Política de Privacidad



Este documento contiene información propietaria de Indexa S.A, Global Electronic Connection Bussiness S.A y Asesorías y Gerenciamientos de Servicios Ltda., que ha sido preparada estrictamente con el propósito de ser utilizada en las operaciones de las Empresas y no podrá ser proporcionada, refraseada o revelada parcial o totalmente a terceros sin la autorización expresa del Comité de Seguridad de la Información.

ÍNDICE

CSMS2000.1. INTRODUCCIÓN 3
CSMS2000.1.1. Objetivo 3
CSMS2000.1.2. Rol de la empresa: Encargada del tratamiento 3
CSMS2000.1.3. Alcance 3
CSMS2000.1.4. Roles y responsabilidad 3
CSMS2000.1.5. Comunicación 4
CSMS2000.1.6. Vigencia 4
CSMS2000.2. INFRAESTRUCTURA DE ALMACENAMIENTO (HOUSING) 5
CSMS2000.3. TRATAMIENTO DE DATOS 5
CSMS2000.3.1. Categoría de datos tratados 5
CSMS2000.3.2. Procesamiento de datos 5
CSMS2000.3.3. Consecuencias de no consentir o revocar el consentimiento para el tratamiento de sus datos personales 6
CSMS2000.3.4. Destinatarios y transferencia 6
CSMS2000.3.5. Medidas de seguridad aplicadas 6
CSMS2000.3.6. Comunicación con el titular de los datos 6
CSMS2000.3.7. Requerimiento de información 7
CSMS2000.3.8. Canal para reclamaciones 7
CSMS2000.3.9. Retención y destrucción segura 7
CSMS2000.3.10. Medición 7
CSMS2000.3.11. Monitoreo y control 7
CSMS2000.4. AUDITORÍAS EXTERNAS Y CUMPLIMIENTO 8
CSMS2000.5. POLÍTICAS 9
CSMS2000.6. REPORTE DE INCIDENTES O QUIEBRES 10
CSMS2000.7. CUMPLIMIENTO LEY MARCO DE CIBERSEGURIDAD (LEY N° 21.663) 11
CSMS2000.8. ACCIONES DISCIPLINARIAS 11
CSMS2000.9. DOCUMENTOS Y REFERENCIAS 11

CSMS2000.1. INTRODUCCIÓN

CSMS2000.1.1. Objetivo

El presente documento tiene por objeto transparentar de forma estricta el tratamiento de datos (recolección, almacenamiento y procesamiento) realizados por Indexa en su condición de proveedor de servicios de apoyo al giro bancario, especializado en la prestación de servicios operacionales y el diseño, provisión y mantenimiento de soluciones tecnológicas estructuradas bajo la modalidad de Software as a Service (SaaS).
Es importante recalcar, que esta política guarda estrecha relación con la de protección de personales de la organización, de seguridad, ciberseguridad y riesgo aplicando, además, en la gobernanza de la información el marco normativo de la Ley de Ciberseguridad y la de Protección de datos personales.

CSMS2000.1.2. Rol de la empresa: Encargada del tratamiento

Para todos los efectos emanados de la prestación de sus servicios, indexa asume de manera exclusiva la posición de Encargada del Tratamiento respecto de la totalidad de los datos personales almacenados, transmitidos o procesados en sus plataformas.

• responsable del Tratamiento: La Institución Financiera clienta conserva en todo momento la propiedad, control originario y condición de responsable del Tratamiento sobre los datos de sus clientes, usuarios finales o empleados.

• límites del Tratamiento: Indexa solo procesará los datos única y exclusivamente bajo las instrucciones específicas, formales y escritas del responsable, quedando estrictamente prohibida la utilización de dicha información para fines propios, comercialización o transferencias no autorizadas.

CSMS2000.1.3. Alcance

La presente política es de aplicación general y abarca todos los aspectos relacionados con la administración, distribución, control, acceso, almacenamiento, tratamiento y destrucción de datos de carácter personal sean estos de colaboradores propios de la organización y/o datos que como proveedor(encargado) se deba tratar única y exclusivamente para los fines acordados contractualmente para la prestación del servicio contratado, revisar en detalle alcances presentados en Política de protección de datos de la organización [1].

