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

CATALINA RESTREPO CARVAJAL

Directora Ejecutiva

ASTRID MADELEINE ÁLVAREZ

Subdirectora de Relaciones Administrativas

JOHN FABIO GÓMEZ GARCÍA

Auxiliar Administrativo de Sistemas e Informática

2018

CONTENIDO

Pág.

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 intervienen en el manejo y custodia de la información en la ACI Medellín, con el fin de salvaguardar el mayor activo de la Agencia la información.

1.2 Objetivos específicos

- ✓ Concientizar y comprometer a todos los funcionarios 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.
- ✓ 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 benéficos que trae su aplicación y los efectos malignos para la entidad por su desconocimiento y una posible ejecución.

2 ALCANCE

Este plan de tratamiento de riesgos de seguridad y privacidad de la información, suministra metodologías y conceptos para la Agencia que apalancaran la administración y gestión de los riesgos a nivel de los 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 se depende no solo del plan, también de las partes involucradas y su participación activa, es preciso identificar los actores que intervienen.

Comité Directivo: aprueban los lineamientos conceptuales y metodológicos definidos en el mapa de riesgos institucionales con respecto a la seguridad y privacidad de la información de la entidad, es responsable de fortalecer e incentivar las políticas allí definidas dando cumplimiento a la administración del riesgo.

Subproceso del Sistema Integrado de Gestión: es el ente encargado de generar la metodología para la administración del riesgo de seguridad y privacidad de la información con apoyo del auxiliar administrativo en sistemas e informática de la entidad; coordina, lidera, asesora y capacita en su objeto funcional.

Integrantes de los procesos tanto misionales como administrativo: 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 y el Auxiliar Administrativo en Sistemas e informática, 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 pueden aportar a la identificación de posibles riesgos que puedan afectar la información institucional.

Control Interno: es su responsabilidad verificar y evaluar la elaboración, la visibilización, el seguimiento y el control del mapa de riesgos, conforme a la 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 guía 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 servidores 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 de 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 o de manera intencional.
- Alteración de claves y de información.
- Corte del servicio de internet por parte del ISP (Proveedor del Servicio de Internet).
- Daño de equipos y 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.
- 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 muy estable, en cualquier momento se puede caer el canal de internet y quedarían estos servicios fuera del alcance.

Adecuaciones al centro de datos.

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

1. El cuarto técnico no cuenta con el espacio adecuado,

2. En el mismo hay cajas de breques que no es recomendable, ya que puede haber un corto circuito.

3. El cuarto técnico cuenta con un aire acondicionado que solo controla la temperatura (no es de precisión) no controla la humedad y no es automático.

4. No se cuenta con un piso falso, el que se tiene actualmente es de madera, lo que puede generar un incendio y genera estática.

Todo esto puede 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 6 años en funcionamiento excelente, pero existe el riesgo de que algo falle.

6 MAPA DE RIESGOS

HERRAMIENTA ADMINISTRACIÓN DE RIESGOS

Código: FR-SIG-11
Versión: 04
Vigencia: 2018/04/18

TIPO DE PROCESO	Apoyo
PROCESO / 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 de la información y velar por el correcto funcionamiento de todos sus sistemas de información.

RIESGO/OPORTUNIDAD (posibilidad de falla / crecimiento)	Causa	Consecuencia	Riesgo Inherente			Controles	Riesgo Residual			Opciones de manejo	Acciones/Oportunidad	Responsable	Fecha	Registros
			Probab.	Impacto	Nivel de Riesgo		Probab.	Impacto	Nivel de Riesgo					
Pérdida de información y/o documentación digital, producto de una inadecuada custodia de ésta	Virus Informático Sabotaje (ataque informático) Daños de hardware y software Falta de mantenimiento preventivo Corte general del fluido eléctrico	Reprocesos Trastornos en la operación	4	4	zona de riesgo extrema	Realizar copias de seguridad en medios externos como cintas y discos	2	2	zona de riesgo baja	Asumir el riesgo	A: Revisar continuamente los trabajos de copias de seguridad	Auxiliar Administrativo Sistemas e Informática / Subdirección de Relaciones	Permanente	Registro de copias de seguridad
						Antivirus instalados y actualizados en los servidores y equipos					A: Garantizar que la custodia de la cinta de copia de seguridad sea entregada al proveedor de archivo para su custodia	Auxiliar Administrativo Sistemas e Informática/Profesional	Según necesidad	Formato de transferencia documental
						Se tiene seguridad en el perímetro de la red, mediante un firewall					A: Realizar la contratación cada año de la renovación del software de copias de seguridad	Auxiliar Administrativo Sistemas e Informática / Subdirección de Relaciones	Noviembre	Expediente contractual
						Se cuenta con la herramienta de almacenamiento en la nube OneDrive					O: realizar visita a las instalaciones de Alpopular para verificar la adecuada custodia de las copias de seguridad	Auxiliar Administrativo Sistemas e Informática/Profesional	Segundo semestre	Acta de reunión
						Se tienen diseñados recursos compartidos para cada uno de los procesos, con el fin de que sea almacenada allí la información institucional								
Inadecuado funcionamiento del clúster de servidores	Corte general del fluido eléctrico Daños de hardware y software Falta de mantenimiento preventivo Falta de actualizaciones de software Obsolescencia de tecnología	Trastornos en la prestación del servicios Los usuarios no pueden realizar sus labores diarias Sistemas de información no operativos	4	3	zona de riesgo extrema	Mantener actualizadas las licencias del software de virtualización Vmware	2	1	zona de riesgo baja	Asumir el riesgo	O: Analizar la oportunidad de realizar la actualización de las UPS con que cuenta la entidad	Auxiliar Administrativo Sistemas e Informática	Segundo semestre	Acta de reunión y/o expediente contractual
						Realizar copias de seguridad a las máquinas virtuales								
Inadecuado y deficiente funcionamiento de equipo de computo	Corte general del fluido eléctrico Daños de hardware y software Falta de mantenimiento preventivo Falta de actualizaciones de software Sabotaje (ataque informático) obsolescencia de tecnología	Trastornos en la prestación del servicios Los usuarios no pueden realizar sus labores diarias Sistemas de información no operativos Reprocesos en las actividades del desarrollo de las funciones	4	3	zona de riesgo extrema	Realizar el mantenimiento preventivo y correctivo	2	1	zona de riesgo baja	Asumir el riesgo	O: Tener presente en los proyecto de renovación y adquisición de la infraestructura tecnológica, extender la garantía de los equipos al tiempo máximo que de el fabricante	Auxiliar Administrativo Sistemas e Informática	Cuando aplique	Garantías de los equipos adquiridos
						Contar con la garantía de los equipos vigentes								
Perdida del servicio de internet	Corte del servicio de internet por daños en la infraestructura del proveedor Fallas en la prestación de servicios de internet dentro de la red LAN	Paro de funciones Trastornos en las labores de los funcionarios de la ACI Sistemas de información en la nube no operativos	3	3	zona de riesgo alta	Contar con equipos como switches de red y accespoint	1	1	zona de riesgo baja	Asumir el riesgo	O: Contar con un segundo canal de internet con otro ISP (Proveedor de servicio), no necesariamente de la misma capacidad del actual, pero sí que permita tener conexión a la nube para no quedar fuera de los servicios cloud por la falla del primer canal	Auxiliar Administrativo Sistemas e Informática / Subdirección de Relaciones Administrativas	Segundo semestre	Acta de reunión y/o expediente contractual
						Contar con el soporte por parte del proveedor								
Deficiente funcionamiento del centro de cómputo	Incendio Inundación Terremoto Daños de hardware y software Sabotaje (ataque informático) Fallas en el servicio eléctrico Corto Circuito	Paro de funciones Trastornos en las labores de los funcionarios de la ACI Sistemas de información en la nube y locales no operativos	3	3	zona de riesgo alta	Contar con extintores para eventos de incendios	1	1	zona de riesgo baja	Asumir el riesgo	O: Reestructurar el centro de datos con un espacio mínimo de 14 metros cuadrados, lejos de instalaciones hidrosanitarias evitando filtraciones de agua; ubicarlo donde no haya tableros electrónicos, generadores o transformadores; preferiblemente el data center debe estar ubicado en un lugar central a las estaciones de trabajo, tener un aire acondicionado óptimo donde se regule tanto la	Auxiliar Administrativo Sistemas e Informática / Subdirección de Relaciones Administrativas	Segundo semestre	Acta de reunión y/o expediente contractual
						Contar con las pólizas de las aseguradoras vigentes								
						Controlar el accedo a personas no autorizadas								
Obsolescencia de la infraestructura tecnológica	Cambios en la normativa Falta de capacitación en el manejo del software cuando se actualiza Falta de presupuesto y recursos escasos Falta de proyectos para desarrollo y renovación de la plataforma tecnológica	Atraso tecnológico de la entidad Desgaste administrativo por gestión deficiente Inconformidad de los usuarios Lentitud en procesamiento de información	3	3	zona de riesgo alta	Proyecto de renovación y adquisición de la infraestructura tecnológica	1	1	zona de riesgo baja	Asumir el riesgo	A: Renovación periodica de equipos, teniendo en cuenta su hoja de vida y las garantías que dan los fabricantes. O: Reuniones y visitas técnicas con proveedores expertos en temas de centro de datos, los cuales den opiniones claras que ayuden a la Agencia a tomar decisión de compra de equipos nuevos, continuar con lo que se tiene y ver como mitigar el riesgo o arrendar en modo	Auxiliar Administrativo Sistemas e Informática / Subdirección de Relaciones Administrativas	Cuando aplique	Concepto técnico
						Mantener actualizadas las licencias de Office 365, antivirus, CRM, sistema operativo								
						Destinación presupuestal para la adquisición de tecnología								
Vulnerabilidad de la red informática por parte de personal no autorizado con el fin de beneficiar un interés particular	Sabotaje (ataque informático)	Trastorno en la prestación del servicios Reprocesos	1	10	zona de riesgo baja	Se tienen definidos los permisos de acceso a la información, de acuerdo a los perfiles del cargo	1	10	zona de riesgo baja	Eliminar o reducir	A: Aplicar los permisos a los recursos compartidos	Auxiliar Administrativo Sistemas e Informática	Permanente	Configuración avanzada de seguridad de cada unidad de red
						Se tiene implementada una plataforma de antivirus en los equipos y servidores					A: Realizar la contratación de las renovaciones del antivirus		Cuando aplique	Expediente contractual
						Se cuenta con el firewall fortigate 90D el cual se encarga de controlar los accesos externos a la Red interna de la ACI Medellín					A: Realizar los procesos de contratación para la compra y actualización de la plataforma tecnológica		Cuando aplique	Expediente contractual
						Se tienen diseñadas políticas de seguridad de la información					O: Socializar y capacitar a los funcionario de la Agencia sobre las políticas de seguridad informática		Segundo semestre	Acta de reunión
Uso indebido de la información	No hacer buen uso de las herramientas definidas para el proceso y falta de apropiación de las herramientas definidas Falta de principios, valores, ética laboral	Pérdida de integridad, confidencialidad y resguardo de la información	2	20	zona de riesgo Alta	Cláusula de manejo de información en el contrato laboral	2	20	zona de riesgo alta	Tomar las medidas necesarias para llevar el riesgo a zona moderada, baja o eliminarlo	O: Socializar y capacitar a los funcionario de la Agencia sobre las políticas de seguridad informática	Auxiliar Administrativo Sistemas e Informática	Segundo semestre	Acta de reunión
						Usar los canales oficiales de comunicación								
						Toda la información oficial debe estar guardada en los sistemas de información implementados en la Agencia y en las unidades de red de cada proceso								

