Términos de seguridad de eAlicia.com

Sistema de Gestión de Seguridad de la Información – SGSI

Documento:	EAIT_20251124_SGSI_eAlicia_Terminos_Seguridad_2.0.0
Versión:	2.0.0
Fecha de emisión:	24 de noviembre de 2025
Responsable:	RunCall Systems, S.L.
Estado	Aprobado
Confidencialidad	Público

Control de versiones

Versión	Fecha	Autor	Descripción del Cambio
1.0	2025/06/01	RunCall Systems, S.L.	Creación inicial del documento.
2.0	2025/11/24	RunCall Systems, S.L.	Revisión mayor y reestructuración de la Sección 8.

Contenido

Glosario y Definiciones:

Según se utilizan en este documento, los siguientes términos tendrán los significados que se establecen a continuación:

- *"eAlicia" significa "SaaS eAlicia private cloud", y/o cualquiera de sus respectivos accesos, según corresponda (individual o colectivamente).*
- *"Información Confidencial", en adelante "ICF", tiene el significado que se le da a dicho término, incluyendo otros similares términos con intención similar, según el acuerdo del Proveedor con eAlicia.*
- *"**Cliente**", en adelante "**CLIENTE**" significa cualquier cliente que utilice o utilizará el servicio prestado por esta plataforma, según corresponda.*
- *"Datos Personales", en adelante "DTPS", tiene el significado que se le da a dicho término, incluyendo otros términos similares intención similar, por la ley de protección de datos y/o privacidad aplicable.*

*El servicio de **eAlicia** se ofrece en la modalidad de SaaS (Software as a Service), en formato "private cloud", en servidores alojados en un CPD de COLT Telecom.*

1 Seguridad del sitio físico y entorno

Las medidas de seguridad de las que dispone el CPD, propiedad de VODAFONE SPAIN, en el que se hallan ubicados los servidores, son Áreas/zonas de seguridad establecidas, y es dónde se almacenarán los DTPS, así como el resto de Información calificada con Confidencial, son las siguientes:

- ISO/CEI 27001:2013 | Gestión de la seguridad de la información
- ENS (nivel alto) | Esquema Nacional de Seguridad
- GDPR | Reglamento General de Protección de Datos
- ISO 9001:2015 | Sistema internacional de gestión de la calidad
- ISO 22301:2012 | Gestión de la continuidad del negocio
- ISO/IEC 27017:2015 | Seguridad de la información para servicios en nube
- ISO 14001:2015 | Gestión medioambiental
- ISO 50001 | Sistema de gestión energética
- Detección de humo de alta sensibilidad y un sistema de supresión de incendios del centro de datos reconocido por la industria
- Puertas bloqueadas electrónicamente
- Sistema de lectura electrónica de tarjeta de acceso
- Gestión de accesos, documentación e histórico de los titulares con acceso permitido
- El exterior del edificio dispone de una estructura reforzada, de hormigón armado, y no tiene ventanas.
- Hay personal de seguridad, presencial, disponible las 24 horas, los 7 días de la semana y los 365 días del año
- Servicio de seguridad en la Recepción, con registro obligatorio para todos los visitantes, con validación de la correspondiente autorización de entrada.
- Sistema de alarma antirrobo
- Sistema de gestión de vigilancia del edificio con CCTV, y de sus diferentes estancias, con monitorización interna y externa, con cámaras infrarrojas de detección de movimiento horizontal y vertical
- Escáneres biométricos

2 Control de disponibilidad

Las medidas tomadas para garantizar que la ICF o los DTPS estén protegidos contra la destrucción o pérdida accidental de datos, se describen a continuación:

- Acceso con código numérico al armario rack
- La estancia donde se encuentra alojado el rack que contiene todos los equipos electrónicos y de comunicaciones, está dotada de múltiples unidades de aire acondicionado para proporcionar garantizar una temperatura óptima para el funcionamiento de estos equipos.
- Se dispone de doble línea de red eléctrica
- SAI/UPS y APC
- Se cuenta con doble línea, y doble operador, de acceso a Internet, con ancho de banda garantizado de 500/500 MB
- Firewalls Fortinet FG100F, redundados y en HA, con múltiples capas y políticas de seguridad independientes por cada VLAN y/o servicio
- Switchs de comunicaciones, redundados
- Conectividad con fibra óptica
- Segmentación de la red con VLANs
- Los sistemas están redundados, al igual que los servidores, que cuentan con configuración de matrices de RAID

Las copias de seguridad, inmutables, se almacenan en diversos NAS del propio CPD. Como complemento a éstas, se realiza una segunda copia en una ubicación geográfica alternativa.

3 Seguridad a nivel de red

Se han desplegado medidas para evitar el acceso no autorizado al entorno de procesamiento de datos e impedir que los posibles atacantes vulneren la red del proveedor. Las medidas de seguridad incluyen tecnología en las siguientes categorías:

- Firewalls Fortinet FG100F perimetrales, redundados y en HA, siempre actualizados con la última versión, y controles de acceso basados en VPN para proteger las redes de servicios privados y los servidores back-end.
- Detección/prevención avanzada de amenazas persistentes
- Protección contra denegación de servicio
- Prevención de pérdida de datos
- Gestión de dispositivos móviles
- Seguridad de aplicaciones web
- Monitoreo continuo de seguridad de infraestructura, con PRTG
- Examen periódico de los riesgos de seguridad por parte de empleados internos y auditores externos, incluidos auditoría de vulnerabilidades y pentesting (pruebas de penetración en los sistemas)
- Control de acceso basado en roles, implementado de acuerdo con el principio de mínimo privilegio

Acceso remoto protegido mediante tokens de autenticación de dos factores o autenticación multifactor.

4 Características de los servidores

Los servidores de eAlicia están específicamente configurados para el tratamiento seguro de la Información Confidencial (ICF) y los Datos Personales (DTPS). Incorporan características como servidores redundados con matrices RAID y conectividad con fibra óptica para asegurar la disponibilidad y el rendimiento. Además, se han implementado robustas defensas para proteger contra intrusiones, incluyendo procedimientos de gestión de parches, soluciones antivirus y antimalware, y el cifrado de todos los datos en tránsito y de los medios de copia de seguridad.

Características principales de configuración de los servidores para el tratamiento de ICF y de DTPS:

- Servidores redundados, que cuentan con configuración de matrices de RAID
- Conectividad con fibra óptica
- Sistema Operativo Windows Server 2019 STD y Windows Server 2025 STD
- SQL SERVER 2019 Standard

Defensas implementadas de protección contra intrusión, antivirus y antimalware:

- Se implementan procedimientos de gestión de parches que prioricen los parches de seguridad en los sistemas utilizados para procesar ICF o DTPS del CLIENTE.
- Se mantienen registros de todas las actividades de auditoría, monitoreo y seguridad durante 120 días en un entorno seguro.
- Hay implementados antivirus, protección de endpoints y capacidades de respuesta.

Se han adoptado medidas para garantizar que la ICF o los DTPS no puedan leerse, copiarse, modificarse ni eliminarse sin autorización durante la transmisión o el transporte electrónico, y que sea posible verificar y determinar a qué organismos se prevé la transferencia de ICF o STPS mediante instalaciones de transmisión de datos:

- Todos los datos (en particular, los DTPS Sensibles) se cifran en tránsito utilizando los protocolos de transmisión segura más recientes, Transport Layer Security (TLS) 1.3 con intercambio de claves RSA de 2048 bits o superior.
- El acceso a los informes queda registrado.
- Los medios de copia de seguridad están cifrados.
- No se utiliza almacenamiento extraíble.

