LISTA DE VERIFICACIÓN DE CUMPLIMIENTO

☐ **Comisión Federal de Regulación de Energía - Corporación de Confiabilidad Eléctrica de América del Norte (FERC-NERC)**
La normativa **FERC-NERC** se aplica a las organizaciones que trabajan con electricidad o que están relacionadas con la red eléctrica de Estados Unidos y Norteamérica. Las organizaciones tienen la obligación de prepararse, mitigar y notificar cualquier posible incidente de seguridad que pueda afectar negativamente a la red eléctrica.
Las organizaciones están obligadas legalmente a cumplir con los Estándares de confiabilidad de protección de infraestructura crítica (**CIP**) definidos por la **FERC**.

Explicación: NA

☑ **Reglamento General de Protección de Datos (GDPR)**
El **GDPR** es un reglamento 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 dentro y fuera del territorio de la UE. Además, si se produce una infracción y se ven comprometidos los datos de un ciudadano de la UE, se le debe informar en un plazo de 72 horas desde el incidente.

Explicación: Botium Toys debe cumplir con el RGPD porque realiza negocios y recopila información personal de personas de todo el mundo, incluida la UE.

☑ **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: Botium Toys debe cumplir con PCI DSS porque almacena, acepta, procesa y transmite información de tarjetas de crédito en persona y en línea.

☐ **Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA)**
HIPAA es una ley federal establecida en 1996 para proteger la información médica de los pacientes estadounidenses. Esta ley prohíbe que se comparta la información de los pacientes sin su consentimiento. Las organizaciones tienen la obligación legal de informar a los pacientes sobre cualquier violación de la información.

Explicación: NA

☑ **Controles de sistemas y organizaciones (SOC tipo 1, SOC tipo 2)**
SOC1 y SOC2 son una serie de informes que se centran en las políticas de acceso de los usuarios de una organización en diferentes niveles organizacionales. Se utilizan para evaluar el cumplimiento financiero y los niveles de riesgo de una organización. También cubren la confidencialidad, la privacidad, la integridad, la disponibilidad, la seguridad y la seguridad general de los datos. Las fallas de control en estas áreas pueden dar lugar a fraudes.

Explicación: Botium Toys debe establecer y hacer cumplir el acceso de usuario apropiado para el personal interno y externo (proveedores externos) para mitigar el riesgo y garantizar la seguridad de los datos.