VERSIÓN 1.0
ENERO 2019

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

1. INTRODUCCIÓN

La Administración de riesgos es un método sistemático que permite establecer a las entidades identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos en función de la tecnología, equipos, infraestructura etc., asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todo el equipo humano del instituto de turismo del Meta, en cumplimiento de sus funciones, está expuesto a riesgos, por lo tanto, se hace necesario establecer una estructura y metodología en conjunto con lo dictaminado por el Ministerio de las Tics, para identificar las causas y consecuencias evitando la materialización de los eventos detectados, teniendo como fin la seguridad de la información bajo los principios de Integridad, Disponibilidad y Confidencialidad de la información.

2. OBJETIVOS

2.1 Objetivo General

Establecer la estructura metodológica para la administración de riesgos en la Instituto de Turismo del Meta.

2.2 Objetivos Específicos

- ✓ Generar pautas para la determinación de los riesgos en el ITM.
- ✓ Fomentar el uso y apropiación de la Política de Seguridad vigente en los funcionarios y contratistas.
- ✓ Involucrar y comprometer a todos los funcionarios y contratistas en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

3. ALCANCE

El presente documento está enfocado en mejorar la estrategia para el análisis, diseño, ejecución y control de los riesgos, generados en las actividades cotidianas por el uso frecuente de información.

La mitigación de los riesgos como debe ser establecida bajo un proceso estructurado y sistemático es por ello que esta guía contiene desde la definición de los roles y responsabilidades hasta los formatos que deben ser diligenciados en el proceso de identificación.

4. DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- ✓ **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.
- ✓ **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- ✓ Amenaza: situación externa que no controla la entidad y que puede afectar su operación
- ✓ **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- ✓ **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- ✓ **Causa**: medios, circunstancias y/o agentes que generan riesgos.
- ✓ **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- ✓ **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
- ✓ **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.

- ✓ **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- ✓ **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- ✓ **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- ✓ **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
- ✓ **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
- ✓ **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- ✓ **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
- ✓ **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- ✓ **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
- ✓ **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- ✓ **Mapa de riesgos:** documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- ✓ **Materialización del riesgo:** ocurrencia del riesgo identificado
- ✓ **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- ✓ **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
- ✓ **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

- ✓ **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- ✓ **Proceso:** conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.
- ✓ **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.

5. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

El instituto de turismo del Meta adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, mediante el apoyo del director, subdirectores, funcionarios y contratistas por lo que se comprometen a:

1. Conocer y cumplir la política de seguridad de la información municipal.
2. Replicar con sus equipos de trabajo fortaleciendo el trabajo mancomunado con la oficina de tecnología fortaleciendo la conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
3. Aprobar la revisión frecuente de los procesos y procedimientos para la identificación de nuevos riesgos o control de los existentes.
4. Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto

Para mitigar y lograr lo mencionado anteriormente es necesario que sean asignados recursos humanos, presupuestales y tecnológicos que permitan cerrar las brechas detectadas y mejorar los controles existentes.

6. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

A continuación, se presenta cada una de las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

6.1 Análisis contexto estratégico

Definir el contexto estratégico marca la pauta o ruta que la entidad debe asumir frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, evitando establecer las condiciones ideales para la materialización.

Para la definición del contexto estratégico, es fundamental tener claridad sobre cuál es el plan de gobierno hacia dónde va el municipio y cuáles son los planes programas o proyectos a ejecutarse, así mismo diferentes áreas deben trabajar de forma responsable en conjunto con la oficina de gestión tecnológica lo cual mitigaría la toma de decisiones errada en cuanto a tecnología se refiere ya que se identifican de forma temprana los posibles riesgos que se puedan presentar.

6.2 Identificación de riesgos

En esta fase del documento el objetivo es evaluar todos los activos que se encuentran, considerando las dependencias existentes entre ellos y realizando una valoración sobre estos. De esta forma se definirá claramente un punto de salida de todos los activos, sean estos tangibles o no, dentro de la compañía y pudiendo analizar a qué amenazas podrían estar expuestos estos activos.

