**Política de correos electrónicos institucionales**

**1. Introducción**

La política de correos electrónicos institucionales de la delegación tiene como objetivo establecer directrices claras para el uso de los servicios de correo electrónico por parte de los empleados y representantes de la organización. El correo electrónico es una herramienta de comunicación esencial que requiere responsabilidad y consideración para garantizar su eficacia y seguridad.

**2. Propósito**

El propósito de esta política es:

2.1. Promover un uso efectivo y eficiente del correo electrónico como herramienta de comunicación en el ámbito institucional.

2.2. Establecer pautas para garantizar la seguridad y la confidencialidad de la información transmitida por correo electrónico.

2.3. Definir las responsabilidades de los usuarios en relación con el correo electrónico institucional.

**3. Responsabilidades**

**Delegaciones:**

Las delegaciones deben de utilizar en sus cuentas de correos electrónicos dominios oficiales relacionados con sus sitios web y evitar utilizar cuentas gratuitas como @hotmail, @gmail para la comunicación corporativa.

**Usuarios:**

Los empleados y representantes de la organización son responsables de utilizar el correo electrónico de manera adecuada, cumplir con esta política y ser conscientes de la seguridad de la información.

**Departamento de TI:**

El equipo de tecnologías de la información es responsable de administrar y mantener el sistema de correo electrónico, implementar medidas de seguridad y brindar soporte técnico.

**4. Uso Adecuado**

4.1. Los correos electrónicos institucionales deben utilizarse para comunicaciones relacionadas con el trabajo y tareas oficiales. El uso personal debe mantenerse al mínimo y seguir las directrices de la organización.

4.2. No se permite el envío de correos electrónicos no solicitados (spam) o correos electrónicos que violen las leyes y regulaciones aplicables.

**5. Seguridad de la Información**

5.1. Los usuarios deben proteger sus credenciales de correo electrónico y no compartirlas con terceros.

5.2. Los datos confidenciales o sensibles no deben enviarse por correo electrónico sin cifrar adecuadamente.

5.3. Los usuarios deben ser conscientes de las amenazas de phishing y seguir prácticas seguras para evitar caer en trampas de seguridad.

**6. Retención y Eliminación de Correos Electrónicos**

6.1. La organización debe establecer políticas de retención de correos electrónicos para garantizar el cumplimiento de las regulaciones y la eficiencia operativa.

**7. Cumplimiento Legal y Regulatorio**

7.1. Los usuarios deben cumplir con todas las regulaciones legales y regulaciones de privacidad de datos aplicables al enviar y recibir correos electrónicos.

**8. Auditorías y Monitoreo**

8.1. La organización se reserva el derecho de realizar auditorías y monitorear el uso del correo electrónico para garantizar el cumplimiento de esta política y la seguridad de la información.

**9. Sanciones**

9.1. El incumplimiento de esta política puede dar lugar a medidas disciplinarias, que pueden incluir la suspensión o la terminación del acceso al correo electrónico institucional.