Lista de control de cumplimiento normativo

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

_____ La Comisión Federal de Regulación 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:

_X_ Reglamento General de Protección de Datos (RGPD) (SE APLICA)

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: Como menciono el gerente de TI de Botium Toys la prescencia en linea de la tienda crece a gran escala, una tienda ubicada en EE.UU que tiene alcance a territorios de la Union Europea, es de aplicacion obligatoria para todas las organizaciones que procesan datos personales de residentes en la UE, independientemente de dónde se encuentre la organización.

_X_ Estándares de seguridad de datos del sector de las tarjetas de pago(PCI DSS) (SE APLICA)

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: Esta normativa es exigida por aquellas principales compañias de pago(Visa, Mastercard, American Expert...). Todas las entidades que procesan, almacenan o transmiten datos de tarjetas de pago deben cumplir con este estándar. Se utiliza para garantizar la seguridad de los datos de tarjetas de pago durante todo el proceso de transacción, desde la captura inicial hasta el almacenamiento y la transmisión. Su objetivo principal es proteger la información confidencial de los titulares de tarjetas, reduciendo el riesgo de fraudes relacionados con el robo de datos de tarjetas.

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 sea compartida sin su consentimiento. Las organizaciones tienen la obligación legal de informar a los/las pacientes en caso de que esta información se filtre.

Explicación:

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

El SOC1 y el SOC2 se enfocan en las políticas de acceso de los usuarios y las usuarias 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: