|  |  |  |
| --- | --- | --- |
| **Versión** | **Descripción de Cambios al Documento** | **Fecha** |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **Elaborado por:** | **Revisado por:** | **Autorizado por:** |
|  |  |  |
|  |  |  |

Políticas:

1.- Acceso a páginas web no permitidas, ejemplo: redes sociales, películas o videos en línea

2.-Páginas de descarga (software, piratería)

3.-Alterar los equipos de cómputo, infraestructura de red.

4.-Uso de dispositivos de almacenamiento portátil (USB, CD, celulares)

5.-Extracción de equipo de cómputo de la agencia aduanal sin previa autorización.

6.-Instalación de software no autorizado

7.-Desinstalar software

8.-Mantener la confidencialidad de las contraseñas

9.-La configuración de correo electrónico en equipos de comunicación debe ser solo en el autorizado y asignado según el puesto, y debe apegarse a las políticas de uso de aparatos de comunicación, no se dará asistencia por parte del área de sistemas cuando sea equipo de comunicación personal.

10.-Las contraseñas de correo electrónico no son entregadas al usuario, solamente se configura en los equipos autorizados.

11.-Queda prohibido anotar contraseñas en cualquier documento que se encuentre a la vista delas demás personas.

12.-Todos los equipos de cómputo estarán protegidos bajo contraseñas

13.-Cada usuario debe contar con permisos para acceder a cada equipo cómputo, con el fin de restringir en nivel de acceso al sistema informático.

14.-Ninguna persona ajena ala agencia aduanal tiene acceso a los sistemas informáticos.

15.-Se cuenta con un perfil de red para invitados, cuando se requiera hacer uso del internet para la transferencia de información con un cliente o proveedor de servicios.

Normas de Aplicación:

* Cuando ingresa un nuevo empleado, Recursos humanos determina en base al perfil de puesto a que recursos informáticos tendrá acceso, tales como cuenta de correo electrónico, equipo de cómputo, herramientas de trabajo (SICA “Sistema Contable Aduanal”, SITA “Sistema Integral de Tráfico Aduanal” ) e informa al Gerente de Sistemas para generar sus contraseñas y asignación de equipo cuando aplique.
* El Gerente de Sistemas autoriza la asignación de equipo y la creación de nuevas contraseñas.
* Auxiliar de sistemas es el encargado de generar las contraseñas y entregarlas al usuario.
* El usuario debe firmar una carta responsiva de ***entrega de equipo de cómputo, contraseñas***, esta carta será resguardada en el expediente del empleado y Sistemas se quedará con una copia en su archivo.
* El usuario debe tener conocimiento de las políticas de Seguridad de las TI así como darle cumplimiento.
* El formato de las contraseñas debe ser de 8 caracteres, compuestos de mayúsculas, minúsculas y un símbolo especial.
* Las contraseñas deben ser cambiadas de manera semestral.
* La baja de contraseñas se dará cuando recursos humanos notifique la baja de personal, o por petición de los jefes de área.
* Todos los usuarios y contraseñas se mantienen protegidos en un archivo electrónico, bajo responsabilidad del departamento de sistemas.

**Criterios**

Cualquier falla en los equipos de cómputo y/o infraestructura de TI, debe informarse a su respectivo departamento con el fin de evitar que personas no autorizadas, actúen provocando alteraciones o desconfiguraciones.

La identificación de los equipos se debe hacer ya sea mediante el número de serie o etiqueta de servicio y estar registrada en el inventario de equipo.