POLÍTICA DE SEGURIDAD

Foot Analytics - Versión: 1.2

Fecha de aprobación: 21 de julio de 2025

Estado: Aprobado

Documentos de referencia

Documento	Comentarios
Artículo 12 Política de Seguridad	Real Decreto 311/2022 de 3 Mayo (BOE)
5.1 Políticas para la seguridad de la información	ISO 27002:2022 (Bloque 5. Organización)
5.2 Roles y Responsabilidades en Seguridad de la Información	ISO 27001:2022 (Bloque 5. Organización)
5.5 Responsabilidades de la Dirección	ISO 27001:2022 (Bloque 5. Organización)

Índice

1. ORGANIZACIÓN E IMPLEMENTACIÓN DEL PROCESO DE SEGURIDAD (ART.13) 4
2. ÁMBITO DE APLICACIÓN 4
3. VIGENCIA 4
4. REVISIÓN Y EVALUACIÓN 5
5. MARCO NORMATIVO 5
7. FUNCIONES DE SEGURIDAD COMITÉ DE SEGURIDAD 6
Procedimiento de Designación y Renovación 8
8. NIVEL DE ESCALADO 9
9. ANÁLISIS Y GESTIÓN DE LOS RIESGOS (ART. 14) 10
10. GESTIÓN DE PERSONAL (ART. 15) 11
11. PROFESIONALIDAD (ART. 16) 11
12. AUTORIZACIÓN Y CONTROL DE LOS ACCESOS (ART. 17) 12
13. PROTECCIÓN DE LAS INSTALACIONES (ART. 18) 12
14. ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD (ART. 19) 12
15. MÍNIMO PRIVILEGIO (ART. 20) 13
16. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA (ART. 21) 14
17. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO (ART. 22) 14
18. PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS (ART. 23) 14
19. REGISTRO DE LA ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO (ART. 24) 15
20. INCIDENTES DE SEGURIDAD (ART. 25) 15
21. CONTINUIDAD DE LA ACTIVIDAD (ART. 26) 16
22. MEJORA CONTINUA DEL PROCESO DE SEGURIDAD (ART. 27) 16
23. APROBACIÓN DEL DOCUMENTO 16

1. ORGANIZACIÓN E IMPLEMENTACIÓN DEL PROCESO DE SEGURIDAD (ART.13)

Esta "Política de Seguridad de la Información" es efectiva desde su entrada en vigor el 24 DE MARZO DE 2025 para Foot Analytics.

La Política es revisada por el responsable de Seguridad de la Información a intervalos planificados, sin exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización, comunicándose de forma efectiva.

Los cambios sobre la Política de Seguridad de la Información serán aprobados por la Dirección de Foot Analytics. Cualquier cambio sobre la misma deberá ser comunicado vía correo electrónico para conocimiento de toda la Organización.

La dirección de la empresa es consciente del valor de la información y está profundamente comprometida con la política descrita en este documento.

2. ÁMBITO DE APLICACIÓN

Además, es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en Foot Analytics, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de este.

Por tanto, se entiende por usuario cualquier empleado perteneciente o ajeno a Foot Analytics, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con Foot Analytics y que utilice o posea acceso a los Sistemas de Información de Foot Analytics.

3. VIGENCIA

En la presente Política de Seguridad de Foot Analytics se han establecido las directrices generales para el uso adecuado de los recursos de tratamiento de información que Foot Analytics pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de Foot Analytics.

4. REVISIÓN Y EVALUACIÓN

La gestión de esta Política de Seguridad corresponde al Comité de Seguridad[1].

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad revisará la presente Normativa General, que se someterá, de haber modificaciones, a la aprobación del Órgano de Gobierno.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios normativos, infraestructura tecnológica, etc.

Será el responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5. MARCO NORMATIVO

El marco normativo en materia de seguridad de la información en el que Foot Analytics desarrolla su actividad, se encuentra en el documento vivo: Marco Normativo Cumplimiento Legal.xlsx

MISIÓN y OBJETIVOS

En Foot Analytics S.L. (en adelante Foot Analytics) ayudamos a que las oficinas un mejor lugar para trabajar, optimizando el uso del espacio con datos. A través de la tecnología y análisis inteligente, proporcionamos información clave sobre la ocupación y el uso del espacio. Esto permite a las organizaciones tomar decisiones informadas para mejorar la eficiencia, reducir costes, impulsar la sostenibilidad y ofrecer una mejor experiencia a las personas que trabajan en estos espacios.

Foot Analytics, ha 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

[1] Según la disposición adicional tercera del RD 311/2022 por el que se regula el Esquena Nacional de Seguridad, *"el Comité de Seguridad de la Información de las AAPP, dependiente del Comité Sectorial de Administración electrónica, contará con un representante de cada una de las entidades presentes en dicho Comité Sectorial."*

27001:2013, 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 Foot Analytics, 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 Foot Analytics ante un hipotético incidente de seguridad de la información.

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

1. Contribuir desde la gestión de la seguridad, al cumplimiento de la misión y objetivos establecidos por Foot Analytics.
2. Disponer de las medidas de control necesarias para garantizar el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos de carácter personal.
3. Asegurar la accesibilidad, confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los activos de información.
4. Asegurar la prestación continuada de los servicios, tanto de forma preventiva, como de forma reactiva ante los incidentes de seguridad.
5. Proteger los activos de información de Foot Analytics, y la tecnología que los soporta frente a cualquier amenaza, intencionada o accidental, interna o externa.

Los objetivos explicados anteriormente tienen la finalidad de garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

6. FUNCIONES DE SEGURIDAD COMITÉ DE SEGURIDAD

Foot Analytics ha nombrado un Comité de Seguridad con sus Funciones y Responsabilidades.

El establecimiento de este comité, así como la designación de los diferentes roles se hallan registrados en el Acta de Constitución del comité:

El Comité de Seguridad de la Información del ENS está formado por:

- Responsable de Seguridad
- Responsable de Sistemas
- Responsable de la Información
- Responsable del Servicio

Y este Comité de Seguridad contará con Suplentes para cada uno de los Responsables del Comité de Seguridad.

Se deben identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización. Se detallarán en la política de seguridad de la organización las atribuciones de cada responsable.

Los nombramientos los establece la Dirección de la organización y se revisan cada 2 años o cuando un puesto queda vacante. Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité de Seguridad y prevalecerá en todo caso el criterio de la Dirección ejecutiva.

Los diferentes roles junto con sus respectivas funciones y responsabilidades:

El **Responsable de la Información** tendrá como funciones:

- Identificar, clasificar y custodiar la información sensible de la organización.
- Establecer procedimientos para la gestión del ciclo de vida de la información (creación, almacenamiento, acceso y destrucción).
- Garantizar que el acceso a la información esté restringido a usuarios autorizados.
- Coordinar con el Responsable de Seguridad para garantizar la protección de los datos.

El **Responsable del Servicio** tendrá las funciones:

- Asegurar que los servicios tecnológicos cumplan con los niveles de seguridad establecidos en el ENS.
- Supervisar los acuerdos de nivel de servicio (SLA) con los proveedores externos.
- Gestionar la continuidad de los servicios en caso de incidentes de seguridad o interrupciones.

- Informar al Responsable de Seguridad sobre cualquier anomalía en la provisión de los servicios.

El **Responsable de Sistemas** tendrá las funciones:

- Garantizar la disponibilidad, integridad y confidencialidad de los sistemas de información.
- Implementar y gestionar las medidas técnicas de seguridad (firewalls, cifrado, backups, etc.).
- Detectar, registrar y gestionar incidentes de seguridad relacionados con los sistemas de información.
- Realizar el mantenimiento preventivo y correctivo de los sistemas.

El **Responsable de Seguridad** tendrá las funciones:

- Coordinar y supervisar la implementación de las medidas de seguridad establecidas en el ENS.
- Evaluar riesgos de seguridad y proponer acciones para mitigarlos.
- Elaborar y mantener actualizada la política de seguridad de la información.
- Realizar auditorías internas y gestionar las externas para verificar el cumplimiento del ENS.
- Proporcionar formación y sensibilización en seguridad a los empleados de la organización.

Procedimiento de Designación y Renovación

En el momento de la implantación inicial del ENS, la **Dirección de la organización** ha procedido a la **designación formal** de los responsables mencionados, mediante resolución interna, garantizando que:

- **Ningún rol crítico recae en la misma persona** si puede dar lugar a conflictos de interés.
- Se respeta la **segregación de funciones**, especialmente entre quienes supervisan y quienes ejecutan controles de seguridad.

Esta designación ha quedado documentada en el **registro de roles de seguridad**, firmado por la Dirección.

Criterios de Designación

Para la designación de cada rol se tendrán en cuenta los siguientes criterios:

- Competencia técnica y experiencia en funciones relacionadas.
- Pertenencia al área organizativa correspondiente (funcional o técnica).
- Independencia funcional cuando aplique (ej. el Responsable de Seguridad no puede depender jerárquicamente del Responsable del Sistema).
- No acumulación de funciones que comprometan el control cruzado.

