**Política de Seguridad Integral de [**[EJEMPLO NETTIX](https://www.nettix.com.mx/)**]**

Fecha de Entrada en Vigencia: 01 de Enero 2021

**Objetivo:** Esta política tiene como objetivo proteger la integridad, confidencialidad y disponibilidad de la información y los sistemas de [Nombre de la Empresa] y garantizar la seguridad cibernética de la organización.

**1. Responsabilidades del Personal:**

* Todos los empleados son responsables de cumplir con las políticas y procedimientos de seguridad de la organización.
* Deben informar cualquier incidente de seguridad, violación o sospecha de incumplimiento de políticas a [Nombre del Contacto de Seguridad].
* Se espera que los empleados protejan los recursos de información y sistemas de la organización y se adhieran a las prácticas de seguridad.

**2. Gestión de Cuentas y Contraseñas:**

* Los empleados deben proteger sus credenciales y contraseñas y cambiarlas regularmente.
* No deben compartir contraseñas y deben utilizar contraseñas seguras.

**3. Uso Adecuado de Activos de Información:**

* Los activos de información deben utilizarse solo con fines comerciales y autorizados.
* No se deben instalar programas o aplicaciones no aprobados en los sistemas de la organización.

**4. Protección de Datos Sensibles:**

* Los datos sensibles deben manejarse de acuerdo con las políticas de privacidad y protección de datos.
* Los empleados no deben divulgar ni compartir datos confidenciales con personas no autorizadas.

**5. Seguridad de la Red:**

* El uso de la red de la organización debe ser seguro y responsable.
* Los empleados deben evitar visitar sitios web maliciosos o potencialmente peligrosos.

**6. Correo Electrónico y Comunicaciones Electrónicas:**

* Los empleados deben tener precaución al abrir correos electrónicos y adjuntos de fuentes desconocidas.
* No deben compartir información confidencial a través de medios no seguros.

**7. Dispositivos Móviles:**

* Los dispositivos móviles deben estar protegidos con contraseñas y encriptación, y se deben informar inmediatamente las pérdidas o robos.

**8. Actualizaciones y Mantenimiento de Software:**

* Se deben mantener todos los sistemas y software actualizados con parches de seguridad.
* No se deben usar software no autorizado en los sistemas de la organización.

**9. Prevención de Amenazas y Malware:**

* Los empleados deben estar alerta ante amenazas cibernéticas y no descargar ni ejecutar software sospechoso.
* Se deben informar de inmediato las amenazas de malware y los incidentes de seguridad.

**10. Cumplimiento Legal y Regulaciones:**

* Todos los empleados deben cumplir con las leyes y regulaciones de seguridad aplicables a [Nombre de la Empresa].

**11. Consecuencias del Incumplimiento:**

* El incumplimiento de esta política puede resultar en acciones disciplinarias, incluida la terminación del empleo.

Entiendo y acepto las políticas y procedimientos de seguridad de [Nombre de la Empresa] y me comprometo a cumplir con ellos.

Firma: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Nombre: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Fecha: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_