Lista de verificación de cumplimiento

Para revisar las normas y estándares de cumplimiento, lea el documento sobre controles, marcos y cumplimiento.

- ☐ **Comisión Federal Reguladora de Energía - Corporación Norteamericana de Confiabilidad Eléctrica (FERC-NERC)**

  La normativa FERC-NERC se aplica a las organizaciones que trabajan con electricidad o que participan en la red eléctrica de Estados Unidos y Norteamérica. Estas organizaciones tienen la obligación de prepararse para cualquier incidente de seguridad potencial que pueda afectar negativamente a la red eléctrica, mitigar sus efectos e informar sobre él. Asimismo, están legalmente obligadas a cumplir con las Normas de Fiabilidad para la Protección de Infraestructuras Críticas (CIP) definidas por la FERC.

  Explicación: NA

- ☑ **Reglamento General de Protección de Datos (GDPR)**

  GDPR es una normativa general de protección de datos de la Unión Europea (UE) que protege el tratamiento de los datos de los ciudadanos de la UE y su derecho a la privacidad tanto dentro como fuera del territorio de la UE. Además, si se produce una violación de seguridad y los datos de un ciudadano de la UE se ven comprometidos, este debe ser informado en un plazo de 72 horas desde el incidente.

  Explicación: Botium Toys aplica porque la empresa ofrece bienes o servicios a europeos. Le sirve en la protección de datos, ayudándole a cumplir con los derechos del usuario (acceso, rectificación, borrado), y a llevar un control de registro que ayude a mitigar brechas de datos confidenciales.

☑ **Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)**

PCI DSS es un estándar de seguridad internacional destinado a garantizar que las organizaciones que almacenan, aceptan, procesan y transmiten información de tarjetas de crédito lo hagan en un entorno seguro.

Explicación: Es obligatorio ya que Botium Toys está basada en Estados Unidos, y tiene clientes internacionales (incluyendo UE), procesa pagos online, y maneja datos personales de empleados, clientes y proveedores. Estos estándares ayudan a segmentar la información de tarjetas, aplica controles de acceso estrictos, y conlleva un registro y monitoreo continuo.

☐ **La Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA)**

HIPAA es una ley federal establecida en 1996 para proteger la información de salud de los pacientes estadounidenses. Esta ley prohíbe que se comparta la información del paciente sin su consentimiento. Las organizaciones tienen la obligación legal de informar a los pacientes en caso de una violación de seguridad.

Explicación: NA

☑ **Controles de sistemas y organizaciones (SOC tipo 1, SOC tipo 2)**

Los informes SOC1 y SOC2 se centran en las políticas de acceso de usuarios de una organización en diferentes niveles organizativos. Se utilizan para evaluar el cumplimiento financiero y los niveles de riesgo de la organización. También abarcan la confidencialidad, la privacidad, la integridad, la disponibilidad, la seguridad y la protección general de los datos. Las deficiencias en los controles de estas áreas pueden dar lugar a fraudes.

Explicación: Botium Toys necesita establecer y hacer cumplir el acceso adecuado de los usuarios de personal interno y externo para mitigar riesgos. Solicitar informes SOC 1 o SOC 2 es esencial, ya que utilizan plataformas en línea para ventas o datos de clientes, y se mantiene relaciones comerciales con proveedores. SOC 1 es aplicable con los procesos Botium Toys porque afecta la información financiera de sus clientes. SOC 2 es aplicable porque la empresa procesa y almacena datos confidenciales de clientes.

☑ **Ley de Privacidad del Consumidor de California (CCPA/CPRA)**

Es una ley estatal de protección de datos que otorga a los residentes de California derechos sobre su información personal, como el derecho a acceder, eliminar y optar por no vender sus datos.

Explicación: Esta ley aplica para todos los clientes de Botium Toys ubicados en California.

☑ **Ley de Protección de la Privacidad Infantil en Internet (COPPA)**

Es una ley federal de Estados Unidos que establece un estricto conjunto de directrices que deben seguir las empresas en línea para proteger la privacidad de los menores de 13 años. Diseñada para limitar la cantidad de información que las empresas recopilan de niños pequeños

Explicación: Esta ley aplica a Botium Toys ya que procesa datos de niños en Estados Unidos, e internacionalmente, a esta empresa en especial porque es una empresa de juguetes.