	Nombre Aplicación 1	Intiza
	Descripción aplicación 1	Sistema para la gestión de cobranzas.

ID	Descripción del requerimiento	Respuesta / Comentarios de la empresa en revisión
Aplicación		
APL.01	¿Cuál es el origen de su software de aplicación? ¿Desarrollado internamente, paquete comprado?	Desarrollo propio
APL.02	Enumere todos los componentes/dependencias de su aplicación, incluyendo: - Sistema operativo (incluya la versión) - Base de datos (incluya la versión) - Servidor web (si procede, incluya la versión) - Lenguajes de programación/lenguajes de script (incluya la versión) - Plugins del navegador/aplicaciones de ayuda: programas Java, Silverlight, Flash, Shockwave y otros programas de ayuda personalizados. - cualquier cliente (pesado o ligero) que deba instalarse en el equipo cliente - cualquier otro código instalado en el servidor o en el equipo cliente	- Sistema operativo (incluya la versión) : Windows Server 2022 versión datacener - Base de datos (incluya la versión) : Sql server - Servidor web (si procede, incluya la versión) : IIS - Lenguajes de programación/lenguajes de script (incluya la versión) : (c#.net Netframwork 4.7 y react js version 18.3.1) - Plugins del navegador/aplicaciones de ayuda: programas Java, Silverlight, Flash, Shockwave y otros programas de ayuda personalizados. : (no aplica) - cualquier cliente (pesado o ligero) que deba instalarse en el equipo cliente : (no aplica) - cualquier otro código instalado en el servidor o en el equipo cliente : (no aplica)
APL.03	¿Sus aplicaciones de negocio internas están separadas de las aplicaciones que contienen datos de negocio de los clientes?	Si.
APL.04	¿Puede su personal utilizar IDs privilegiados para administrar/soportar el entorno desde cualquier dispositivo que no sea propiedad/gestionado por la empresa? En caso afirmativo, ¿cómo se habilita esa capacidad	No.
APL.05	¿Utiliza instancias/infraestructura de bases de datos dedicadas o compartidas multiarrendatario / multi tenant?	La instancias de bases de datos son compartidas con separación lógica entre clientes. En caso de requerirse puede implementarse una instancia dedicada (tiene costo adicional)
APL.06	¿El aplicativo usa alguno de los siguiente protocolos de SSO: Open ID Connect (OIDC), SAML 2.0, Oauth 2.0 Bearer Token ? ¿Si no, cual forma de autenticación utiliza?	Si.

APL.07	Qué requerimiento de contraseña utilizada la aplicación (si no existe SSO): Longitud mínima Número máximo de intentos no válidos Días mínimos permitidos antes del cambio de contraseña Historial de contraseñas Duración del bloqueo Intervalo de cambio de contraseña (nº de días antes de que el sistema le obligue a cambiar la contraseña) Bloqueo de ids inactivos Eliminación de ID inactivos Contraseñas ocultas al introducirlas ¿Contienen caracteres alfabéticos, numéricos, mayúsculas, minúsculas, símbolos?	La estructura de la contraseña se configura para cada cliente ajustandonos a sus políticas de contraseñas. La aplicación permite configurar todos los puntos mencionados. Son parámetros de configuración que se establecen con el cliente durante la implementación de la herramienta.
APL.08	¿Puede configurarse la aplicación para forzar tiempos de salida (timeout) del ID por inactividad del usuario o por tiempo de uso? Si hay un tiempo de salida del sistema por defecto, por favor indique cuál es el valor del tiempo de espera.	Si. Forma parte de los parámetros de configuración que se establecen con el cliente.
APL.09	¿Permite el software crear nuevos roles de permiso de usuario que incluyan/excluyan diferentes combinaciones de funciones del sistema? Por ejemplo: un rol que permita sólo la lectura de ciertas funciones y la actualización de otras funciones.	Si
APL.10	Proporcione un informe de muestra que enumere los usuarios y las funciones de permiso de usuario asignadas al usuario. Proporcione un informe de muestra que enumere las funciones del sistema permitidas en cada función de permiso de usuario. Proporcione un informe de muestra que muestre los ajustes de seguridad de la aplicación y los ajustes de configuración.	En el sistema existen los siguientes permisos de usuario: - Usuario administrador: acceso full a datos, configuración y gestión de usuarios. - Usuario solo lectura: solo puede visualizar y puede limitarse por segmentos. - Usuario invitado al cual está asociado una serie de permisos que se habilitan o deshabilitan según se requiera. Durante la implementación se definen con Primax los roles a estableccer y los permisos de usuario requeridos para cada rol.
APL.11	¿Podría facilitarnos una muestra de los registros de auditoría de la actividad de los usuarios de la aplicación (altas/bajas/modificaciones de registros empresariales)? ¿Incluyen estos registros: quién realizó la acción (nombre/identificación), cuándo se realizó la acción (fecha/hora), qué se modificó (tabla, registro, elemento de datos?), valor antes y después? ¿Es inmutable el registro? (¿Cómo se protege el registro para que nadie pueda modificarlo?)	Adjunto: Imagen Registro de actividad de usuarios.png El registro incluye fecha, hora, usuario que ejecutó, acción ejecutada y sobre que cliente se ejecutó la acción.Estos registros solo se pueden acceder en modo lectura desde la aplicación.

