Política de Certificación de firma, mensajería y entrega

Información general

Control documental

Clasificación de seguridad:	Público
Versión:	2.1
Fecha edición:	14/04/2025
Fichero:	**PSC-6-PC_Firma_Entrega_UCO_v2.1**
Código	PSC-6-

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Alejandro Grande Fecha: 14/04/2025	Nombre: Fabiola Ortega Fecha: 14/04/2025	Nombre: Elias Barzallo Fecha: 14/04/2025

Control de versiones

Versión	Partes que cambian	Descripción cambio	Autor cambio	Fecha cambio
1.0	Original	Creación del documento	Alejandro Grande	27/03/2025
2.0	Completo	Modificación completa del documento para denominarse Política de certificación. Inclusión de mayor detalle de las distintas modalidades de servicio	Alejandro Grande	10/04/2025
2.1	3.5.4	Se ha incluido mayor detalle respecto del concepto y aplicación de los affidavits.	Alejandro Grande	14/04/2025

Índice

INFORMACIÓN GENERAL 2

CONTROL DOCUMENTAL 2
ESTADO FORMAL 2
CONTROL DE VERSIONES 3

ÍNDICE 4

1. POLÍTICAS Y DOCUMENTOS APLICABLES 7

1.1. ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS 7
1.2. PERSONA DE CONTACTO 8
1.3. FRECUENCIA DE PUBLICACIÓN 8
1.4. PUBLICACIÓN Y DIFUSIÓN DEL DOCUMENTO 8

2. ALCANCE DE APLICACIÓN DEL DOCUMENTO 9

2.1. PARTICIPANTES EN LOS SERVICIOS DE CERTIFICACIÓN 9
2.1.1. Entidad de Certificación Digital 9
2.1.2. Suscriptores del servicio de certificación 9
2.1.3. Partes usuarias 10
2.1.4. Emisor y receptor 10
2.1.5. Terceros que confían 10
2.1.6. Otros 10
2.2. APLICABILIDAD 11
2.3. CONFORMIDAD 11

3. ECD DE FIRMA, MENSAJERÍA Y ENTREGA 12

3.1. DETERMINACIÓN Y ALCANCE DE LOS SERVICIOS 12
3.1.1. Servicio de Firma 12
3.1.2. Servicio de Mensajería y Entrega Certificada 12
3.2. DEFINICIÓN DE RESPONSABILIDADES 13
3.2.1. Responsabilidades y obligaciones de UANATACA COLOMBIA 13
3.2.2. Responsabilidades y obligaciones del suscriptor 14
3.2.3. Responsabilidades y obligaciones de los Terceros que confían 14
3.2.4. Limitación de responsabilidad 14
3.2.5. Resolución de disputas 15
3.3. GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES 16
3.3.1. Generación de las claves del servicio 16
3.3.2. Protección de la clave privada 16
3.3.3. Distribución de la clave pública 17
3.3.4. Re-emisión de la clave 17
3.3.5. Término del ciclo de vida de la clave privada 17

3.4. CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO 18
3.5. SERVICIO DE CERTIFICACIÓN DE FIRMA, MENSAJERÍA Y ENTREGA 19
3.5.1. Acceso al servicio 19
3.5.2. Autenticación del emisor 20
3.5.3. Autenticación del receptor 20
3.5.4. Eventos y evidencias 20
3.6. SINCRONIZACIÓN DEL RELOJ CON EL UTC 22
3.7. GESTIÓN DE LA SEGURIDAD 22
3.7.1. Organización de la seguridad de la información 22
3.7.2. Política de seguridad de la información 22
3.7.3. Gestión de riesgos 23
3.7.4. Documentación 23
3.7.5. Seguridad en el trato con terceros 23
3.7.6. Clasificación y gestión de activos 23
3.7.7. Seguridad del personal 24
3.7.8. Seguridad física y del entorno 26
3.7.9. Gestión de operaciones 28
3.7.10. Manejo de medios y seguridad 30
3.7.11. Planificación del sistema 30
3.7.12. Reportes de incidentes, informes de seguimiento y solución 31
3.7.13. Seguridad en redes 31
3.7.14. Monitoreo 31
3.7.15. Intercambio de datos y software 32
3.7.16. Gestión de accesos a los sistemas 32
3.7.17. Archivo 32
3.7.18. Desarrollo y mantenimiento 34
3.7.19. Control de cambios 34
3.8. COMPROMISO DE LOS SERVICIOS DE CERTIFICACIÓN 34
3.9. TÉRMINO DE LA ORGANIZACIÓN QUE ADMINISTRA EL SERVICIO DE CERTIFICACIÓN 35
3.10. REGISTROS DE INFORMACIÓN CONCERNIENTE A LA OPERACIÓN 36
3.11. AUDITORÍA 38
3.11.1. Frecuencia de la auditoría de conformidad 38
3.11.2. Auditoría de registros y archivos 38
3.11.3. Auditor 39
3.12. OTROS ASPECTOS LEGALES DE LA OPERACIÓN DEL SERVICIO DE CERTIFICACIÓN 39
3.12.1. Tarifas y políticas de reembolso 39
3.12.2. Cobertura de seguro de responsabilidad civil 39
3.12.3. Información confidencial y/o privada 40
3.12.4. Información no privada 40
3.12.5. Derechos de Propiedad intelectual 40
3.12.6. Notificaciones y comunicaciones entre participantes 41

3.12.7. Conformidad con la Ley aplicable 41
3.12.8. Exención de garantías 41
3.12.9. Indemnizaciones 41
3.12.10. Fuerza mayor 42
3.12.11. Disposiciones aplicables 42

ANEXO I: ACRÓNIMOS 43

1. Políticas y documentos aplicables

Este documento declara la política de certificación para los servicios de certificación de Firma electrónica, Mensajería y Entrega certificada de Uanataca Colombia, S.A.S, en adelante "*UANATACA COLOMBIA*", dando cumplimiento a lo previsto en la Ley 527 de 1999, Decreto Ley 019 de 2012 y demás normas y decretos reglamentarios aplicables a la prestación de servicios de certificación digital. Así como de los requisitos contenidos en la CEA-3.0-07 Criterios Específicos De Acreditación Entidades De Certificación Digital – vigente y establecido por el Organismo Nacional de Acreditación de Colombia – ONAC para la prestación de servicios de certificación digital.

