AGENCIA DE COOPERACIÓN E INVERSIÓN DE MEDELLÍN
Y EL ÁREA METROPOLITANA
República de Colombia

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

ASTRID MADELEINE ÁLVAREZ

Directora de Relaciones Administrativas

LEONARDO DÍAZ CÁRDENAS

Auxiliar Administrativo de Sistemas e Informática

2020

CONTENIDO

INTRODUCCIÓN

La administración de los riesgos de seguridad y privacidad de la información es un método lógico y sistemático para identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados a la información generada por los diferentes procesos de tal forma que permita a la entidad minimizar pérdidas y maximizar oportunidades de mejora.

Todas las instituciones públicas, en busca del cumplimiento de sus funciones, misiones y objetivos, están sometidas a riesgos que pueden hacer fracasar la gestión de un proceso y hasta de toda la organización; por lo tanto, es necesario tomar las medidas apropiadas, para identificar las causas y posibles consecuencias de la materialización de dichos riesgos.

Por esta razón, el presente plan tiene como objetivo facilitar y orientar la implementación de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación, el monitoreo y mitigación máxima de los mismos; enfatizar en la importancia de la administración del riesgo en la seguridad y privacidad de la información, sus fundamentos técnicos y dando lineamientos sencillos y claros para su adecuada gestión.

1 OBJETIVOS

1.1 Objetivo general

Minimizar y controlar los riesgos asociados con los sistemas de información y la infraestructura tecnológica que interviene en el manejo y custodia de la información en la ACI Medellín, con el fin de salvaguardar la información como el mayor activo de la Agencia.

1.2 Objetivos específicos

1.2.1 Concientizar y comprometer a todos los servidores de la Agencia sobre la necesidad e importancia de gestionar de manera adecuada los sistemas de información y los recursos tecnológicos, mitigando los riesgos inherentes a los que esto conlleva.

1.2.2 Promover la cultura de la administración de riesgos en la seguridad y privacidad de la información creando conciencia al interior de la Agencia de los beneficios que conlleva su aplicación y los efectos negativos para la entidad por su desconocimiento y materialización.

2 ALCANCE

Este plan de tratamiento de riesgos de seguridad y privacidad de la información, suministra metodologías y conceptos para la Agencia que apalancarán la administración y gestión de los riesgos a nivel de todos los procesos; orienta sobre las actividades y buenas prácticas aplicadas a los procedimientos que tienen que ver con el uso y custodia de la información, identificando los riesgos, su valoración y la definición de opciones de manejo que pueden requerir la posible formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

3 ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para lograr los objetivos de la administración del riesgo en la seguridad y privacidad de la información no solo se depende del plan, también de las partes involucradas y su participación, por ello es preciso identificar los actores que intervienen.

Comité Directivo: aprueban los lineamientos conceptuales y metodológicos definidos en la GI-SIG-01 guía de administración de riesgos, siendo responsable de fortalecer, incentivar y hacer cumplir las políticas allí definidas.

Subproceso del Sistema Integrado de Gestión: es el encargado de generar la metodología para la administración de riesgo; coordina, lidera, asesora y capacita en su objeto funcional.

Integrantes de los procesos institucionales: identifican, analizan, evalúan y valoran los riesgos del proceso o subproceso por lo menos una vez al año, si bien están apoyados por el Profesional Senior en Calidad, son los responsables de garantizar que en el proceso se definan los riesgos de la información que le competen, se establezcan los controles y se adelanten las actividades para mitigarlos.

Contratistas: ejecutar en sus funciones los controles y acciones definidas en los lineamientos de la administración del riesgo, también aportan a la identificación de posibles amenazas que puedan afectar la información institucional.

Control Interno: su responsabilidad es verificar y evaluar la elaboración, la visibilización, el seguimiento y el control del mapa de riesgos, conforme a la GI-SIG-01 guía de administración de riesgo.

4 METODOLOGÍA

El plan de tratamiento de riesgos de seguridad y privacidad de la información de la ACI Medellín, se regirá por lo estipulado en la GI-SIG-01 Guía de Administración de Riesgos, la cual tiene como objetivo: "Establecer disposiciones y criterios institucionales que orienten a la ACI Medellín en la correcta identificación, análisis, valoración y administración de los riesgos, con el fin de reducir la probabilidad de ocurrencia y el grado de impacto de aquellos riesgos que pueden afectar el logro de los objetivos institucionales en el marco de los procesos".

Para ello todos los funcionarios y contratistas de la Agencia se comprometen a:

- ✓ Conocer, cumplir y apropiarse de los lineamientos en la administración del riesgo en la seguridad y privacidad de la información de acuerdo con los controles y acciones definidas en el mapa de riesgos de la Agencia.

- ✓ Aplicar a los procesos y procedimientos una permanente revisión y análisis de riesgos en la seguridad y privacidad de la información para poder tomar acciones y controles con el objetivo de mitigarlos.