CSMS2000.1.4. Roles y responsabilidad

General

Son responsables de lo descrito en este documento: los comités corporativos *(continuidad, seguridad y riesgo)*, las gerencias, los administradores de la plataforma tecnológica y todos los funcionarios que utilicen, administren, traten, almacenen, y/o interactúen con datos personales.

Específicas

Gerencia de Desarrollo y tecnología: equipo multidisciplinario encargado de proporcionar todas las herramientas de almacenamiento, tratamiento, control, transmisión, destrucción y/o resguardo de datos personales, en formato digital.

[1] *CSMS1900_PI_Política global de protección de datos personales*

Gerencia de Operaciones: equipo multidisciplinario encargado de proporcionar el almacenamiento, tratamiento, control, transporte y resguardo de datos personales registrados de forma física, de los clientes Indexa.

RRHH y finanzas: área encargada de recopilar, almacenar, custodiar, actualizar y destruir la información de carácter personal de los funcionarios de indexa conforme a las especificaciones del ordenamiento jurídico vigente, además de resguardar su confidencialidad, disponibilidad e integridad.

Comité de Gerencia: equipo multidisciplinario responsable de velar por el resguardo, tratamiento, almacenamiento, protección y destrucción de los datos personales *(físicos y lógicos)* en alcance a su gestión, conforme a las especificaciones legales.

Comité de seguridad de la información: equipo multidisciplinario encargado de apoyar la gestión de datos de carácter personal conforme a la ley.

Contraloría: Responsable de evaluar de forma independiente el cumplimiento de la normativa, verificando la efectividad de los controles implementados, la adecuada gestión de riesgos, la correcta aplicación de los procedimientos y la integración del modelo con otros sistemas de control de la organización. Asimismo, deberá reportar sus conclusiones de auditoría a la alta dirección.

CSMS2000.1.5. Comunicación

El comité de seguridad de la información debe asegurar que todos los funcionarios que interactúen con datos personales estén debidamente familiarizados con esta política. Para esto, se efectuarán actividades de difusión y capacitación que mantengan informada a la organización respecto a la protección de datos, su manejo y administración.

CSMS2000.1.6. Vigencia

Esta política se encuentra vigente a partir de 22-09-2026, El Comité de Seguridad de la información quien es el propietario de este documento debe revisar y actualizar el mismo, al menos una vez al año o por directrices entregadas por la alta dirección o como consecuencia de

- Nuevas normas legales o reglamentarias o nuevos instrumentos internacionales.
- Actualización normativa vigente
- Cambios en los procesos, tecnologías o actividades de tratamiento
- Resultados de auditorías internas o externas
- No conformidad de la alta dirección y/o de órganos reguladores

Sin perjuicio de lo anterior, la Política deberá ser revisada, de manera inmediata, y modificada en su caso, cuando:

Cambios en el uso de datos: Si la organización empieza a recolectar nuevos tipos de información, o a utilizarla con fines distintos o a aplicarla en tecnologías basadas en inteligencia artificial.

Nuevos servicios o productos: El lanzamiento de un servicio, sitio web o funcionalidad requiere detallar qué datos se obtendrán a través de ella.

Alianzas con terceros: La integración de nuevos socios comerciales, plataformas de pago, herramientas de análisis o proveedores que accedan o procesen datos de los usuarios.

CSMS2000.2. INFRAESTRUCTURA DE ALMACENAMIENTO (HOUSING)

Con el objetivo de garantizar los más altos estándares de resiliencia, disponibilidad y continuidad operacional en los servicios SaaS prestados a instituciones financieras, Indexa contrata infraestructura de Data Center en modalidad de Housing. Este esquema asegura la máxima protección, confidencialidad y privacidad de los datos personales, en estricto cumplimiento de la normativa legal vigente.