APL.12	¿Podría facilitar una muestra de los registros de actividad de auditoría de la actividad administrativa de la aplicación (añadir/eliminar/modificar la gestión de usuarios, la configuración del sistema, etc.)? ¿Incluyen estos registros: quién realizó la acción (nombre/identificación), cuándo se realizó la acción (fecha/hora), qué se modificó (tabla, registro, elemento de datos?), valor antes y después? ¿Es inmutable el registro? (¿Cómo se protege el registro para que nadie pueda modificarlo?)	Adjunto: Imagen Registro de actividad Admin - Configuración.png Imagen Registro de actividad Admin - Alta usuario.png
APL.13	Describa las prácticas de codificación de aplicaciones utilizadas, más concretamente, las siguientes: - Prácticas de codificación seguras basadas en normas del sector (indique qué norma), - Revisiones manuales del código por parte interna o externa - Herramientas utilizadas para revisar y probar el código y la aplicación - ¿Realiza análisis o utiliza otras prácticas de revisión del código?	Adjunto norma de desarrollo seguro donde se detallan los lineamientos que aplicamos: NO-SI-21 Desarrollo seguro_v3_2024-07-10.pdf
APL.14	¿Cómo protege el código fuente de aplicaciones, programas, macros, ejecutables, API, scripts, etc. de accesos y actualizaciones no autorizados? ¿Utiliza software de control de código fuente? Describa las prácticas de control de código fuente. ¿En qué entorno/segmento de red tiene lugar la codificación del desarrollo y la gestión del código fuente? ¿Se realiza en la misma red que los sistemas empresariales internos o en la zona de aplicaciones en la nube del cliente o en algún otro lugar (descríbalo)?	Adjunto: - NO-SI-21 Desarrollo seguro_v3_2024-07-10.pdf - NO-SI-09 - Gestión de ambientes_2024-07-10_v1.2.pdf - NO-TI-04 Gestión de Cambios_v2.2_2025-10-28.pdf
APL.15	Describa el proceso de desarrollo y lanzamiento de una nueva versión de software de su aplicación, incluidos los procesos de gestión de cambios del sistema, comunicación con el usuario, control de calidad, pruebas de aceptación del usuario y puesta en marcha.	Adjunto: - NO-SI-21 Desarrollo seguro_v3_2024-07-10.pdf - NO-SI-09 - Gestión de ambientes_2024-07-10_v1.2.pdf - NO-TI-04 Gestión de Cambios_v2.2_2025-10-28.pdf
APL.16	Describa las medidas de seguridad y control de acceso en entornos de prueba de aplicaciones. ¿Utiliza datos reales en entornos de desarrollo/aceptación/prueba?	Los entornos de prueba están separados de desarrollo y producción. No se utilizan datos reales para pruebas, solo se usan datos ficticios. Adjunto: - NO-SI-21 Desarrollo seguro_v3_2024-07-10.pdf - NO-SI-09 - Gestión de ambientes_2024-07-10_v1.2.pdf - NO-TI-04 Gestión de Cambios_v2.2_2025-10-28.pdf