- ✓ Desarrollar acciones de contingencia asegurando la disponibilidad de la información en los eventos donde pueda que se materialice un riesgo en la seguridad y privacidad de la información poniendo en peligro los objetivos y la misión de la Agencia.

- ✓ Presentar propuestas de mejora continua que permitan optimizar los proceso aumentando la eficacia y efectividad en el manejo de la información.

- ✓ Controlar permanentemente los cambios en las calificaciones de los riesgos en la seguridad y privacidad de la información para realizar ajustes pertinentes al mapa de riesgos institucional.

5 ANALISIS DE VULNERABILIDAD

5.1 Situaciones no deseadas

- Hurto de información por robo de equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales, por intromisión.
- Incendio en las instalaciones de la entidad por desastre natural, instalaciones inadecuadas o de manera intencional.
- Alteración de claves y cuentas de acceso.
- Corte del servicio de internet por parte del ISP - Proveedor del Servicio de Internet.
- Corte del fluido eléctrico no programado.
- Daño de equipos físicos y corrupción de información.
- Retraso en asistencia técnica gestionada mediante la mesa de ayuda.
- Fuga de información al interior de la entidad, por parte de los funcionarios y contratistas.
- Manipulación indebida de información.

5.2 Análisis de vulnerabilidad

A continuación, se describirán las amenazas y debilidades tecnológicas, con el fin de determinar las falencias y establecer los controles necesarios para mitigar la materialización de un posible riesgo.

Fortalecimiento de la conectividad a internet.

La Agencia cuenta con sistemas de información en la nube como lo son office 365 (correo electrónico, almacenamiento en la nube OneDrive, SharePoint intranet, Skype comunicaciones unificadas), CRM institucional Salesforce, plataforma de envió masivos de mail, y aunque se tiene un canal dedicado con fibra óptica de 40 MB, en cualquier momento puede fallar y quedarían estos servicios fuera de alcance.

Adecuaciones al centro de datos.

Actualmente, el centro de datos de la Agencia no cumple con las buenas prácticas de TI, debido a:

1. El cuarto técnico necesita un espacio adecuado.

2. Se encuentran cajas de breakers sin tapa, generando riesgos como cortos circuitos.

3. Se tiene la necesidad de un aire acondicionado de precisión, que controle la humedad y sea automático.

4. Actualmente los materiales del cuarto son inadecuados y además son en elementos combustibles que pueden propiciar un incendio.

Todas estas condiciones pueden afectar los servidores físicamente al igual que el sistema de almacenamiento, switches y cableado.

Renovación de servidores y almacenamiento centralizado.

En la Agencia se cuenta con un gabinete de 6 servidores físicos y un almacenamiento centralizado, a pesar de que funcionan actualmente muy bien se encuentran fuera de garantía, se implementaron desde 2012 y a la fecha ya son 7 años en buen funcionamiento, pero existe el riesgo de que pueda fallar.

Durante el año 2019 se realizó el estudio para identificar cual es el mecanismo óptimo para minimizar estos riesgos, los cuales incluyen migración y/o cambio de servidores, unidades de almacenamiento centralizado y operación de sistemas de información en nube.

6 MAPA DE RIESGOS

ACI Medellín	MAPA DE RIESGOS DE GESTIÓN Y CORRUPCIÓN	Código: FR-SIG-11 Versión: 06 Vigencia: 05/12/2019
TIPO DE PROCESO	Apoyo	
PROCESO / SUBPROCESO	Subproceso gestión de recursos tecnológicos	
OBJETIVO DEL PROCESO O SUBPROCESO	Administrar la plataforma tecnológica de la ACI Medellín identificando las necesidades de actualización, asegurando la integridad, confidencialidad y disponibilidad de la	

Identificación del riesgo						Valoración del riesgo				Aplicación de controles				Monitoreo y seguimiento						Indicador	Acciones
						Riesgo Residual															
No.	Proceso/ Subproceso	Nombre del Riesgo	Clasificación	Causas	Consecuencias	Probabilidad	Impacto	Nivel	Opción de manejo	Control Existente	Frecuencia	Evidencia	Responsable del control	Acciones preventivas Corrupción/Aplicación de controles Gestión	Responsable de la acción	Evidencia ejecución de acciones preventivas	Frecuencia	Fecha de inicio	Fecha de terminación		Acción de contingencia ante posible materialización
#######	Gestión de los recursos tecnológicos	Uso indebido de la información que conlleve a la falta de confidencialidad, disponibilidad e integridad de información	Corrupción	Probabilidad de ocurrencia de múltiples factores que afectan al subproceso (tales como fuga de información, pérdida de trazabilidad, pérdida de información, etc.)	Pérdida de información. Pérdida de credibilidad en la agencia.	Improbable	Mayor	Moderado	Evitar	Manual de políticas de seguridad informática de la ACI	Inducción al cargo de nuevo personal de la ACI	Registro de inducción al cargo	Auxiliar Administrativo de Sistemas e Informática	Divulgación del manual de políticas de seguridad informática de la ACI	Auxiliar Administrativo de Sistemas e Informática	N.A.	N.A.	N.A.	N.A.	% cumplimiento lista de chequeo de las políticas de seguridad (meta 90%)	Notificar al Coordinador de control interno Tomar las medidas legales correspondientes a la situación detectada
										Perfil del usuario	Cada ingreso de personal nuevo	Actualización de los estados de los usuarios (activos y retirados)		Aplicación de GPO de acuerdo al perfil del usuario						Actualización de los estados de los usuarios (activos y retirados) (meta 100%)	
										Copias de seguridad de la información	Diario, semanal, mensual y anual	Informe diario de ejecución del backup		Copias de seguridad de la información, de acuerdo a una programación diaria, semanal y mensual						Informe diario de ejecución del backup y registro de acciones en casos no exitosos	

7 CRONOGRAMA

	PLAN OPERATIVO					Código: FR-DES-06		
						Versión:01		
						Vigencia:26/12/2019		
DIRECCIÓN	Relaciones Administrativas - Recursos Tecnológicos							
OBJETIVO ESTRATEGICO	**OBJETIVO TACTICO**	**ACTIVIDAD**	**INDICADOR**	**META INDICADOR**	**ENTREGABLE**	**Responsable**	**Fecha inicio**	**Fecha fin**
9. Consolidar un sistema de información dinámico, que favorezca resultados óptimos de los procesos de la organización y que permita generar oportunidades de cooperación e inversión para todo el territorio de Antioquia	N.A	Administrar el clúster de servidores virtualizados vía VMware y servidores físicos de la Agencia (crear, eliminar, modificar cuentas de usuario, políticas de red, seguridad en la infraestructura Informática, administrar la sincronización de los servicios informáticos locales con los de la nube).	N.A.	N.A.	Disponibilidad y buen funcionamiento de los servidores de la Agencia para poder gestionar los servicios de usuarios finales.	Auxiliar Administrativo Sistemas e Informática	01/01/2020	31/12/2020

	N.A	Administrar el sistema del backup de información (revisar las copias de seguridad diarias, semanales y mensuales en el servidor ACIMED 02) sistemas de contingencia.	Backup de información	Copias mensuales estado correcto 100%, copias semanales estado correcto 80%, copias diarias estado correcto 80%	Matriz de seguimiento a las copias de seguridad en el sitio ACIMEDELLIN de office 365.	Auxiliar Administrativo Sistemas e Informática	01/01/2020	31/12/2020
	N.A	Realizar en mantenimiento físico de los equipos de cómputo.	Garantizar la ejecución de los mantenimientos a los equipos de cómputo.	100%	Registro del mantenimiento por cada equipo.	Auxiliar Administrativo Sistemas e Informática	junio Diciembre	junio Diciembre
	N.A	Realizar el proceso de contratación del licenciamiento de software de copias de seguridad.	N.A.	N.A.	Expediente contractual, certificados del licenciamiento.	Auxiliar Administrativo Sistemas e Informática	27/10/2020	10/12/2020
	N.A	Realizar el proceso de contratación para renovar licencias y consola de administración de antivirus de la ACI Medellín.	N.A.	N.A.	Expediente contractual, certificados de licenciamiento, consola de administración y definiciones de virus actualizadas.	Auxiliar Administrativo Sistemas e Informática	17/03/2020	23/04/2020
	N.A	Realizar el proceso de contratación para renovar soporte y actualización de Fortigate 90D.	N.A.	N.A.	Expediente contractual, vigencia de soporte y actualización de dispositivo de seguridad perimetral.	Auxiliar Administrativo Sistemas e Informática	12/03/2020	31/03/2020

	N.A	Realizar el proceso de contratación de virtualización, migración y mantenimiento de servidores en nube privada con canal redundante.	N.A.	N.A.	Expediente contractual, documentación infraestructura T.I y informes mensuales de operación.	Auxiliar Administrativo Sistemas e Informática	Segundo semestre	31/12/2020
	N.A	Elaborar el Modelo de Seguridad y Privacidad de la Información.	N.A	N.A	Actualizar y ajustar el Modelo de Seguridad y Privacidad de la Información.	Auxiliar Administrativo Sistemas e Informática	Anual	Anual
	N.A	Revisar políticas de seguridad y su aplicación, software instalado en los equipos de cómputo como medida de control para evitar la instalación de software pirata.	N.A.	N.A.	Listado de equipos revisados con su respectivo usuario.	Auxiliar Administrativo Sistemas e Informática	Mensual	Mensual

8 RESUMEN DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
2018/07/17	Se crea el plan de tratamiento de riesgos de seguridad y privacidad de la información	01
2019/01/30	Se hizo revisión de todo el documento para ajustar el plan operativo	02
2020/01/16	Se realiza una revisión de todo el documento y se alinea al plan operativo	03