Una vez disponemos de un listado de las amenazas reales que pueden afectar a nuestros activos, estaremos en disposición de poder realizar la evaluación del impacto que sufrirá la compañía en caso de que se materialicen estas amenazas.

El impacto, junto con los resultados anteriormente explicados dará una serie de datos que nos permitirán priorizar el plan de acción y, al mismo tiempo, evaluar como se ve modificado este valor una vez se apliquen las contramedidas o bien, el riesgo que estamos dispuestos a asumir (riesgo residual) por parte del instituto.

Como resultado de esta fase, podremos obtener:

- ✓ Un análisis detallado de los activos relevantes de seguridad de la entidad.
- ✓ Un estudio de las posibles amenazas sobre los sistemas de información, así como su impacto.
- ✓ El resultado final, será el impacto potencial que tendrá la materialización de las diferentes amenazas a las que están expuestos nuestros activos.

6.2.1 Inventario de activos

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

Los resultados de este estudio se recogerán en una tabla que facilitará posteriores estudios. La tabla se dividirá en dos columnas donde se recogerá la información aquí dispuesta y clasificada. Para la primera columna se encontrará el ámbito del activo con el objetivo de realizar las agrupaciones y, en la segunda columna se encontrará el activo concreto.

7. DIMENSIONES DE SEGURIDAD

Desde el punto de vista de la seguridad, junto a la valoración de los activos, se ha de indicar cuál es el aspecto de la seguridad más crítico. Esto será de gran ayuda en el momento de pensar en posibles medidas de prevención, ya que serán enfocadas en aquellos aspectos más críticos.

Una vez identificados los activos, se ha de realizar la valoración de estos. Esta valoración mide la criticidad a las cinco dimensiones de la seguridad de la información gestionada por el proceso de la entidad. Esta valoración nos permitirá, a posteriori, valorar el impacto que tendrá la materialización de la amenaza sobre la parte del activo expuesto.

El valor que reciba el activo puede ser propio o acumulado. El valor propio se asignará a la información, quedando el resto de los activos subordinados a las necesidades de explotación y protección de la información. De esta manera, los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se apoyan en ellos. Cada activo de información puede tener un valor diferente en cada una de las diferentes

dimensiones para la organización que deseamos analizar. Por esto, se ha de tener presente siempre que representa cada dimensión.

Las cinco dimensiones de las que se habla son:

- ✓ [C] Confidencialidad. Únicamente las personas autorizadas tienen acceso a la información sensible o privada.
- ✓ [I] Integridad. La información y los métodos de procesamiento de esta información son exactos y completos, y no se han manipulado sin autorización
- ✓ [D] Disponibilidad. Los usuarios que están autorizados pueden acceder a la información cuando lo necesiten.
- ✓ [A] Autenticidad. Hay garantía de la identidad de los usuarios o procesos que gestionarán la información.
- ✓ [T] No repudio. Hay garantía de la autoría de una determinada acción y está asociada a quien ha producido esta acción.

Una vez detalladas las cinco dimensiones se ha de tener presente la escala en que se realizarán las valoraciones. En este caso se utilizará una escala de valoración de 1 – 4 siguiendo los siguientes criterios.

VALOR	CRITERIO
1	Zona de Riesgo Bajo
2	Zona de Riesgo Moderado
3	Zona de Riesgo Alto
4	Zona de Riesgo Extremo

8. ANÁLISIS DE AMENAZAS

Las amenazas pueden afectar diferentes aspectos de la seguridad de los activos, por tanto, uno de nuestros objetivos es el análisis de qué amenazas pueden afectar los activos de la entidad. Una vez hecho esto se ha de estimar la vulnerabilidad de cada activo respecto a las amenazas potenciales.

El primer paso para realizar este análisis es disponer de una tabla de amenazas, para obtener este listado de amenazas las cruzaremos con los activos que hemos detallado en el punto anterior.

