# DIRECTIVA

## DIR-GTI-GTI-002

# DIRECTIVA PARA EL USO DE LOS CONTROLES CRIPTOGRÁFICOS Y GESTIÓN DE CLAVES

## CONTROL DE MODIFICACIONES

| Versión | Tipo y N°Documento | Fecha | Modificaciones |
|---|---|---|---|
| 1.0 | Acta del Comité N° 02/2015 | 25/06/2015 | Se aprueba la política “Criptografía” |
| 2.0 | Resolución de Superintendente Nº 095-2020-SMV/02 | 30/09/2020 | -Se incluyen precisiones sobre los controles criptográficos en los medios de almacenamiento internos y externos.<br>- Se adecúa el formato del documento a Directiva de acuerdo a los lineamientos establecidos en la Directiva de Documentos Normativos Internos (DNI) |

## 1. Objetivos

El presente documento tiene por objeto establecer disposiciones para el uso de los controles criptográficos, salvaguardando la confidencialidad, autenticidad e integridad de la información que genera o utilice la Superintendencia del Mercado de Valores (SMV) en el ejercicio de sus funciones.

## 2. Alcance

La SMV dispone el establecimiento de una directiva de uso de los controles criptográficos, así como también de la gestión de las claves asociadas a estos. Esta directiva es de aplicación a todo el personal de la SMV.

## 3. Responsables

- Oficina de Tecnologías de Información (OTI).
- Personal de la SMV.

## 4. Documentos de consulta

- Directiva de Documentos Normativos Internos - DIR-SIG-PLS-001, aprobada con Resolución de Superintendente Nº 122-2017-SMV/02.
- Norma ISO/IEC 27001:2013.
- MGE-SIG-PLS-001 Manual del SGSI.
- Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por el Decreto Supremo N°052-2008-PCM y sus modificatorias.

## 5. Términos y Definiciones

- **Certificado Digital**: Es el documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de claves con una persona natural o jurídica confirmando su identidad.
- **Controles criptográficos:** Sirve para proteger la confidencialidad, autenticidad o integridad de la información con la ayuda de técnicas criptográficas.
- **Clave privada**: Es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un documento electrónico y es mantenida en reserva por el titular de la firma digital.
- **Clave pública**: Es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para verificar la firma

digital puesta en dicho documento. La clave pública puede ser conocida por cualquier persona.

- **Criptografía Asimétrica.-** Es la rama de las matemáticas aplicadas que se ocupa de transformar documentos electrónicos en formas aparentemente ininteligibles y devolverlas a su forma original, las cuales se basan en el empleo de funciones algorítmicas para generar dos "claves" diferentes pero matemáticamente relacionadas entre sí. Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible (clave privada), y la otra para verificar una firma numérica o devolver el documento electrónico a su forma original (clave pública). Las claves están matemáticamente relacionadas, de tal modo que cualquiera de ellas implica la existencia de la otra, pero la posibilidad de acceder a la clave privada a partir de la pública es técnicamente ínfima**.**
- **Entidad de Certificación**.- Es la persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.
- **Firma Digital**: Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su control, de manera que está vinculada únicamente al signatario y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior, tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica - IOFE, y que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro II del Código Civil.
- **No repudio.-** Es la imposibilidad para una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una Entidad de Certificación acreditada en cooperación de una Entidad de Registro o Verificación acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas digitales acreditado, y siempre que cumpla con lo previsto en la legislación civil.

  En el ámbito del artículo 2 de la Ley de Firmas y Certificados Digitales, el no repudio hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que no puede negar su vinculación con él ni reclamar supuestas modificaciones de tal documento (falsificación).
- **Seguridad de la Información**: Preservación de la confidencialidad, integridad y disponibilidad de la información.

## 6. Disposiciones

### 6.1. Sobre el uso de los controles Criptográficos

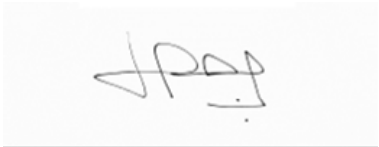
- La SMV reconoce a las firmas digitales como controles criptográficos que emplea para garantizar la autenticidad, integridad y no repudio de su documentación oficial.
- El personal al cual se asigna la capacidad de realizar firmas electrónicas sobre documentos es responsable del reconocimiento de los mismos y no podrá repudiarlos.
- Todo documento con la firma digital de un usuario cuenta con el mismo valor que un documento firmado físicamente.
- La SMV procurará el uso de controles criptográficos sobre los medios de almacenamiento (internos / externos) en base a los niveles de riesgo asociados a su uso.

### 6.2. Gestión de Claves

- La OTI es responsable de administrar la asignación y garantizar la operación adecuada de estos controles, para lo cual proveerá el software y herramientas adecuadas para el personal autorizado que necesite usarlos.
- Se cuenta con un proveedor de certificados digitales para las firmas, la OTI es el área responsable de manejar a nivel de gestión y de operación la interacción con este proveedor.

## 7. Formatos y Modelos Asociados

No aplica

| **Elaborado por:** |
|---|
|  <br>Firmado por: SILVA-SANTISTEBAN SIERRA Luis Alexandr<br>Razón: |
| **Revisado por:** |
|  <br>Firmado por: ESPINOZA ALDAVE Jose Antonio FAU 2013<br>Razón: |
| **Conformidad de Oficina de Planeamiento y Presupuesto** |
|  <br>Firmado por: CONHY LOPEZ Janeth Gabriela FAU 201310<br>Razón:<br>  <br>Firmado por: MARTINEZ GOYONECHE Paola Marialuisa F<br>Razón: |
| **Aprobado por:** |
|  <br>Firmado por: PESCHIERA REBAGLIATI Jose I<br>Razón: |