POLÍTICA Y DECLARACIÓN DE PRÁCTICAS DE REGISTRO

ENTIDAD DE REGISTRO (ER)

Cód: POL_DPR

Versión 3.0

Firmado por
MIGUEL ANTONIO HERNANDEZ GARCIA
DNI:10218167 RUC:20554785469

O = IN SOLUTIONS S.A.C
T = GERENTE GENERAL
e-mail = Miguel.hernandez@insolutions.pe
Date: 30/01/2024 21:32

Control de versiones

Versión	Secciones modificadas	Descripción del cambio	Fecha de aprobación	Revisado por	Aprobado por
1.0	Original	Creación del documento	26/JUL/2023	Miguel Hernández	Miguel Hernández
2.0	13.2	Protección de los registros	11/DIC/2023	Miguel Hernández	Miguel Hernández
3.0	8.2.1.1.	Verificación mediante consulta a bases de datos nacionales	29/ENE/2024	Miguel Hernández	Miguel Hernández
3.0	8.2.2.1.	Acreditar la existencia de la persona jurídica	29/ENE/2024	Miguel Hernández	Miguel Hernández

Contenido

1. Introducción

In Solutions S.A.C., con RUC N° 20554785469 es una empresa dedicada a brindar soluciones tecnológicas, entre las que destacan los softwares y/o aplicaciones de servicios de verificación biométrica contactless, firma digital, portal de firma digital firmalo.pe y como Entidad de Registro dentro de la Infraestructura Oficial de Firma Electrónica (IOFE).

El presente documento ha sido elaborado para describir las prácticas y procedimientos empleados por la IN SOUTIONS para la prestación de sus servicios como Entidad de Registro acreditada ante la AAC-INDECOPI.

1.1. Visión General

La Entidad de Registro IN SOLUTIONS tiene su sede central en la ciudad de Lima, Perú y tiene como principal objetivo asegurar la correcta identidad del solicitante en los servicios de emisión y revocación de certificados digitales, verificando y registrando la información recibida.

2. Participantes

2.1. Entidad de Registro:

In Solutions, en su papel como Entidad de Registro acreditada, es la persona jurídica acreditada que se encarga de verificar la validez de la información suministrada por el solicitante y verificar fehacientemente su identidad.

2.2. Entidad Certificación:

Las Entidades de Certificación asociadas a la ER In Solutions, son las personas jurídicas acreditadas que se encargan de prestar servicios de emisión, gestión, revocación, y otros inherentes a los certificados digitales.

2.3. Titular

Persona natural o jurídica que actúa como responsable y se le atribuye de manera exclusiva un certificado digital. En el caso de las personas naturales los roles de titular y suscriptor recaen sobre la misma persona. En el caso de las personas jurídicas, el rol de titular recae sobre el representante legal.

2.4. Suscriptor

Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

2.5. Tercero que confía

Se refiere a las personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado

2.6. Otros participantes

Todas las funciones, operaciones y actividades estarán a cargo de la ER IN Solutions. No obstante, en la eventualidad de que se requiera contratar los servicios de un tercero para realizar algún servicio de la ER, se contará con contratos y con cláusulas específicas relacionadas con la confidencialidad de la información del negocio y la protección de los datos personales.

3. Organización que administra los documentos de la ER

La presente Declaración de Prácticas de Registro y demás documentos de la ER son administrados por la empresa In Solutions S.A.C

3.1. Persona de contacto

La persona responsable de los Servicios de Valor Añadido, en la modalidad de Sistema de Intermediación Digital es Miguel Hernandez, Gerente General de In Solutions S.A.C. Para cualquier consulta, pueden dirigirse a:

- Teléfono: +51 1 3108149
- Correo Electrónico: info@insolutions.pe
- Dirección: Calle Enrique Palacios 360, oficina 102. Miraflores, Lima, Lima.
- Web: http://insolutions.pe/

4. Definiciones y Acrónimos

Ver Anexo 1

5. Publicación y difusión del documento

In Solutions publica toda la documentación vigente relacionada a la Entidad de Registro en su página web http://insolutions.pe/.

5.1. Frecuencia de publicación

El presente documento es revisado y actualizado periódicamente, según sea necesario. En caso de actualizaciones mayores, estas serán presentadas a la AAC antes de realizar la modificación del documento publicado.

6. Responsabilidades

6.1. Responsabilidad de la ER

La ER In Solutions tiene como responsabilidad brindar correctamente los servicios de registro o verificación conforme a las Guías de Acreditación del INDECOPI y sus Anexos.

