DIRECTIVA PARA EL USO DE FIRMAS Y CERTIFICADOS DIGITALES					
Número:	003-2022-OSCE/SGE	**N° Resolución:**	036-2022-OSCE/SGE	**Fecha de Emisión:**	13/05/2022
Reemplaza a:	No Aplica	**N° Resolución:**	No Aplica	**Fecha de Emisión:**	No Aplica
Órgano / Unidad Administrador :	Oficina de Tecnologías de la Información / Unidad de Arquitectura y Soporte de Tecnologías de Información y Comunicaciones				
Elaborado por:	OTI	**Revisado por:**	UOYM - OAJ	**Aprobado por:**	Secretaría General

I. FINALIDAD

Establecer los lineamientos para la emisión, uso y cancelación de firmas y certificados digitales en el Organismo Supervisor de las Contrataciones del Estado - OSCE.

II. ALCANCE

Las disposiciones de la presente directiva son de aplicación obligatoria para todas/os las/os servidoras/es civiles de los órganos, unidades orgánicas y proyectos del OSCE, independientemente de su vínculo contractual, cuenten con firma y/o certificado digital, y que en el ejercicio de sus funciones y/o actividades deben firmar digitalmente documentos electrónicos en el marco de los procesos de las unidades orgánicas y/o funcionales a las que pertenecen.

III. BASE LEGAL

3.1 Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado
3.2 Ley N° 27269, Ley de Firmas y Certificados Digitales.
3.3 Decreto Supremo N° 052-2018-PCM, Reglamento de la Ley de Firmas y Certificados Digitales.
3.4 Decreto Supremo N° 076-2016-EF, que aprueba el Reglamento de Organización y Funciones del OSCE.

Las referidas normas incluyen sus respectivas disposiciones ampliatorias, modificatorias y conexas, de ser el caso.

IV. DEFINICIONES

4.1 **Certificado Digital:** Es un documento electrónico usado como credencial, que ha sido generado y firmado digitalmente por una Entidad de Certificación y que permite identificar a la persona natural o jurídica que emitirá la firma digital.

4.2 **Clave privada:** Es una clave 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.

4.3 **Firma Digital:** Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios, incluso a distancia, que garantizan que éste mantiene bajo su control con un elevado grado de confianza, de manera que está vinculada únicamente al

Firmado digitalmente por DAVILA CAJAHUANCA Carmen Blancy FAU 20419026809 hard
Motivo: Doy V° B°
Fecha: 10.05.2022 18:41:28 -05:00

Firmado digitalmente por SUAREZ BAO Milagros Danitza FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 10.05.2022 17:51:41 -05:00

Firmado digitalmente por CASTILLO RIOS Maria Angelica FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 09.05.2022 18:12:27 -05:00

Firmado digitalmente por PECHO CHINCHAY Milagros Anais FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 09.05.2022 17:11:07 -05:00

Firmado digitalmente por ESPINOZA SAUCEDO Juan Miguel FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 09.05.2022 17:16:06 -05:00

Firmado digitalmente por MELGAR DAVILA Victor Ivan FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 09.05.2022 17:19:31 -05:00

Firmado digitalmente por TAIPE DOMINGUEZ Daniel Ivan FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 09.05.2022 17:44:16 -05:00

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, y que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro IV del Código Civil.

4.4 **Visto Bueno Digital:** Es la firma digital configurada como un tipo de firma adicional, que corresponderá a cada uno de los firmantes responsables de revisar y dar Visto Bueno al documento.

4.5 **Token Criptográfico:** Es un dispositivo de almacenamiento, que tiene una apariencia similar a una memoria USB, que almacena de forma segura y confiable el certificado digital asignado a una persona titular que le permite firmar digitalmente.

4.6 **Pin:** Es un número de identificación personal utilizado como clave privada para acceder de manera segura a ciertos sistemas informáticos.

4.7 **Representante del Titular:** Persona natural que cuenta con facultades para representar al OSCE en los trámites de certificado digital ante la EREP-RENIEC.

4.8 **Suscriptor/a:** Es el/la servidor/a civil o el/la consultor/a individual o experto/a contratado para los proyectos del OSCE, responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente.