7 CRONOGRAMA

SUB-DIRECCIÓN	Relaciones Administrativas - Plan de Tratamiento y Riesgos y Seguridad de la Información

PLAN INSTITUCIONAL	OBJETIVO TACTICO	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	INDICADOR	META INDICADOR	ENTREGABLE	Fecha inicio	Fecha fin	ENERO				FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE			
									s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4
Plan de Tratamiento y Riesgos y Seguridad de la Información	8. Establecer un modelo de trabajo institucional acorde con las tendencias internacionales (organización flexible), que permita mayor eficiencia en el desarrollo de los procesos.	Actualizar la herramienta para la construcción de los mapas de riesgo, según la guía del DAFP, teniendo en cuenta el componente de riesgos de corrupción.	Estudiar la metodología definida por el DAFP para la administración de riesgos y realizar la actualización del formato FR-SIG-11 Herramienta de riesgos	N.A.	N.A.	Herramienta para la construcción de los mapas de riesgos actualizada	19/02/2018	28/02/2018							x	x																																				
		Capacitar a todos los servidores en la herramienta para la construcción y/o actualización de los mapas de riesgos, según la guía del DAFP, incluyendo el componente de los riesgos de corrupción.	Adelantar reuniones con cada uno de los procesos y subprocesos para capacitar en los ajustes realizados al formato FR-SIG-11 Herramienta de riesgos	N.A.	N.A.	Servidores capacitados	02/03/2018	16/03/2018									x	x	x																																		
		Revisar y ajustar de ser necesario los mapas de riesgos de los procesos y subprocesos, incluyendo el componente de los riesgos de corrupción.	Adelantar reuniones con cada uno de los procesos y subprocesos para revisar y ajustar los mapas de riesgos	N.A.	N.A.	Mapa de riesgos actualizados	05/03/2018	20/03/2018										x	x																																		
		Consolidar el mapa de riesgos institucional, incluyendo el componente de riesgos de corrupción.	Construir el mapa de riesgos incluyendo el componente de corrupción de la ACI Medellín	N.A.	N.A.	Mapa de riesgos definitivo	23/03/2018	23/03/2018											x																																		
		Realizar la publicación del Mapa de Riesgos en la página web institucional.	Solicitar a Juan Carlos Valencia por medio de correo electrónico la publicación del mapa de riesgos en la página web de la ACI Medellín	N.A.	N.A.	Mapa de riesgos publicado	03/04/2018	03/04/2018															x																														
		Realizar actualización a la política de administración de riesgos adoptada en el 2016 mediante la Resolución Nro. 206, conforme a la normativa vigente.	Realizar reunión con control interno para actualizar la política de riesgos	N.A.	N.A.	Política de administración de riesgos actualizada	23/02/2018	23/02/2018							x																																						
		Consolidar cada seis meses el resultado del monitoreo realizado a la gestión de los riesgos, con el fin de garantizar que los controles establecidos en los mapas de riesgos son efectivos, aplicar los ajustes necesarios.	Elaborar informe con los resultados del monitoreo realizado a los mapas de riesgos	N.A.	N.A.	Seguimiento a los mapas de riesgos	21/05/2018 16/11/2018	30/05/2018 23/11/2018																					x	x																				x	x				

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