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

Oficina de Información y Comunicaciones
Barranquilla 2019
Versión 1.0

Historia de Revisión

Fecha	Versión	Descripción	Autor
26/11/2019	1.0	Creación del documento	Leonardo F. Pérez López

Contenido

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

1. Introducción

La administración de la información abarca aspectos que van desde el manejo de documentos en medio análogo (papel) como el proceso de almacenaje y recuperación conocido como gestión documental, hasta los sistemas de información que tenga la organización para gestionar los procesos o sistemas externos en los que publica información para entidades de control, pasando por aspectos como el almacenamiento de los datos digitales, políticas de respaldo y planes de contingencia para asegurar el continuo funcionamiento de la entidad y lograr los objetivos.

Es por ello que los activos de información han pasado a formar parte de la actividad cotidiana de organizaciones e individuos; los dispositivos electrónicos almacenan información, la procesan y la transmiten a través de redes y canales de comunicación, abriendo posibilidades a sufrir alguna amenaza, de tal manera que realizar un análisis de riesgo a la información es de crucial importancia para prever posibles riesgos que pueda sufrir la información.

2. Objetivo

Con el presente plan se pretende brindar al Área Metropolitana de Barranquilla una herramienta que ayude a desarrollar, planear, establecer y fortalecer los conceptos para una óptima administración, análisis y tratamiento de riesgos para los activos de información.

2.1. Objetivos Específicos

- Especificar la metodología para aplicar el plan de tratamiento de riesgo de seguridad y privacidad de la información, que contenga la identificación de los activos de información, con sus posibles vulnerabilidades y amenazas, así como el riesgo que implican y los controles a aplicar.
- Analizar y valorar los riesgos de seguridad de la información en la probabilidad de impacto en la ocurrencia de un evento
- Abordar y mitigar los riesgos por medio de la identificación, análisis, valoración, tratamiento y control de los activos de información más relevantes que se presentan en los activos de información en la entidad Área Metropolitana de Barranquilla.

3. Alcance

Esta metodología podrá ser aplicada a todos los procesos del Area Metropolitana de Barranquilla y pretende abordar todos los activos de información para aplicaciones, para servidores y servicios que son los

procesos más importantes considerados por la Oficina de Información y Comunicaciones, siguiendo los lineamientos del marco normativo en la ley

4. Marco conceptual[1]

4.1. Administración de riesgos

Conjunto de elementos de control que, al interrelacionarse, permiten a la Institución evaluar aquellos eventos negativos tanto internos como externos, que pueden afectar o impedir el logro de los objetivos institucionales, o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función.

4.2. Amenaza

Situación que potencialmente cause perdidas.

4.3. Análisis costo- beneficio

Es una herramienta de la administración del riesgo usada para tomar decisiones sobre las técnicas propuestas por el grupo para la administración de los riesgos, en la cual se valoran y comparan los costos, financieros y económicos, de implementar la medida, contra los beneficios generados por la misma. Una medida de la administración del riesgo será aceptada siempre que el beneficio valorado supere al costo.

4.4. Análisis de riesgo

Determinar el impacto y la probabilidad del riesgo, dependiendo de la información disponible, pueden emplearse desde modelos de simulación, hasta técnicas colaborativas.

[1] Definiciones tomadas: GUÍA DE ADMINISTRACIÓN DEL RIESGO – DAFP

4.5. Causas

Son los medios, circunstancias y agentes que generan riesgo.

4.6. Consecuencias

Efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso de la Institución. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento[2].

4.7. Control

Es toda acción que tiende a modificar los riesgos, significa analizar el desempeño de las operaciones, evidenciando posibles desviaciones frente al resultado esperado para la adopción de medidas preventivas. Los controles proporcionan un modelo operacional de seguridad razonable en el logro de los objetivos.

4.8. Costo

Se entiende por costo las erogaciones, directas e indirectas, en que incurre la Institución en la producción, prestación de servicio o manejo de un riesgo.

4.9. Evento

Se entiende como un incidente o suceso, el cual ocurre durante un determinado intervalo de tiempo específico.

4.10. Factores de riesgo

Manifestaciones o características medibles u observables de un proceso, que indican la presencia de Riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la Institución.

4.11. Identificación de riesgo

Establecer la estructura del riesgo; fuentes o factores internos o externos generadores del riesgo; puede hacerse a cualquier nivel total por unidad, por

[2] Función Pública. Manual Técnico del Modelo Estándar de Control Interno para el Estado Colombiano -MECI- 2014

áreas, por procesos, incluso, bajo el viejo paradigma, por funciones, desde el nivel estratégico hasta el operativo.

4.12. Impacto

Son las consecuencias o efectos que puede generar la materialización del riesgo de corrupción en la entidad.

4.13. Indicador

Es la valoración de una o más variables que informa sobre una situación y soporta la toma de decisiones, es un criterio de medición y de evaluación cuantitativa o cualitativa.

4.14. Mapa de riesgo

Herramienta metodológica que permite hacer un inventario de los riesgos de manera ordenada y sistemática, definiéndolos e identificando la descripción de cada uno de ellos y las posibles consecuencias.

4.15. Plan de manejo de riesgo

Plan de acción propuesto por el grupo de trabajo, cuya evaluación de beneficio-costo resulta positiva y es aprobado por la Alta Dirección.

4.16. Probabilidad Oportunidad de ocurrencia de un riesgo.

Se mide según la frecuencia (número de veces en que se ha presentado el riesgo en un período determinado) o por la factibilidad (factores internos o externos que pueden determinar que el riesgo se presente)[3]

4.17. Proceso

Conjunto de actividades mutuamente relacionadas o que interactúan para generar un valor.

[3] ICONTEC. NTC31000:2011. Gestión del Riesgo. Términos y Definiciones

4.18. Riesgo

Posibilidad de ocurrencia de toda aquella situación que pueda entorpecer el normal desarrollo de las funciones de la Institución y le impidan el logro de sus objetivos o afectar aspectos en el patrimonio institucional, el logro de los objetivos misionales y el diseño y desarrollo de las estrategias institucionales.

4.19. Riesgo Residual

Es el riesgo que queda cuando las técnicas de la administración del riesgo han sido aplicadas.

4.20. Seguimiento

Recolección de información regular y sistemática sobre la ejecución del plan, que sirve para actualizar y mejorar la planeación futura.

4.21. Seguridad de la información

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

4.22. Sistemas

Conjunto de elementos coordinados y ordenados, relacionados entre sí, que generan un determinado resultado o salida.

4.23. Técnicas para el tratamiento del riesgo

Evitar o prevenir, reducir, dispersar, compartir o transferir y asumir riesgos.

4.24. Valoración del riesgo

Es el resultado de confrontar la evaluación del riesgo con los controles existentes.

4.25. Vulnerabilidad

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

5. Metodología de análisis de riesgo

Son desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas. Existen dos tipos: Las cuantitativas y las cualitativas, de las que existen gran cantidad de ambas clases y sólo se centrará en la utilizada para el proyecto y caso de estudio específico en la Entidad Área Metropolitana de Barranquilla. La metodología que el proyecto adopta es MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información):

El desarrollo del presente proyecto se realiza en diferentes partes, las cuales se describen a continuación:

Para la ejecución del análisis de riesgos se adopta el ciclo de mejora continua PHVA como lo recomienda la norma ISO/IEC 2700:

Ilustración 1: PHVA

- **Parte 1**.

  Identificación de los activos de información dentro de la organización en materia de seguridad de la información.

  ✓ Actividades:

- Recolectar información en las diferentes áreas a fin de identificar el estado actual de los diferentes procesos y catalogar el nivel de importancia que tiene para la entidad los activos de información.
- Realizar un análisis cualitativo y cuantitativo de los activo de información.

- **Parte 2.**

  En segunda instancia realizar el análisis del estado actual, esta parte busca recolectar la mayor cantidad de información posible con respecto al estado actual, estudios o proyectos que tengan relación con el análisis de riesgos y en general en materia de seguridad informática en la institución

  ✓ Actividades: Teniendo en cuenta el análisis obtenido de la recolección y organización de la información recolectada para determinar la calificación de los riesgos.