6.2. Responsabilidades del titular y/o suscriptor

Las obligaciones y responsabilidades de los titulares y/o suscriptores se encuentran contenidas en el contrato de certificado digital.

6.3. Responsabilidades de los terceros que confían

Es responsabilidad de los terceros que confían, verificar el estado del certificado digital de acuerdo con los mecanismos de verificación que pone a disposición la ER IN SOLUTIONS

6.4. Terceros contratistas

Es responsabilidad de los terceros contratistas, brindar el servicio para el cual son contratados manteniendo la confidencialidad de la información del negocio y la protección de los datos personales.

7. Tipos de certificados digitales emitidos

La ER IN Solutions Brinda los siguientes tipos de certificados digitales:

- Titular de persona jurídica
- Trabajador (suscriptor) de persona jurídica
- Persona natural como trabajador profesional
- Agente Automatizado

7.1. Uso apropiado de los certificados digitales

Los certificados digitales podrán ser utilizados podrán ser utilizados únicamente para los propósitos indicados en las extensiones keyUsage (KU) y extendedKeyUsage (EKU), ya sea firma digital, autenticación o cifrado.

8. Solicitud de emisión de certificados digitales

8.1. Habilitados para presentar la solicitud de emisión un certificado

8.1.1. Persona jurídica atributos y/o AGA

Los autorizados para solicitar un certificado digital de persona jurídica o de Agente Automatizado son los representantes legales de la entidad solicitante.

Además, para solicitar certificados de suscriptor de persona jurídica, primero se debe contar con un titular que ya cuenta con certificado digital y autoriza la emisión del certificado del suscriptor

8.1.1.1. Acreditar facultades del solicitante

Las facultades del solicitante se deben acreditar mediante documentos oficiales que indiques que se encuentra habilitado para suscribir contratos.

8.1.2. Persona natural

Las personas naturales autorizadas para solicitar certificados digitales a la ER IN SOLUTIONS son aquellas que requieran un certificado digital para el ejercicio de sus funciones como trabajador profesional.

Cabe señalar que la emisión de certificados digital de persona natural como ciudadano peruano es competencia únicamente de la EREP-RENIEC dentro del DNI electrónico.

8.2. Verificación de los datos de la solicitud de emisión

8.2.1. Verificación de datos en general

8.2.1.1. Verificación mediante consulta a bases de datos nacionales

La ER In SOLUTIONS verifica la existencia de la persona jurídica mediante el documento de creación correspondiente y su vigencia será confirmada verificando los datos consignados en SUNARP. La persona jurídica debe encontrarse como “ACTIVO” y su domicilio en condición de “HABIDO”, siendo verificado a través de la SUNAT.

La verificación de la identidad de los suscriptores se realiza de la siguiente manera:

- Para el caso de los ciudadanos peruanos, la validación de la identidad del solicitante consiste en verificar su identidad empleando la Base de Datos del RENIEC, para lo cual la ER IN SOLUTIONS cuenta con el convenio correspondiente.

- Para el caso de los extranjeros, la comprobación de la identidad del solicitante se realiza mediante la consulta a la Base de Datos de la Superintendencia Nacional de Migraciones, disponible a través de su página web. Caso contrario, deberá presentar la copia autenticada por Notario, de su Carné de Extranjería vigente.

8.2.1.2. Verificación de datos de titulares y/o suscriptores

La verificación de los datos se realiza según lo indicado en el item 8.2.1.1.

8.2.1.3. Verificación presencial de identidad

Según lo indicado en la Guía de Acreditación de ER, la verificación de identidad del titular debe realizarse de manera presencial.

8.2.1.4. Información no verificada del suscriptor o titular

La ER IN SOLUTIONS no aceptará información que no pueda ser verificada.

8.2.2. Verificación de los datos de solicitud de persona jurídica y/o AGA

8.2.2.1. Acreditar la existencia de la persona jurídica

La ER In SOLUTIONS verifica la existencia de la persona jurídica mediante el documento de creación correspondiente y su vigencia será confirmada verificando los datos consignados en SUNARP. Adicionalmente, el RUC de la persona jurídica debe encontrarse como “ACTIVO” y su domicilio en condición de “HABIDO”, siendo verificado a través de la SUNAT.

Las facultades del solicitante se deben acreditar mediante documentos oficiales que indiquen que se encuentra habilitado para suscribir contratos.

8.2.2.2. Reconocimiento de nombres y marcas registradas

La ER IN SOLUTIONS solicita la documentación indicada en el item 8.2.2.1 para garantizar que un nombre o marca pertenece o corresponde al solicitante del certificado digital. Sin embargo, no es su función de la ER IN SOLUTIONS resolver controversias relativas a la propiedad de nombres de personas, naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

En el caso de validación de personas jurídicas, no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.

8.2.2.3. Verificación de las facultades laborales de los suscriptores

En el caso que un certificado sea solicitado para acreditar el ejercicio de un cargo en concreto, la ER IN SOLUTIONS requerirá a este solicitante las pruebas que evidencien su cargo, incluyendo las limitaciones y facultades de actuar como empleado de la persona jurídica correspondientes a dicho cargo.

8.2.2.4. Procedimiento de la petición del certificado AGA

Si el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por un representante designado por la persona jurídica dueña del dispositivo. En este caso, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

8.2.2.5. No repudio de la petición del certificado AGA

La petición del certificado de Agente Automatizado se solicita de acuerdo al estándar PKCS#10 (conocido también como CSR), de modo que no pueda ocurrir una suplantación.

8.2.3.Verificación de datos de la solicitud de persona natural

La verificación de los datos se realiza según lo indicado en el item 8.2.1.1.

8.2.4.No repudio de la solicitud

La solicitud de un certificado digital debe ser realizada por medios no repudiables para lo cual, los operadores de registro ingresan la solicitud a través de una plataforma a la cual se conectan utilizando certificados digitales.

8.2.5.Aprobación o Rechazo de la solicitud

La ER IN Solutions, tiene como facultad aprobar o rechazar una solicitud relacionada con el ciclo de vida de los certificados digitales que ofrece.

En caso se verifique fehacientemente la identidad y facultades del solicitante, se procederá con la aprobación de la solicitud. Caso contrario, en caso de suplantación de identidad, o no se hubiese podido comprobar la identidad y facultades del solicitante; se procederá con el rechazo de la solicitud.

8.2.6.No repudio de la invitación de generación de claves e instalación del certificado

La invitación para la generación de claves e instalación del certificado se realiza a través de un medio sobre el cual, sólo el suscriptor verificado tiene control, incluyendo el uso de módulos criptográficos que se encuentran en posesión de los suscriptores o los casos de generación en sistemas centralizados de gestión de claves.

8.2.7.Tiempo de procesamiento de la solicitud

Una vez aprobada la solicitud, la ER IN SOLUTIONS se comunicará inmediatamente con las EC asociadas y se procederá con la solicitud relacionada al ciclo de vida del certificado:

- En el caso de solicitudes de emisión, se procesarán en un plazo no mayor a 7 días calendario.
- En el caso de solicitudes de revocación, una vez aceptada la solicitud se debe proceder en un tiempo no mayor a 2 horas para la actualización de consultas OCSP y un tiempo no mayor a 24 horas para la actualización de listas CRL.
- En el caso de solicitud de suspensión, se procederá en un plazo no mayor a 5 días calendario.

8.2.8. Conformidad del titular

Se solicita conformidad del titular, a través de la firma del contrato, respecto a la emisión de los certificados para los suscriptores

8.3. Contrato con el titular/suscriptor

8.3.1. Diferencias con titulares y suscriptores

Los contratos son diferenciados para titulares y suscriptores, en el caso que los roles recaigan sobre personas diferentes.

8.3.2. Asignación de suscriptores

Para el caso de personas jurídicas, la asignación de suscriptores debe ser autorizada por el titular de la entidad, quien debe contar con un certificado digital vigente.

8.3.3. Verificación de la identidad de los suscriptores

Se realiza de acuerdo con lo indicado en el numeral 8.2.1.1.

9. Entidades de Certificación afiliadas a la ER

La ER IN SOLUTIONS se encuentra afiliada a la EC BIT4ID S.A.C. que se encuentra debidamente acreditada ante la AAC-INDECOPI.

9.1. Publicación de Entidades

La lista de entidades de certificación afiladas, se publica en su página web http://insolutions.pe/.

9.2. Publicación de CP y CPS de la EC asociada

La CP y CPS de la EC asociada, se publica en http://insolutions.pe/.

9.3. Publicación de certificaciones de la EC asociada

Se publica en http://insolutions.pe/.