APL.17	¿Incluye la aplicación algún ID o contraseña por defecto que no se pueda cambiar? En caso afirmativo, describa en qué circunstancias se utilizaría este ID.	No.
APL.18	¿Se han realizado pruebas de vulnerabilidad y/o penetración en la programación de la aplicación? ¿Son estas pruebas únicamente escaneos informatizados con verificación humana o se realizan pruebas humanas por separado?	Si. Pruebas con escaneos informatizados y revisiones humanas por separado.
APL.19	¿Con qué frecuencia se realizan pruebas manuales y humanas de vulnerabilidad de las aplicaciones?	semestralmente.
APL.20	En el caso de las aplicaciones basadas en web, describa cómo se protegen las sesiones de usuario, incluidos, entre otros, el posible hijacking/breakin de sesión, las cookies maliciosas, la exposición a credenciales de usuario, etc.	Validación y Filtrado de Entradas. Autenticación y Control de Acceso Robustos. Gestión Segura de Sesiones. Manejo de Errores y Registros
APL.21	¿Es posible que una persona tenga varias sesiones de aplicación abiertas al mismo tiempo (es decir, que se utilice un identificador para más de una sesión)?	Es configurable de acuerdo a lo que se requiera.
APL.22	¿Está disponible la autenticación multifactor para los IDs de usuario final? En caso afirmativo, ¿qué forma de autenticación multifactor se utiliza?	Si. Se envía un código de verificación a la dirección de mail del usuario con el cual se autentica en la aplicación junto con usuario y contraseña.
APL.23	¿Su solución hace referencia o incluye código gestionado por terceros (es decir, a través de un iframe o inyectado mediante javascript en la página web)?	No.
APL.24	¿Quién gestionará el acceso de los usuarios de Primax al sistema?	Primax desde la aplicación con usuario administrador.
APL.25	¿Las contraseñas se almacenan utilizando un hash unidireccional o están cifradas? Si están cifradas, ¿qué nivel de cifrado se utiliza?	Hash unidireccional.
Aplicación Móvil		
MOV.01	¿Las aplicación móvil se instala unicamente por Google Play o Instalador de Aplicaciones de Apple?	Google Play y Apple
MOV.02	¿Se cuenta con autenticación de múltiples factores (MFA) para los usuarios de la aplicación móvil?	Si
MOV.03	¿Implementan medidas de seguridad como HTTPS/TLS para asegurar la comunicación entre la aplicación móvil y los servidores?	Si
MOV.04	¿Los datos de los usuarios se almacenan exclusivamente en servidores seguros? ¿Dónde están ubicados estos servidores?	Microsoft Azure - USA
MOV.05	¿Cómo gestionan el acceso a características sensibles del dispositivo, como la cámara, micrófono o ubicación?	No aplica para la appl.

MOV.06	¿Cómo aseguran que cada usuario tenga acceso únicamente a las funciones y datos necesarios?	Utiliza los mismos roles y perfiles de usuarios que la versión Web.
MOV.07	¿Qué medidas adoptan para proteger la aplicación móvil en redes inseguras, como Wi-Fi públicas?	Encriptación, HTTPS/TLS SHA256.
MOV.08	¿Qué métodos de encriptación utilizan para proteger los datos sensibles de los usuarios almacenados en sus aplicaciones móviles?	No aplica.
MOV.09	¿Realizan análisis regulares de código y pruebas de penetración en las aplicaciones móviles?	Si.
MOV.10	¿Qué controles implementan para asegurar que las APIs utilizadas por la aplicación móvil sean seguras y autentiquen a los usuarios y dispositivos correctamente?	Adjunto: NO-SI-20 Cifrado de la Información_v1.1_2024-07-10.pdf
MOV.11	¿Siguen estándares reconocidos como OWASP Mobile Security Project para el desarrollo seguro?	Si