- **Parte 3.**

  Realizar El análisis de Riesgos que vincula los activos utilizados en el área de Tecnologías de la información.

  ✓ Actividades:

  - Realizar la identificación de las amenazas en conjunto por la Oficina de Información y Comunicaciones del Area Metropolitana de Barranquilla.
  - Realizar la identificación de Vulnerabilidades que pueden tener mayor afectación en la Oficina de Información y Comunicaciones.
  - Realizar la identificación de Salvaguardas ya sean físicos o lógicos que permitan reducir los riesgos que se puedan presentar.

- Realizar la evaluación del Riesgo en el cual la Oficina de Información y Comunicaciones priorice los de problemas potenciales en los cuales puede incurrir.
- Realizar el tratamiento del riesgo por parte de la Oficina de Información y Comunicaciones.

- **Parte 4.**

  Crear la metodología para el análisis de riesgo que serán aplicadas al área de tecnologías de la información del Área Metropolitana de Barranquilla para mitigar los riesgos.

5.1.1. Identificación de activos de información

El primer punto para el análisis es estudiar los activos vinculados a la información. Es habitual agrupar los activos por grupos para ello. En nuestro caso, podemos agrupar los activos por grupos en los que nos centraremos son:

- [L] Lugar
- [HW] Hardware
- [SW] Software
- [COM] Red
- [O] Organización
- [P] Personal

En esta parte se presenta el inventario y clasificación de los activos de información que son manejados por los funcionarios de la entidad a través del proceso de Informática Métodos y Procedimientos, con el fin principal de determinar qué activos posee el área de informática, reconocer el valor de

cada activo, y determinar su clasificación para que sea utilizada adecuadamente.

La realización de un inventario y clasificación de activos de información hace parte de la debida diligencia que a nivel estratégico ha considerado el área de informática dentro de sus elementos a tratar con respecto a la seguridad para los activos de información de la Empresa.

Las mejores prácticas de seguridad de la información a nivel nacional e Internacional recomiendan de manera imperativa la realización de un inventario y clasificación de los activos de información de las organizaciones, para determinar cómo deben ser utilizados en los procesos del negocio, los roles y las responsabilidades que tiene el personal sobre la misma, reconociendo adicionalmente los niveles de confidencialidad que a cada activo debe dársele.

De esta forma y con base en las normas técnicas colombianas NTC ISO/IEC 27001 en el ítem “Gestión de Activos” se persigue dar cumplimiento a dos puntos principales que son explícitos en las mismas así:

Inventario de Activos: Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes de la entidad.

Propiedad de los Activos: Toda la información y los activos asociados con los servicios de procesamiento de información deben ser “propiedad”3 de una parte designada de la entidad.

5.1.1.1. Identificación de activos

Los activos presentes en la Organización Area Metropolitana de Barranquilla, son identificados y clasificados tomando como base el Libro II de la metodología MAGERIT versión 3, en donde nos presenta el catálogo de elementos:

Tabla 1: Activos

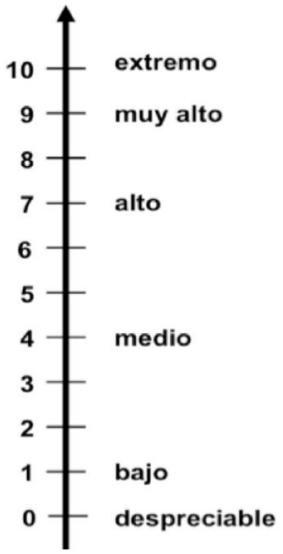
ITEM	TIPO	NOMBRE DEL ACTIVO
1	APLICACIONES INFORMATICAS	1. [SW_SINCOW] Sistema de Información Administrativa y Financiera. 2. [SAAS_MOVILIZA] Sistema de Gestión de Tramites de Transporte Publico e Individual Metropolitano. 3. [SW_ITS] Aplicativo BPMS para la gestión de procesos en Gestión Documental 4. [SO] Sistema Operativo. 5. [HER_SW] Herramientas Software. 6. [ANT_VIR] Anti virus EnPoints
2	SERVICIOS	7. [SV_DNS] Servidor DNS 10. [SV_DHCP] Servidor DHCP 11. [SV_BD] Servidor Bases de Datos 12. [SV_CAM] Servidor Cámaras
3	REDES DE COMUNICACIONES	13. [RO_ISP] Router Proveedor de Servicios de Internet.
4	EQUIPAMIENTO AUXILIAR	14. [CAB_RED] Cableado de Red 15. [UPS] Sistema de Alimentación interrumpida.
5	INSTALACIONES	16. [GAB] Gabinete de Red
6	PERSONAL	17. [PU_TIC] Profesional Universitario Tecnologías de Información y Comunicaciones 18. [AS_TIC] Asesor Tecnologías de Información y Comunicaciones 19. [CO] Contratista.