9.4. Publicación de un documento que acredite representación de la EC

Se publica en http://insolutions.pe/.

9.5. Limitación de responsabilidades

Se publica en http://insolutions.pe/.

10. Re-emisión de certificados digitales

No aplica

11. Suspensión de certificados digitales

11.1. Solicitantes autorizados

Los autorizados para solicitar suspensión de certificados digitales son, únicamente, los titulares o suscriptores.

11.2. Periodo de suspensión

El tiempo máximo en el que el certificado digital puede ser suspendido está limitado por su fecha de expiración.

11.3. No repudio de la solicitud de suspensión

La solicitud de suspensión de un certificado digital es realizada por medios no repudiables, a fin de garantizar su autenticidad y no repudio.

11.4. Aprobación o rechazo de la solicitud de suspensión

Se aprueban solicitudes de certificados vigentes realizadas por los solicitantes autorizados. Caso contrario, se rechaza la solicitud de suspensión de un certificado no vigente o revocado o que sea realizada por un solicitante no autorizado.

11.5. Tiempo de procesamiento de la solicitud de suspensión

En el caso de solicitud de suspensión, se procederá en un plazo no mayor a 5 días calendario

12. Revocación de certificados digitales

12.1. Solicitantes autorizados

Conforme a la normativa peruana, los solicitantes autorizados para solicitar una revocación son:

- El titular o suscriptor del certificado
- La EC/ER que emitió el certificado
- Un juez que, de acuerdo con Ley, decida revocar el certificado.
- Un tercero que tenga pruebas fehacientes
- Un representante asignado por el titular de la persona jurídica para lo cual debe presentar documentación que acredite su representación y facultades asignadas.

12.2. No repudio de la solicitud de revocación

La solicitud de revocación se realiza mediante medios no repudiables, los que serán indicados en el Contrato al realizar la emisión del certificado.

12.3. Aprobación o rechazo de la solicitud de revocación

Se aprueban solicitudes de suspensión de certificados no revocados previamente ni suspendidos, realizadas por los solicitantes autorizados. Caso contrario, se rechaza la solicitud de revocación de un certificado suspendido o revocado previamente o que sea realizada por un solicitante no autorizado.

12.4. Ejecución de la revocación

Una vez aceptada la solicitud de revocación se procesará en un tiempo no mayor a 2 horas para la actualización de consultas OCSP y un tiempo no mayor a 24 horas para la actualización de listas CRL

12.5. Tiempo de procesamiento

El tiempo de procesamiento de la solicitud se realizará de acuerdo con lo indicado por la EC.

13. Protección de registros

13.1. Tipos de eventos registrados

De acuerdo con lo indicado en las Guías de Acreditación de ER y sus Anexos, como mínimo se registran los siguientes eventos:

- Información de contacto de los solicitantes de servicios
- Solicitudes de emisión, suspensión, revocación de certificados
- Resultados de evidencias de cada proceso de validación de identidad, incluyendo resultados positivos como procesos fallidos en los que se denegó la solicitud a un cliente
- Contratos con titulares y suscriptores
- Registros de evidencias de las solicitudes de emisión, suspensión y revocación realizadas por los operadores de registro a las Entidades de Certificación asociadas.
- Registro de contratación de operadores de registro

13.2. Protección de los registros

Los registros son protegidos de forma virtual en servidores de Microsoft Azure y la documentación administrativa y contratos se almacenan en una cuenta empresarial de Sharepoint.

13.3. Archivo de los registros

Se archivan los registros para ser conservados, de manera que se asegura su duración y conservación. Se almacenan en servidores de Microsoft Azure y la documentación administrativa y contratos en una cuenta empresarial de Dropbox. Solo personas autorizadas pueden acceder al archivo

13.4. Tiempo de almacenamiento del archivo

De acuerdo con lo indicado en las Guías de Acreditación y sus Anexos, La destrucción de un archivo de auditoría solo se podrá llevar a cabo con la autorización de INDECOPI, siempre y cuando haya transcurrido un periodo mínimo de 10 años.

14. Seguridad en las comunicaciones con la EC

14.1. Uso de canales seguros

Los operadores de registro se autentican en la plataforma de emisión y revocación de certificados utilizando certificado digital emitido a su nombre.

14.2. Autenticación de operadores de registro

La autenticación contra la plataforma de la entidad de registro se realiza mediante certificados digitales, emitidos a nombre de cada operador de registro.

