# Lista de verificación de cumplimiento

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

* **La Comisión Federal Reguladora de Energía - Corporación de Confiabilidad Eléctrica de América del Norte (FERC-NERC)**

La regulación FERC-NERC se aplica a organizaciones que trabajan con electricidad o que están involucradas con la red eléctrica de EE. UU. y América del Norte. Las organizaciones tienen la obligación de prepararse, mitigar e informar cualquier posible incidente de seguridad que pueda afectar negativamente a la red eléctrica. Las organizaciones están obligadas por ley a cumplir con los Estándares de confiabilidad de protección de infraestructuras críticas (CIP) definidos por la FERC.

**Explicación:**

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

GDPR es una regulación general de datos de la Unión Europea (UE) que protege el procesamiento de datos de la UE. Los datos de los ciudadanos y su derecho a la privacidad dentro y fuera de la UE. territorio. Además, si se produce una infracción y un acuerdo de la UE. Los datos de un ciudadano se ven comprometidos, deben ser informados dentro de las 72 horas posteriores al incidente.

**Explicación: Debe cumplir con este reglamento ya que debe ofrecer confidencialidad de datos a los clientes debido a que se manejan datos sensibles, además porque realiza negocios y recopila información personal de personas en 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: Debe cumplir con este Estándar porque se trata de una empresa que solicita almacena, acepta, procesa y transmite información de tarjetas de crédito en persona y en línea, como una forma de pago, y debe darle seguridad al cliente para que pueda utilizar dicho medio.**

* **La Ley de Responsabilidad y Portabilidad 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 de cualquier incumplimiento.

**Explicación:**

* **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 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, privacidad, integridad, disponibilidad, seguridad y seguridad general de los datos. Las fallas de control en estas áreas pueden conducir al fraude.

**Explicación: Botium Toys necesita establecer y hacer cumplir el acceso de usuario adecuado para el personal interno y externo (proveedor externo) para mitigar el riesgo y garantizar la seguridad de los datos.**