POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE UTE

Con el objeto de difundir los principios generales que deben regir las actuaciones en materia de seguridad de la información, el Directorio de la Administración Nacional de Usinas y Trasmisiones Eléctricas (UTE) dispuso la publicación del presente documento, titulado Política de Seguridad de la Información de UTE (en adelante, la "Política").

1. Objetivo

UTE reconoce la importancia de identificar y proteger los activos de información del organismo. Para ello, se compromete a velar por la confidencialidad, integridad y disponibilidad de la información, así como la de los sistemas que la almacenan, procesan o transmiten. Se entiende como:

- **Confidencialidad:** asegurar que solo quienes estén autorizados puedan acceder a la información.
- **Integridad:** asegurar que la información y sus métodos de procesamiento sean exactos y completos.
- **Disponibilidad:** asegurar que los usuarios autorizados tengan acceso a la información cuando lo requieran.

2. Ámbito de aplicación

El ámbito de aplicación comprende a todos los procesos, el personal y las terceras partes (proveedores, socios de negocio, clientes de servicios de consultoría, entre otros), que tengan o hayan tenido acceso a activos de información de UTE.

3. Principios básicos de actuación

UTE asume y promueve los siguientes principios básicos de actuación que deben presidir todas sus actividades en materia de seguridad de la información corporativa:

a) Conformar un Comité de Seguridad de la Información que tiene como principal objetivo promover, difundir y apoyar la seguridad de la información, garantizando que la misma sea parte del proceso de planificación.
b) Designar un "Responsable de la Seguridad de la Información", encargado de velar por la implementación, mantenimiento y revisión de la Gestión de la Seguridad de la Información.
c) Desarrollar políticas específicas con el fin de concientizar al personal y terceras partes en temas concretos estableciendo pautas de actuación para minimizar riesgos de Seguridad de la Información.
d) Diseñar una estrategia de Seguridad de la Información, con una planificación de objetivos anual.
e) Desarrollar un proceso de gestión de riesgos de Seguridad de la Información.
f) Desarrollar e implementar los planes necesarios para asegurar la continuidad de las operaciones y proteger las infraestructuras involucradas.
g) Establecer y difundir políticas y procedimientos para el reporte y la gestión de incidentes de Seguridad de la Información.
h) Asegurar el derecho a la protección de los datos personales de todas las personas físicas y jurídicas que se relacionan con UTE.

i) Promover una cultura de la Seguridad de la Información en la empresa, mediante la realización de acciones de divulgación, educación y formación en la materia; actuar, en todo momento, al amparo de la legislación y normativa vigentes y dentro del marco establecido por el Código de Ética y demás normas internas.

4. Responsabilidades y cumplimiento

- **Directorio, Gerencias y Jefaturas** son responsables de apoyar la difusión de la Política Pública de Seguridad de la Información de UTE y las políticas específicas toda vez que el Comité de Seguridad de la Información así lo solicite y de brindar los recursos necesarios para el cumplimiento de las mismas.

- Todas las **Gerencias y Jefaturas** son responsables de la implementación en sus unidades organizativas y de la adhesión del personal a su cargo de la Política de Seguridad de la Información de UTE y las políticas específicas.

- El **Comité de Seguridad de la Información** es responsable de proponer a Directorio mejoras a esta política y de elaborar las políticas específicas de Seguridad de la Información para su aprobación por Gerencia General.

- El **personal y las terceras partes** sin importar su relación contractual son responsables por la adhesión y el cumplimiento de la presente política y de las políticas específicas de Seguridad de la Información.

- Se destaca que el incumplimiento de la presente política y de las políticas específicas de Seguridad de la Información, aumenta la exposición de la información y el riesgo de tener un incidente de seguridad de la información. Ante la verificación de un incumplimiento la Dirección tomará las medidas que se considere pertinentes, a efectos de darle el debido cumplimiento.