5 Control de acceso

Este apartado describe las medidas de control de acceso implementadas en los servidores para salvaguardar la Información Confidencial (ICF) y los Datos Personales (DTPS). Se establecen estrictos procedimientos para prevenir el uso no autorizado de los sistemas de tratamiento de datos, incluyendo la autenticación personal y el uso de contraseñas seguras. Además, se detallan los controles para asegurar que únicamente el personal autorizado tenga acceso a los datos pertinentes, y que cualquier acción sobre la ICF o los DTPS quede registrada y sea auditable.

Se han adoptado medidas para evitar que los sistemas de tratamiento de datos se utilicen sin autorización:

- Inicio de sesión personal e individual al acceder al sistema o a la red corporativa.
- Los procedimientos de contraseña exigen un mínimo de 8 caracteres, incluyendo una mayúscula, una minúscula y un dígito numérico. Si la cuenta de usuario tiene cinco intentos de inicio de sesión fallidos, se bloqueará. Todas las contraseñas caducan a los 90 días. Tras la verificación del nombre de usuario y la contraseña, la aplicación utiliza un sistema de autenticación de token basado en la sesión.
- El acceso remoto para mantenimiento requiere autenticación de dos factores
- Bloqueos de pantalla automáticos después de un período de inactividad definido
- Bloqueos de pantalla protegidos con contraseña
- Todas las contraseñas se documentan electrónicamente y se protegen contra el acceso no autorizado mediante cifrado.
- Las cuentas de usuario se auditan dos veces al año

Se han activado controles para garantizar que las personas con derecho a usar un sistema de procesamiento de datos tengan acceso únicamente a la ICF o a los DTPS a los que tengan derecho de acceso, y que dicha ICF o DTPS no puedan leerse, copiarse, modificarse ni eliminarse sin autorización durante su procesamiento o uso, ni después de su almacenamiento:

- La autenticación del usuario se basa en un nombre de usuario y una contraseña segura.
- Los datos se almacenan cifrados en reposo.
- Todos los registros transaccionales contienen identificadores para distinguir los registros de los clientes.
- El procesamiento del sistema utiliza un mecanismo basado en roles para adaptar el acceso a los datos a usuarios y roles específicos.
- El acceso, la inserción y la modificación de datos quedan registrados en registros de logs o transacciones.

Se implementan medidas de control de entrada, para garantizar que sea posible verificar y determinar quién ha introducido, modificado o eliminado ICF o DTPS en los sistemas de procesamiento de datos, en el caso de que esto ocurra:

- Uso de credenciales de identificación de usuario
- El acceso a registros está restringido a un conjunto definido de roles
- Toda entrada tiene fecha y hora e incluye identificadores para el recurso o funcionalidad a la que se accede

Se implementan firewalls y sistemas de prevención de intrusiones para evitar el acceso no autorizado.

6 Controles de desarrollo de software

Se abordan las rigurosas medidas de seguridad implementadas durante el desarrollo de software para proteger la Información Confidencial (ICF) y los Datos Personales (DTPS). Se detallan los preceptos considerados en las mejoras y cambios, incluyendo el uso de sistemas de control de versiones seguros, el análisis de código y dependencias, y la adopción de prácticas que mitigan vulnerabilidades. Además, se describe el control de separación de datos, asegurando que la información sea procesada de forma independiente en entornos dedicados.

Cuando se realicen mejoras o cambios, a petición del CLIENTE, que incluyan desarrollo de software, se tendrán en cuenta los siguientes preceptos:

- El código fuente se gestiona mediante un sistema seguro de control de versiones.
- Los datos secretos (como contraseñas, claves API, etc.) no se almacenan en el código fuente.
- El código fuente se somete a análisis estáticos (SAST) periódicos.
- Las dependencias de software (como bibliotecas de código, paquetes, módulos y frameworks) se someten a análisis de composición de software (SCA).
- Las prácticas de desarrollo y las metodologías de prueba (incluidas las técnicas de análisis mencionadas anteriormente) tienen en cuenta los vectores de vulnerabilidad comunes y las bases de datos de vulnerabilidades actualizadas.
- Por ejemplo, OWASP Top 10, NIST NVD.

Control de Separación: Se han desplegado medidas para garantizar que la ICF o los DTPS recopilados para diferentes fines se procesen por separado.

- Se utilizan sistemas de tres niveles para separar físicamente la presentación, el procesamiento comercial y el almacenamiento.
- Los datos del CLIENTE se almacenan en bases de datos independientes o en arquitecturas lógicamente separadas.
- Se aplica la separación de funciones internamente para garantizar que las funciones superen los procesos de control de cambios.
- Se mantienen entornos de desarrollo, test y producción por separado.
- Todo el enrutamiento de datos para su procesamiento se controla mediante motores de reglas automatizados.
- El procesamiento y el almacenamiento se realizan en equipos propiedad del Proveedor.

7 Gobernanza y políticas de seguridad

Este apartado se enfoca en cómo la organización establece y mantiene un marco de seguridad robusto, a través de directrices claras y responsabilidades definidas, para asegurar el cumplimiento normativo, la gestión proactiva de riesgos y la mejora continua de las defensas de la información sensible.

- Se mantienen, y actualizan, políticas y procedimientos de seguridad de la información por escrito, así como programas de respuesta a incidentes, necesarios para cumplir, como mínimo, con (i) todas las leyes de protección de datos aplicables y (ii) los estándares de la industria generalmente aceptados para la protección de datos, incluyendo la norma **ISO 27001:2013**.
- Simulacros para probar procedimientos de seguridad de la información y programas de respuesta a incidentes, al menos una vez al año, conservando los informes escritos de los resultados.
- Se cuenta con personal responsable de la determinación, revisión e implementación de políticas y medidas de seguridad.
- Control de asignaciones: Se activa para garantizar que, en caso de procesamiento por encargo de ICF o DTPS, estos datos se procesen estrictamente de acuerdo con las instrucciones del CLIENTE.
    - Se han establecido acuerdos de confidencialidad para todas las personas con acceso a los datos.
    - Se imparte capacitación sobre privacidad y seguridad de la información durante la incorporación y de forma periódica.
    - No se utilizan terceros para el procesamiento de datos, salvo lo descrito en los Acuerdos.
    - La política de privacidad describe los derechos y obligaciones del agente y del CLIENTE.

En el supuesto de que se tratasen datos de tarjetas de pago en el servicio del CLIENTE, al procesar o acceder a los datos del titular de la tarjeta en nombre de eAlicia, se cumple con los estándares de gestión de tarjetas de crédito aplicables según el emisor. eAlicia está alineado con el Estándar de Servicios de Datos de la Industria de Tarjetas de Pago (PCI-DSS) y proporcionará pruebas de cumplimiento anualmente.

8 Seguridad de modelos de IA

8.1 Procedimientos con modelos de IA

Propósito del modelo de gestión

Esta sección describe y desarrolla las especificaciones técnicas, operativas y de cumplimiento normativo de la plataforma **eAlicia**, desarrollada y gestionada por **GRUPO MST**.

El objetivo es proporcionar a los departamentos de seguridad, tecnología y cumplimiento de los clientes una descripción exhaustiva de la infraestructura, los modelos de inteligencia artificial (IA) utilizados, los mecanismos de protección de datos, las medidas de seguridad y las certificaciones aplicables al servicio.

8.1.1 Alcance

El documento cubre el diseño arquitectónico de eAlicia, sus procesos de tratamiento de datos (voz, texto y diferentes tipos de ficheros e imágenes), las tecnologías utilizadas, las políticas de seguridad y privacidad, y los principios éticos que rigen el uso de la IA en el marco del **AI Act** y del **GDPR**. Incluye además la descripción de los mecanismos de *anonimización*, los procedimientos de auditoría, la gestión de sesgos y la supervisión humana de los sistemas automatizados.

8.1.2 Objetivo funcional de eAlicia

eAlicia es una plataforma de calidad orientada a la **auditoría inteligente de interacciones con clientes**, utilizada por empresas que gestionan directamente o a través de **BPOs o contact centers** sus servicios de atención al cliente.

Permite la **evaluación automática y objetiva** de interacciones multicanal (llamadas telefónicas, correos electrónicos, chats, mensajes instantáneos y redes sociales) mediante modelos de **IA generativa y analítica**.

El sistema genera **transcripciones, resúmenes, indicadores de desempeño y recomendaciones de mejora**, tanto para los agentes como para los procesos de servicio.

8.1.3 Enfoque corporativo y cumplimiento normativo

El desarrollo de eAlicia se ha realizado bajo un enfoque de **seguridad por diseño y cumplimiento por defecto** (*Security & Compliance by Design*), garantizando que todas las fases —desde la captura de datos hasta el análisis de resultados— cumplan con las normativas europeas e internacionales aplicables:

CERTIFICACIONES

- **GDPR** (General Data Protection Regulation).
- **ISO 27001** (Sistema de Gestión de Seguridad de la información - SGSI).
- **ISO 22301** (Sistema de Gestión de Continuidad del Negocio - SGCN).

CUMPLIMIENTO DE RECOMENDACIONES

- **AI Act** (European Artificial Intelligence Act).
- **ENS** (Esquema Nacional de Seguridad).

- **SOC 2 Type II** y **NIST SP 800-53** (estándares de control y auditoría de sistemas).

8.1.4 Principios rectores de la plataforma

eAlicia se sustenta en los siguientes principios:

- **Privacidad y confidencialidad**: la conexión es cifrada y los datos críticos son tratados bajo cifrado, con políticas estrictas de acceso y retención mínima.
- **Transparencia y auditabilidad**: cada proceso automatizado genera trazabilidad verificable.
- **Supervisión humana**: la decisión generada por IA está validada por humanos antes de ser considerada en auditorías o reportes oficiales.
- **Imparcialidad y ausencia de sesgo**: los modelos se entrenan y validan con *datasets* representativos, aplicando técnicas de mitigación de sesgos.

Soberanía del dato: Toda la infraestructura de eAlicia se encuentra desplegada en entornos de private cloud ubicados exclusivamente en países de la Unión Europea, lo que garantiza el pleno cumplimiento del principio de residencia y soberanía del dato. Este enfoque asegura que toda la información tratada permanezca dentro del marco jurídico europeo, cumpliendo estrictamente con los requisitos del RGPD, las directrices del EDPB y las obligaciones contractuales establecidas con los clientes.

8.2 Arquitectura Técnica

La plataforma **eAlicia** se sustenta en un modelo **SaaS** desplegado sobre un entorno de **nube privada** gestionado por **GRUPO MST**, con infraestructura física alojada en los **centros de datos de VODAFONE y COLT**. Esta configuración garantiza **redundancia geográfica**, **baja latencia** y **alta disponibilidad** de los servicios críticos.

El diseño de la arquitectura está orientado a la escalabilidad horizontal, la seguridad perimetral y lógica, y la modularidad funcional, permitiendo adaptar el entorno a los requerimientos técnicos, operativos y normativos de cada cliente.

Cada componente de la solución se encuentra en contenedores Docker, lo que facilita el aislamiento de servicios, la portabilidad de entornos y la estandarización de despliegues. La orquestación de contenedores se gestiona a través de una capa interna de control y administración, responsable de la gestión de versiones, despliegues, monitorización y escalado dinámico.

Esta arquitectura modular y automatizada permite:

- Un **mantenimiento ágil** y controlado de los entornos.
- La **replicación rápida** de configuraciones en entornos de desarrollo, preproducción o producción.
- Un **aislamiento efectivo** entre instancias de cliente, garantizando la **seguridad y confidencialidad** de la información.

En conjunto, el modelo adoptado proporciona una infraestructura **resiliente, flexible y segura**, alineada con las mejores prácticas de **arquitecturas *private cloud* orientadas a servicios (SaaS)**.

8.2.1 Componentes principales

a) Capa de adquisición de datos

Responsable de recibir, validar y almacenar los datos de entrada (audios, textos y metadatos). Los canales soportados incluyen:

- Llamadas de voz (ficheros WAV, MP3, OGG).
- Transcripciones textuales.
- Interacciones digitales (correos, chats, redes sociales, mensajería instantánea).
- Ficheros PDF, DOCX, XLSX, etc.
- Ficheros de Imágenes

Cada flujo se procesa de forma **asíncrona y cifrada desde SFTP o APIs**, garantizando la integridad de los datos.

b) Capa de procesamiento de IA

Se encuentra diseñada conforme a los principios de **seguridad, aislamiento y control de la información**, y constituye el núcleo funcional responsable del análisis avanzado de datos no estructurados.

Esta capa integra servicios dedicados a la **extracción de texto** desde múltiples tipos de ficheros, la **transcripción de audio**, el **análisis semántico y lingüístico**, la **generación automatizada de resúmenes** y la **detección de patrones e insights relevantes**.

Todas las operaciones de inteligencia artificial se ejecutan **dentro del entorno privado y controlado de GRUPO MST**, sin dependencia de servicios externos ni transmisión de información fuera del perímetro corporativo.

De este modo, se garantiza:

- El **aislamiento completo** de los datos tratados.
- La **no exposición** de información a terceros o a entornos públicos de procesamiento.
- El **cumplimiento estricto** de las normativas de **protección de datos personales y seguridad de la información**.

La capa de IA combina diferentes tipologías de modelos:

- **Modelos generativos**, empleados para la generación de texto y el análisis contextual avanzado.
- **Modelos propios de Machine Learning y Deep Learning**, desarrollados internamente por GRUPO MST y entrenados sobre datos anonimizados y controlados, con el objetivo de cubrir casos de uso específicos.
- **Modelos open source modificados y validados internamente** (tipo *Whisper*, *Llama* o *Mistral*), adaptados a los requisitos técnicos, lingüísticos y regulatorios de cada cliente.

Cada modelo se somete a un proceso de **evaluación, ajuste y validación** previo a su despliegue, asegurando la **robustez, trazabilidad y control del ciclo de vida** de los algoritmos empleados. Asimismo, se mantiene una **segmentación lógica y de red** entre los entornos de entrenamiento, validación y producción, minimizando el riesgo de exposición o fuga de información.

Esta arquitectura proporciona una **infraestructura de IA segura, gobernada y auditable**, alineada con los principios de **seguridad por diseño**, **minimización de datos** y **cumplimiento normativo** aplicables a entornos de análisis inteligente de información.

c) Capa de almacenamiento y persistencia

La capa de almacenamiento y persistencia de eAlicia está diseñada para garantizar la integridad, confidencialidad y disponibilidad de los datos gestionados por la plataforma.

Toda la información se almacena en volúmenes dedicados, con una separación lógica estricta entre clientes que impide el acceso cruzado a datos o configuraciones.

