La Infraestructura de Clave Pública (PKI) de la Empresa de Tecnología de la Información y Automática (ATI) se estableció con el objetivo de garantizar y fomentar el intercambio de información entre las diferentes entidades del Ministerio de Energía y Minas, preservando la autenticidad, integridad, confidencialidad ***y no repudio*** de la información digital.

Es en función de la consecución de estos objetivos que se establecen las presentes **normas** para el uso de los certificados digitales, las cuales son de **estricto cumplimiento** por todos los usuarios poseedores de un certificado digital en la Empresa de Tecnología de la Información y Automática (ATI).

Sobre los Certificados Digitales

- Serán emitidos por la Autoridad de Certificación ATI para uso interno de la Institución, por lo que serán reconocidos solos los de dicha entidad.
- Tendrán un período máximo de validez de 3 años desde el día en qué sean emitidos, figurando en los mismos la fecha de caducidad.
- Podrán ser revocados antes de la fecha de expiración a solicitud de los usuarios, alegando la causa de la revocación, y serán emitidos nuevos certificados en esos casos.
- Se entregarán a los usuarios en un fichero con formato PKCS12 o en algún dispositivo portable. En cualquier caso el contenedor del certificado digital de clave pública, contendrá además la clave privada protegida criptográficamente y a la que el usuario accederá mediante una contraseña alfanumérica.
- Podrán ser usados para la firma digital de documentos electrónicos, el cifrado de la información digital, la protección del correo electrónico y la autenticación de los usuarios.

Responsabilidades del titular del certificado

- Los usuarios deberán verificar la veracidad de los datos contenidos en el certificado digital desde el mismo instante en que reciben el mismo. Ante cualquier problema deberán notificarlo inmediatamente a la Autoridad de Certificación de ATI.
- Es responsabilidad y obligación del titular la modificación de la contraseña, autogenerada en el proceso de creación del certificado digital, de manera inmediata a la recepción del mismo y previo a su primer uso, a través de las herramientas informáticas que se ponen a su disposición.
- Los usuarios deberán verificar la validez de los certificados digitales en el momento de realizar cualquier operación basada en los mismos, como el cifrado de datos, la firma digital de documentos o el establecimiento de una conexión segura entre un cliente y un servidor; a partir de los mecanismos de revocación establecidos por la Autoridad de Certificación de ATI.
- Los usuarios deberán proteger y conservar el fichero o dispositivo portable donde se encuentra almacenado en forma segura el certificado digital, tomando todas las precauciones necesarias para evitar su pérdida, alteración o uso no autorizado.
- El titular deberá solicitar inmediatamente la revocación de un certificado en caso de tener conocimiento o sospecha del compromiso de la clave privada, o que la información contenida en el certificado haya sufrido cambios.
- Se deberán configurar adecuadamente todas las aplicaciones informáticas que hagan uso de los certificados digitales, de forma tal que tengan acceso al directorio donde se encuentran publicados todos los certificados digitales de clave pública y las listas de revocación de certificados, emitidas y actualizadas constantemente por la Autoridad de Certificación de ATI.

Los certificados digitales que son asignados a los usuarios serán preservados de forma segura por la Autoridad de Certificación de ATI, con el objetivo de verificar el cumplimiento de los compromisos contraídos.

La Empresa de Informatica y Automática se reserva la facultad de sancionar a los usuarios que incumplan con las normas para la utilización de los Certificados Digitales establecidas en el presente documento.