel de seguridad del equipo.

8. Contexto del proceso para la gestión del riesgo

De acuerdo a los objetivos, estrategias alcance y parámetros de las actividades de la organización, la gestión del riesgo debe emprender con total consideración la necesidad de justificar los recursos utilizados para llevar a cabo dicha gestión. A continuación se presenta de acuerdo a los tipos de activos la vulnerabilidades y amenazas que podrían afectarlos

Tipo de Activo	Vulnerabilidades	Amenzas
Hardware	Bajo mantenimiento	Puede ocurrir al bajo número de programaciones de mantenimiento o limitarse al mantenimiento correctivo
	Alto riesgo de daño por caída del servicio de electricidad	Daño en los equipos de forma permanente, debido a cortos circuitos en su procesador
	Falta de protocolos para el reemplazo de componentes fuera de servicio	Potencial pérdida de información o equipos completamente fuera de uso
	Almacenamiento sin protección	Hurto de componentes o información
Software	Falta de logs de uso del equipo	Hacer mal uso del equipo
	Falta de documentación	Errores al usar el sistema operativo y demás aplicaciones
	Acceso a archivos con contraseñas	Mal uso de archivos o aplicaciones con acceso restringido
Intranet	Acceso no restringido a terminales	Manipulación de la información
	Envío de contraseñas sin encriptación entre terminales	Potencial falsificación de usuarios
Internet	Uso inadecuado del servicio	Saturación del ancho de banda para la navegación
	Falta de implementación de un rompefuegos o sistema proxy	Posibles ataques externos y uso inadecuado de la red para acceder a sitios no permitidos por el Estado
Personal	Malas prácticas del uso de equipos	Error en el uso
	Falta de políticas para el uso de correo electrónico	Uso no adecuado de los recursos de la entidad
	Ausencia del talento humano para el uso de los equipos asignados	Potencial abuso de los terminales por terceros
Organización	Falta de auditorias	Mal uso de los recursos
	Actualización en el retiro o cambio de usuarios y funciones	Uso indebido de los derechos antiguos

9. Clasificación de los riesgos

De acuerdo a la características de cada riesgo, se establecen parámetros de clasificación los cuales permiten un tratamiento adecuado para su mitigación.

CLASES DE RIESGO	Definición
Estratégico	Son los riesgos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
Operativo	Relacionados con el funcionamiento y operatividad de los sistemas de información de la entidad: definición de procesos, estructura de la entidad, articulación entre dependencias.
Financieros	Relacionados con el manejo de los recursos de la entidad: ejecución presupuestal, elaboración estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes.
Cumplimiento	Capacidad de cumplir requisitos legales, contractuales, ética pública y compromiso con la comunidad.
Tecnología	Capacidad para que la tecnología disponible satisfaga las necesidades actuales y futuras y el cumplimiento de la misión.
Imagen	Tienen que ver con la credibilidad, confianza y percepción de los usuarios de la entidad.

Fuente: Plan Estratégico de Riesgos de Seguridad y Privacidad de la Información – INFOTEP

Escala para calificar la PROBABILIDAD del riesgo		
Nivel	Concepto	Frecuencia
Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
Improbable	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
Moderado	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
Casi certeza	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Fuente: Plan Estratégico de Riesgos de Seguridad y Privacidad de la Información – INFOTEP

Escala para calificar el IMPACTO del riesgo							
Tipos de efecto o impacto		**a) Estratégico**	**b) Operativo**	**c) Financieros**	**d) Cumplimiento**	**e) Tecnología**	**f) Imagen**
INSIGNIFICANTE	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos o bajos sobre la institución	Afecta el cumplimiento de algunas actividades	Genera ajustes a una actividad concreta	La pérdida financiera no afecta la operación normal de la institución	Genera un requerimiento	Afecta a una persona o una actividad del proceso	Afecta a un grupo de servidores del proceso
MENOR	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la institución	Afecta el cumplimiento de las metas del proceso	Genera ajustes en los procedimientos	La pérdida financiera afecta algunos servicios administrativos de la institución	Genera investigaciones disciplinarias, y/ o fiscales y/o penales	Afecta el proceso	Afecta a los servidores del proceso
MEDIANO	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la Institución	Afecta el cumplimiento de las metas de un grupo de procesos	Genera ajustes o cambios en los procesos	La pérdida financiera afecta considerablemente la prestación del servicio	Genera interrupciones en la prestación del bien o servicio	Afecta varios procesos de la institución	Afecta a todos los servidores de la institución
MAYOR	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas de la institución	Genera intermitencia en el servicio	La pérdida financiera afecta considerablemente el presupuesto de la institución	Genera sanciones	Afecta a toda la entidad	Afecta el sector
CATASTRÓFICO	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas del sector y del gobierno	Genera paro total de la institución	Afecta al presupuesto de otras entidades o a de la del departamento	Genera cierre definitivo de la institución	Afecta al Departamento	Afecta al Departamento, Gobierno, Todos los usuarios de la institución

Fuente: Plan Estratégico de Riesgos de Seguridad y Privacidad de la Información – INFOTEP con modificaciones de autor

Con los resultados de la clasificación presentada, se puede definir una zona de ubicación del riesgo de acuerdo a las siguientes sugerencias:

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Mediana	Mayor	Catastrófico
Raro	B	B	B	M	M
Improbable	B	M	M	A	A
Moderado	B	M	A	A	E
Probable	M	A	A	E	E
Casi certeza	M	A	E	E	E

Fuente: Plan Estratégico de Riesgos de Seguridad y Privacidad de la Información – INFOTEP con modificaciones de autor

Color	ZONA DE RIESGO
B	Zona de riesgo baja
M	Zona de riesgo moderada
A	Zona de riesgo alta
E	Zona de riesgo extrema

Fuente: Plan Estratégico de Riesgos de Seguridad y Privacidad de la Información – INFOTEP

10. Evaluación del riesgo inherente

A continuación se presenta la evaluación del riesgo en la matriz de evaluación, lo que es denominado como evaluación del riesgo inherente.

Tipo de Activo	Riesgo	Clase	Probabilidad	Impacto	Zona de Riesgo
Hardware	Bajo mantenimiento	Tecnología	Moderado	Insignificante	Baja
	Alto riesgo de daño por caída del servicio de electricidad	Tecnología	Improbable	Mediano	Moderada
	Falta de protocolos para el reemplazo de componentes fuera de servicio	Tecnología	Moderado	Menor	Moderada
	Almacenamiento sin protección	Tecnología	Probable	Mediano	Alta
Software	Falta de logs de uso del equipo	Tecnología	Moderado	Mediano	Alta
	Falta de documentación	Tecnología	Probable	Mayor	Extrema
	Acceso a archivos con contraseñas	Tecnología	Raro	Mediano	Baja
Intranet	Acceso no restringido a terminales	Operativo	Raro	Catastrófico	Moderada
	Envío de contraseñas sin encriptación entre terminales	Estratégico	Casi certeza	Catastrófico	Extrema
Internet	Uso inadecuado del servicio	Imagen	Moderado	Mayor	Alta
	Falta de implementación de un rompefuegos o sistema proxy	Estratégico	Raro	Catastrófico	Moderada
Personal	Malas prácticas del uso de equipos	Estratégico	Raro	Mayor	Moderada
	Falta de políticas para el uso de correo electrónico	Imagen	Raro	Mediano	Baja
	Ausencia del talento humano para el uso de los equipos asignados	Cumplimiento	Raro	Mediano	Baja
Organización	Falta de auditorias	Operativo	Moderado	Mayor	Alta
	Actualización en el retiro o cambio de usuarios y funciones	Operativo	Raro	Mediano	Baja

11. Controles para el tratamiento de riesgos

Los controles son un determinado número de acciones que permiten minimizar la probabilidad de ocurrencia o el impacto del riesgo, estos deben estar directamente relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas. Un control debe tener un objetivo, ser pertinentes, realizables, medibles, periódicos, efectivos y asignables.

Tipo de Activo	Riesgo	Preventivo	Correctivo
Hardware	Bajo mantenimiento	Crear y Ejecutar cronogramas de mantenimiento	Realizar los mantenimientos no planeados
	Alto riesgo de daño por caída del servicio de electricidad	Adquisición de UPS	Reemplazar dispositivos quemados
	Falta de protocolos para el reemplazo de componentes fuera de servicio	Desarrollo guía para reemplazo de componentes fuera de servicio	Lista el procedimiento utilizado durante el reemplazo
	Almacenamiento sin protección	Asignar espacios y mecanismos para proteger los dispositivos	Ubicar el dispositivo en un espacio protegido
Software	Falta de logs de uso del equipo	Implementación de logs	Programar logs de uso
	Falta de documentación	Levantar y solicitar documentación	Alimentar base de datos para la creación de documentación
	Acceso a archivos con contraseñas	Indicar a los funcionarios el no uso de contraseñas en archivos	Eliminar contraseñas de archivos
Intranet	Acceso no restringido a terminales	Asignar a cada terminal acceso restringido	Restringir el acceso a terminales
	Envío de contraseñas sin encriptación entre terminales	Utilizar canales o herramientas para encriptado de información	Revisar canal de comunicación de la información compartida
Internet	Uso inadecuado del servicio	Programación proxy y firewall	Bloqueo de servicios no autorizados
	Falta de implementación de un firewall o sistema proxy	Actualización e implementación de firewall y proxy	Implementación de Firewall y Proxy
Personal	Malas prácticas del uso de equipos	Socialización Política uso de equipos	Actualización de políticas
	Falta de políticas para el uso de correo electrónico	Diseño e implementación de la política	Actualización de política y procedimientos
	Ausencia del talento humano para el uso de los equipos asignados	Capacitación y selección de talento humano	Talleres o jornadas de capacitación
Organización	Falta de auditorias	Programar y ejecutar auditorías	Diseñar cronograma de auditorias
	Actualización en el retiro o cambio de usuarios y funciones	Establecer procedimiento para el retiro y cambio de usuarios y funciones	Construcción guía para el cambio de usuarios y funciones

12. Seguimiento de riesgos

Dentro de las tareas principales por parte de la Oficina de Control interno, está se encargará de realizar por lo menos de forma semestral un seguimiento al control de riesgos formulado y verificará aspectos como el cumplimiento de las políticas, guías y directrices establecidos. Es necesario que los resultados de la evaluación y las observaciones serán presentados a la Alta Dirección, para tomar las medidas necesarias de acuerdo a los resultados de la evaluación realizada.