JIG digital

proyectos
con alma

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código:	PO_A5_11_Politica de seguridad de la información
Versión:	2.0
Fecha de la versión:	21-04-2024
Creado por:	Javier Gurría
Aprobado por:	Dirección
Nivel de confidencialidad:	Público

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
23-11-2017	0.1	José María Pulgar	Descripción básica del documento
18-12-2017	0.2	Javier Gurría	Confirmación documento
22-02-2018	1.0	Javier Gurría	Corrección erratas tras difusión a empleados
04-07-2018	1.1	Javier Gurría	Corrección Grupo JIG
28-02-2020	1.2	Javier Gurría	Renovación de la validez del documento
12-12-2021	1.3	Gonzalo Ezquerro	Definición de nuevos objetivos
10-05-2023	1.4	Hugo Domínguez	Definición de nuevos objetivos Incluir nuevos roles
24-11-2023	1.5	Hugo Domínguez	Añadir nuevos roles Añadir contacto con las autoridades y grupos de interés Añadir nuevo objetivo: Medidas seguridad WordPress
21-04-2024	2.0	Javier Gurría	Revisión del documento para adaptarlo a los requisitos del ENS

Tabla de contenido

1. Misión y objetivos de la política de seguridad de la información

JIG Easy Services S.L., y JIG Internet Consulting S.L. (en adelante en el documento, **Grupo JIG o JIG**) han establecido un alineamiento con la gestión de la seguridad de la información, según lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en el estándar de mercados ISO/IEC 27001:2023, reconociendo como activos estratégicos la información y los sistemas que la soportan.

Uno de los objetivos fundamentales de la implantación de esta Política de Seguridad de la Información es establecer las bases sobre las que tanto empleados internos, como otras partes interesadas, puedan acceder a los servicios ofrecidos por JIG, en un entorno seguro y de confianza.

La Política de Seguridad de la Información define el marco global para la gestión de la seguridad de la información, protegiendo todos los activos de información y garantizando la continuidad en el funcionamiento de los sistemas.

Se pretende de esta forma minimizar los riesgos derivados de un posible fallo en la gestión de la seguridad de la información, y asegurar el cumplimiento de los objetivos de JIG ante un hipotético incidente de seguridad de la información.

Para ello, se establecen los siguientes objetivos generales en materia de seguridad de la información:

a) Contribuir desde la gestión de la seguridad, al cumplimiento de la misión y objetivos establecidos por JIG.
b) Tener medidas de control necesarias para garantizar el cumplimiento de los requisitos legales aplicados por la actividad desarrollada, especialmente en lo relativo a la protección de datos personales.
c) Asegurar la accesibilidad, confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los activos de información.
d) Asegurar la prestación continuada de los servicios, tanto de forma preventiva, como de forma reactiva ante los incidentes de seguridad.
e) Proteger los activos de información de JIG, y la tecnología que los soporta frente a cualquier amenaza, intencionada o accidental, interna o externa.

Esta Política de Seguridad de la Información asegura un compromiso continuo y manifiesto de JIG, para la difusión y consolidación de la cultura de la seguridad.

2. Alcance

Esta Política de Seguridad de la Información se aplicará a todos los activos de información de JIG. A estos efectos, se entiende por JIG:

a) La sede central de la organización, ubicada en C. Piqueras, 24, Logroño, 26006, La Rioja.

Esta Política no se limita a los datos de carácter personal, y es independiente de que el tratamiento sea manual o automatizado.

3. Marco normativo

Sin carácter exhaustivo, la legislación y normativa en materia de seguridad de la información que debe servir de referencia es la siguiente:

a) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

b) Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia
c) Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
d) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
e) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
f) Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
g) Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
h) Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
i) Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
j) Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
k) Norma UNE-EN ISO/IEC 27001.
l) Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD).
m) Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos de carácter personal y sus normas de desarrollo.
n) Ley 10/2021, de 9 de julio, de trabajo a distancia.

4. Revisión de la política

En relación con las revisiones que puedan realizarse sobre la redacción del texto que constituye la Política de Seguridad de la Información, se distinguirán dos tipos de actividades:

a) Revisiones periódicas sistemáticas: Deberán realizarse cuando se detecten incidencias o cambios en el marco legal que puedan cuestionar la validez de la Política. La revisión de la Política de Seguridad de la Información deberá garantizar que ésta se encuentra alineada con la estrategia, la misión y visión de JIG en materia de seguridad de la información y que asegura el cumplimiento de los objetivos de control establecidos. Las revisiones periódicas se realizan al menos con una periodicidad anual.
b) Revisiones no planificadas: Estas revisiones deberán realizarse en respuesta a cualquier evento o incidente de seguridad que pudiera suponer un incremento significativo del nivel de riesgo actual o haya causado un impacto en la seguridad de la información de JIG.

5. Organización de la seguridad

Aunque la gestión de la seguridad de la información corresponde a todo el personal de JIG, se designa a determinados órganos y cargos, con las funciones que se señalan para cada uno en este apartado: Comité de Gestión de la Seguridad de la Información de JIG, Responsables de la Información, Responsables del Servicio, Responsables de Seguridad y Responsables del Sistema de Información.

a) Comité de Gestión de la Seguridad de la Información de JIG.

   i. El Comité de Gestión de la Seguridad de la Información es el organismo que centraliza la gestión de la seguridad de la información en JIG.

b) El Responsable de la Información será la persona con competencia suficiente para decidir sobre la finalidad, contenido y uso de dicha información y determinará, dentro del marco establecido en el Anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, los requisitos de seguridad de la información tratada. A tal efecto:
   i. Determinará los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 41 del Real Decreto citado.
   ii. Realizará, junto a los Responsables del Servicio y del Responsable de Seguridad, los preceptivos análisis de riesgos, y seleccionarán las salvaguardas que se han de implantar.
   iii. Aceptará los riesgos residuales respecto de la información calculados en el análisis de riesgos.
   iv. Realizará el seguimiento y control de los riesgos, con la participación del Responsable de Seguridad.

c) El Responsable del Servicio será la persona con competencia suficiente para decidir sobre la finalidad y prestación de dicho servicio y determinará dentro del marco establecido en el Anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en el ámbito de la Administración Electrónica los requisitos de seguridad de los servicios prestados. A tal efecto:
   i. Realizará, junto a los Responsables de la Información y de Seguridad, los preceptivos análisis de riesgos, y seleccionarán las salvaguardas que se han de implantar.
   ii. Aceptará los riesgos residuales respecto de la información calculados en el análisis de riesgos.
   iii. Realizará el seguimiento y control de los riesgos, con la participación del Responsable de Seguridad.
   iv. Suspenderá, de acuerdo con el Responsable de la Información y el Responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

d) El Responsable de Seguridad será la persona determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Tendrá las siguientes funciones:
   i. Las incluidas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en el ámbito de la Administración Electrónica.
   ii. Proponer al Responsable del Servicio la determinación de los niveles de seguridad en cada dimensión de seguridad siempre que se le solicite.
   iii. Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
   iv. Realizar el seguimiento y control del estado de seguridad de los sistemas de información.
   v. Proponer al Comité de Gestión de la Seguridad de la Información las normas de seguridad y los procedimientos de seguridad.

e) El Responsable del Sistema de Información tendrá las siguientes funciones:
   i. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
   ii. Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
   iii. Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
   iv. El Responsable del Sistema puede proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la dirección de la entidad, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad.

Los roles citados, son designados inicialmente por la junta directiva de JIG, y su renovación deberá contar con la aprobación del Comité de Gestión de la Seguridad de la Información.

6. Resolución de conflictos

En caso de conflicto entre los responsables de la estructura organizativa de la Política de Seguridad de la Información, este lo resolverá la Junta Directiva de JIG, y prevalecerán las mayores exigencias derivadas de la protección de datos personales.

7. Clasificación de la información

JIG clasificará e inventariará los activos de la información en virtud de su naturaleza.

El nivel de protección y las medidas a aplicar se basarán en el resultado de dicha clasificación.

8. Datos de carácter personal

Cuando un sistema de información de JIG maneje datos de carácter personal, le será de aplicación lo dispuesto en la Ley Orgánica 3/2018, del 5 de diciembre, de Protección de Datos de Carácter Personal y sus normas de desarrollo, sin perjuicio de los requisitos establecidos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y la norma UNE-EN ISO/IEC 27001.

Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal.

9. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos.

Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

a) al menos una vez al año (mediante revisión y aprobación formal).
b) cuando cambie la información manejada.
c) cuando cambien los servicios prestados.
d) cuando ocurra un incidente crítico de seguridad.

Las contramedidas medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos identificados.

10. Instrumentos de desarrollo

Se establece un marco normativo en materia de seguridad de la información estructurado por diferentes niveles de forma que los objetivos marcados por el presente documento tengan un desarrollo específico.

La política de seguridad estructurará su marco normativo en los siguientes niveles:

a) La presente Política de Seguridad de la Información, que establece los requisitos y criterios de protección de carácter global.
b) Las normas de seguridad, que definen qué hay que proteger y los requisitos de seguridad deseados.
    i. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los entornos de los sistemas de información de JIG.
    ii. Establecen un conjunto de expectativas y requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política.

iii. Las propone el Responsable de Seguridad y las aprueba el Comité de Gestión de la Seguridad de la Información, a través de la figura del Responsable del Sistema de Gestión de la Seguridad de la Información implementado en JIG.

c) Los procedimientos de seguridad en los que se describirá de forma concreta cómo proteger lo definido en las normas y las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento.
   i. Son documentos que especifican cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.
   ii. Su aprobación dependerá de su ámbito de aplicación, que podrá ser en un ámbito específico o en un sistema de información determinado.