Cada instancia de cliente cuenta con políticas de retención configurables, adaptadas a sus requisitos operativos y normativos.

El sistema realiza copias de seguridad diarias, almacenadas en entornos inmutables y aislados del entorno operativo, garantizando la recuperación íntegra ante incidentes de pérdida, corrupción o ataque. Las copias se verifican periódicamente mediante procedimientos de validación y restauración controlada, asegurando su disponibilidad y consistencia.

Esta arquitectura de almacenamiento proporciona un marco de **persistencia seguro, auditable y conforme a los principios de seguridad ENS e ISO 27001**, permitiendo el cumplimiento de las políticas de continuidad y protección de la información definidas por cada cliente.

d) Capa de aplicación y reporting

La capa de presentación y acceso de eAlicia proporciona los mecanismos seguros para la visualización, consulta y explotación de resultados, métricas e informes generados por la plataforma.

El acceso a la información se realiza a través de una interfaz web segura y una API REST que permite la integración con sistemas externos autorizados.

Ambos canales están protegidos mediante autenticación robusta y un sistema de control de acceso basado en roles (RBAC – Role-Based Access Control), que garantiza que cada usuario o sistema consumidor acceda únicamente a los recursos y datos para los que dispone de permisos explícitos.

Los informes y paneles de control (dashboards) se generan en tiempo real, ofreciendo indicadores actualizados sobre los procesos y resultados.

Cada visualización incluye trazabilidad completa del origen de los datos, permitiendo auditar y verificar la consistencia de la información presentada en cualquier momento.

Esta capa se apoya en mecanismos de **registro de actividad, auditoría y protección frente a accesos indebidos**, asegurando el cumplimiento de las políticas de **confidencialidad, integridad y disponibilidad** definidas por GRUPO MST y por los requisitos específicos de cada cliente.

e) Capa de integración (datos externos)

La **capa de integración** de **eAlicia** permite la **interoperabilidad segura con sistemas externos** corporativos, facilitando el intercambio controlado de información entre la plataforma y entornos de terceros.

Esta capa incorpora **conectores y servicios web** basados en **SOAP** y **REST**, que posibilitan la integración con sistemas de gestión empresarial (**ERP**), gestión de relaciones con clientes (**CRM**) y **plataformas de contact center**, entre otros.

Dicha integración está diseñada bajo principios de **modularidad, trazabilidad y seguridad por diseño**, garantizando la consistencia y protección de los datos durante todo el ciclo de comunicación.

Todos los puntos de conexión y transferencia de información están **protegidos mediante cifrado TLS 1.3 y SSL**, asegurando la **confidencialidad e integridad de los datos en tránsito**.

El proceso de autenticación se gestiona a través del **estándar OAuth2**, que permite un control granular de accesos y autorizaciones.

Además, se aplica **validación mutua de certificados SSL**, reforzando la **autenticación de extremo a extremo** entre los sistemas que intervienen en la comunicación.

Esta capa dispone, asimismo, de **mecanismos de registro y auditoría** que permiten monitorizar las operaciones de integración y detectar posibles anomalías o intentos de acceso no autorizado, en cumplimiento con las políticas de seguridad de **GRUPO MST** y los estándares **ENS** e **ISO/IEC 27001**.

8.2.2 Diseño de red y seguridad perimetral

La infraestructura está diseñada bajo un enfoque de **segmentación por zonas de seguridad**, con el objetivo de garantizar el **aislamiento funcional**, la **protección perimetral** y el **control de flujos de información** entre los distintos componentes del sistema.

El diseño se estructura en las siguientes zonas:

- **Zona pública (DMZ):** gestiona las comunicaciones externas con los usuarios y sistemas integrados. Incluye balanceadores de carga, firewalls de aplicación (WAF) y sistemas de detección y prevención de intrusiones (IDS/IPS), que filtran, inspeccionan y mitigan posibles amenazas antes de que alcancen las capas internas.
- **Zona de servicios internos:** alberga los microservicios de negocio y los módulos de procesamiento de IA, aislados de la red pública. Solo acepta conexiones autenticadas y cifradas procedentes de la DMZ o de zonas internas autorizadas, garantizando la confidencialidad y trazabilidad de cada interacción.
- **Zona de datos:** dedicada al almacenamiento cifrado y a las bases de datos segregadas por cliente o entorno. El acceso está restringido a los servicios internos mediante políticas de control de acceso mínimo (least privilege) y autenticación reforzada.
- **Zona de monitorización y backup:** concentra los sistemas de observabilidad, métricas, registros de auditoría y copias de seguridad. Está completamente aislada de las redes operativas de usuario, asegurando la integridad de los datos de monitorización y recuperación ante incidentes.

Cada comunicación entre zonas se cifra mediante **certificados** emitidos por una entidad certificadora autorizada.

Este diseño de red asegura una **defensa en profundidad**, minimiza la superficie de exposición y mantiene el cumplimiento de los principios de **seguridad por diseño**, **segmentación lógica** y **protección perimetral avanzada** definidos por el **Esquema Nacional de Seguridad (ENS)** y las **normas ISO 22301 e ISO/IEC 27001 y 27002**.

8.2.3 Disponibilidad y resiliencia

- **Redundancia geográfica:** todos los servicios críticos están duplicados entre los CPDs de VODAFONE y COLT, manteniendo backups en Barcelona y Madrid.
- **Escalabilidad automática:** el sistema puede aumentar recursos (CPU, memoria o nodos) en función de la demanda.
- **Monitorización continua:** métricas de rendimiento, seguridad y disponibilidad supervisadas 24/7.
- **Procedimientos de failover:** conmutación automática ante incidentes y restauración verificada.

8.2.4 Gestión de versiones y despliegues

El ciclo de vida de los servicios de eAlicia sigue un modelo **CI/CD (Continuous Integration / Continuous Deployment)** que garantiza la trazabilidad, calidad y seguridad en todas las fases del desarrollo.

Las versiones del software se gestionan mediante **repositorios internos** y se validan en **entornos de pruebas aislados**, estructurados en los entornos de **desarrollo**, **preproducción** y **producción**.

Cada despliegue requiere:

- **Validación automatizada** mediante pruebas unitarias, funcionales y de integración.
- **Revisión de seguridad**, que incluye análisis estático, escaneo de vulnerabilidades y comprobaciones de cumplimiento.
- **Registro de auditoría**, asegurando la trazabilidad completa de las acciones realizadas.

Todos los cambios son **documentados y registrados** conforme a las políticas de **calidad y seguridad del Grupo MST**, garantizando el cumplimiento de los estándares internos y normativos aplicables.

8.2.5 Monitorización y alertas

La plataforma cuenta con **sistemas de monitorización continua** que permiten detectar incidencias, fallos operativos y desviaciones de rendimiento en tiempo real.

Los **registros (logs)** se centralizan y almacenan en un **entorno seguro de análisis**, con políticas de **retención limitada**, **acceso restringido** y mecanismos que garantizan la **integridad y trazabilidad** de la información recopilada.

Asimismo, el sistema dispone de **alertas automatizadas** que notifican a los equipos responsables ante cualquier evento anómalo, facilitando una respuesta rápida y eficaz.

Se monitorizan los eventos relevantes del sistema y se aplican los procedimientos de gestión y respuesta ante incidentes definidos según la norma **ISO 22301**, garantizando la continuidad del servicio y la actuación coordinada ante cualquier anomalía.