4.9 **Administrador/a del Certificado Digital:** Es el/la servidor/a civil designado/a por el OSCE, responsable de Coordinar las Gestiones de Certificados Digitales ante el Registro Nacional de Identificación y Estado Civil – RENIEC.

4.10 **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. Para el Estado Peruano es el Registro Nacional de Identificación y Estado Civil – RENIEC.

4.11 **Entidad de Registro o Verificación para el Estado Peruano (EREP):** Es la persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión y cancelación. De acuerdo al Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales aprobado con Decreto Supremo N° 052-2008-PCM, el RENIEC es la única entidad de certificación, verificación y registro en nuestro país.

V. RESPONSABILIDADES

5.1. De los/as suscriptores/as del OSCE:

5.1.1 Son responsables del uso y aplicación de la firma digital en los archivos gestionados a través de sistemas y servicios informáticos utilizados en el OSCE.

5.1.2 Todo/a suscriptor/a que tiene asignado un token criptográfico u otro dispositivo de almacenamiento de certificado digital es responsable de cambiar el PIN para su uso, salvaguardando la confidencialidad de la misma.

5.1.3 Emplear adecuadamente su certificado digital, conforme a la normativa vigente.

5.1.4 Transcurrido el plazo de vigencia del certificado digital, debe modificar la clave privada, a fin de salvaguardar la confidencialidad de la misma.

5.1.5 Proteger el acceso y uso del equipo o dispositivo donde se almacene el certificado digital.

5.1.6 Los/as suscriptores/as son responsables del contenido de los documentos electrónicos firmados digitalmente.

5.1.7 Una vez firmado digitalmente el documento, queda prohibida la modificación del mismo.

5.2. Del Administrador del Certificado Digital:

Solicitar la emisión, renovación o cancelación de los certificados digitales ante la Entidad de Registro o Verificación para el Estado Peruano – EREP RENIEC.

5.3. De la Oficina de Tecnología de la Información:

5.3.1 Brindar capacitación y asistencia técnica en el uso del dispositivo de almacenamiento de certificado digital o token criptográfico.

5.3.2 Atender las incidencias técnicas de los/las suscriptores/as con respecto a la instalación de los certificados digitales y uso de las firmas digitales.

VI. DISPOSICIONES GENERALES

6.1 De las Firmas y Certificados Digitales

6.1.1 La suscripción de un documento electrónico con firma digital generado desde un certificado digital vigente, es un mecanismo tecnológico que posee validez y eficacia jurídica.

6.1.2 La firma digital electrónica tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve a manifestación de voluntad; y si a esta firma electrónica se le aplica un software de firma digital acreditado ante la autoridad administrativa competente, entonces la firma electrónica se convertirá en una firma digital.

6.1.3 El Administrador del Certificado Digital debe seguir los pasos establecidos en los documentos de orientación, manuales, guías, procedimientos, entre otros, que la EREP- RENIEC disponga, para la tramitación de la solicitud de la emisión o cancelación del Certificado Digital, según corresponda.

VII. DISPOSICIONES ESPECIFICAS

7.1 Emisión Del Certificado Digital

7.1.1 El trámite de certificado digital se inicia con la manifestación de el/la suscriptor/a ante la necesidad de firmar digitalmente los documentos, lo cual se solicita mediante "Declaración Jurada de Identificación No Presencial para solicitar Certificado Digital - Persona Jurídica en el Marco de los D.S N°008-2020-SA y D.S 044-2020-PCM que declara El Estado de Emergencia Nacional", previa autorización de el/la titular del Órgano o Unidad Orgánica a la que pertenece, la que es alcanzada al Administrador de Certificados Digitales, para su trámite correspondiente.

7.1.2 En caso de que el Administrador del Certificado Digital considere conveniente, determinará quién o quiénes podrán hacer uso de la instalación del certificado digital mediante un token criptográfico u otro dispositivo de almacenamiento del certificado digital. Se solicitará que el/la suscriptor/a ingrese un Pin, el cual servirá, para que pueda firmar a partir de ese momento los documentos electrónicos.

7.2 Del uso del Certificado Digital para la Firma Digital de los/as suscriptores/as

7.2.1 Los/las titulares de los órganos, unidades orgánicas y proyectos del OSCE, deberán velar por el correcto uso de la firma digital y token criptográfico de los/las suscriptores/as a su cargo.

