DEFINICIÓN DE LAS POLÍTICAS DE SEGURIDAD

Normas y políticas de seguridad de la información

La información es el activo más importante de cualquier empresa, por ello los servicios prestados a las empresas son de uso exclusivo de los funcionarios de dichas entidades y por ello cualquier tipo de cambio a la normativa de seguridad, deberá de ser expresada y adecuada, en conjunto con la empresa prestadora del servicio deberá de nombrar un comité de seguridad, el cual será encargado de hacer el respectivo control y seguimiento a las normas y políticas de seguridad plasmadas en los contratos de prestación de servicios, ayudando a reconocer, determinar y minimizar cualquier tipo de riesgo al cual se pueda ver comprometida la integridad de la información, generando en los funcionarios buenas prácticas para el manejo de la información, mediante el uso de las normas ISO27000. Para la creación de diversas funciones entre las cuales se encuentran.

• Elaboración de planes de seguridad y Capacitar a los usuarios en temas relacionados a la seguridad de la información.

• Velar por la seguridad de los activos informáticos y gestionar el procesamiento de la información, y el cumplimiento de las políticas

• Crear planes de contingencia, que dé sustento o solución, a problemas de seguridad dentro de las entidades

• Generar reportes de seguridad, informando a la cabeza mayor de la compañía, indicando las acciones a tomar y el posible impacto de estas.

Acciones a tener en cuenta por parte de las compañías

Las compañías contratantes, a modo de demostrar del compromiso adquirido con la empresa prestadora de servicio, garantiza el control, seguimiento e implementación de las pruebas de seguridad propuestas por el comité encargado, el cual garantizara la integridad de la información y los procesos desarrollados en esta alcaldía permitiendo al comité de seguridad.

• Aprobar las políticas de seguridad propuestas

• Realizar charlas respectivas a la promoción de una cultura de seguridad.

• Verificación el cumplimiento de las políticas de seguridad establecidas.

• Divulgar a los funcionarios material respectivo a las buenas prácticas de seguridad

• Garantizar los recursos necesarios para implementar las propuestas de seguridad de la información.

Políticas organizacionales y condiciones de uso para la confidencialidad de la información

Las compañías contratantes deberán de establecer normas de responsabilidad, mediante las cuales se tendrán que regir sus funcionarios, todo esto en aras de mejorar el desempeño y la gestión de la seguridad de la información. Las siguientes son las normas que rigen para la estructura organizacional de seguridad de la información:

Personal Técnico Comité de Seguridad Informática y de Riesgos.

- Presentar informes con las políticas de seguridad establecidas a la fecha, metodología de análisis ante contingencias y procedimiento a llevar a cabo en caso de ataque informáticos a gran escala.

- Asignación de funciones y responsabilidades al personal administrativo, que desempeñaran sus funciones en las plataformas tecnológicas.

- Crear lineamientos para la gestión de la seguridad de la información instaurando controles a nivel técnico y administrativo en base a un análisis de riesgos realizado previamente.

- Realizar monitoreos de manera constantes y establecer reportes de seguridad en base a los resultados obtenidos.

- Verificar y documentar el cumplimiento de las políticas se seguridad y la asignación de funciones, responsabilidades a cada uno de los funcionarios.