Términos de seguridad de eAlicia.com

Sistema de Gestión de Seguridad de la Información – SGSI

Fecha de emisión:	julio de 2025
Responsable:	RunCall Systems, S.L.

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 CPDs de países de la Unión Europea.*

1 Seguridad del sitio físico y entorno

Las medidas de seguridad del CPD, donde se encuentran los servidores, incluyen áreas y zonas de seguridad establecidas. En estas zonas se almacenarán tanto los DTPS como el resto de la información clasificada como confidencial:

- ISO/CEI 27001:2013 | Gestión de la seguridad de la información
- ENS - Certificado de conformidad del Esquema Nacional de Seguridad
- ISO 9001:2015 | Sistema internacional de gestión de la calidad
- ISO 22301:2012 | Gestión de la continuidad del negocio
- ISO 14001:2015 | Gestión medioambiental
- 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.
- Firewalls de ultima generación, redundados y en HA, con múltiples capas y políticas de seguridad independientes por servicio
- Switchs de comunicaciones, redundados y en HA
- Conectividad con fibra óptica
- Segmentación de la red
- 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 perimetrales de gama alta, redundados y en HA, siempre actualizados con la última versión, y controles de acceso 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 software dedicado
- 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

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
- Ultimas versiones de Sistema Operativo y parches aplicados

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 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.
- 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.
- Bloqueos de pantalla automáticos después de un período de inactividad definido
- Bloqueos de pantalla protegidos con contraseña

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 proceso de autenticación segura y fiable.
- 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 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.

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 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

La seguridad de los modelos en eAlicia IA se enfoca en la protección de datos y el cumplimiento normativo mediante los siguientes puntos clave:

- **Entrenamiento Local de Modelos de IA**: Los modelos de eAlicia IA se entrenan localmente y sin conexión a internet, asegurando que los datos sensibles no sean transferidos a terceros ni expuestos a la red pública.
- **Uso de Datos Controlados y Específicos**: Los modelos se adaptan y entrenan con datos históricos específicos del sector y datos contractuales del cliente, no con modelos genéricos de internet, lo que garantiza la relevancia y el control de la información.
- **Anonimización y Pseudonimización**: La información identificable de los clientes se anonimiza y pseudonimiza durante el análisis para reducir los riesgos de exposición.
- **Políticas Claras de Retención de Datos**: Se establecen políticas transparentes para la eliminación segura de información sensible una vez que ya no es necesaria.

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.