La Política de Certificación (en adelante PC) se define como un conjunto de prácticas adoptadas por una Entidad de Certificación Digital (en adelante ECD) para la certificación de Firma, mensajería y Entrega.

En general, este documento contiene toda la información detallada sobre su sistema de seguridad, administración, soporte y sobre el servicio para la generación de firmas, gestión de la mensajería y entrega de estas, además de definir la relación de confianza existente entre el Usuario o Suscriptor y la ECD que en la presente será UANATACA COLOMBIA.

Este documento debe ser un documento claro, comprensible y sólido, que proporcione una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo de vida de los certificados, etc., por parte de la ECD.

1.1. Organización que administra los documentos

UANATACA COLOMBIA en su papel de Entidad de Certificación Digital (ECD) abierta, es la persona jurídica privada que presta indistintamente en el país servicios y actividades inherentes a la certificación digital, que actúa de acuerdo con la legislación de Colombia, conformada por la Ley 527 de 1999, el Decreto Ley No. 019 de 2012, Decreto Único del Sector Comercio, Industria y Turismo – DURCSIT, 1074 de 2015, así como las normas técnicas del ETSI aplicables a la expedición y gestión de certificados principalmente, EN 319 401, EN 319 411-1, EN 319 412; sellado de tiempo ETSI 319 421, y otros como ETSI

319 521, así como los mejores estándares internacionales, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

1.2. Persona de contacto

Los datos adicionales de contacto de la ECD, son los siguientes:

- Entidad: UANATACA COLOMBIA, S.A.S.
- Web: https://www.uanataca.com/co/.
- Email: info@uanataca.co
- Teléfono: +593 99 970 3430.
- Domicilio postal: Calle 93 B 12 28 OF 203 204 Bogotá, Colombia

1.3. Frecuencia de publicación

La información de la ECD, se publicarán el día siguiente a su aprobación por la ONAC. Los cambios en la PC se rigen por lo establecido en el procedimiento de gestión de este documento y de acuerdo con la normativa de aplicación.

1.4. Publicación y difusión del documento

La presente PC es administrada por la ECD, y está publicada, para su consulta por cualquier tercero interesado, en su web https://www.uanataca.com/co/, junto con el resto de documentación relativa a su servicio de certificación.

En el sitio web de UANATACA COLOMBIA se podrán localizar todas las versiones de todos los documentos públicos relacionados con los servicios prestados por parte de la ECD.

El sitio de la ECD se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de la ECD, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo de acuerdo con los plazos y procedimientos establecidos con respecto de la continuidad del negocio.

2. Alcance de aplicación del documento

2.1. Participantes en los servicios de certificación

2.1.1. Entidad de Certificación Digital

La ECD es la persona autorizada y facultada para emitir certificados en relación con las firmas digitales de las personas, la gestión de la mensajería, y entrega y ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

La ECD es la persona jurídica privada que presta indistintamente en el país servicios y actividades inherentes a la certificación digital, que actúa de acuerdo con la legislación de Colombia, conformada por la Ley 527 de 1999, el Decreto Ley No. 019 de 2012, Decreto Único del Sector Comercio, Industria y Turismo – DURCSIT, 1074 de 2015, así como las normas técnicas del ETSI aplicables a la expedición y gestión de certificados principalmente, EN 319 401, y EN 319 521, y los mejores estándares internacionales, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

A la ECD le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante el ONAC, a fin de lograr y mantener la acreditación correspondiente.

2.1.2. Suscriptores del servicio de certificación

Los suscriptores son los usuarios finales de los servicios de certificación gestionados por la ECD. Los suscriptores del servicio pueden ser:

- Personas jurídicas (empresas, entidades, corporaciones u organizaciones) que solicitan a UANATACA COLOMBIA (directamente o a través de un tercero) el uso de sus servicios en su ámbito empresarial, corporativo u organizativo.
- Personas físicas que solicitan el servicio para sí mismas.

2.1.3. Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben la intermediación mediante certificados, firmas electrónicas, sellos de tiempo, o mensajes electrónicos de la ECD.

Como paso previo a confiar en estos mensajes, las partes usuarias deben verificarlos, como se establece en esta PC así como en las instrucciones disponibles en la página web de la ECD.

2.1.4. Emisor y receptor

Los emisores y receptores son personas físicas y/o jurídicas, identificadas en la mayoría de las ocasiones con cuentas de correo electrónico y teléfonos móviles, pertenecientes a las partes usuarias, que emiten o reciben mensajes electrónicos cuya entrega sea verificada.

2.1.5. Terceros que confían

Los terceros que confían son las personas físicas o jurídicas que confían en la intermediación mediante certificados, firmas electrónicas, sellos de tiempo, o mensajes de UANATACA COLOMBIA, y que han sido emitidos en los términos y condiciones previstas en la presente PC.

2.1.6. Otros

Para la ejecución de los servicios de certificación de la presente PC puede que sea necesario, por parte de UANATACA COLOMBIA, pactar, contratar o utilizar servicios de terceros para la prestación parcial o total de alguna de sus actividades. En todo momento, en dichas contrataciones se estará a lo indicado en la presente PC.

2.2. Aplicabilidad

La PC, no se utilizará para fines distintos de los especificados en el presente documento. Del mismo modo, el servicio deberá emplearse únicamente de acuerdo con la regulación aplicable en materia de prestación de este tipo de servicios, y según la legislación de Colombia.

2.3. Conformidad

UANATACA COLOMBIA como ECD se somete a las evaluaciones periódicas obligatorias de la ONAC para evidenciar que sus operaciones y controles son conformes con los documentos normativos como la presente PC.

3. ECD de Firma, Mensajería y Entrega

3.1. Determinación y alcance de los servicios

Los servicios de firma, mensajería y entrega certificada de UANATACA COLOMBIA se dividen en diferentes modalidades contando con los siguientes servicios:

- EVISIGN
- EVISMS
- EVIMAIL
- EVINOTICE

3.1.1. Servicio de Firma

El servicio de firma de UANATACA COLOMBIA se presta bajo la modalidad única de EVISIGN.

- **EVISIGN** es el sistema de certificación que garantiza la evidencia electrónica, generada a partir de la firma electrónica del documento y/o anexos, tras la lectura y declaración de voluntad sobre el contenido aquí mostrado, facilitando los medios para verificar la identidad de los firmantes, la integridad del contenido, del proceso de visualización y firma, de las fechas de admisión, fecha de entrega y fecha de firma, así como de las declaraciones de voluntad.

3.1.2. Servicio de Mensajería y Entrega Certificada

El servicio de Mensajería y Entrega Certificada de UANATACA COLOMBIA se presta bajo 3 modalidades distintas: EVISMS, EVIMAIL y EVINOTICE.

- **EVISMS** es el sistema de certificación de evidencias mediante SMS certificado, garantizando la autenticidad del origen/destino de las comunicaciones mediante SMS, la integridad del contenido, las fechas y detalles de los sucesos relacionados con su tramitación, como el envío, la transmisión, recepción, acuses de recibo y/o declaraciones de voluntad de las partes implicadas.

- **EVIMAIL** es el sistema de certificación de evidencias mediante correo electrónico certificado, garantizando la autenticidad del origen/destino las comunicaciones, la integridad del contenido y/o anexos, así como las fechas y detalles de los sucesos relacionados con su tramitación.

- **EVINOTICE** en el sistema de certificación de evidencias mediante comunicaciones certificadas, garantizando la autenticidad del origen/destino de las comunicaciones, la integridad del contenido y/o anexos, así como las fechas y detalles de los sucesos relacionados con su entrega.

3.2. Definición de responsabilidades

3.2.1. Responsabilidades y obligaciones de UANATACA COLOMBIA

UANATACA COLOMBIA garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la PC, siendo el responsable del cumplimiento de los procedimientos descritos, de acuerdo con las indicaciones contenidas en este documento.

La ECD presta los servicios de certificación conforme y en los términos previstos con esta PC.

La ECD vincula a los suscriptores y terceros que confían en sus servicios de certificación, mediante esta PC, en lenguaje escrito y comprensible, con todas aquellas exigencias llevadas a cabo por ley, así como teniendo en cuenta los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en el presente documento.
- Límites de uso de los servicios de certificación.
- Información sobre cómo validar un certificado, firmas electrónicas, sellos de tiempo, certificaciones de entrega o mensajes de la ECD, incluyendo el requisito de comprobar el estado de este, y las condiciones en las cuales se puede confiar razonablemente en él, que resulta aplicable cuando el suscriptor actúa como tercero que confía en la intermediación.
- Forma en que se garantiza la responsabilidad patrimonial de la ECD.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la ECD acepta o excluye su responsabilidad.

- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.

3.2.2. Responsabilidades y obligaciones del suscriptor

Las obligaciones de los suscriptores con respecto a los servicios de certificación de la ECD son:

- Respetar lo dispuesto en esta PC.
- Formalizar un contrato de prestación de servicios de certificación con La ECD.
- Utilizar los servicios de certificación de la ECD de acuerdo con los procedimientos y, si fuera necesario, los componentes técnicos suministrados por la ECD, de conformidad con lo que se establece en la PC o en la documentación técnica de la ECD.
- Notificar cualquier incidente o hecho que afecte a los servicios de certificación de la ECD.

3.2.3. Responsabilidades y obligaciones de los Terceros que confían

Las obligaciones de terceros que confían y usan los distintos servicios de certificación son:

- Cumplir y facilitar el cumplimiento de todo lo estipulado en esta PC, y en sus documentos relacionados.
- El tercero deberá conocer y seguir lo establecido en esta PC y en sus documentos relacionados, siendo de obligado cumplimiento como si del propio servicio de certificación se tratara.
- Verificar los certificados, firmas electrónicas, entregas certificadas, sellos de tiempo, o mensajes incluyendo la validez del certificado usado en los diferentes servicios de certificación y de entrega certificada de la ECD.

3.2.4. Limitación de responsabilidad

La ECD, en la documentación que la vincula con suscriptores y terceros que confían, establece y rechaza garantías, y limitaciones de responsabilidad aplicables, donde:

- Garantiza al suscriptor que los servicios de certificación cumplen con todos los requisitos materiales establecidos en esta PC, así como las normas de referencia.

- Garantiza al tercero que confía en sus servicios de certificación que la información contenida o incorporada por referencia en los certificados, firmas electrónicas, entregas certificadas, sellos de tiempo, o mensajes, excepto cuando se indique lo contrario.
- Rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en este documento.
- Limita su responsabilidad a la prestación de los servicios de certificación, los cuáles se regularán por el contrato oportuno con dicho suscriptor o usuario.
- No será responsable de ningún daño directo y/o por terceros como consecuencia del uso indebido de los servicios de certificación que haya podido ser causado por un uso inadecuado o poco diligente por parte de los usuarios o suscriptores.
- Incluye en esta PC cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.
- Establece, en el contrato con el suscriptor y/o en sus documentos relacionados que la ley aplicable a la prestación de los servicios de certificación, incluyendo la PC, es la Ley de Colombia, indicadas anteriormente en la presente PC.

3.2.5. Resolución de disputas

Las peticiones, quejas, reclamos y solicitudes (PQRS) sobre los servicios prestados por UANATACA COLOMBIA, son recibidas directamente por el responsable competente.

Los Solicitantes, Suscriptores, Terceros que confían o el público en general indicarán su PQRS con respecto a los servicios de certificación digital ofrecidos por UANATACA COLOMBIA enviando un correo electrónico a la dirección info@uanataca.co en el que se detalla la situación por la que se presenta.

Los PQRS serán gestionados por el Responsable de realizar tales funciones., quien se encargará de derivar la incidencia al Departamento o rol respectivo. Dicha gestión se llevará a cabo, dando lugar a una solución en un lapso no mayor a quince (15) días. El usuario recibirá un mensaje de correo electrónico confirmando la recepción de la PQRS y cuando ésta sea resuelta.

UANATACA COLOMBIA cuenta con el procedimiento interno para el tratamiento de PQRS que detalla cada uno de los procesos y se encuentra publicado en la página web.

3.3. Gestión del ciclo de vida de las claves

La ECD emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

3.3.1. Generación de las claves del servicio

La ECD se asegurará de crear las claves criptográficas del servicio en un entorno seguro y totalmente controlado.

Para la generación de las claves se han seguido los procedimientos de ceremonia de claves de UANATACA COLOMBIA, dentro del perímetro de alta seguridad destinado a esta tarea.

- Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado.
- Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

Para la generación de la clave del certificado de la ECD se utilizan dispositivos con las certificaciones *Common Criteria EAL4+*, que tienen un nivel igual o superior a *FIPS 140-2 level 3*.

Los certificados del servicio de certificación y de entrega segura han sido generados por los UANATACA COLOMBIA en calidad de Entidad de Certificación Digital para la emisión de certificados electrónicos, de acuerdo con lo indicado en la propia Política de Certificación disponible en la página web: https://www.uanataca.com/co.

3.3.2. Protección de la clave privada

La ECD se asegurará de custodiar de manera segura la clave privada del servicio, conservando la misma únicamente dentro de los dispositivos criptográficos donde se han generado, y mediante los procedimientos indicados por el fabricante de dicho dispositivo.

La ECD realiza copias de seguridad de las claves privadas de los certificados, de tal manera que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de estas. Tanto la generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas, y siempre siguiendo los procedimientos del fabricante del dispositivo criptográfico.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia alternativo.

3.3.3. Distribución de la clave pública

Los certificados de la ECD son comunicados a los terceros que confían, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en la web de la ECD. Los usuarios tendrán la capacidad de acceder al depósito para obtener las claves públicas.

El certificado de las Autoridades de Certificación Raíz y Subordinadas estarán a disposición de los usuarios en la página web de la ECD que ha generado los certificados de la ECD.

3.3.4. Re-emisión de la clave

Los algoritmos utilizados para la generación de las claves y certificados están de acuerdo con lo indicado en la norma ETSI TS 119 312. Las claves se volverán a emitir nuevamente, cuándo los algoritmos utilizados se consideren débiles y ETSI recomiende su renovación.

Los certificados se renovarán, por lo menos, con un mes de antelación a su fecha de expiración.

3.3.5. Término del ciclo de vida de la clave privada

Para la destrucción de las claves privadas se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente de tal manera que no se puedan volver a utilizar.

Con anterioridad a la destrucción de las claves, se solicitará la revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de la ECD. Para el reinicio se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.
Finalmente se destruirán de forma segura las copias de seguridad.

3.4. Ciclo de vida del módulo criptográfico

La ECD realizará y ejecutará los procedimientos técnicos necesarios para confirmar la seguridad del ciclo de vida del hardware utilizado por los servicios de certificación, en particular:

- La ECD asegura que el hardware criptográfico usado por el servicio de certificación y entrega certificada, no se ha manipulado durante su transporte mediante la inspección del material entregado.
- La ECD se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado. El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación. La ECD registra toda la información pertinente del dispositivo para añadir al catálogo de activos.
- El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza. Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.
- Las claves privadas del servicio de certificación se generan directamente en los módulos criptográficos de la ECD donde se almacenan cifradas.
- La activación y duplicación de dichas claves en el hardware del módulo criptográfico se ha realizado por personal que ocupa roles de confianza, mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, usando al menos un control de acceso de dos personas en un ambiente físico seguro. En relación con lo establecido anteriormente, la ECD realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo. El dispositivo hardware criptográfico solo es manipulado por personal confiable.

- La gestión de acceso a las claves privadas de los certificados del servicio de certificación y de entrega segura, se realiza según los controles establecidos por el HSM donde se custodian.
- La clave privada de firma de la ECD almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo. La configuración del sistema de la ECD, así como sus modificaciones y actualizaciones son documentadas y controladas. Del mismo modo, la ECD se asegurará que el hardware de firma funciona correctamente.
- Para la desactivación de las claves privadas de la ECD se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.
- Las claves de firma del servicio de certificación que son almacenadas en un módulo criptográfico son borradas antes de que el dispositivo sea retirado.
- En el apartado "Término del ciclo de vida de la clave privada" se indica que para la destrucción de las claves privadas se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente de tal manera que no se puedan volver a utilizar.

3.5. Servicio de Certificación de Firma, Mensajería y Entrega

El Servicio de Entrega Certificada permite asegurar el envío, recepción y comprobación de comunicaciones electrónicas, asegurándose en todo momento de las características de integridad, autoría, trazabilidad y no repudio de la misma. Para ello La ECD permite certificar el envío como la recepción de los mensajes de datos, y que los emisores/receptores son quienes se exponen en la comunicación.

El servicio de entrega puede generar información necesaria para identificar la comunicación de manera unívoca mediante un identificador del correo electrónico certificado en el sistema, con enlace de verificación de trazabilidad que permitan acceder al contenido de la misma y la información relativa del correo electrónico.

3.5.1. Acceso al servicio

El acceso a las diferentes URL del servicio de entrega cualificada siempre se realizará mediante protocolos seguros y comunicaciones cifradas provistos por parte de la ECD.

3.5.2. Autenticación del emisor

La autenticación del emisor para enviar comunicaciones se hará mediante usuario (vinculando a su correo electrónico) y contraseña, proveyendo el servicio medio para aplicar políticas complejas de contraseñas y reseteo seguros de las mismas.

3.5.3. Autenticación del receptor

La autenticación del receptor se realiza mediante doble factor de autenticación con una URL temporal aleatoria, y la posibilidad de añadir un OTP (*One-Time Password*) que será enviado al email o teléfono móvil (SMS o *WhatsApp*) del receptor.

3.5.4. Eventos y evidencias

El Servicio de Certificación de Firma, Mensajería y Entrega es un servicio que permite transmitir datos entre partes terceras por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada, por lo tanto el servicio de la ECD permite recopilar evidencias que permitan asegurar que los mensajes electrónicos del emisor son entregados al receptor de los mismos garantizando la integridad de la evidencia y la veracidad de la misma.

El encargado de garantizar esta integridad y veracidad es la propia ECD, a través de una serie de procesos criptográficos como la aplicación de firmas electrónicas y sellos de tiempo. Tanto los procesos de firma como los sellos de tiempo son proporcionados por la ECD dados de alta en la ONAC.

A efectos del Servicio de Certificación de Firma, Mensajería y Entrega, se define como Affidavit el documento electrónico generado automáticamente por el propio servicio, que recopila y conserva evidencia técnica detallada de un determinado evento relacionado con los servicios de firma, mensajería y/o entrega.

La función principal del Affidavit es dejar constancia de forma fehaciente de que dicho evento ha ocurrido, y que la información en el affidavit no ha sido modificada desde su generación.

Los affidavits se configuran como las evidencias en la ECD. Cada affidavit contiene la información pericial que permite demostrar que un evento relevante del proceso de entrega de mensajes se ha producido correctamente o ha fallado, incluyendo todos los datos asociados, bajo condiciones de integridad, trazabilidad y sellado temporal. En los *affidavits* se puede encontrar:

- Datos de información del emisor y receptor de los mensajes electrónicos.
- El contenido emitido, junto con los documentos adjuntos procesados, además se incorporan resúmenes criptográficos de los mismos.
- En los *affidavits* se puede encontrar información sobre los siguientes eventos:
    - Envío y emisión al servidor de correo del destinatario.
    - Entrega al servidor de correo del destinatario o fallo si no se pudiera entregar.
    - Apertura del mensaje.
    - O acciones posteriores del receptor (si es que se producen).
    - La referencia temporal estará indicada en horario *Coordinated Universal Time* (UTC).

Cada affidavit es firmado electrónicamente por el servicio, y se le incluye un sello de tiempo cualificado, para de esta manera garantizar la integridad del documento y que éste no haya sido modificado con posterioridad.

El emisor tendrá acceso a todos sus *affidavits* en el servicio de entrega certificada de la ECD, durante el periodo de custodia contratado con un periodo mínimo de 10 años.
El receptor podrá acceder a los *affidavits* a través del servicio de soporte o por información del emisor. Una vez que el periodo de vigencia contratado haya concluido ninguna de las partes tendrá acceso a los *affidavits*.

En el caso de producirse un fallo con la integridad de los *affidavits*, o se produjera cualquier incidencia asociada a la integridad del contenido durante el proceso de entrega se comunicará desde el servicio de soporte de la ECD a las partes interesadas.

3.6. Sincronización del reloj con el UTC

UANATACA COLOMBIA tiene un procedimiento de sincronización de tiempo coordinado vía NTP, que accede y que realizan el registro del instante de tiempo en los que tienen lugar los eventos. El tiempo de los sistemas proviene de una fuente fiable de hora. Todos los sistemas de UANATACA COLOMBIA sincronizan su instante de tiempo con esta fuente. Las fuentes de tiempos utilizadas, basadas en el protocolo NTP (Network Time Protocol) se auto calibran por distintos caminos, utilizando como referencia la Hora Legal de la República de Colombia tomada directamente de los patrones de referencia del Instituto Nacional de Metrología de Colombia (INM).

- La primera sincronización del tiempo para los servicios de la ECD se obtiene mediante consulta al Instituto Nacional de Metrología (INM) de Colombia, institución encargada de mantener, coordinar y difundir la hora legal de la República de Colombia. Los servidores se mantienen actualizados con la hora UTC, mediante sincronización a través del protocolo NTP v4, conforme al estándar RFC 5905 “Network Time Protocol Version 4: Protocol and Algorithms Specification”.
- La segunda dispone de una sincronización complementaria, vía NTP, Servicio basado en antenas y receptores GPS que permite un nivel de confianza de STRATUM 1 (con dos sistemas en alta disponibilidad)

3.7. Gestión de la seguridad

3.7.1. Organización de la seguridad de la información

La ECD ha implementado un Sistema de Gestión de la Seguridad de la Información y de la Calidad (SGSIC) que tiene como alcance todos los servicios descritos en la presente PC.
La gestión de la seguridad depende directamente de la Dirección de la ECD así como del Comité de Seguridad del SGSIC.

3.7.2. Política de seguridad de la información

La ECD cuenta con una política de seguridad que se puede consultar en la web de la ECD (https:// www.uanataca.com/co) y que ha sido comunicada tanto internamente como

externamente a cualesquiera terceros interesados. El alcance de la política de seguridad cubre todas las operaciones del servicio de certificación de la ECD.

3.7.3. Gestión de riesgos

La ECD realiza de manera periódica un análisis de riesgos para todos los activos de la organización, entre los que están incluidos los activos del servicio de certificación de la presente PC. En dicho análisis se evalúan los activos, las amenazas que tienes y el impacto que se generaría si una amenaza se materializa sobre un activo.

Una vez evaluado el riesgo, se determinan las salvaguardas que se deben de implementar para aceptar, reducir o transferir los riesgos detectados.

3.7.4. Documentación

La ECD, como parte de lo requerido en su Sistema de Gestión de Seguridad de la Información y de la Calidad, tiene documentado, versionados y publicados internamente todos los procedimientos operativos y de seguridad de los servicios prestados por la ECD.

3.7.5. Seguridad en el trato con terceros

La ECD exige medidas de seguridad equivalentes a cualquier tercero o proveedor externo implicado en las labores del servicio de certificación. Adicionalmente, todos los terceros que presten servicios son auditados por el equipo de seguridad de la ECD.