Fuente: Autor

5.1.2. Criterio de valoración

Magiret, presenta una escala de valoración logarítmica, cuyo objetivo es hacer una valoración cualitativa respondiendo a valoraciones subjetivas por parte del personal de la entidad.

Ilustración 2: Escala de Valores[4]



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Existen dimensiones de valoración, que son características de cada activo. De cada uno de ellos se determina cuan relevante es ese activo y cómo afectaría a la entidad si la amenaza llegara a materializarse.

5.1.3. Valoración de activos.

Para realizar el proceso de valoración de activos de acuerdo a la metodología MAGERIT Versión 3; se usa las siguientes dimensiones:

- [D] disponibilidad: Para calificar el criterio de disponibilidad debemos responder a cuál sería la importancia que tendría el activo sino estuviese disponible.

[4] Tomado de: Magerit_v3_libro2_catalogo de elementos_es_NIPO_630-12-171-8

- [I] integridad de los datos: Calificación de la importancia del activo si este es modificado sin autorización.
- [C] confidencialidad de la Información: Se define por la importancia que tendría el activo si accediera de manera no autorizada.

5.2. Análisis actual de la Información

Mediante el análisis, observación y entrevistas se determinaran los estados actuales, tanto estructurales, de sistemas de información y de activos, con el fin de crear un esquema actualizado global y determinar en que estado se encuentra actualmente la seguridad de la información en el AMB.

5.3. Mapa de riesgo

De la valoración de los activos realizada se han considerado las amenazas que producen más daños, para evaluar el nivel de degradación, frecuencia y el riesgo implicado aplicado solo a los activos de información.

5.4. Caracterización de las salvaguardas

La caracterización de salvaguardas se realiza de acuerdo al nivel de criticidad delos activos incluidos en el análisis de riesgos de la Entidad Area Metropolitana de Barranquilla, basados en el catálogo de elementos que proporciona Magerit v 3.0.

Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar.

5.5. Estimación del estado del riesgo

Actividad realizada con el propósito de analizar los datos recopilados en las actividades anteriores y evaluar el estado de riesgo, donde se incluye la estimación de impacto y riesgo. Se toma la siguiente escala para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

Tabla 1: Escala para calificar el valor de los activos

Muy Alto	MA	
Alto	A	
Medio	M	
Bajo	B	
Muy Bajo	MB	

5.6. Verificación

El Área Metropolitana de Barranquilla en coordinación con la Oficina de Información y Comunicaciones, toma especial importancia en los registros de evidencias o eventos que dejan los diferentes controles, asi como los indicadores que permiten verificar el correcto funcionamiento del plan de tratamiento, mediante mecanismos que le permitan la evaluación eficaz y de éxito en los controles implementados.

5.7. Controles

Para especificar los controles del AMB de acuerdo al ciclo PHVA se deben contemplar los siguientes: Controles relacionados con terceros, acuerdos de control de accesos, controles contra software malicioso, administración de medios informáticos removibles, seguridad del correo electrónico, control de

acceso al sistema operativo, procedimientos de conexión de terminales, identificación y autenticación de los usuarios, sistema de administración de contraseñas y control de acceso a las aplicaciones.