**Políticas informáticas**

Alcance

El documento que se presenta se aplica a los empleados en general o a la persona que en algún momento tenga acceso a la información de la empresa.

Sobre la asignación y el uso de los recursos

**Sobre la asignación y el uso de los recursos**

1. Para al acceso al equipo de cómputo debe ingresar con un usuario y contraseña.  
2.    El personal debe hacer uso adecuado de los recursos informáticos (PC, impresoras, programas, correo, etc.) y el personal de sistemas debe asegurar que se cumpla esta política. Además, todo el personal deberá informar a sistemas sobre cualquier falla, desperfecto o mal uso del equipo de cómputo, para su adecuado seguimiento.

Sobre la seguridad de la información

1. El inventario se realiza de manera mensual para actualizar la información.

2. Los empleados de la empresa no pueden dar información

3. Cualquier cambio que se realice deberá ser autorizado por el dueño de la empresa

Sobre el mantenimiento y buen uso de la infraestructura

1. El equipo deberá contar con un antivirus para evitar fallas

2. Se realizara una revisión de los datos, para verificar que no haya datos erróneos

3. El equipo contara con el mantenimiento correspondiente para evitar que este tenga daños con el paso del tiempo.

4. Se actualizara el software para optimizar su rendimiento y este siempre permita trabajar de una manera eficaz.

1ºControles Generales Organizativos

* Plan estratégico de información: es importante organizar como se va a llevar cabo la organización de la información y asignación de tareas en la organización para evitar perdidas

|  |  |  |  |
| --- | --- | --- | --- |
| RIESGOS | PREVENTIVO | DETECTIVO | CORRECTIVO |
| Asignación incorrecta de tareas | Calendarizar las tareas por tiempo y asignación al personal | Llevar un registro en una agenda electrónica de los cumplimientos de las tareas. | Recordatorios de la agenda electrónica para avisar que el plazo está por agotarse. |
| Que los clientes no les llegue la factura que solicitaron | Pedir a los clientes crear una cuenta de correo para poder enviar las facturas que lleguen a solicitar. | Verificar que todos los clientes tengan una cuenta de correo vigente. | Solicitando al cliente u nuevo correo funcional a donde le pueda llegar la información que requiere o bien pedir una cuenta extra en caso de no recibir la información en la primera opción |
| Asignación incorrecta de días que se visitara a los clientes | Calendarizar los días de visitas para cada cliente. | Usado una agenda que indique que día, hora y lugar además de señalar cuando ya se cumpla la visita establecida. | Que la calendarización muestre un mensaje que se tiene un retraso. |

* Planificación de seguridad física y lógica:

La seguridad de la información dentro de la organización es muy importante para el funcionamiento correcto es por eso que debemos tomar en cuenta algunos puntos:

|  |  |  |  |
| --- | --- | --- | --- |
| RIESGOS | PREVENTIVO | DETECTIVO | CORRECTIVO |
| Daños al equipo de la organización. | Evitar que personal ajeno a la empresa haga uso del equipo. | El equipo no está funcionando como regularmente lo hace | Evitar que el equipo se encuentre expuesto a personal externo a la organización |
| Ataque de virus que pueda dañar al sistema operativo | Realizar un análisis por medio del antivirus para asegurase de que todo está en orden. | Por medio de los resultados que arroje el análisis de detección de virus. | Asegurarse que el análisis de detección de virus esté funcionando como lo requerimos de manera diaria. |

2ºControles de desarrollo, adquisición y mantenimiento de información

* Garantizar que el sistema que se implementara sea seguro y se pueda ejecutar sin ningún temor de que el sistema pueda quedar vulnerable

|  |  |  |  |
| --- | --- | --- | --- |
| RIESGOS | PREVENTIVO | DETECTIVO | CORRECTIVO |
|  |  |  |  |

3º Controles de explotación de sistemas de información

* Controles para usar de manera efectiva los recursos en computadores

|  |  |  |  |
| --- | --- | --- | --- |
| RIESGOS | PREVENTIVO | DETECTIVO | CORRECTIVO |
| Falta de inversión para alguna necesidad de mantenimiento del equipo | Reservando los recursos que se utilizaran para alguna necesidad que se presente en relación con el equipo | Llevando el control de los gastos que se requieren para los quipos | Organizar en una lista electrónica los gastos y ganancias que se le den al equipo |

4º Controles en aplicaciones

* Seguridad física y lógica para garantizar la entrada de datos actualización y validez de los mismos

|  |  |  |  |
| --- | --- | --- | --- |
| RIESGOS | PREVENTIVO | DETECTIVO | CORRECTIVO |
| Intrusos en el equipo de la organización | La máquina de la organización después de un tiempo de estar encendida sin uso se apagara. | Mandar un mensaje de alerta de que alguien ha intentado iniciar sesión en el equipo de manera sospechosa | Limitar el uso de intentos para acceder a la sección dl equipo |
| Mal uso de la información de las aplicaciones | Manual de usuario donde se especifique como utilizar las aplicaciones y los posibles errores que se podrían presentar | Envió de mensajes donde se indique que se está usando de forma incorrecta la aplicación,  (Indicando cual es el error). | Contar con un respaldo de la información restaurado el daño. |

5ºControles específicos de ciertas tecnologías

* Controles en sistema de gestión de base de datos: para asegurar que la base de datos este protegida y la información tenga cierta integridad y se eviten perdidas de datos dentro de la base de datos y pueda afectar a la organización.

|  |  |  |  |
| --- | --- | --- | --- |
| RIESGOS | PREVENTIVO | DETECTIVO | CORRECTIVO |
| Datos erróneos que puedan afectar la información de la organización | Verificando los datos antes de enviarlos. | Con limitaciones para la entrada de datos | Respaldar la información que se encuentra en la base de datos. |
| Modificación de la información por personal no autorizado | Porque son datos que no coinciden con el respaldo | Incongruencia en los datos de la base de datos | Permitiendo solo modificaciones para el usuario root |
| Modificación no autorizada de los datos | Proteger la confidencialidad, autenticad o integridad de los datos a través de contraseñas. | Alerta de violación en la seguridad, por medio de un mensaje al correo donde se informara que en la cuenta se ha intentado acceder de forma sospechosa. | Implementar un límite de tiempo de contraseñas para el usuario, restringir los caracteres que serán usados de contraseñas, exigiendo que se usen contraseñas difíciles de des encriptar. |
| Introducción de datos erróneos | Validación de datos condicionar solo par que el usuario desde teclado no introduzca valores que no correspondan al campo | Por medio de mensajes que indiquen cual es el error. | Verificando que las restricciones sean las adecuadas para evitar que el usuario introduzca valores incorrectos |