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:

- ☐ **Reglamento General de Protección de Datos (RGPD)**

  El RGPD 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:

☐ **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:

☐ **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:

☐ **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 jerárquicos. 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: