ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACON Y SERVICIOS_ IZENPE S.A.

PLIEGO DE PRESCRIPCIONES TÉCNICAS RELATIVO A LA CONTRATACION DEL SERVICIO DE AUDITORÍAS INTERNAS.

Expdte: IZNP_S_001_2023

Beato Tomás de Zumárraga
71 - 1ª Planta
01008
Vitoria - Gasteiz

www.izenpe.com
info@izenpe.com
Tel.: 945 017 490

Tabla de contenido

1 OBJETO 3
1.1 Auditoría cumplimiento ISO/IEC 27001:2014/2022 y ENS 3
1.2 Auditoría de servicio de emisión de certificados de autenticación Web 4
1.3 Auditoría de servicio de emisión de certificados de persona física y persona jurídica 4
1.4 Auditoría de servicio de sellado de tiempo 5
1.5 Auditoría de servicio de validación de firmas 5
1.6 Auditoría del servicio de video identificación 5
1.7 Auditoría técnica albergue 6
1.8 Auditoría 27701 6
1.9 Bolsa de horas 6
1.10 Resumen de entregables 7
COLABORACIÓN DE IZENPE 7

1 OBJETO

El objeto del presente contrato es la prestación del conjunto de los servicios denominados Servicios de auditoría internas cuya finalidad es garantizar que el sistema de gestión de la seguridad de Izenpe cumple con los requisitos que establece la norma o legislación vigente, y si se estima oportuno determinar las medidas adecuadas para mitigar o reducir los riesgos detectados y mejorar la eficacia y eficiencia del sistema.

Las metodologías, deberán ser acotadas por los auditores de acuerdo a los escenarios que se encuentren en cada momento con el fin de realizar las pruebas más oportunas optimizando los recursos disponibles, siempre con el visto bueno por parte de Izenpe.

1.1 Auditoría cumplimiento ISO/IEC 27001:2014/2022 y ENS

El objetivo es revisar el cumplimiento de las siguientes normas:

- ✓ ISO/IEC 27001:2014/2022
- ✓ ISO/IEC 27005: 2018/2022
- ✓ Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema nacional de Seguridad

El alcance del SGSI de Izenpe cubre los procesos de:

- ✓ Emisión de certificados
- ✓ Revocación de certificados
- ✓ Validación online de certificados (OCSP)
- ✓ Validación offline de certificados (CRL)
- ✓ Validación de firmas electrónicas (ZAIN)
- ✓ Custodia de certificados
- ✓ Generación y validación remota de sellos electrónicos (ZAIN)
- ✓ Emisión y autenticación de BAK/BAKQ
- ✓ Emisión y autenticación de Giltza profesional
- ✓ Broker de identidades (GILTZA)
- ✓ Sellado de tiempo (TSA)
- ✓ Plataforma de video identificación
- ✓ Plataforma NISAE (ENS)

Algunos de los procesos que involucran estas actividades se desarrollan por parte de personal externo y en instalaciones ajenas a Izenpe.

Los entregables incluirán:

- ✓ Plan de adecuación a la ISO/IEC 27001:2014/2022 y a la ISO/IEC 27005:2018/2022

  Informe en el cual se reflejará el estado de cumplimiento de cada uno de los aspectos de ambas normas y un plan de actuación para abordar los incumplimientos que se detecten.

  El alcance de los servicios abarca las personas, procesos y tecnologías de la organización afectados por la mencionada normativa.

- ✓ Plan de adecuación al Esquema Nacional de Seguridad

  Informe en el cual se reflejará el estado de cumplimiento de cada uno de los aspectos de la norma y un plan de actuación para abordar los incumplimientos que se detecten.

  El alcance de los servicios abarca las personas, procesos y tecnologías de la organización afectados por la mencionada normativa.

1.2 Auditoría de servicio de emisión de certificados de autenticación Web

El objetivo es revisar el cumplimiento de las siguientes normas:

- ✓ ETSI EN 319 401 General Policy Requirements for Trust Service Providers
- ✓ ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates (General requirements)
- ✓ ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing qualified certificates
- ✓ CABForum Baseline Requirements
- ✓ CABForum EV Certificate Guidelines
- ✓ CABForum Network Security Requirements
- ✓ Mozilla Root Store Policy
- ✓ Microsoft Root Store Policy
- ✓ Apple Root store play
- ✓ Google Root store play

Sobre las siguientes políticas: DVCP, OVCP QEVCP-w, QNCP-w, los entregables incluirán:

- ✓ Plan de adecuación. Informe en el cual se reflejará el estado de cumplimiento de cada uno de los aspectos de las normas indicadas anteriormente (ETSI, CABForum, Mozilla y Microsoft) y un plan de actuación para abordar los incumplimientos y observaciones que se detecten.

1.3 Auditoría de servicio de emisión de certificados de persona física y persona jurídica

El objetivo es revisar el cumplimiento de las siguientes normas:

- ✓ ETSI EN 319 401 General Policy Requirements for Trust Service Providers
- ✓ ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates (General requirements)
- ✓ ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates (Requirements for trust service providers issuing EU qualified certificates)
- ✓ ETSI EN 419 241-2 Trustworthy Systems Supportying Server Signing-Part 2: Protection profile for QSCD for Server Signing
- ✓ ETSI TS 119 431-1 Electronic Signatures and infrastructures (ESI): Policy and security requirements for trust service providers; Part 1: TSP service components operating remote QSCD/SCDEV

Sobre las siguientes políticas: QCP-l, QCP-n,

Los entregables incluirán:

- ✓ Plan de adecuación. Informe en el cual se reflejará el estado de cumplimiento de cada uno de los aspectos de las normas indicadas anteriormente (ETSI,) y un plan de actuación para abordar los incumplimientos y observaciones que se detecten.

1.4 Auditoría de servicio de sellado de tiempo

El objetivo es revisar el cumplimiento de la siguiente norma:

- ✓ ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

Los entregables incluirán:

1.5 Plan de adecuación. Informe en el cual se reflejará el estado de cumplimiento de cada uno de los aspectos de la norma ETSI EN 319 421 y un plan de actuación para abordar los incumplimientos y observaciones que se detecten. Auditoría de servicio de validación de firmas

El objetivo es revisar el cumplimiento de la siguiente norma:

- ✓ ETSI TS 119 441 Electronic Signatures and infrastructures (ESI); Policy requirements for TSP providing validation services

Los entregables incluirán:

- ✓ Plan de adecuación. Informe en el cual se reflejará el estado de cumplimiento de cada uno de los aspectos de la norma ETSI TS 119 441 y un plan de actuación para abordar los incumplimientos y observaciones que se detecten.

1.6 Auditoría del servicio de video identificación

El objetivo es revisar el cumplimiento de la siguiente norma:

- ✓ Orden ETD/465/2021, de 6 de mayo por la que se regulan los métodos de identificación remota por video para la expedición de certificados cualificados
- ✓ Orden ETD/743/2022, de 26 de julio, por la que se modifica la Orden ETD/465/2021 de 6 de mayo, por la que se regulan los métodos de identificación remota por video para la expedición de certificados cualificados

Los entregables incluirán:

- ✓ Plan de adecuación. Informe en el cual se reflejará el estado de cumplimiento de cada uno de los aspectos de la norma referenciada y un plan de actuación para abordar los incumplimientos y observaciones que se detecten.

1.7 Auditoría técnica albergue

El objetivo es revisar desde el punto de vista más técnico los sistemas que dan soporte a los servicios de Izenpe. Para ello se realizarán visitas presenciales al proveedor de estos servicios, y se realizarán entrevistas con cada uno de los soportes implicados. Todas las entrevistas se realizarán de forma coordinada con Izenpe y con el proveedor.

Los entregables incluirán:

- ✓ Plan de adecuación. Informe en el cual se reflejará el estado de cumplimiento de cada uno de los aspectos de la Política de Seguridad de Izenpe y un plan de actuación para abordar los incumplimientos y observaciones que se detecten.

1.8 Auditoría 27701

Izenpe en el desarrollo de sus actividades para prestar servicios a los ciudadanos, administraciones públicas y empresas maneja información de carácter personal, por lo cual debe implantar el Reglamento Europeo de Protección de Datos, aprobado en mayo de 2016, y de aplicación a partir de mayo de 2018. Con el objeto de dar cumplimiento a los mencionados aspectos, se requiere la prestación de los servicios de soporte para el proceso de adecuación al RGPD. En concreto se realizarán las siguientes actividades:

- ✓ Análisis de la situación, generando un informe de diagnóstico del cumplimiento y un plan de adecuación.
- ✓ Desarrollo documental de los procedimientos jurídicos que se identifiquen en el plan.
- ✓ Soporte consultivo para que Izenpe pueda llevar a cabo las acciones resultantes del plan.

El alcance de los servicios abarca las personas, procesos y tecnologías de la organización afectados por la mencionada normativa.

Los entregables incluirán:

- ✓ Informe de diagnóstico y plan de acción para la adecuación al RGPD (UE) 679/2016.
- ✓ Documento de procedimientos del marco jurídico del RGPD.

1.9 Bolsa de horas

Se solicita al licitador una oferta en concepto de bolsa de horas para el soporte a la aplicación de las medidas correctoras identificadas en las auditorías incluidas en el presente contrato, y en previsión de que pudieran existir tareas no planificadas u oportunidades de mejora adicionales que se identifiquen durante el contrato, así como soporte al establecimiento de medidas que faciliten la definición de un sistema gestión de calidad continuo. Esta bolsa de horas tendrá un máximo de **80 horas** y se ejecutará bajo demanda de Izenpe, pudiendo quedar sin efecto alguno en caso de que no exista necesidad de ejecución.

Izenpe realizará las peticiones correspondientes a este servicio con suficiente detalle y antelación para que el proveedor planifique las intervenciones necesarias. Estas peticiones incluirán los entregables que se requieren y los requisitos asociados. En contestación a la petición, el proveedor facilitará una estimación del esfuerzo que conllevan los trabajos correspondientes. La aceptación de dicha estimación por parte de Izenpe autorizará el inicio los trabajos planificados

Finalizadas las actividades, se suministrarán los entregables pactados y, en caso de que satisfagan los requisitos asociados a ellos, el proveedor facturará las horas/jornadas correspondientes.

1.10 Resumen de entregables

ESTÁNDARES	ENTREGABLE
✓ ISO/IEC 27001:2014/2022 ✓ ENS	1x
✓ ETSI EN 319 401 ✓ ETSI EN 319 411-1 política DVCP, OVCP ✓ ETSI EN 319 411-2 política QEVCP-w, QNCP-w	1x
✓ ETSI EN 319 411-2 políticas QCP-n, y QCP-l	1x
✓ ETSI EN 319 421	1x
✓ ETSI TS 119 441	1x
✓ Auditoría Video identificación	1x
✓ Auditoría técnica albergue	1x
✓ ISO/IEC 27701	1x

COLABORACIÓN DE IZENPE

- ✓ Izenpe nombrará un contacto durante toda la duración de los servicios.
- ✓ Izenpe se compromete a proporcionar toda la documentación solicitada por los auditores.
- ✓ Izenpe garantiza el acceso a todas las localizaciones dentro del alcance de la auditoría.

Dª. Raquel Garay Ruiz de Azua RAQUEL GARAY RUIZ DE AZUA - 16060119R Firmado digitalmente por RAQUEL GARAY RUIZ DE AZUA - 16060119R Fecha: 2023.01.12 15:27:05 +01'00' Técnico Responsable del Contrato	Dª. Izaskun Urrestarazu Amundarain 15990846G MARIA IZASKUN URRESTARAZU (R: A01337260) Firmado digitalmente por 15990846G MARIA IZASKUN URRESTARAZU (R: A01337260) Fecha: 2023.01.12 14:36:28 +01'00' Órgano de Contratación