Además, se podrán establecer guías con recomendaciones y buenas prácticas.

En la medida de lo posible, toda esta documentación será gestionada según establece el procedimiento vigente de Control de documentos en JIG, que tendrá como objetivo establecer los criterios para el control de la documentación utilizada en el Sistema de Gestión de la Seguridad de la Información, y que se extiende a toda la documentación que da soporte al cumplimiento del Esquema Nacional de Seguridad y de la norma UNE-EN ISO/IEC 27001.

11.Obligaciones del personal

Todo el personal con responsabilidad en el uso, operación, o administración de sistemas de tecnologías de la información y las comunicaciones tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad derivada, independientemente del tipo de relación jurídica que les vincule con JIG.

Las actuaciones del personal serán supervisadas para verificar que se siguen los procedimientos establecidos.

Todas las personas recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

La Política de Seguridad estará accesible para todo el personal que preste sus servicios en los órganos y entidades a que se refiere el punto relativo al 'Alcance'.

Con el objetivo de fomentar la 'Cultura de la seguridad', el Comité de Gestión de la Seguridad de la Información promoverá un programa de concienciación continúa para formar a todo el personal.

Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

El incumplimiento de la Política de Seguridad y su normativa de desarrollo dará lugar al establecimiento de medidas preventivas y correctivas encaminadas a salvaguardar y proteger los sistemas de información, sin perjuicio de la correspondiente exigencia de responsabilidad disciplinaria.

12.Profesionalidad

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidentes y desmantelamiento.

El personal designado de JIG recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios.

13.Autorización y control de accesos

El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

14.Protección de las instalaciones

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Como mínimo, las salas deben estar cerradas y disponer de un control de llaves.

15.Adquisición de productos de seguridad

n la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por JIG, se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.

La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, y regulado por la orden PRE/2740/2007, de 19 de septiembre, dentro de sus competencias, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados. El proceso indicado, se efectuará teniendo en cuenta los criterios y metodologías de evaluación, determinados por las normas internacionales que recoge la orden ministerial citada.

Para la contratación de servicios de seguridad, si fueran necesarios, se estará a lo dispuesto en los apartados anteriores y en el artículo “Relaciones con terceros” de la presente Política.

16.Seguridad por defecto

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

a) El sistema proporcionará la mínima funcionalidad requerida para que JIG alcance sus objetivos.
b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, las que sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

17.Integridad y actualización del sistema

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

18.Protección de la información almacenada y en tránsito

En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, smartphones, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por JIG.

Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de una información electrónica, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de estos.

19.Prevención ante otros sistemas de información interconectados

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el apartado 32 del Anexo II, de la Ley 9/2014 de 9 de mayo, General de Telecomunicaciones.

En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

20.Registro de actividad

Con la finalidad exclusiva de lograr el cumplimiento del objeto de la presente Política, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

21.Incidentes de seguridad

Se establecerá un sistema de detección y reacción frente a código dañino.

Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.

Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

22.Continuidad de la actividad

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

23.Mejora continua del proceso de seguridad

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

24.Relaciones con terceros

Cuando JIG preste servicios o ceda información a terceras partes, se les hará partícipe de esta Política de Seguridad de la Información y de las normas e instrucciones derivadas.

Asimismo, cuando JIG utilice servicios de terceros, o ceda información a terceros, se les hará igualmente partícipe de esta Política de Seguridad de la Información y de la normativa e instrucciones de seguridad que ataña a dichos servicios o información.

Si JIG necesitara servicios de seguridad de terceros, exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados, y con unos niveles idóneos de gestión y madurez en los servicios prestados

Los terceros quedarán sujetos a las obligaciones y medidas de seguridad establecidas en dicha normativa e instrucciones, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de detección y resolución de incidencias.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad de la información, al menos al mismo nivel que el establecido en esta Política de Seguridad de la Información.

En concreto, los terceros deberán garantizar el cumplimiento de la Política de Seguridad de la Información basadas en estándares auditables que permitan verificar el cumplimiento de estas políticas. Asimismo, se garantizará mediante auditoría o certificado de destrucción/borrado, que el tercero cancela y elimina los datos pertenecientes a JIG a la finalización del contrato.

Cuando algún aspecto de la Política de la Seguridad de la Información no pueda ser satisfecho por una tercera parte, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el Responsable de la Información y de los Servicios afectados, antes de seguir adelante.

25.Terminología básica sobre seguridad de la información

Confidencialidad: característica de la información por la cual solo está disponible para personas o sistemas autorizados.

Integridad: característica de la información por la cual solo es modificada por personas o sistemas autorizados y de una forma permitida.

Disponibilidad: característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.

Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de gestión de seguridad de la información: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

Director de Seguridad
Javier Gurría

Firmado por GURRIA DE LA TORRE JAVIER - ***5842** el día 22/04/2024 con un certificado emitido por AC FNMT Usuarios

_____

[21-04-2024]