14.3. Registros de auditoría (Logs)

Se generan registros de auditoría (logs) sobre las solicitudes de emisión, , revocación o suspensión de certificados, indicando el personal que hizo la solicitud, y el resultado positivo o fallido de la misma.

14.4. Seguridad Computacional

Las computadoras de los Operadores de Registro cuentan con antivirus y los parches del sistema antivirus actualizados.

14.5. Gestión de Residuos

Se cuenta con procedimientos para la gestión y destrucción de residuos que garantizan la imposibilidad de recuperación de la información.

15. Seguridad del personal

15.1. Definición de roles

Los roles se encuentran definidos en la Memoria Descriptiva.

15.2. Verificación de antecedentes

Tal como indica la Guía de Acreditación para ER y sus anexos, se realiza la verificación de antecedentes penales, policiales y crediticios del personal de la ER.

15.3. Cualidades, requisitos, experiencia y certificados

Se exige al personal de la ER que administra los sistemas de emisión, revocación o suspensión, tener conocimientos y experiencia en el uso de certificados digitales o seguridad de la información.

15.4. Compromiso contractual de confidencialidad

El personal de la ER In Solutions cuenta con cláusulas contractuales de confidencialidad

15.5. Responsabilidades contractuales

El personal de la ER In Solutions firma términos contractuales respecto de la protección de la privacidad y confidencialidad de toda la información presentada por los clientes de la ER.

15.6. Compromiso de cumplir la política de seguridad

El personal de la ER In Solutions firma términos contractuales respecto del compromiso de cumplir la política de seguridad.

15.7. Rotación en el trabajo

La seguridad y protección de datos personales se mantiene incluso en casos de rotación del personal, o periodos vacacionales retirando los permisos de acceso físico y lógico a

los Operadores de Registro cuando terminan su relación con la ER o cuando cambian de rol.

15.8. Capacitación

Se encuentra definido en la Política de Seguridad.

15.9. Sanciones por acciones no autorizadas

Se encuentran definidas en la Política de Seguridad

16. Auditoría

16.1. Auditoría de registros

Los registros son revisados, como parte de la auditoría de la AAC, de manera anual.

16.2. Auditoría del archivo

El archivo es revisado, como parte de la auditoría de la AAC, de manera anual.

16.3. Auditoría de los procedimientos y controles

Los procedimientos y controles implementados son auditados por la AAC de manera anual.

Por su parte, las auditorías internas se llevan a cabo, como mínimo, una vez al año en la ER.

16.4. Auditor

El auditor es autorizado por la AAC-INDECOPI y no debe haber laborado ni tener ninguna relación comercial ni efectos de auditoría en el mismo alcance de evaluación en el último año.

17. Medidas de contingencia

17.1. Protección contra compromisos de las claves del suscriptor

Si ocurre compromiso de claves del suscriptor dentro de las operaciones de registro, se procede a reportar el evento a la AAC-Indecopi y a revocar inmediatamente el certificado.

17.2. Compromiso de las claves del operador de registro

En caso de conocimiento del compromiso de claves del operador de registro, se procederá con la revocación del certificado, lo más pronto posible. Además, se tomarán las medidas pertinentes para verificar el impacto que pueda haber ocasionado.

17.3. Contingencia en caso de indisponibilidad de servicios de recepción de solicitudes de revocación

En caso de indisponibilidad de recepción de solicitudes de revocación mediante el procedimiento habitual, se dispondrá de un canal alterno; por ejemplo, recepción de solicitudes vía telefónica.

17.4. Contingencia en caso de indisponibilidad de servicios de recepción de solicitudes de re-emisión

No aplica

18. Finalización de la ER

18.1. Procedimiento de finalización

En caso la ER IN SOLUTIONS finalice sus actividades, adoptará todas las medidas posibles para minimizar el impacto que pueda ocasionar en sus usuarios y terceros confían.

Se informará a la AAC con un mínimo de 60 días de anticipación y a los titulares, suscriptores y terceros que confía sobre el fin de las operaciones con un mínimo de 30 días calendario de anticipación.

18.2. Transferencia de los registros de auditoría

La ER debe tomará las medidas necesarias para transferir los registros de auditoría a la AAC u otra entidad de registro, por el periodo establecido por la AAC de 10 años luego de generado el registro.

18.3. Garantías y responsabilidades

La ER IN SOLUTIONS establece procedimientos para el cumplimiento de las cláusulas de garantías y responsabilidades de la ER luego de su finalización.