8.3 Procesamiento de Datos e Inteligencia Artificial

El procesamiento de datos en eAlicia se rige por los principios de **minimización, *anonimización*, seguridad y trazabilidad**, garantizando la integridad de la información y el cumplimiento de los estándares europeos de protección de datos y ética en IA.

La plataforma combina procesos automatizados de captura, tratamiento y análisis, con supervisión humana en las fases críticas, para asegurar resultados confiables y auditables.

8.3.1 Captura y afinado de audio

Los audios procedentes de interacciones de clientes (llamadas, grabaciones de voz, etc.) se someten a una **etapa previa de afinado acústico** antes de su transcripción.

Las técnicas aplicadas incluyen:

- **Normalización de volumen y frecuencia.**
- **Filtrado de ruido de fondo.**
- **Separación de canales y *diarización*** (bajo petición).
- **Detección de silencios y pausas significativas.**

Estos procesos mejoran la precisión de los modelos de reconocimiento de voz y la calidad final de las transcripciones.

8.3.2 Transcripción automática

La **transcripción de voz a texto** se realiza mediante **modelos *open source* de reconocimiento automático del habla**, incluyendo Whisper, sus variantes y otros modelos específicos implantados en los entornos controlados del **Grupo MST**.

Todas las transcripciones se procesan exclusivamente en la **red interna de MST**, garantizando que **no existe acceso a los modelos de transcripción desde servicios externos** ni transferencia a proveedores.

Cada transcripción se **valida automáticamente** mediante métricas de calidad, **precisión semántica** y **detección de entidades clave**, y un porcentaje mensual es posteriormente **revisado por auditores humanos** dentro de los procesos internos de control y validación de calidad.

8.3.3 Generación de resúmenes y extracción de insights

Los **modelos generativos**, basados en tecnologías *open source* y en sus adaptaciones internas, procesan las transcripciones para **generar resúmenes, clasificaciones e indicadores de calidad del servicio**. Estos modelos permiten **identificar patrones y tendencias relevantes**, facilitando el análisis y la toma de decisiones operativas.

La **IA generativa** opera exclusivamente según **criterios predefinidos por eAlicia** y en **entornos de red privada**, sin exposición a servicios externos y bajo supervisión continua. Este modelo de funcionamiento, junto con su

uso acotado y controlado, sitúa la solución dentro de los **límites regulatorios del AI Act**, clasificándola como un **sistema de riesgo limitado**, cumpliendo así los requisitos de transparencia y seguridad aplicables.

8.3.4 Medidores de calidad y variables configurables

eAlicia incorpora un sistema de **medición dinámica del desempeño**, basado en variables configurables definidas por cada cliente y adaptadas a sus necesidades operativas. Estas variables pueden incluir, entre otras:

- Cumplimiento normativo.
- Exactitud de la información.
- Eficiencia comunicativa.
- Cortesía, tono y empatía.
- Resolución de la consulta.
- Cumplimiento del protocolo interno.

El sistema de evaluación de eAlicia se fundamenta en principios de objetividad, no discriminación, imparcialidad y transparencia, garantizando que los resultados no estén influenciados por factores como género, edad, origen, idioma u otras características personales. Estos principios cumplen con las obligaciones del AI Act para sistemas de riesgo limitado, asegurando evaluaciones equitativas y auditables.

Los modelos analíticos calculan los resultados de forma ponderada y estandarizada, generando un **Índice Global de Calidad (IQS)** y métricas complementarias por agente, equipo y campaña, proporcionando una visión precisa y justa de la calidad del servicio.

8.3.5 Supervisión humana y explicabilidad

Todos los procesos de IA en eAlicia están sujetos a **supervisión humana obligatoria**. Los resultados automatizados no sustituyen la evaluación profesional, sino que la complementan. Además, la plataforma implementa principios de **IA explicable (Explainable AI – XAI)** que permiten a los auditores visualizar:

- Qué elementos de la conversación motivaron la calificación.
- Qué criterios o variables fueron aplicados.
- Qué factores influyeron en la recomendación o *insight* generado.

Esta transparencia es fundamental para cumplir con el **AI Act** y con las políticas éticas de GRUPO MST.

8.4 Cumplimiento Legal y Normativo

eAlicia ha sido desarrollada bajo una estrategia de **Compliance by Design**, garantizando que la plataforma y sus procesos se diseñan desde el origen para cumplir con las normativas europeas y nacionales en materia de **seguridad, privacidad y protección de datos**.

Las principales normativas y marcos de referencia aplicables son:

- **AI Act** (European Artificial Intelligence Act).
- **GDPR** (Reglamento General de Protección de Datos) y LOPDGDD (Ley Orgánica 3/2018).
- **ISO 27001**, **ENS** (Esquema Nacional de Seguridad), SOC 2 Type II y NIST SP 800-53.

eAlicia, la plataforma y sus procesos están **alineados con sus requisitos y mejores prácticas**, adoptando controles técnicos y organizativos inspirados directamente en dichos marcos. Este enfoque garantiza un nivel elevado de seguridad, gobernanza y gestión del riesgo en todo el ciclo de vida del sistema.

8.4.1 Cumplimiento del AI Act

El marco normativo del **AI Act** establece una clasificación de los sistemas de inteligencia artificial según su nivel de riesgo.

eAlicia se considera un **sistema de riesgo limitado**, dado que:

- Su función es **de apoyo** a la auditoría, medición y análisis de interacciones.
- **No toma decisiones autónomas** que afecten a derechos fundamentales.
- Opera en **entornos de red privada**, sin conexión a servicios externos ni transferencia a terceros.
- Sus resultados están **siempre sujetos a supervisión humana**.

Medidas adoptadas para el cumplimiento del AI Act:

1. Documentación técnica exhaustiva
2. Registro y trazabilidad completa de resultados
3. Supervisión humana obligatoria
4. Evaluaciones periódicas de sesgos, rendimiento y equidad
    - Ajuste continuo de los modelos para mitigar desviaciones.
5. Gobernanza de IA y ciclo de vida controlado
    - Monitorización activa del comportamiento de los modelos.
    - Validación previa a despliegue en entornos de preproducción.
6. Entornos de ejecución seguros y privados
    - Procesamiento en la **red interna de MST**
    - Aislamiento de datos personales y controles estrictos de acceso.
7. Transparencia y reportes de cumplimiento para clientes
8. Políticas internas de uso responsable de la IA
    - Alineado a nivel ético, no discriminación y proporcionalidad.
    - Procedimientos para detectar usos indebidos o desviaciones.
    - Formación continua del personal técnico y analítico.

8.4.2 Cumplimiento del GDPR y LOPDGDD

Los datos tratados por eAlicia se procesan conforme a los principios del **GDPR** y la legislación española complementaria (**LOPDGDD**):

- **Limitación de propósito:** los datos se utilizan exclusivamente para auditorías de calidad.
- **Minimización:** solo se capturan los datos estrictamente necesarios.
- **Anonimización y pseudonimización:** las identidades se sustituyen por identificadores irreversibles.
- **Derechos del interesado:** mecanismos para ejercer acceso, rectificación, supresión y portabilidad.
- **Evaluación de impacto (DPIA):** obligatoria en cada nuevo proyecto o cliente.
- **Transferencias internacionales:** no se realiza ninguna transferencia fuera del EEE.

8.4.3 Certificaciones y/o cumplimiento de estándares

eAlicia adopta los principales estándares internacionales:

- **ISO 27001:** Sistema de Gestión de Seguridad de la Información.
- **ISO 22301:** Sistema de Gestión de Continuidad de Negocio.
- **ENS:** cumplimiento del Esquema Nacional de Seguridad español.
- **SOC 2 Type II:** controles internos de seguridad, disponibilidad y confidencialidad.
- **NIST SP 800-53:** marco de referencia para la gestión de riesgos en sistemas de información.

