OBJETIVO:

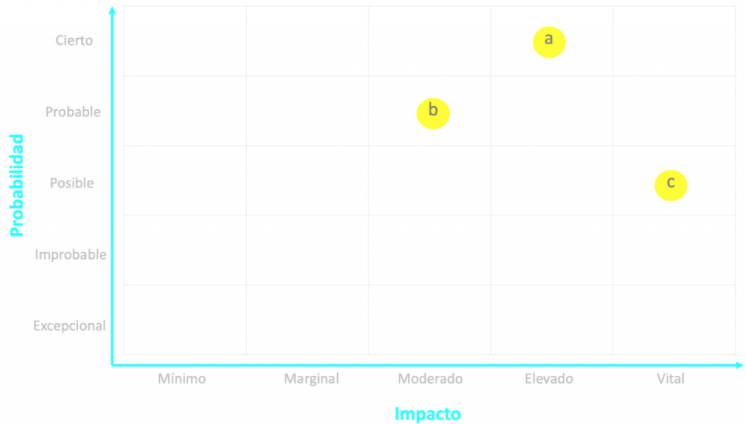
El objetivo de este plan de gestión de riesgos y oportunidades es potenciar los efectos deseables de las Oportunidades del área aumentando la probabilidad y el impacto de los eventos positivos. Disminuir o eliminar la probabilidad y el impacto de los eventos negativos es decir las debilidades y amenazas. Para ello es necesario realizar una correcta gestión de los riesgos del departamento de sistemas.

ALCANCE

El alcance para este plan es la gestión de riesgos y oportunidades del departamento de sistemas y para los equipos propiedad de Giotex que se encuentren dentro de la planta y oficinas. Dicha gestión incluye los procesos necesarios para llevar a cabo la planificación de la gestión de los riesgos y oportunidades, identificación, análisis, evolución, tratamiento a los riesgos, control y seguimiento de estos.

PLANIFICACIÓN DE LA GESTIÓN.

La planificación de la gestión trata de definir como se realizarán las actividades de gestión de riesgos y oportunidades del departamento de sistemas y a los equipos de cómputo todo esto será llevado a cabo por el jefe de sistemas y el auxiliar de sistemas, ya se esta llevando a cabo la identificación de riesgos de las áreas antes mencionadas. Los riesgos serán priorizados según su gravedad es decir cuanto mayor sea la probabilidad y mayor sea el impacto, mayor ha de ser la prioridad. Para realizar un análisis cualitativo se utilizará una herramienta llamada Matriz de probabilidad de impacto como se muestra en el siguiente ejemplo.



Matriz de probabilidad de impacto: Tabla de doble entrada que combina la probabilidad que ocurra un evento, el impacto que este pueda causar en el área o departamento de esta manera se consigue establecer una priorización de los riesgos.

IDENTIFIACION DE LOS RIESGOS

En esta fase se identificarán los riesgos que estén o puedan afectar al departamento de sistemas, equipos de cómputo y la infraestructura de TI, tanto de manera negativa como positiva.

La identificación del riesgo deberá considerar el impacto de los riesgos sobre los objetivos del departamento. De esta manera la identificación de riesgos permitirá que el equipo del departamento de sistemas pueda anticipar los posibles impactos de estos impidiendo en gran medida que los riesgos sigan en aumento.

Para que los riesgos sean identificados de manera correcta se utilizara la matriz de probabilidad posteriormente se empleara un formato el cual permita establecer los riegos y las acciones a tomar para cada uno.

A continuación, se describirán las partes que componen el formato de registro de riesgos

* Procesos, organización y partes interesadas: En este apartado se establecen las personas involucradas en el riesgo.
* Identificación del riesgo: Aquí se describe el riesgo que fue encontrado.
* Riesgo: amenaza/oportunidad: clasificación del riesgo en: riesgo positivo(oportunidad), Riesgo negativo (Amenaza) y No se identifica.
* Acciones a tomar: acciones a realizar para mitigar el riesgo.
* Fecha de inicio: Cuando se empezara a mitigar el riesgo.
* Responsable: Quien lleva a cabo la solución del riesgo.
* Estado del riesgo: Para este campo se necesita con claridad la etapa en la cual va el riesgo si ya se comenzó el trabajo, está pendiente, no se ha planificado, acción no satisfactoria.
* Recursos: Todo aquello que fue necesario para completar el trabajo.
* Evaluación de las acciones tomadas: en este apartado se reflexiona sobre las acciones que fueron realizadas si fueron las correctas, existen impedimentos o complicaciones.
* Observaciones: establecer algún comentario sobre las acciones relacionadas a los puntos anteriores.

Toda identificación de un riesgo deberá tener en cuenta el efecto de este sobre sus actividades, así como su efecto en el resto de las áreas.

TRATAMIENTO DE LOS RIESGOS Y OPORTUNIDADES.

Eliminar el riesgo: Siempre será la mejor solución, pero pocas veces será posible para ello debemos centrarnos en analizar el foco y origen del riesgo para tratarlo y así eliminar el riesgo.

Reducir la probabilidad: Al tomar acciones sobre un determinado riesgo podremos centrarnos de que este se materialice y por tanto reducir dicho riesgo. Por ejemplo, invertir en un antivirus reducirá la probabilidad de que los equipos informáticos de la organización sean infectados.

Limitar el impacto: La otra opción es realizar acciones para reducir su impacto en el caso que suceda.

Asumir el riesgo: Cuando el riesgo puede asumirse como tolerable o trivial, existe la opción de asumir dicho riesgo y por tanto no tomar ningún tipo de acción para corregirlo.