En último lugar, para valorar el impacto de las amenazas en los activos que tenemos definidos, deberemos asignar valores al impacto que produciría en el instituto de turismo la materialización de la amenaza, este valor será estimado de 1 – 4 y se define en la siguiente tabla:

VALOR	IMPACTO
1	Insignificante
2	Menor
3	Moderado
4	Mayor
5	Catastrófico

Se hacen las siguientes aclaraciones adicionales para comprender la clasificación realizada:

- ✓ Se ha realizado la división o agrupación de activos según ámbito (Instalaciones, hardware, software, etc.). Sin embargo, por darle más sentido al análisis, en algunos de los ámbitos se ha procedido a agrupar los activos según quién accede a ellos. Como las principales actividades son servicios orientados a la comunidad, se han dividido los activos que se acceden desde el exterior y los activos que únicamente se accede desde el interior. Un ejemplo de esto sería una aplicación web, donde se accede a ella desde cualquier red mundial, un portátil o un sistema operativo, donde únicamente se puede acceder desde la red de la organización. También se ha de tener en cuenta que no todas las dimensiones de la seguridad se ven afectadas por una amenaza, existirán amenazas dirigidas a vulnerar la integridad de un sistema y en cambio otras, únicamente a la disponibilidad, así como combinaciones de varias dimensiones afectadas.
- ✓ Otra decisión ha sido la de separar los datos y servicios de logs del resto de servicios, ya que la función de esta se aleja del objetivo de los servicios ofrecidos por la organización y, por tanto, no sería realista juzgarlos de igual forma y otorgar amenazas que no les involucran
- ✓ Para cada uno de los activos y sus agrupaciones, se han intentado escoger las amenazas con más sentido. Un ejemplo de esto es en algunos casos de amenazas que, por estructura o lógica de la entidad, estas no aplican. Se detallan algunas de estas en los siguientes puntos.

- ✓ Los datos de las aplicaciones se han separado del resto de datos, ya que a estos datos se pueden acceder desde el exterior, porque son gestionados por terceros que tiene acceso a ella, por tanto, no pueden tener el mismo nivel de impacto una amenaza sobre estos que sobre los datos que gestionan las funciones de la entidad, como por ejemplo los datos del sistema operativo, antivirus, etc.

Es decir, se ha intentado dar un poco de sentido a los datos, agrupando los activos según qué tipo de servicio ofrecen y quién podrá acceder a ellos. De esta manera, se enriquecen los números y se ajusta más a la realidad, ya que no es lo mismo acceder a un servicio interno como un antivirus, que a un servicio externo al que se puede acceder desde el exterior y manipular datos en ellos. Este es el motivo principal por el que se ha optado a agrupar los activos según las tablas que se presentan a continuación.

9. AMENAZAS

ACTIVO	AMENAZA
[L] Lugar	Daño en equipos y servidores por falta de un Equipo climatización centro de datos
	Mal estado de Equipos extintores
[HW] Hardware	Alteración, suplantación, eliminación o Divulgación Datos Servidor correo
	Daño o alteración Equipos de Escritorio
	Daño, alteración o fuga de información Equipos Portátiles
	Daño o alteración Impresoras
	Daño, alteración o fuga de información Servidor Aplicaciones
	Daño, alteración o fuga de información Servidor backup
	Daño, alteración o fuga de información Servidor de correo
	Malware, troyano, gusanos, descargas o visitas a través de Unidades extraíbles
[SW] Software	Daño Aplicación Sistemas Operativos
	Daño o alteración Aplicaciones ofimática
	Alteración, Suplantación o eliminación Correo electrónico
	Alteración, eliminación o Divulgación Programas de administración (contabilidad, manejo de personal, etc.)
[COM] Red	Daño o alteración Equipos de la red cableada (router, switch, etc.)
	Daño o alteración Equipos de la red inalámbrica (router, punto de acceso, etc.)

	Malware, troyano, gusanos, descargas o visitas a través de Navegación en Internet
[O] Organización	Alteración o eliminación Contables
	Alteración o eliminación Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)
	Alteración o eliminación Financieros
	Alteración o eliminación Jurídicos
[P] Personal	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de funcionarios y contratistas

10. IMPACTO POTENCIAL

Una vez terminado el análisis de los activos, presentado en las tablas anteriores y el análisis de las amenazas, podemos calcular el impacto potencial que pueden suponer para la entidad la materialización de estas amenazas.

