Ejemplo de la lista de control de cumplimiento normativo

Para revisar las regulaciones y estándares de cumplimiento, lee el documento sobre controles, marcos y cumplimiento normativo.

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

La normativa FERC-NERC se aplica a organizaciones que trabajan con electricidad o que están involucradas con la red eléctrica de los Estados Unidos y América del Norte. Las empresas tienen la obligación de prepararse, mitigar y reportar cualquier incidente de seguridad potencial que pueda afectar negativamente a la red eléctrica. También están legalmente obligadas a cumplir con los Estándares de Confiabilidad de Protección de Infraestructura Crítica (CIP) definidos por la FERC.

Explicación: no disponible

__**X**__ **Reglamento General de Protección de Datos (RGPD)**

El RGPD es una regulación general de datos de la Unión Europea (UE) que protege el procesamiento de los datos de sus residentes y su derecho a la privacidad dentro y fuera del territorio. Además, si se produce una filtración y los datos de una persona se ven comprometidos, esto debe ser informado en un plazo de 72 horas posteriores al incidente.

Explicación: Botium Toys debe cumplir con el RGPD porque trabaja con personas (y recopila su información) de todo el mundo, incluida la UE.

__**X**__ **Estándares de seguridad de datos del sector de las tarjetas de pago (PCI DSS)**

PCI DSS es un estándar 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 las PCI DSS porque almacena, acepta, procesa y transmite información de tarjetas de crédito tanto de forma presencial como en línea.

_____ **Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA)**

La HIPAA es una ley federal de los Estados Unidos establecida en 1996 para proteger la información médica de las personas. Esta ley prohíbe que la información de un/a paciente se comparta sin su consentimiento. Las organizaciones tienen la obligación legal de informar a los/as pacientes en caso de que esta información se filtre.

Explicación: no disponible

__**X**__ **Controles de Sistemas y Organizaciones (SOC tipo 1, SOC tipo 2)**

El SOC1 y el SOC2 se enfocan en las políticas de acceso de las usuarias y los usuarios de una organización en los diferentes niveles. Se utilizan para evaluar el cumplimiento financiero de una organización, así como los niveles de riesgo asociados. También abordan aspectos críticos como la confidencialidad, privacidad, integridad, disponibilidad, seguridad y protección general de los datos. Es importante destacar que cualquier falla en el control de estos aspectos puede resultar en posibles fraudes.

Explicación: Es necesario que Botium Toys cree y haga cumplir el acceso adecuado del personal interno y externo (proveedores externos), a fin de mitigar los riesgos y garantizar la seguridad de los datos.