Se establece que:

- Los roles serán **revisados anualmente** o cuando ocurran cambios organizativos o de personal.
- Toda renovación se documentará igual que la primera designación.
- Cualquier **sustitución temporal** se realizará con autorización escrita y respetando la segregación de funciones.

El Responsable de Seguridad supervisará que:

- Las designaciones estén actualizadas.
- Se cumplan los principios de segregación y trazabilidad.
- El registro de roles esté disponible para auditoría del cumplimiento ENS.

Para formalmente tener correctamente designado a las personas se ha establecido y este será el mecanismo para hacerlo de:

- Documento firmado por la Dirección.
- Comunicación escrita al interesado.
- Inclusión en el **registro actualizado de roles ENS**, indicando:
- Fecha de designación
- Vigencia (si aplica)
- Funciones asignadas
- Sustituto en caso de ausencia

7. NIVEL DE ESCALADO

El administrador de seguridad reporta al Responsable del Sistema o al Responsable de la Seguridad, según sea su dependencia funcional:

- Incidentes relativos a la seguridad del sistema o acciones de configuración, actualización o corrección.

- El Responsable del Sistema informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.
- El Responsable del Sistema informa al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.
- El Responsable del Sistema reporta al Responsable de la Seguridad:
    - Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema
    - Resumen consolidado de los incidentes de seguridad.

8. ANÁLISIS Y GESTIÓN DE LOS RIESGOS (ART. 14)

Se realizará un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis será la base para determinar las medidas de seguridad que se deben adoptar, además de los mínimos establecidos según lo previsto en el artículo 7 y 14 del BOE, se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando haya un incidente de seguridad relacionado con la normativa LOPDGDD
- Cuando haya una brecha de seguridad relacionada con la información tratada de un usuario según la normativa LOPDGDD.

Los criterios de evaluación de riesgos se especificarán en la metodología de evaluación de riesgos y de incidentes de seguridad que elaborará la organización, basándose en estándares, buenas prácticas reconocidas y normas jurídicas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave. Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios, o repercuta a dicha información tratada durante el servicio.

Los criterios de evaluación de riesgos se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas. Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave. Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios de Foot Analytics en los clientes.

El propietario de un riesgo debe ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema de información entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente propietario.

9. GESTIÓN DE PERSONAL (ART. 15)

El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto 311/2022, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad.

Su actuación, deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

10. PROFESIONALIDAD (ART. 16)

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

Las entidades del ámbito de aplicación de este real decreto exigirán, 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.

Foot Analytics determinará los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

11. AUTORIZACIÓN Y CONTROL DE LOS ACCESOS (ART. 17)

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Los privilegios de acceso de un recurso (persona) al sistema de información de Foot Analytics, quedan restringidos por defecto al mínimo necesario para el desarrollo de sus funciones.

El sistema de información de Foot Analytics se mantendrá siempre configurado, de tal manera que evite que un recurso (persona) pueda acceder accidentalmente a recursos con derechos distintos de los autorizados.

12. PROTECCIÓN DE LAS INSTALACIONES (ART. 18)

Los sistemas de información y su infraestructura de comunicaciones asociados a Foot Analytics deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

13. ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD (ART. 19)

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional (en

adelante, CCN), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

a. Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
b. Otras certificaciones de seguridad adicionales que se requieran normativamente.
c. Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.

14. MÍNIMO PRIVILEGIO (ART. 20)

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a. El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
b. Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados.
c. Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. 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.
d. Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

15. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA (ART. 21)

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal del Responsable de Seguridad de Foot Analytics.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos. La Responsabilidad será a cargo del responsable de seguridad de Foot Analytics.

16. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO (ART. 22)

En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

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

17. PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS (ART. 23)

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de

Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

18. REGISTRO DE LA ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO (ART. 24)

Con el propósito de satisfacer el objeto de este real decreto, 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, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá 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 una determinada actividad.

19. INCIDENTES DE SEGURIDAD (ART. 25)

La entidad titular de los sistemas de información del ámbito de este real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero , por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de 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.

20. CONTINUIDAD DE LA ACTIVIDAD (ART. 26)

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

21. MEJORA CONTINUA DEL PROCESO DE SEGURIDAD (ART. 27)

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 la gestión de la seguridad de las tecnologías de la información.

22. APROBACIÓN DEL DOCUMENTO

Documento: Política de Seguridad

Estado: Aprobado

Firmado:

