ID	Descripción del requerimiento	Respuesta / Comentarios de la empresa en revisión
POL.01	¿A los empleados se les permite trabajar desde redes públicas / sitios públicos o wifi? ¿Qué seguridad es suministrada a esta conectividad?	Adjunto nuestra norma de teletrabajo. NO-TI-02- Teletrabajo_V2.1_2025-05-15.pdf
POL.02	¿Se bloquean los computadores de la empresa para evitar que se instale en el computador software no autorizado e imponer el uso de antivirus?	Si. Adjunto: NO-SI-06- Escritorio y Pantallas limpias_v2.1_2024-11-27.pdf
POL.03	¿Están protegidos todos los computadores y servidores con software antivirus o software de seguridad similar para evitar la ejecución de virus u otro software malicioso?	Si. Adjunto: NO-TI-03- Software Malicioso_v2.1_2025-05-02.pdf
POL.04	¿Utiliza algún software de protección contra fuga/pérdida de datos (DLP) en su entorno?	Disponemos de un conjunto de Software que cumplen la funcion de DLP.
POL.05	¿Prohíbe al personal conectar dispositivos de almacenamiento externo (por ejemplo, memorias USB) a sus computadores? ¿En qué circunstancias se permiten los dispositivos de almacenamiento externo?	Está prohibido el uso de dispositivos de almacenamiento externo y bloqueados los puertos de todos los equipos para la conexión de los mismos.
POL.06	¿Qué comprobaciones de antecedentes se exigen al personal que presta soporte o tiene acceso a datos y sistemas de la compañía?	Adjunto nuestra norma NO-RH-01 Contratación de Recursos Humanos_v2.1_2025-04-30.pdf donde se detallan los aspectos que se revisan para la contratación.
POL.07	¿Todo el personal, incluidos terceros, y contratistas utilizados para prestar servicio de TI, debe firmar acuerdos de confidencialidad para proteger la información de la compañía?	Si. Todos nuestros colaboradores firman un NDA, el código de ética y el documento de inducción de Seguridad de la Información. Adjunto: NO-SI-07- Contratación, Seguridad y Control de Proveedores_v2.1_2024-10-15.pdf
POL.08	¿Existe una persona o grupo claramente definido que sea responsable de la gestión de los controles y que tenga autoridad para garantizar que se aplican políticas de control eficaces? ¿Quién(es)?	Si. En Intiza contamos con un área de Seguridad de la Información, a cargo de un CISO, que lleva adelante toda la gestión de seguraidad (SGSI) de la compañía. Nuestro SGSI está alineado con las normas ISO 27001, en la cual estamos certificados.
POL.09	Describa el programa de entrenamiento y concientización continua que posee la empresa sobre ciberseguridad para todos sus empleados y contratistas.	Adjunto: NO-SI-05- Concientizacion y Capacitacion de Seguridad_v2.1_14-11-2024.pdf
POL.10	¿Dispone de una política de contraseñas documentada y aplicada que deban seguir todos sus empleados/contratistas (proveedores)? (es decir, el número de caracteres, si se requieren mayúsculas y minúsculas, si se requieren símbolos especiales). ¿Se puede reutilizar una contraseña? ¿Cuántos días hay que esperar para cambiar la contraseña?) Por favor, describa todos los ajustes de contraseña en su política.	Si. Adjunto NO-SI-03 - Gestión de Contraseñas.pdf Adicionalmente, nuestros sistemas críticos están integrados a nuestro gestor de direcciones por SSO, desde donde se establece por sistema que las contraseñas cumplan con un largo mínimo de 8 caracteres, que contenga mayusculas minusculas y caracteres especiales, como así también que se actualicen obligatoriamente en forma periodica.
POL.11	¿Todas las contraseñas por defecto/de instalación de los sistemas / aplicativos / dispositivos usados son cambiados antes de su entrada al ambiente de producción?	Si.
POL.12	¿Dispone de una política documentada que prohíba al personal compartir usuarios y contraseñas?	Si. Adjunto NO-SI-03 - Gestión de Contraseñas.pdf

POL.13	¿Dispone de una política documentada que garantice que todos los accesos a sus sistemas son aprobados y revisados por el nivel de gestión adecuado?	Si. Adjunto: NO-SI-02- Gestión de Cuentas de Usuarios.pdf
POL.14	¿Dispone de certificaciones como SOC1, SOC2, ISO27001:2013? En caso afirmativo, ¿puede compartir una copia del informe detallado?	Si. Estamos certificados en ISO27001. Adjunto: Certificados 27001_2025.pdf
POL.15	¿Recopila o crea metadatos sobre los datos del cliente en el sistema? ¿Permiten a los clientes optar por no participar en la recopilación de datos / creación de metadatos?	No recopilamos ni creamos metadatos de clientes.
POL.16	Describa la política/procedimiento disponible que tiene para limitar el acceso a datos confidenciales y datos de clientes desde los dispositivos portátiles/móviles del personal del proveedor. (si el personal no tiene acceso a datos de clientes a través de dispositivos portátiles/móviles, indíquelo)	El personal de Intiza solo accede a información del cliente ante la necesidad de Soporte del mismo. De todas maneras contamos con una norma de seguridad en Dispositivos. Adjunto: NO-SI-26- Seguridad en Dispositivos Móviles_v1.1_02-05-2025.pdf
POL.17	¿Cuántos empleados trabajan para su empresa? Elija una de las siguientes opciones: <100 personas, 100-499 personas, 500-999 personas, 1000-4999 personas, 5000+ personas	<100 personas
POL.18	¿Cuántas personas (empleados, contratistas, etc.) componen el personal informático? Seleccione una de las siguientes opciones: <50 personas, 50-99 personas, 100-199 personas, 200-499 personas, 500-999 personas, 1000+ personas	<50 personas
POL.19	¿Cuánto personal no empleado se utiliza para implementar o proporcionar apoyo al ciclo de vida del sistema/servicio (es decir, 10%, 30%, etc.)	0%. Todo el personal es empleado de Intiza.
POL.20	Enumere los subcontratistas que tienen acceso a los datos y qué servicio se presta (es decir, empresa x - verificación de direcciones de correo, empresa b - servicios de centro de llamadas, empresa c - gestión de infraestructuras).	Microsoft Azure - Servicio de nube.
POL.21	¿Qué proceso tiene para evaluar los requisitos de riesgo y control de todos los sistemas y aplicaciones utilizados para prestar su servicio?	Adjunto: NO-SI-04- Gestión de Riesgo del SGSI_2024-11-21_v3.0.pdf.
Cumplimiento		
CUM.01	¿De qué capacidades dispone para marcar y conservar datos con el fin de garantizar que los datos sujetos a litigios o investigaciones gubernamentales se conservan y están disponibles para su recopilación, en caso necesario? ¿Se trataría de una solución a medida? ¿Existen funciones integradas de eDiscovery diseñadas para gestionar la conservación o recopilación de datos?	Se siguen los lineamientos de nuestras políticas: PO-SI-02- Proteccion de Datos Personales_v1.2_13-11-2024.pdf y NO-SI-15 Resguardo y Recupero de la Información_2024-07-16_v1.1.pdf.
CUM.02	Explique cómo cumplen sus sistemas y procesos con legislaciones sobre privacidad de datos.	Se siguen los lineamientos de nuestra política PO-SI-02- Proteccion de Datos Personales_v1.2_13-11-2024.pdf.
CUM.03	Enumere (o facilite una lista) de los campos de identificación personal capturados por el sistema	Los campos que se gestionan en el sistema son configurados de acuerdo a las necesidades de cada cliente Los mismos son datos de clientes (nombre, razon social, cuit/documento de identidad, datos de contacto -telef, email, dirección) y datos de facturación asociadas a dichos clientes (nro de factura, monto, estado)

ID	Descripción del requerimiento	Respuesta / Comentarios de la empresa en revisión
Acceso a infraestuctura		
AUT.01	Suministre el número de empleados del proveedor que tendrían acceso PERSISTENTE a los datos de Primax Con acceso de sólo lectura Con acceso administrativo	Ningún empleado tiene acceso persistente a los datos de clientes. Solo se accede desde la aplicación ante la necesitdad de soporte. A nivel Infraestructura solo accede el CTO con usuario administrador en caso de ser necesario.
AUT.02	Suministre el número de empleados del proveedor que tendrían acceso TEMPORAL (Sistema de gestión de identificación privilegiada - Checkin/Checkout) a los datos de Primax Con acceso de sólo lectura Con acceso administrativo	5 personas para realizar soporte.
AUT.03	Si alguien deja de trabajar en la empresa, ¿cuánto tiempo se tarda en eliminar el acceso físico e informático? ¿Realiza una revisión periódica del acceso (en caso afirmativo, con qué frecuencia realiza esta revisión)?	Al desvincularse un colaborador se deshabilitan todos sus accesos en el mismo día de su desvinculación. Contamos con un control automático que realiza la revisión de accesos (hay un proceso que se ejecuta c/ 1 hora).
AUT.04	¿Los IDs privilegiados son solicitados y usados cuando se necesitan o se concede el acceso todo el tiempo al personal de soporte?	Solo cuando se necesita.
AUT.05	¿Se comparten los IDs privilegiados? En caso afirmativo, ¿cómo se gestiona la responsabilidad individual?	No. No se comparten usuarios.
AUT.06	¿Registra el uso y la actividad de los IDs privilegiados, Superusuario y/o Administrador para la Infraestructura?	Si.
AUT.07	¿Con qué frecuencia se revisan los registros de uso y actividad de los IDs privilegiados para comprobar que su uso es adecuado (es decir, que las actividades son coherentes con la necesidad documentada de utilizar estos IDs)?	Cada 6 meses.
AUT.08	¿Utiliza la autenticación multifactor para el uso de IDs privilegiados utilizados por su personal? En caso afirmativo, ¿para qué se utilizan? ¿Cuáles son los factores de autenticación múltiple utilizados (además del identificador/contraseña)?	Todos nuestros accesos tienen activados el doble factor de autentificación a travez de Microsoft Authenticator.
Manejo de datos (backups, restauración, encripción)		
MGD.01	¿Cuál es su metodología de copia de seguridad? ¿Está utilizando copias de seguridad incrementales diarias con una copia de seguridad completa semanal o está utilizando copias de seguridad continuas con replicación casi en tiempo real a otro sitio?	Se realiza backup completo en forma diaria. Adjunto norma: NO-SI-15 Resguardo y Recupero de la Información_2024-07-16_v1.1.pdf

MGD.02	¿Quién es responsable de garantizar que los trabajos de copia de seguridad se realizan correctamente, que las copias de seguridad se mantengan durante los periodos de tiempo establecidos y que las copias de seguridad se destruyan adecuadamente tras el periodo de conservación? Describa el proceso para garantizar que las copias de seguridad se realizan cuando están programadas y pueden utilizarse correctamente para la restauración, cuando sea necesario.	Adjunto: NO-SI-15 Resguardo y Recupero de la Información_2024-07-16_v1.1.pdf El proceso está descripto en el adjunto.
MGD.03	¿Existe un proceso de archivo periódico o de purga periódica de datos? En caso afirmativo, describa las opciones de configuración disponibles (¿por periodo de tiempo? conservar durante x días tras la entrega del pedido, etc.)	Mientras el cliente esté activo, solo se elimina información del mismo ante un pedido formal del Cliente solicitando dicha eliminación. Al finalizar el contrato con un cliente, se elimina la información de dicho cliente luego de pasados los 30 días de finalización del contrato. Adjunto: NO-SI-19 Retención y Eliminación de Información_v2.1_2025-02-25.pdf
MGD.04	Si Primax dejara de utilizar su servicio, ¿cómo podría obtener una copia de los datos y cómo se eliminarían o destruirían posteriormente?	La aplicación permite generar un backup de sus datos en cualquier momento que el usuario lo requiera. En caso de dejar de utilizar el servicio la información queda disponible para generar una copia por 30 días a partir de la fecha de baja del servicio.
MGD.05	¿Cómo aíslan y protegen los datos de Primax de los de otros clientes?	Existe una separación lógica de datos. El id de acceso contempla la combinación de: Empresa-Usuario-contraseña
MGD.06	¿Se utiliza el cifrado para proteger los datos en reposo (db, archivos, soportes de copia de seguridad)?	Si. Adjunto: NO-SI-20 Cifrado de la Información_v1.1_2024-07-10.pdf
MGD.07	¿Codifica los datos en tránsito por la Internet pública, así como durante las transferencias de archivos o datos a través de su red? ¿Qué tipo de método de cifrado se utiliza? ¿Se cifran los datos mientras el servidor/dispositivo de almacenamiento está encendido?	Si. Adjunto: NO-SI-20 Cifrado de la Información_v1.1_2024-07-10.pdf
MGD.08	¿Puede Primax alojar las claves de cifrado dentro de nuestro cortafuegos (mantener su propia clave)?	No.
MGD.09	¿La clave de cifrado es específica de Primax o se utiliza la misma clave para los datos de varios clientes?	Se gestionan por cada unidad de BBDD, Pueden ser compartidas con otros clientes.
MGD.10	¿Quién tiene acceso a la clave de cifrado (proveedor de IaaS? ¿Otro?) Aproximadamente, ¿cuántas personas tienen acceso para ver la clave de cifrado?	Solo el Administrador de la Infraestructura.
MGD.11	¿Las claves de cifrado se almacenan en un HSM (módulo de almacenamiento de hardware) o en algún otro método?	Microsoft Azure.
MGD.12	¿Con qué frecuencia se rotan las claves de cifrado?	6 meses
MGD.13	¿Puede realizar copias de seguridad en un almacenamiento inmutable (inalterable) que no sea vulnerable a ciberataques?	Las copias de seguridad se realizan bajo estrictas normas de seguridad de Microsoft Azure en diferentes locaciones.
Infraestructura y disponibilidad		
INF.01	¿Quién proporciona los servicios de infraestructura? ¿Cuál es el alcance de los «servicios»?	Intiza gestiona el servicio de infraestructura en la nube de Microsoft Azure.