Las auditorías internas se realizan anualmente y los clientes pueden solicitar la verificación de cumplimiento.

8.4.4 Auditorías éticas y responsabilidad

GRUPO MST mantiene un **programa sistemático de auditorías éticas** orientado a verificar el **comportamiento justo, transparente y no discriminatorio** de los modelos de IA utilizados por eAlicia. Estas auditorías evalúan tanto los modelos de transcripción como los modelos analíticos y generativos, garantizando que su funcionamiento se alinea con los principios de **equidad, proporcionalidad y respeto a los derechos fundamentales**.

El programa incluye:

- **Revisión periódica de sesgos** relacionados con género, edad, origen, acento o cualquier otro factor personal que pudiera afectar a la objetividad de los resultados.
- **Evaluaciones de impacto ético**, centradas en la interpretabilidad de los resultados y la ausencia de decisiones automatizadas que afecten a derechos o libertades.
- **Validación del comportamiento ponderado** del Índice Global de Calidad (IQS) y demás métricas, asegurando que los criterios de evaluación son **coherentes, imparciales y auditables**.
- **Análisis de transparencia**, garantizando que los clientes y auditores humanos pueden comprender cómo se generan las métricas, resúmenes y clasificaciones.

- **Revisión del cumplimiento normativo**, asegurando la alineación con el **AI Act** para sistemas de riesgo limitado y con las políticas de uso responsable de la IA del Grupo MST.

Los resultados de estas auditorías se **documentan formalmente**, se comunican a los responsables de seguridad y calidad y se integran en el **ciclo de mejora continua**, permitiendo ajustar modelos, reglas, parámetros o procedimientos en caso de detectarse desviaciones o áreas de mejora.

Este enfoque refuerza el compromiso de GRUPO MST con una IA **responsable, supervisada y segura**, manteniendo altos estándares de calidad y confianza.

8.5 Seguridad de la Información

La seguridad en eAlicia se articula sobre tres ejes:

1. **Infraestructura segura y aislada.**
2. **Cifrado integral de datos en tránsito.**
3. **Gestión rigurosa de accesos, identidades y vulnerabilidades.**

8.5.1 Cifrado y comunicaciones

- **Datos en tránsito:** protegidos mediante **TLS 1.3** y **SSL**.
- **Cifrado credenciales:** cifrados con **AES-256**
- **Canales internos:** uso exclusivo de VPN corporativas (VPN IPSec entre PDs)
- **Integridad:** firmas digitales y verificación de *checksum* en todos los ficheros críticos.

8.5.2 Control de accesos

- **Autenticación** y política de contraseñas robustas.
- **Autorización basada en roles (RBAC)**.
- **Principio de mínimo privilegio.**
- **Registros de acceso auditables y revisiones periódicas.**

8.5.3 Monitorización y respuesta ante incidentes

El **SOC interno de MST** supervisa la infraestructura 24/7, con herramientas de detección de intrusiones (**IDS/IPS**) y sistemas de correlación de eventos.

Cualquier incidente genera una alerta automática y un procedimiento de respuesta estandarizado con niveles de severidad definidos.

8.5.4 Continuidad y recuperación

Los centros VODAFONE y COLT operan en **modo activo-activo**, garantizando continuidad de servicio ante incidentes.

- **RTO (Recovery Time Objective):**
  - Incidencia leve: inferior a 30 minutos.
  - Incidencia grave: 3 horas
  - Incidencia muy grave: hasta 36 horas
- **RPO (Recovery Point Objective):**
  - Incidencia leve: inferior a 30 minutos
  - Incidencia grave/muy grave: Backup diario

Los planes de contingencia y respaldo están descritos en nuestra certificación **ISO 22301**.

8.6 Privacidad y Protección de Datos

El tratamiento de la información en eAlicia se rige por los principios fundamentales del **GDPR** y la **LOPDGDD**, aplicados desde el diseño inicial de la plataforma: *Privacy by Design* y *Security by Default*. Cada módulo y proceso se construye considerando la privacidad como requisito estructural y no como funcionalidad adicional.

8.6.1 Anonimización y pseudonimización

Antes de cualquier entrenamiento de modelos, todos los datos personales son sustituidos por identificadores irreversibles.

- **Texto:** se eliminan nombres, teléfonos, correos y cualquier identificador personal bajo petición expresa por servicio.
- **Metadatos:** se limitan a la información técnica imprescindible.
- Los algoritmos de anonimización son revisados periódicamente para garantizar su eficacia.

8.6.2 Retención y eliminación

El ciclo de vida de los datos está claramente definido:

- Los datos se conservan únicamente durante el período necesario para cumplir el propósito de auditoría.
- Una vez finalizado, se destruyen de forma segura y verificable bajo petición expresa.
- Los clientes pueden solicitar informes de eliminación certificados.
- Las grabaciones de audios se conservan durante un máximo de 3 meses, pudiéndose modificar este plazo bajo petición expresa.

8.6.3 Evaluaciones de impacto (DPIA)

Antes de incorporar nuevos clientes o implementar nuevas funcionalidades, la organización realiza un análisis de riesgos integral orientado a identificar cualquier impacto potencial sobre los derechos y libertades de las personas. Este análisis se desarrolla conforme a los principios del RGPD —como la minimización de datos, la proporcionalidad, la transparencia y la responsabilidad proactiva— y, cuando corresponda, a los requisitos de evaluación y clasificación de riesgos establecidos por la Ley de IA.

Con base en los riesgos detectados, se definen e implementan medidas de mitigación técnicas y organizativas adecuadas, garantizando un tratamiento de datos seguro, ético y conforme a la normativa vigente. Cuando procede, se lleva a cabo una Evaluación de Impacto en Protección de Datos (EIPD) o una Evaluación de Impacto en Sistemas de IA de Alto Riesgo, asegurando la adopción de controles adicionales para salvaguardar los derechos fundamentales.

8.6.4 Derechos del interesado

Los mecanismos para el ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad se encuentran plenamente habilitados para todos los interesados, de conformidad con lo establecido en el **Reglamento General de Protección de Datos (GDPR)** y la **LOPDGDD**.

GRUPO MST actúa en todo momento como **encargado del tratamiento**, aplicando únicamente las instrucciones documentadas proporcionadas por el **responsable del tratamiento (cliente)** y garantizando la implementación de las medidas técnicas y organizativas adecuadas conforme a los estándares del GDPR y los controles aplicables de la **ISO 27001**.

Todos los procedimientos relativos al ejercicio de derechos, así como las obligaciones y garantías asociadas al tratamiento de datos personales, se encuentran descritos y desarrollados en la **Política de Privacidad** publicada por el responsable del tratamiento y accesible a los usuarios a través del sitio web correspondiente.

8.7 Integraciones Tecnológicas

eAlicia pone a disposición de sus clientes y de los BPOs integradores varios mecanismos seguros de interoperabilidad, incluyendo APIs RESTful, Web Services SOAP y transferencia de ficheros mediante **SFTP**. Todos estos métodos están diseñados para garantizar la confidencialidad, integridad y trazabilidad de la información intercambiada.

- **Cifrado de las comunicaciones (HTTPS):**

Las APIs REST y Web Services SOAP se exponen exclusivamente a través de canales cifrados mediante HTTPS (SSL/TLS), asegurando que los datos en tránsito no puedan ser interceptados o modificados.

- **Transferencia de ficheros mediante SFTP:**

Para integraciones basadas en intercambio de ficheros, se proporciona un canal seguro mediante SFTP, que emplea cifrado robusto y autenticación reforzada para proteger la transmisión de datos.

- **Gestión de errores y trazabilidad:**

Los servicios implementan códigos de respuesta normalizados (HTTP 200–500) y generan trazas detalladas que permiten un adecuado diagnóstico, seguimiento y auditoría técnica conforme a las buenas prácticas y controles establecidos en **ISO 27001**.

Esta arquitectura asegura que las integraciones con eAlicia se realicen de forma segura, consistente y alineada con los requisitos normativos y de protección de la información.

8.7.1 Compatibilidad

La plataforma es compatible con los principales entornos empresariales:

Salesforce, Microsoft Dynamics, Genesys, Avaya, Zendesk, SAP, Oracle y otras soluciones de CRM/ERP/IVR.

8.7.2 Webhooks y eventos

eAlicia ofrece la posibilidad de integrar *Webhooks* que permiten el envío de notificaciones en tiempo real hacia los sistemas del cliente, facilitando la automatización y el seguimiento inmediato de eventos relevantes. Entre los eventos que pueden ser notificados se incluyen:

- Finalización de auditorías.
- Actualización de métricas operativas.
- Generación y disponibilidad de nuevos reportes.
- Emisión de alertas automáticas ante desviaciones o incidencias detectadas.

Nota: La activación, diseño y despliegue de estos *Webhooks* se realiza bajo petición del cliente, adaptándose a sus necesidades técnicas y operativas.

8.8 Reporting y Analítica

La plataforma eAlicia dispone de una interfaz avanzada que incorpora *dashboards* configurables, diseñados para ofrecer una visualización clara y flexible de los resultados operativos y de calidad. Estos paneles permiten analizar información de forma agregada o detallada, ya sea por agente, campaña o centro de contacto, adaptándose a las necesidades de supervisores, auditores y gestores de operaciones.

Entre los indicadores clave que pueden visualizarse se incluyen:

- Índice de Calidad Global (IQS).
- Cumplimiento de guiones y protocolos operativos.
- Resolución en Primera Llamada (FCR).
- Indicadores de empatía, experiencia del cliente y niveles de satisfacción.

Estos dashboards permiten un seguimiento continuo del desempeño y facilitan la toma de decisiones basada en datos objetivos y auditables.

8.8.1 Reportes personalizados

La plataforma eAlicia permite la generación de reportes tanto de forma automática como bajo demanda, garantizando la disponibilidad continua de información precisa y actualizada. Estos reportes pueden exportarse en múltiples formatos, incluyendo PDF, XLSX, JSON y CSV, y es posible programar su envío periódico para asegurar la distribución regular de la información a los equipos correspondientes.

Cada cliente dispone de plantillas personalizadas y criterios de evaluación adaptados a sus procesos, lo que asegura que los reportes reflejen de manera exacta sus necesidades operativas, métricas internas y estándares de calidad.

8.8.2 Analítica avanzada

Los módulos analíticos de eAlicia permiten realizar evaluaciones avanzadas orientadas a la optimización del rendimiento y la toma de decisiones basada en datos. Entre sus principales capacidades se incluyen:

- **Comparación del desempeño** entre diferentes BPOs, centros de contacto o unidades operativas.
- **Identificación de patrones y oportunidades de mejora continua**, mediante análisis detallados y correlaciones significativas.
- **Examen de la evolución histórica de métricas clave**, facilitando el seguimiento de tendencias y la detección temprana de desviaciones.
- **Integración de datos con sistemas externos de Business Intelligence (BI)** a través de la API, permitiendo consolidar la información en plataformas analíticas corporativas.

Estos módulos ofrecen una visión completa y estratégica del rendimiento, contribuyendo a la eficiencia operativa y a la mejora sostenida de los niveles de calidad.

8.9 Gobernanza y Continuidad

Políticas de Backup

La plataforma cuenta con políticas de respaldo definidas para garantizar la disponibilidad, integridad y recuperación oportuna de la información crítica. Estas políticas incluyen:

- **Frecuencia de Copias de Seguridad:**

  Se realizan **backups diarios**, asegurando la captura regular y actualizada de los datos esenciales.

- **Retención de Información:**

  Los respaldos se conservan durante un período de **90 días**, en cumplimiento con las políticas internas de continuidad y los requisitos acordados con los clientes.

- **Replicación Geográfica:**

  Los datos respaldados se replican de forma segura entre los centros de datos de **VODAFONE** y **COLT**, garantizando resiliencia ante fallos locales y disponibilidad en escenarios de contingencia.

- **Verificación y Pruebas de Restauración:**

Se llevan a cabo **restauraciones de prueba de manera anual**, con el fin de validar la integridad de los backups y asegurar la efectividad de los procedimientos de recuperación ante desastres.

Estas medidas contribuyen a un marco robusto de continuidad operativa conforme a las buenas prácticas internacionales y a los controles establecidos en **ISO 27001**.

8.9.1 Monitorización y soporte

El Security Operations Center (SOC) y el Network Operations Center (NOC) de GRUPO MST aseguran la monitorización continua (24/7) del estado de los servicios críticos, abarcando parámetros de disponibilidad, rendimiento y seguridad.

Esta supervisión permanente permite la detección temprana de incidentes, el análisis proactivo de anomalías y la aplicación de medidas correctivas o preventivas en tiempo real.

Además, se aplican indicadores y métricas de SLA (Service Level Agreement) orientados a garantizar niveles de servicio exigentes, con objetivos de disponibilidad superiores al 99,9%, en línea con las mejores prácticas del sector y los controles de gobernanza tecnológica establecidos en marcos como **ISO 27001**.

8.9.2 Gestión del ciclo de vida

Cada componente de la plataforma sigue un **ciclo de vida documentado** que abarca las fases de **desarrollo**, **pruebas**, **despliegue** y **revisión**, asegurando la calidad, estabilidad y trazabilidad de los cambios introducidos.

Los cambios se gestionan mediante un **sistema formal de control de versiones** y requieren **revisión por pares (peer review)** antes de su aprobación, garantizando la integridad del código, la detección temprana de errores y el cumplimiento de los estándares internos de desarrollo seguro.

Todos los registros asociados al proceso —incluyendo evidencias de pruebas, aprobaciones, versiones, incidencias y documentación técnica— se **conservan durante un período de cinco años** para permitir su consulta en procesos de **auditoría interna o externa**, cumpliendo con los requisitos establecidos por los controles de **ISO 27001** y buenas prácticas de DevSecOps.

8.9.3 Plan de continuidad y contingencia

GRUPO MST dispone de **procedimientos documentados y consolidados de Recuperación ante Desastres (DRP)**, diseñados para garantizar la continuidad operativa y la rápida restauración de servicios en escenarios de contingencia. Estos procedimientos se estructuran conforme a las buenas prácticas internacionales y están **certificados bajo el estándar ISO 22301 de Continuidad de Negocio**.

Entre las capacidades implementadas se encuentran:

- **Conmutación Automática (Failover):**

  Mecanismos de conmutación automática que permiten restaurar servicios de forma inmediata ante fallos críticos o indisponibilidad de un componente del sistema.