3.7.6. Clasificación y gestión de activos

La ECD mantiene un inventario de activos donde están recogidos todos los activos de la compañía incluyendo también los que forman parte del servicio de certificación . El inventario de activos depende directamente del análisis y gestión de riesgos del Sistema de Gestión de Seguridad de la Información y de la Calidad, y sobre dicho activo se han establecido la clasificación de seguridad en base a sus requisitos de Autenticación, Confidencialidad, Integridad, Disponibilidad y Auditorías, documentando las reglas del control de acceso.

3.7.7. Seguridad del personal

Requisitos de historial, calificaciones, experiencia y autorización

Todo el personal está cualificado y/o ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal que haya sido designado para llevar a cabo puestos de confianza no tiene intereses personales que entren en conflicto con el desarrollo de la función que tenga encomendada.

En general, la ECD retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de conflictos de interés y/o la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

La ECD no asignará un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por una falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales.
- Referencias profesionales.

Procedimientos de investigación de historial

La ECD, antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

La ECD obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales en cumplimiento de la normativa vigente en materia de protección de datos personales.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.

- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

Requisitos de formación

La ECD forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

Los programas de formación son revisados periódicamente, y son actualizados para su mejora y mejorados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad de la ECD. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

Requisitos y frecuencia de actualización formativa

La ECD, actualiza la formación del personal de acuerdo con las necesidades, y con la frecuencia suficiente para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación.

Sanciones para acciones no autorizadas

La ECD dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable en Colombia.

Las acciones disciplinarias incluyen la suspensión, separación de las funciones y hasta el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por la ECD. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la PC, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, la ECD, será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación del servicios de certificación por tercero distinto a la ECD.

Suministro de documentación al personal

La ECD suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

3.7.8. Seguridad física y del entorno

Controles de seguridad física

La ECD ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, y los equipamientos empleados para las operaciones para la prestación del servicio de certificación .

En concreto, la política de seguridad de la ECD aplicable a los servicios de certificación establece prescripciones sobre lo siguiente:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios de la ECD.

Estas medidas resultan aplicables a las instalaciones desde donde se presta el servicio de certificación, en sus entornos de producción y contingencia, las cuales son auditadas periódicamente de acuerdo con la normativa aplicable y a las políticas propias de la ECD destinadas a este fin.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia las 24 horas siguientes al aviso.

Localización y construcción de las instalaciones

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y está ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

Las salas donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos (CPD) cuenta con redundancia en sus infraestructuras, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.

Acceso físico

UANATACA COLOMBIA dispone a través del proveedor de la infraestructura, de tres niveles de seguridad física en el CPD (entrada del Edificio donde se ubica, acceso a la sala del CPD y acceso al Rack), debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias donde se opera el servicio de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro de este.
- El acceso a las salas se realiza con lectores de tarjeta de identificación y/o cerraduras electrónicas, gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso a la sala donde se ubican los procesos criptográficos es necesario una autorización previa a los administradores del servicio de *colocation* que disponen de la llave para abrir la sala y la jaula, pero no los armarios.

Electricidad y aire acondicionado

Las instalaciones del CPD disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado.

Exposición al agua

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación. Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

Prevención y protección de incendios

Las instalaciones y activos del CPD cuentan con sistemas automáticos de detección y extinción de incendios.

Almacenamiento de soportes

Únicamente el personal autorizado tiene acceso a los medios de almacenamiento. La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del CPD.

Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garantizan la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se desechan en cuyo caso se destruyen físicamente, o se reutilizan previo proceso de borrado permanente o formateo. En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

Copia de respaldo fuera de las instalaciones

Se utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del CPD.

3.7.9. Gestión de operaciones

La ECD garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de su servicio de certificación.

El personal al servicio de la ECD ejecuta los procedimientos administrativos, operacionales y de gestión de acuerdo con la política de seguridad.

Funciones fiables

La ECD ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Administrador de Sistemas**: responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- **Auditor Interno**: responsable de proporcionar aseguramiento del cumplimiento de los procedimientos operativos por parte de sus responsables. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.
- **Custodio**: responsable de custodiar las tarjetas criptográficas donde se almacena la clave precompartida bajo el modelo de seguridad n de m. Esta función es compatible con el resto de las funciones de esta PC.
- **Oficial de verificación de identidad**: responsable de asegurar los procesos de verificación de la identidad de los suscriptores de alguno de los servicios de confianza de la ECD, como puede ser el de entrega cualificada.
- **Operador de Sistema**s: responsable necesario juntamente con el Administrador de Sistemas del funcionamiento correcto del hardware y software soporte de la plataforma de certificación. El operador es responsable de los procedimientos de copia de respaldo y mantenimiento de las operaciones diarias de los sistemas
- **Propietario de producto:** encargado de coordinar, controlar y gestionar los equipos y entregables de los desarrollos de confianza de la ECD. Debe encargarse de las tareas de triaje de errores y funcionalidades, y será el responsable de desplegarlos en los diferentes entornos.
- **Responsable de Seguridad**: encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de la ECD. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Adicionalmente, la ECD implementa criterios en sus políticas para la segregación de las funciones, como medida de prevención de actividades fraudulentas.

Identificación y autenticación para cada función

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante usuario/contraseña, certificado digital, tarjeta de acceso físico y/o llaves.

Roles que requieren separación de tareas

Las funciones fiables se establecen bajo el principio del mínimo privilegio, garantizado una segregación de funciones, de modo que la persona que ostente un rol no tenga un control total o especialmente amplio de todas las funciones de certificación, asegurando el debido control y vigilancia, limitando así cualquier tipo de comportamiento fraudulento a nivel interno.

La concesión del mínimo privilegio para las funciones de confianza, se hará teniendo en cuenta el mejor desarrollo de la actividad y será lo más limitado posible, considerando la estructura organizativa de la ECD en cada momento.

3.7.10. Manejo de medios y seguridad

La ECD garantiza que todos los medios son operados de manera segura de conformidad con lo establecido en la política de seguridad, y la clasificación de la información los mismos, implantando procedimientos que cubran todo el ciclo de vida de dichos medios en La ECD, teniendo especial cuidado en la reutilización y destrucción de estos cuando ya no sean necesarios.

3.7.11. Planificación del sistema

El departamento de atención al cliente de la ECD mantiene un registro de las capacidades de los equipos. Juntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

3.7.12. Reportes de incidentes, informes de seguimiento y solución

La ECD dispone de un adecuado procedimiento de gestión y respuesta de incidencias, así como una política de incidencias, en la que se establece como proceder ante posibles incidencias mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

En el documento de seguridad de la ECD se desarrolla en detalle el proceso de gestión de incidencias.

La ECD tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

3.7.13. Seguridad en redes

La ECD protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se transfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos TLS o del sistema VPN con autenticación por doble factor.

3.7.14. Monitoreo

La ECD tiene montados varios sistemas de monitorización interna y externa que alertan en caso de pérdida de disponibilidad del servicio. Las alertas de monitorización están integradas con los sistemas de gestión de tickets de UANATACA COLOMBIA generando los tickets necesarios en el caso de producirse una disrupción en el servicio siendo enviadas al servicio de atención al cliente 24h x 7d, que en base a la alerta producida ejecutarán el procedimiento correspondiente, o en su defecto escalarán al segundo nivel de soporte para su resolución dentro de los tiempos comprometidos de SLA con los suscriptores.

Adicionalmente, los servicios de monitorización interna tienen configurados diferentes chequeos que van desde la monitorización de la capacidad del servicio de certificación, la revisión del control de acceso, la integridad de ficheros y procesos, y varios miles de chequeos adicionales que como en el caso anterior y en base a su criticidad provocan diversos tipos de alertas.

3.7.15. Intercambio de datos y software

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de la ECD.
Los análisis de vulnerabilidad deben ser ejecutados, repasados y revisados por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados periódicamente de acuerdo con el procedimiento interno que está previsto para este fin.
Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

3.7.16. Gestión de accesos a los sistemas

La ECD realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.
En particular:

- Se dispone de controles basados en firewalls en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- La ECD dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- La ECD dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.
- El personal de la ECD es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

3.7.17. Archivo

Período de conservación de registros

La ECD archiva los registros especificados anteriormente durante al menos 10 años, o el período que establezca la legislación vigente.
El archivo de información estará disponible para su consulta por un auditor cualificado en función del cumplimiento de la legislación vigente.

Protección del archivo

La ECD protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo está protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.
La ECD asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones seguras externas.

Procedimientos de copia de respaldo

Se dispone de un centro de almacenamiento externo del CPD principal para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido sólo para personal autorizado.
La ECD como mínimo realiza copias de respaldo diarias de todos sus documentos electrónicos para casos de recuperación de datos.

Requisitos de sellado de fecha y hora

Los registros están fechados con una fuente fiable vía NTP. No es necesario que esta información se encuentre firmada digitalmente.

Localización del sistema de archivo

La ECD dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

Procedimientos de obtención y verificación de información de archivo

La ECD dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible. La ECD proporciona la información y medios de verificación al auditor.

3.7.18. Desarrollo y mantenimiento

Las aplicaciones son desarrolladas o implementadas por la ECD de acuerdo con estándares de desarrollo y control de cambios.
Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

3.7.19. Control de cambios

La ECD ha aprobado un control de cambios que contiene los procedimientos necesarios para realizar cualquier cambio o modificación del servicio de certificación, gestionando los mismos en base a la criticidad del cambio a implementar.

3.8. Compromiso de los servicios de certificación

Procedimientos de gestión de incidencias y compromisos
La ECD ha desarrollado políticas de seguridad y continuidad del negocio que le permiten la gestión y recuperación de los sistemas en caso de incidentes y compromiso de sus operaciones.

Corrupción de recursos, aplicaciones o datos
Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión oportunos de acuerdo con las políticas de seguridad y gestión de incidentes de la ECD, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de la ECD.

Compromiso de las claves privadas de la entidad
En caso de sospecha o conocimiento del compromiso de la ECD, se activarán los procedimientos de compromiso de claves de acuerdo con las políticas de seguridad, gestión de incidencias y continuidad del negocio, que permita la recuperación de los sistemas críticos, si fuera necesario en un centro de datos alternativo.

Continuidad del negocio después de un desastre

La ECD restablecerá los servicios críticos de acuerdo con el plan de incidencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.

3.9. Término de la organización que administra el servicio de certificación

La ECD asegura que las posibles interrupciones a los suscriptores de los servicios y a terceras partes sean mínimas como consecuencia del cese de los servicios de la ECD. En este sentido, la ECD garantiza un mantenimiento continuo de los registros definidos y por el tiempo establecido de acuerdo con la presente PC.

No obstante, lo anterior, si procede, la ECD ejecutará todas las acciones que sean necesarias para transferir a un tercero o un depósito notarial, las obligaciones de mantenimiento de los registros especificados durante el periodo correspondiente según esta PC o la previsión legal que corresponda.

Antes de terminar sus servicios, la ECD desarrollará un plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios, incluyendo un seguro de responsabilidad civil, para continuar la finalización de las actividades de revocación.
- Informará a todos los suscriptores del servicio, terceros que confían y en general cualquier otro con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 2 meses.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Destruirá o deshabilitará para su uso las claves privadas encargadas del servicio de certificación.
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos.
- Comunicará a la Autoridad Administrativa Competente, con una antelación mínima de 2 meses, el cese de su actividad.

- Asimismo, le comunicará la apertura de cualquier proceso concursal que se siga contra la ECD, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

3.10. Registros de información concerniente a la operación

La ECD produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad del servicio:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados a los sistemas que dan soporte al servicio de certificación.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones.
- Encendido y apagado de las aplicaciones del servicio de certificación.
- Cambios en los detalles del servicio de certificación y/o sus claves.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste.
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o de la persona física identificada en el certificado, en caso de certificados de organización.

- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al servicio.
- Eventos relativos a la sincronización y recalibración del reloj.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

Frecuencia de tratamiento de registros de auditoría

La ECD revisa sus logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

La ECD mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs.
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporarse en una BBDD para su posterior exploración.