En este apartado y, para el cálculo del impacto, no se tienen en cuenta contramedidas, por tanto, el resultado que obtengamos de este cálculo se podrá extraer un valor de referencia que ayudará para determinar y priorizar un plan de acción. Al aplicar las contramedidas, este valor se verá modificado.

Para realizar el cálculo del impacto potencial, se utiliza la siguiente fórmula:

Impacto Potencial = Activo x Impacto

Donde, es el valor de cada dimensión y el impacto es la degradación en cada dimensión en la que se ve afectado el activo también en caso de materializarse. En la tabla siguiente se presentan los resultados:

Probabilidad	Impacto				
	Insignificante	Menor	Moderado	Mayor	Catastrofico
Raro	3	1	2	0	15
Improbable	0	0	1	4	4
Posible	0	1	2	4	12
Probable	0	0	3	1	1
Casi Seguro	0	0	0	0	2

11. EVALUACIÓN DEL RIESGO

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	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

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

12. VALORACIÓN DE LOS RIESGOS

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

13. MANEJO DE RIESGOS

Estructuralmente el ITM manejara los riesgos identificados de la siguiente manera:

13.1 Controles de clase técnica

Estos controles se basan prácticamente en la gestión operativa y de aseguramiento, de zonas físicas, accesos, manipulación de hardware y software, accesos a sitios web, manejo de la información, etc. Esta es la fase de la implementación de mayor cuidado y costo, pues en este

proceso es donde está en juego la información y el éxito de la implantación del sistema de gestión y la mitigación del riesgo.

13.2 controles de clase documental

En esta fase los controles son dirigidos a reglamentar, aplicar, sensibilizar a todo el personal que labora en las organizaciones además son los controles más complicados pues con base en ello es que se les informa y distribuye el respectivo funcionamiento a los demás trabajadores.

Usualmente estas políticas, instructivos, reglamentos no son muy tenidos en cuenta por los trabajadores dejando de forma incompleta la implantación del sistema de gestión de seguridad. Es aquí donde los planes de capacitación y sensibilización deben ser planificados de la mejor manera para tener la mayor aceptación en cada uno de los trabajadores de la compañía para dar el máximo cumplimiento y sacar el máximo de efectividad con la aplicación de controles técnicos.

13.3 Implementar programas de capacitación y sensibilización

Es ideal que se programen las fechas desde el inicio y las respectivas capacitaciones y sensibilizaciones, pues de esto depende en gran parte el éxito de la implementación del sistema. Al aplicar algunos controles se deberá realizar el debido seguimiento para verificar y cuantificar la funcionalidad del mismo, sin embargo, esto no aplica para todos los

controles; Es ahí donde la sensibilización entra a jugar un papel fundamental en la compañía pues por desconocimiento los trabajadores pueden interferir o estropear el funcionamiento real del control, pues si bien es cierto que el sistema puede ser estable los usuarios son parte fundamental del éxito de cada uno.

13.4 Implementación de procedimiento de manejo de incidentes de seguridad

Cuando se habla de incidente informático, se hace referencia a un suceso que se presentó o que tiene una gran posibilidad de darse en un momento determinado. Este suceso puede ser llevado a cabo a voluntad o accidental. Dependiendo de la gravedad de la situación este puede afectar el funcionamiento normal de la organización. Por lo general el manejo del incidente implica que este se debe solucionar en el menor tiempo posible para evitar una afectación mayor y se debe buscar documentar cada uno de los eventos presentados y el tiempo que transcurrió

entre cada uno de ellos, con el fin de poderlo analizar posteriormente y aplicar correcciones del caso para que en un futuro este no se vuelva a presentar o al menos su impacto sea lo menor posible. Para ello, se pueden seguir los seis pasos ideales para mantener el orden adecuado.

13.4.1 Preparación

En este punto, se debe tener una lista de chequeo la cual ayuda a organizar la reacción ante un incidente, para esto es necesario tener conceptos claros como son:

- ✓ Políticas de la organización. Si estas existen, se debe determinar que está permitido y que no. Conducto regular de comunicación, lista de contactos, la posibilidad o no de dar información a terceros, quien está en capacidad de hacerlo entre otros.
- ✓ Recursos humanos. No basta con saber que se cuenta con determinadas áreas dentro de la organización, se necesita saber quiénes son las personas que están capacitadas para afrontar un incidente, sus números de teléfono, el escalamiento en la comunicación, entre otros.
- ✓ Información: El manejo que se le debe dar a la misma, forma de almacenamiento, importancia según el negocio, confidencialidad, integridad y disponibilidad.
- ✓ Software – Hardware: Con que elementos contamos como antivirus, firewall, ubicación de los mismos, servidores, etc.

- ✓ Comunicaciones. Con que elementos cuenta la organización para llevar a cabo la prestación de los servicios ante un incidente, medios de comunicación alternos, etc.
- ✓ Ups – Plantas Electrices – controles: Determinar claramente cuáles son los dispositivos que cuenta la organización, cuales son principales y cuáles de respaldo, el comportamiento de los mismos, tiempos de funcionamiento, plan de contingencia entre otros.
- ✓ Formatos o Plantillas. Se debe contar con elementos para registras los sucesos, el tiempo en que ocurren, como se afrontaron, observaciones, etc.

13.4.2 Detección y análisis

La detección se puede dar por llamada de algún usuario, cliente, administrador, etc., alarma presentada por algún dispositivo dispuesto para ello, como un firewall, IDS, IPS. Alteración de información, observación, medios informativos, caída de un sistema, base de datos, etc.

Una vez detectado se procede a analizar el impacto de este, con ello se disponen los elementos que se requieran para solucionar el impase. Determinar si no son falsos positivos, validar la evidencia en este caso ver logs de registros, bitácoras.

13.4.3 Contención

En esta fase se procede a neutralizar el incidente, para ello es necesario tener cautela de no eliminar evidencia que posteriormente nos ayude a analizar el origen, el posible atacante, desde cuando está llevando a cabo el proceso, en fin, información que posteriormente se estudiara. Aquí se toman decisiones de como plantear la estrategia de contención, fundamentados en importancia del activo, disponibilidad para la operación de la organización, elementos alternos o sustitutos, grado del ataque.

13.4.4 Erradicación y Recuperación

Con base en la información tomada en la detección y contención es necesario tomar las medidas del caso para que no se vuelvan a presentar. Es posible que la organización tenga que invertir en elementos de protección adicionales. Pero esta decisión debe ser fundamentada en hechos y datos, ser lo más objetivos posibles. En el proceso de

recuperación puede ser necesario restaurar las copias de respaldo, cambio de contraseñas, cambios de direcciones IP.

13.4.5 Reporte y cierre

Se hace necesario llevar a cabo un informe en el cual se documente los procesos realizados, siendo muy claros en los pasos llevados a cabo. Esta información puede servir mas adelante para resolver nuevos impases o determinar si las decisiones tomadas fueron acordes al incidente.

Se debe generar un documento de lecciones aprendidas el cual debe estar redactado por el equipo que afronto el incidente, estas lecciones aprendidas se analizaran posteriormente por una junta la cual se informara y hará los aportes para prevenir futuras situaciones. Por ultimo, dar a conocer las recomendaciones del caso y llevar a cabo las implementaciones a que haya lugar. Es bueno, volver a hacer una revisión periódica tanto a las decisiones tomadas como las inversiones hechas por la organización. Con ello evitamos que una solución planteada hoy mañana sea obsoleta y se nos presente un incidente nuevamente.

14. SEGUIMIENTO DE RIESGOS

Cuando se solicitado por el comité, se presentaran avances sobre el funcionamiento y manejo del riesgo en la administración en cuanto al cumplimiento de las políticas y directrices para la administración del riesgo y la administración de los riesgos por proceso.

Los resultados de la evaluación y las observaciones del comité deben ser posteriormente solucionadas y entregadas al director, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la organización.

15. MAPA DE RIESGOS

Una vez se tenga toda la información relacionada en los numerales anteriores, se documentará la información en el formato Mapa de riesgos de la Institución