INF.02	¿De qué mecanismos dispone para proteger la infraestructura y las aplicaciones de las ciber amenazas (por ejemplo, antivirus, intrusión en host, cortafuegos personal, etc.)?	Utilizamos la suite de Microsoft (Sentinel, Defender for endpoint, Defender for cloud, WAF, Firewalls, etc.) Adjunto: NO-SI-23 Seguridad en Telecomunicaciones_2024-12-30_v2.1 (1).pdf
INF.03	¿Mantiene registros lo suficientemente detallados como para identificar quién hizo un cambio, la fecha/hora del cambio y específicamente qué campo cambió?	Si. Adjunto: NO-SI-12- Monitoreos de Eventos y Análisis de Logs_2025-02-24_v2.1.pdf
INF.04	¿Cómo evitar que los administradores añadan, modifiquen o eliminen registros del registro de auditoría?	Los registros de auditoría no pueden ser modificados. Adjunto: NO-SI-12- Monitoreos de Eventos y Análisis de Logs_2025-02-24_v2.1
INF.05	Describa su plan de recuperación en caso de desastre (DRP)	Adjunto: PO-TI-01- Continuidad de Procesamiento de Datos_v2.1_2024-11-25.pdf
INF.06	Describa su Plan de Continuidad de Negocio	Adjunto: PO-TI-01- Continuidad de Procesamiento de Datos_v2.1_2024-11-25.pdf
INF.07	¿Con qué frecuencia se realizan pruebas de penetración para evaluar la seguridad de sus entornos corporativos? ¿Las pruebas de penetración las realiza un consultor externo o el departamento interno de TI? Indique los nombres de los servicios de consultoría utilizados. ¿Las pruebas se realizan exclusivamente con escáneres automatizados o también se recurre a evaluadores humanos?	Se realizan pruebas de pentetración cada 6 meses. Con consultor externo al menos 1 vez en el año. Adjunto: NO-SI-13 Gestión de Vulnerabilidades y Parches_v2.1_2024-08-09.pdf
INF.08	¿Está autorizado Primax a realizar nuestra propia evaluación de vulnerabilidades de su servicio en un entorno que no sea de producción?	Si.
INF.09	Comparta los resultados de su última evaluación de vulnerabilidad o certificación de una empresa de evaluación de vulnerabilidad, indicando la fecha de la última evaluación y el resumen de los resultados. Describa su proceso de revisión interna de los resultados y el proceso de gestión del proceso de corrección.	Adjunto último informe de Pentest: 20251028-INTIZA-Informe Ejecutivo-Pentest-Externo - V1.3 (2).pdf y norma de gestión de vulnerabilidades: NO-SI-13 Gestión de Vulnerabilidades y Parches_v2.1_2024-08-09.pdf.
INF.10	Describa su política de aplicación de parches a sistemas operativos y tecnología intermedia (middleware).	Adjunto: NO-SI-13 Gestión de Vulnerabilidades y Parches_v2.1_2024-08-09.pdf
Centro de Computo / Instalaciones de TI		
PHY.001	¿En qué países estarán ubicados los servidores de datos?	USA
PHY.002	¿Está certificado el centro de datos y, en caso afirmativo, según qué normas/certificaciones?	Microsoft Azure está certificado, entre otros, en ISO27001, SOC2, et.

PHY.003	Describa la seguridad física existente en las instalaciones donde se alojan y/o procesan los datos. (vigilancia, procedimientos de emergencia, seguridad física, controles de acceso físico y revisión de accesos, alarmas de humedad y fuego, aire acondicionado, luces de emergencia, generadores de respaldo, capacidad de UPS, etc.)	Los datos están en Microsoft Azure por lo que la seguridad física está delegada en ellos. Adjunto la norma de seguridad física de Intiza: NO-RH-02 Acceso y Control Físico.docx_v2.1_2025-02-28.pdf
PHY.004	¿Cómo se gestiona la eliminación de los dispositivos de almacenamiento de información que han llegado al final de su vida útil para evitar la divulgación de datos? ¿Cómo se impide la divulgación de registros archivados o eliminados del sistema?	Adjunto: NO-SI-19 Retención y Eliminación de Información_v2.1_2025-02-25.pdf
PHY.005	¿Se notificará a Primax si un centro de datos deja de estar disponible o si se cambian los servicios a otro centro de datos? ¿En qué plazo se notificará a Primax si se ha producido una conmutación por error en caliente (failover)? ¿Se producirá una conmutación por error en caliente (failover) a un centro de datos del mismo país que el centro de datos original?	Se informa a los clientes de cualquier cambio a partir de un evento de seguridad, no necesariamente así en caso de cambios por performance o alta disponibilidad. De todas maneras, las zonas son dentro del mismo pais.

le Primax

	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