Protección de los registros de auditoría

Los ficheros de registro de auditoría se protegen mediante controles físicos y lógicos de acceso, lecturas, modificaciones, borrados no autorizados.

El acceso a los ficheros de logs está reservado sólo a las personas autorizadas. Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

Procedimientos de copia de respaldo

La ECD dispone de un procedimiento adecuado de copia de seguridad de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

Localización del sistema de acumulación de registros de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y por el software de los servicios de confianza, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registra un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

3.11. Auditoría

3.11.1. Frecuencia de la auditoría de conformidad

La ECD llevará a cabo auditorías de conformidad según lo que indique la ONAC y por lo menos de manera anual, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

3.11.2. Auditoría de registros y archivos

La auditoría verifica respecto a la ECD:

- Que la entidad tiene un sistema de gestión que garantice la calidad del servicio prestado.
- Que la entidad cumple con los requerimientos de la PC del servicio de certificación.

- Que la PC del servicio de certificación y demás documentación jurídica vinculada, se ajusta a lo acordado por la ECD y con lo establecido en la normativa vigente.
- Que la entidad gestione de forma adecuada sus sistemas de información.
- La validez de los registros generados.
- La existencia y validez del archivo.

3.11.3. Auditor

Las auditorías se realizarán por auditores externos autorizados por la ONAC, y serán siempre independientes al Servicio de certificación, y con las limitaciones que la ONAC considere oportunas.

3.12. Otros aspectos legales de la operación del servicio de certificación

3.12.1. Tarifas y políticas de reembolso

UANATACA COLOMBIA ha establecido una política de tarifas para el servicio de firma, mensajería y entrega certificada. No obstante lo anterior, se podrán establecer tarifas particulares en función del proyecto.

Esta se encuentra a disposición de todo el público en la siguiente dirección: https://uanataca.co/documentosGES/GES-PO-05_Politica_Tarifaria.pdf

UANATACA COLOMBIA no ha establecido una política de reintegro específica, aplicando la normativa actual que corresponda.

3.12.2. Cobertura de seguro de responsabilidad civil

La ECD dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, que mantiene de acuerdo con la normativa vigente aplicable.

3.12.3. Información confidencial y/o privada

La ECD mantendrá de manera confidencial la siguiente información:

- Material comercialmente reservado como Servicio de certificación, de los suscriptores de la empresa y de los terceros que confían, incluyendo términos contractuales, planes de negocio y propiedad intelectual;
- Información que pueda permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores de empresa y los terceros que confían;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.
- Cualquier otra información que pudiera perjudicar la normal realización de sus operaciones.

La ECD considerará como información privada, la siguiente:

- De conformidad con lo establecido por la Norma Marco sobre privacidad del APEC, se considera información personal, cualquier información relativa a un individuo identificado o identificable.
- Información que pueda permitir a personas no autorizadas la construcción de un perfil de las actividades de los usuarios de los servicios de certificación.
- En todos los casos, deberá ser suscrita por el mismo, su consentimiento para el tratamiento y almacenamiento de estos datos.

3.12.4. Información no privada

Los certificados utilizados en el servicio del servicio de certificación estarán publicados en su página web.

3.12.5. Derechos de Propiedad intelectual

La ECD establece en el contrato con el suscriptor las cláusulas contractuales de obligaciones y derechos relacionados a la propiedad intelectual.

3.12.6. Notificaciones y comunicaciones entre participantes

La ECD establece en el contrato con el suscriptor las cláusulas por el cual las partes se podrán notificar hechos mutuamente.

3.12.7. Conformidad con la Ley aplicable

La ECD establece en el contrato con el suscriptor las cláusulas de conformidad con la ley aplicable, indicando que la ley aplicable a la prestación del servicio de certificación, incluyendo esta Servicios de certificación, es la Ley de la República de Colombia.

3.12.8. Exención de garantías

La ECD, en la documentación que la vincula con suscriptores y terceros que confían, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

La ECD garantiza al suscriptor que el servicio de certificación cumple con todos los requisitos materiales establecidos en esta Servicios de certificación, así como las normas de referencia.

La ECD garantiza al tercero que confía en su servicio de certificación que la información contenida o incorporada por referencia en el sello es correcta, excepto cuando se indique lo contrario.

La ECD rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en este documento.

3.12.9. Indemnizaciones

La ECD establece en el contrato con el suscriptor las cláusulas aplicables en caso de indemnización.

3.12.10. Fuerza mayor

La ECD establece en el contrato con el suscriptor las cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

3.12.11. Disposiciones aplicables

Cualquier aspecto no regulado expresamente en el presente documento se regirá por lo dispuesto en la Política de Certificación de UANATACA COLOMBIA disponible en este enlace: https://www.uanataca.com/co/.

Anexo I: acrónimos

A continuación de muestra una lista de los acrónimos utilizados en el presente documento:

- CC: *Common Criteria.*
- CPD: Centro de Proceso de Datos.
- CRL: *Certificate Revocation List.*
- CSO: *Chief Security Officer.*
- EAL: *Evaluation Assurance Leve*ls.
- ESI: *Electronic Signatures and Infrastructures*.
- ETSI: *European Telecommunications Standards Institute*.
- FIPS: *Federal Information Processing Standard*.
- HSM: *Hardware Secure Module*.
- HTTP: *Hypertext Transfer Protocol*.
- NTP: *Network Time Protocol*.
- OCSP: Online Certificate Status Protocol.
- ONAC: ONAC. Oficina Nacional de Asesoramiento Científico.
- OTP: *One-Time Password*.
- RFC: *Request For Comments*.
- RSA: *Rivest–Shamir–Adleman* (criptosistema de clave pública).
- SGSI: Sistema de Gestión de la Seguridad de la Información.
- SLA: *Service Level Agreement* (Acuerdo de nivel de servicio).
- TLS: *Transport Layer Security*.
- UE: Unión Europea.
- URL: *Uniform Resource Locator*.
- UTC: *Coordinated Universal Time*
- VPN: *Virtual Private Network*.