- **Protocolos de Notificación a Clientes:**

  Procedimientos formales de comunicación que aseguran la **notificación oportuna a los clientes** en caso de incidente grave, siguiendo los canales establecidos en el Plan de Continuidad.

- **Ensayos y Simulacros anuales:**

  La organización realiza **simulacros de recuperación anual**, validando la eficacia de los procedimientos, la capacidad de respuesta y la coordinación de los equipos implicados.

- **Almacenamiento Redundante en Múltiples Zonas:**

  La infraestructura dispone de **almacenamiento redundante** distribuido en **múltiples zonas geográficas**, reduciendo el riesgo de pérdida de datos y mejorando la resiliencia operativa.

Estos mecanismos permiten asegurar la disponibilidad de los servicios ante eventos disruptivos y cumplen con los requisitos de las normas **ISO 22301** e **ISO 27001**, fortaleciendo la continuidad y la seguridad de la información.

8.10 Auditorías Éticas y Gestión de Sesgos

GRUPO MST promueve el **uso responsable, seguro y ético de la inteligencia artificial**, garantizando que todas las soluciones basadas en IA implementadas en eAlicia cumplan con los principios de **equidad, transparencia, trazabilidad, responsabilidad y fiabilidad**.

Todas las funcionalidades de IA desplegadas en la plataforma se someten a **auditorías éticas internas**, en las que se evalúan aspectos clave como:

- **Equidad y ausencia de sesgos discriminatorios.**
- **Transparencia en los modelos y trazabilidad de decisiones.**
- **Fiabilidad, robustez técnica y comportamiento predecible.**
- **Cumplimiento del principio de minimización de datos y privacidad por defecto (RGPD).**

Cuando corresponde, las implementaciones se alinean con los requisitos del **Reglamento de IA de la Unión Europea (AI Act)**, incluyendo:

- Clasificación del riesgo del sistema.
- Documentación técnica obligatoria.
- Supervisión humana efectiva.
- Gestión continua del ciclo de vida del modelo.
- Evaluaciones de riesgo y registros operativos.

Este marco garantiza que el uso de IA en eAlicia contribuya a mejorar la calidad y eficiencia del servicio **sin comprometer los derechos fundamentales** de las personas.

8.10.1 Identificación y mitigación de sesgos

GRUPO MST aplica un enfoque sistemático para la detección y corrección de sesgos en los modelos de IA, asegurando un funcionamiento justo y no discriminatorio.

Las acciones principales incluyen:

- **Detección de sesgos lingüísticos, culturales y de género:**

Se realizan análisis periódicos para identificar desviaciones que puedan afectar a colectivos específicos o influir de manera no justificada en los resultados del sistema.

- **Validación y revisión humana continua:**

  Los resultados generados por los modelos se someten a supervisión humana periódica, incluyendo calibraciones mensuales, con el objetivo de evitar automatismos que puedan producir decisiones discriminatorias o impactos no deseados sobre los interesados.

Este enfoque se alinea con los principios de equidad, transparencia y responsabilidad proactiva establecidos por el RGPD, así como con los mecanismos de gestión de riesgos y supervisión humana exigidos por el AI Act.

8.10.2 Supervisión continua

Los modelos de IA desplegados en eAlicia están sujetos a un proceso continuo de vigilancia para garantizar su rendimiento adecuado a lo largo del tiempo.

Las principales acciones incluyen:

- **Monitorización en producción:**

  Los modelos se supervisan de manera constante con el fin de detectar desviaciones, anomalías, pérdidas de fiabilidad o degradación del rendimiento.

- **Evaluación periódica de métricas de equidad:**

  Los indicadores de equidad y comportamiento justo se comparan periódicamente con *benchmarks* internos y externos, permitiendo verificar que el rendimiento del modelo continúa siendo equilibrado y no discriminatorio.

Este proceso garantiza que los sistemas de IA mantengan su integridad, estabilidad y equidad durante todo su ciclo de vida operativo.

8.10.3 Documentación técnica: Models Cards

Cada modelo de inteligencia artificial utilizado en eAlicia dispone de su correspondiente ***model card***, un documento técnico estructurado que garantiza la transparencia, trazabilidad y comprensión del comportamiento del sistema. Estas *model cards* incluyen información esencial sobre:

- **Objetivo y alcance del modelo:**

  Se especifica la función concreta del modelo, los escenarios de uso previstos, los casos excluidos y las condiciones necesarias para su funcionamiento adecuado.

- **Dataset de entrenamiento:**

  Se describe el origen, composición, características y criterios de preparación del conjunto de datos utilizado para entrenar el modelo, incluyendo prácticas de curación, limpieza y balanceo.

- **Limitaciones y riesgos conocidos:**

  Se detallan las limitaciones técnicas, el margen esperado de variabilidad, posibles sesgos residuales, y los riesgos identificados durante las pruebas y auditorías.

- **Controles de mitigación aplicados:**

  Se documentan las medidas adoptadas para reducir sesgos, mejorar la equidad, reforzar la seguridad, asegurar la robustez del sistema y mantener el cumplimiento regulatorio.

Las *model cards* forman parte de la documentación oficial exigida por los marcos regulatorios actuales, contribuyendo a la **transparencia**, la **responsabilidad proactiva** y la **supervisión humana efectiva**, en línea con los principios del **AI Act** y del **RGPD**.

8.11 Roadmap Tecnológico

El plan de evolución de eAlicia contempla:

- **IA explicable (XAI)** para mayor transparencia.
- **Modelos multimodales** capaces de analizar texto, audio e imagen.
- **Análisis emocional y de tono** mediante redes neuronales de prosodia.
- **Predicción de satisfacción (Customer Sentiment Forecasting)**.
- **Automatización avanzada del proceso de auditoría**, siempre bajo supervisión humana.

8.11.1 Mejora continua

GRUPO MST mantiene una política de mejora contínua sustentada en:

- Innovación tecnológica constante.
- Auditorías periódicas.
- Retroalimentación de clientes.
- Cumplimiento normativo actualizado.

8.12 Declaración de Conformidad Técnica y Legal

GRUPO MST, como titular y responsable del desarrollo y mantenimiento de la plataforma **eAlicia**, declara que:

1. La infraestructura, los procesos y las tecnologías descritas en este documento cumplen con los estándares europeos e internacionales aplicables en materia de seguridad, privacidad y uso ético de la inteligencia artificial.
2. Los datos tratados se mantienen en entornos de *private cloud* ubicados exclusivamente en países de la Unión Europea y no se transfieren a terceros países fuera del Espacio Económico Europeo.
3. Las operaciones de tratamiento cumplen con el **GDPR**, la **LOPDGDD**, el **AI Act**, el **ENS**, la **ISO 223201**, la **ISO 27001**, el **SOC 2 Type II** y el **NIST SP 800-53**.
4. Todos los modelos de IA empleados han sido auditados internamente, cuentan con supervisión humana y documentan sus métricas de equidad y transparencia.

5. GRUPO MST mantiene un compromiso continuo con la mejora de la seguridad, la calidad y la ética en el desarrollo de soluciones tecnológicas.

9 Comunicaciones

- Se han implementado sistemas y procesos para comunicar los resultados de las investigaciones sobre incidentes de ciberseguridad, si las hubiere, y la respuesta a incidentes.
- Se comunicará con prontitud al CLIENTE los resultados de las investigaciones sobre la respuesta a incidentes de ciberseguridad.
- La comunicación se efectuará enviando un mail al contacto del CLIENTE. Esta dirección de correo electrónico deberá facilitarla el CLIENTE en el momento de activar este servicio.