Plan de mantenimiento

**PROTECCION DE LOS RECURSOS INFORMATICOS**

**1. NIVELES DE ACCESO**

**1.1. USUARIOS**

**1.1.1. Uso Autorizado**

El Uso Autorizado de los recursos informáticos será para propósitos relacionados con la misión del proyecto, por lo que el personal deberá limitar su uso al total cumplimiento de sus funciones con el seguimiento de las actividades fundamentales.

**1.1.2. Usuarios Autorizados**

El jefe(a) de la Unidad de Informática asignará niveles de autorización a los usuarios de los sistemas informáticos tanto para su operación y/o consulta, por razones de seguridad de la información contenida en el sistema. Usuarios Autorizados son: (1) empleados de la Institución; (2) otros cuyos accesos complementen la misión de la institución, siempre y cuando su utilización no interfiera con los accesos de otros usuarios a los recursos. El acceso se otorgará por el jefe(a) de la Unidad de Informática en forma escrita.

**1.2. CUENTAS**

**1.2.1. Cuentas de acceso**

Las cuentas de ingreso a los sistemas informáticos son propiedad de la institución y se usaran exclusivamente para actividades relacionadas con el proyecto de la institución. Ninguna cuenta de usuario autorizado, podrá ser usada para propósitos ilegales, criminales, antiéticos o inmorales.

**1.2.2. Tipos de cuentas**

Los tipos de cuentas de ingreso son:

• Cuantas de acceso a Dominio.

• Cuenta de acceso a Correo Electrónico.

• Cuenta de acceso a sistema ERP

**1.2.3. Vigencia de las cuentas**

Las cuentas tendrán efecto mientras el usuario mantenga una relación laboral u oficial con el proyecto de la institución. El jefe(a) de la Unidad de Informática es la única persona autorizada para dar o delegar la creación de accesos a la red.

**1.3 ACCESOS REMOTOS**

Ningún usuario podrá realizar accesos remotos a los equipos ni desde fuera de la institución, ni desde dentro de la misma, a excepción de aquellos que obtengan la autorización del jefe(a) de la Unidad de Informática.

**1.4. CLAVES DE ACCESO (PASSWORDS)**

**1.4.1. Claves (Passwords)**

No se podrá poner claves de Acceso a las PC's sin previa autorización del jefe(a) de Informática, tanto al iniciar el equipo (BIOS) o al inicio de sesión en equipos que no sean parte de la estructura de Dominio, ya que es propiedad de la institución.

Los equipos utilizados para el desarrollo de aplicaciones institucionales en las cuales se encuentra algún código fuente, podrán estar protegidas por claves; estas serán del conocimiento y administración del jefe(a) de la Unidad de Informática. El jefe(a) de la Unidad de Informática, hará cambios periódicos de Claves en el Servidor de los servicios de Internet y Correo Electrónico y en el servidor de Intranet, para evitar que personas externas puedan tener acceso a los mismos o delegará al responsable de realizar estas tareas.

Ningún usuario tendrá rol de administrador en los equipos locales. Sus cuentas serán creadas en el dominio con sus respectivos accesos. En los casos que las respectivas jefaturas soliciten acceso a la máquina de uno de sus técnicos por ausencia del misma se deberá realizar la solicitud a la Unidad Informática, quien creará una contraseña temporal para que este pueda acceder y luego deberá ser cambiada por el técnico.

**ADMINISTRACION DE SOFTWARE**

1. **LICENCIAS**

La Unidad de Informática mantendrá un inventario de productos de software con licencia, instalados en sus PC's, con el objetivo de estandarizar, retirar equipo obsoleto, evaluar el uso y revisar procedimientos. Se tendrá un control de licencias y un control por tipo de licencias. La institución se reserva el derecho de rehusarse a defender a cualquier empleado ante cualquier asunto legal relacionado a infracciones a las leyes de protección de la propiedad intelectual. Por lo que queda prohibido para el personal en general instalar software, que no sea autorizado por el jefe(a) de la Unidad de Informática. El jefe(a) de la Unidad deberá dar visto bueno a cualquier solicitud de adquisición de Hardware y/o Software que realicen el personal del proyecto empleado, ya sea por mantenimiento, actualización o ampliación del equipo informático o software de la institución.

**2.0 PROPIEDAD INTELECTUAL**

La institución mantiene la propiedad sobre toda la información técnica y administrativa creada o modificada por sus empleados como parte de sus funciones laborales.

**3.0 DESARROLLO DE SOFTWARE.**

Todas las aplicaciones y avances que se desarrollen para el proyecto deben contar con pistas de auditoría a través de bitácoras electrónicas contenidas en todos los sistemas, que permitan verificar la correcta utilización de los programas y de los datos.