18.4. Transferencia de las operaciones de registro para las solicitudes de revocación y re-emisión

La ER IN SOLUTIONS tomará las medidas correspondientes para transferir a otra Entidad de Registro, los servicios de recepción de solicitudes de revocación o re-emisión para sus clientes titulares y suscriptores de certificados, en caso de cese de operaciones.

19. Aspectos legales de la operación de la ER

19.1. Tarifas

Se encuentran definidas en el contrato.

19.2. Políticas de reembolso

Se encuentran definidas en el contrato.

19.3. Responsabilidad financiera

Se encuentra cubierto por el Seguro de Responsabilidad Civil

19.4. Información confidencial

Se encuentra definida en el Plan de Privacidad.

19.5. Información privada

Se encuentra definida en el Plan de Privacidad.

19.6. Información no privada

Se encuentra definida en el Plan de Privacidad.

19.7. Derechos de Propiedad intelectual

Se encuentran definido en el contrato.

19.8. Representaciones y garantías

Se encuentran definido en el contrato.

19.9. Excepciones de responsabilidad de garantías

Se encuentran definido en el contrato.

19.10. Notificaciones y comunicaciones entre participantes

A través de un contrato de prestación de servicios, se define que las notificaciones y comunicaciones entre las partes se realizará en los respectivos datos de contacto indicados en el documento

19.11. Correcciones o enmiendas

En caso de correcciones o enmiendas al presente documento, se comunicará a la AAC-Indecopi y, una vez aprobada la nueva versión, se dará de baja a la versión anterior.

19.12. Procedimiento de resolución de disputas

Se encuentran definido en el contrato.

19.13. Conformidad con la Ley aplicable

Es responsabilidad de la ER IN SOLUTIONS, en la prestación de sus servicios vela por el cumplimiento de la legislación aplicable, Ley N° 27269 Ley de Firmas y Certificados Digitales, su reglamento vigente y sus modificatorias.

19.14. Cumplimiento de la Ley aplicable

Es responsabilidad de la ER IN SOLUTIONS, en la prestación de sus servicios velar por el cumplimiento de la legislación aplicable, Ley N° 27269 Ley de Firmas y Certificados Digitales, su reglamento vigente y sus modificatorias.

19.15. Limitaciones de responsabilidad

Se encuentra definido en el contrato.

19.16. Indemnizaciones

De ser aplicable, se encuentra definido en el contrato.

19.17. Vigencia y conclusión

La Declaración de Prácticas de Registro se encuentra vigente en tanto sea la última versión. En caso de nuevas versiones, se comunicará a la AAC-Indecopi y, una vez aprobada la nueva versión, se dará de baja a la versión anterior.

20. Módulos criptográficos del suscriptor

20.1. Obtención del módulo criptográfico

Los módulos criptográficos usados por los suscriptores cumplen con los estándares FIPS 140-2 nivel 2, como mínimo o Common Criteria EAL4+ como mínimo

20.2. Preparación y personalización

La ER In Solutions no tiene posesión de las claves del suscriptor, se generan dentro del módulo criptográfico. El suscriptor recibe un dispositivo vacío y sin claves.

20.3. Almacenamiento y distribución del módulo criptográfico

La ER In Solutions entrega al suscriptor módulos criptográficos vacíos para que el usuario tenga control sobre la generación del par de claves. Bajo ninguna circunstancia, la ER In Solutions almacena módulos criptográficos que contienen claves de suscriptor.

20.4. Uso del módulo criptográfico

Los módulos criptográficos de los suscriptores cuentan con mecanismos de seguridad para proteger el acceso y uso.

20.5. Desactivación y reactivación

La activación y desactivación del módulo criptográfico es realizada únicamente por el suscriptor. No es manipulada por personal ni contratistas de la ER.

No se realiza el depósito, archivo, almacenamiento o copia de claves privadas de firma y autenticación de los usuarios finales, ni de los módulos hardware que los contienen, estando estos en modo activado.

20.6. Reemplazo del módulo criptográfico

En caso de titulares/suscriptores, no aplica.

En caso de operadores de registro, se realiza revocación del certificado del operador de registro y borrado seguro del módulo criptográfico, según las indicaciones del fabricante.

20.7. Terminación del módulo criptográfico

En caso de titulares/suscriptores, no aplica.

En caso de operadores de registro, se realiza revocación del certificado del operador de registro y borrado seguro del módulo criptográfico, según las indicaciones del fabricante.