7.2.2 Para que un/a suscriptor/a pueda utilizar la firma digital en los documentos electrónicos, debe contar con: Certificado Digital, dispositivo electrónico de seguridad que almacena su clave privada (token criptográfico y/o computador) y Software de Firma Digital.

7.2.3 Los/las suscriptores/as harán uso de los certificados digitales para firmar digitalmente documentos electrónicos de acuerdo a las funciones y actividades de su competencia. El uso de la clave privada de su certificado digital es personal e intransferible, siendo responsabilidad del/la suscriptor/a el uso de la firma de cualquier documento electrónico usando su usuario y clave privada.

7.2.4 Con relación al uso de la clave privada y del certificado digital por parte de el/la suscriptor/a, este/a deberá cumplir con lo siguiente:

a) Emplear adecuadamente su certificado digital conforme a lo dispuesto en la Ley N° 27269 – Ley de Firmas y Certificados Digitales y su Reglamento y sus modificatorias.

b) Mantener el control y absoluta reserva de la clave privada y/o el PIN de acceso.

c) Custodiar su clave privada o PIN de acceso de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.

d) En caso la clave privada quede comprometida en su seguridad, el/la suscriptor/a debe notificar al personal de Soporte Técnico de la Unidad de Arquitectura y Soporte de Tecnologías de Información y Comunicaciones - UAST y al Oficial de Seguridad de la Información, a fin de que por intermedio del Administrador del Certificado Digital se solicite la cancelación del certificado digital.

7.2.5 Para firmar digitalmente un documento electrónico, se deberá seleccionar y cargar el documento electrónico a firmar mediante el Software de Firma.

7.3 De la Cancelación de los Certificados Digitales

7.3.1 El/la suscriptor/a, debe solicitar la Cancelación de su certificado digital, al administrador del Certificado Digital, en los siguientes casos:

a) Cuando por error de el/la suscriptor/a o del Administrador del Certificado Digital, se haya consignado información inexacta en la solicitud.
b) Por la pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada (computador o token criptográfico).
c) Cuando el/la suscriptor/a deja de pertenecer laboralmente a la Entidad.

7.3.2 El administrador del Certificado Digital puede solicitar la cancelación del certificado digital de el/la suscriptor/a la EREP RENIEC en los siguientes casos:

a) Se determine que la información contenida en el certificado digital es inexacta o ha sido modificada.
b) Por muerte, o por inhabilitación o incapacidad declarada judicialmente de la persona natural suscriptor del certificado.

7.4 La administración del Token Criptográfico

7.4.1 El/la Administrador/a del Certificado Digital, autoriza el uso del token criptográfico a cada uno/a de los/as suscriptores/as de los órganos, unidades orgánicas y proyectos del OSCE en caso sean justificados, mediante el formato de Autorización de salida y retorno de Bienes Patrimoniales del OSCE[1].

7.4.2 La Unidad de Arquitectura y Soporte de Tecnologías de Información y Comunicaciones - UAST, instruye a los/as suscriptores/as, respecto al almacenamiento del certificado en el token.

7.4.3 En caso de bloqueo de la clave privada o PIN del token, el/la suscriptor/a está en la obligación de comunicar a la Unidad de Arquitectura y Soporte de Tecnologías de Información y Comunicaciones – UAST, a fin de que se realice la verificación correspondiente. En caso se trate de un bloqueo permanente, el Administrador del Certificado Digital, se comunica con la EREP-RENIEC para solicitar un nuevo certificado digital.

7.4.4 En el caso de cese de labores, el/la suscriptor/a deberá devolver el Dispositivo Electrónico (token) a la Unidad de Arquitectura y Soporte de Tecnologías de Información y Comunicaciones – UAST, como parte de la entrega de cargo.

VIII. DISPOSICIONES COMPLEMENTARIAS

Los documentos electrónicos firmados digitalmente se almacenan en el repositorio de datos del OSCE asignado a cada órgano y/o unidad orgánica, destinado además para el procesamiento, clasificación y consulta, con las medidas de seguridad correspondientes, garantizando el principio de equivalencia funcional y la integridad de su contenido.

[1] De acuerdo a la Directiva para el Registro, Control, Uso y Administración de Bienes Muebles pertenecientes al Patrimonio del OSCE vigente a la fecha