Control Lógico Exclusivo: El Data Center contratado provee de manera exclusiva la seguridad perimetral física —incluyendo controles biométricos, vigilancia presencial y CCTV—, así como suministro eléctrico redundante y climatización ambiental. Indexa mantiene el control lógico absoluto, la administración y la gobernanza del software y de los sistemas operativos instalados en dichos racks privados, garantizando así el aislamiento técnico necesario para asegurar la privacidad, confidencialidad y protección de los datos personales gestionados.

CSMS2000.3. TRATAMIENTO DE DATOS

CSMS2000.3.1. Categoría de datos tratados

Según los servicios llevados a cabo por la organización y acuerdos contractuales con las instituciones financieras que son sus clientes, Indexa procesará de forma transitoria o permanente las siguientes tipologías de información:

- **Datos de identificación**: Nombre, RUT, claves de acceso (cifradas), dirección.
- **Datos financieros:** Líneas disponibles, Saldos de cuentas, historiales de transacciones, registros de transferencias, detalle de impuestos, remuneraciones, pagos.
- **Datos técnicos:** Direcciones IP, registros de auditoría (logs) del sistema, metadatos de transacciones.

La infraestructura y los servicios de Indexa excluyen estrictamente el tratamiento de datos sensibles de tarjetas de pago regulados por el estándar PCI-DSS. En consecuencia, la plataforma no cuenta con la autorización ni el diseño para capturar, procesar, transmitir o almacenar datos tales como el número de tarjeta (PAN), fecha de expiración o códigos de validación (CVV/CVC). Indexa asume la obligación de informar transparentemente a sus clientes sobre esta limitación, siendo responsabilidad de estos últimos garantizar que no se introduzcan dichos datos en el sistema.

CSMS2000.3.2. Procesamiento de datos

Finalidad

En el marco de los servicios prestados por Indexa a sus clientes, la organización recopila y procesa únicamente los datos personales que son indispensables para el desarrollo de las operaciones contratadas. Existiendo el compromiso a no tratar ninguna información que exceda las necesidades operativas de conectividad segura, validación de identidad y prevención del fraude requeridas por cada institución financiera.

Base legal para el tratamiento

La base legal que legítima el tratamiento de los datos personales por parte de Indexa, es el cumplimiento de la relación contractual que mantiene con las instituciones financieras que son sus clientes En su calidad de prestadora de servicios y encargada del tratamiento, Indexa procesa dicha información exclusivamente bajo las instrucciones de la entidad financiera contratante y dentro de los límites estrictos del acuerdo suscrito, el cual es indispensable para la ejecución y entrega de los servicios solicitados.

CSMS2000.3.3. Consecuencias de no consentir o revocar el consentimiento para el tratamiento de sus datos personales

Si el usuario niega o revoca el consentimiento para el uso de sus datos, Indexa no podrá procesar ni validar la información del servicio contratado. La verificación de identidad, la prevención de fraudes y la conexión segura son obligatorias para nuestros servicios. Por lo tanto, la falta de datos vigentes causará la suspensión inmediata del servicio para la persona afectada, eximiendo a Indexa de toda responsabilidad por operaciones rechazadas o no ejecutadas.

CSMS2000.3.4. Destinatarios y transferencia

Indexa debe velar por la absoluta confidencialidad y protección de todos los datos relativos a los servicios contratados por sus clientes. Toda la información recopilada se gestionará de forma interna y exclusiva, asegurando que no es compartida, cedida ni vendida a terceras empresas ni a proveedores tecnológicos externos.

CSMS2000.3.5. Medidas de seguridad aplicadas

De acuerdo con la Ley Marco de Ciberseguridad, Indexa Empresa opera bajo un Sistema de Gestión de Seguridad de la Información (SGSI) dotado con las siguientes salvaguardas:

- Cifrado: Cifrado de datos en reposo, mediante estándar AES-256 y de datos en tránsito, mediante protocolos de red seguros TLS 1.2+.
- Secreto y Confidencialidad: Todo personal de Indexa que participa en la prestación del Servicio contratado por la institución financiera, se encuentra sujeto a acuerdo de confidencialidad, manteniendo vigentes sus obligaciones incluso tras finalizar su vinculación con la empresa.

- Uso de Datos Sintéticos: Se encuentra prohibido el uso de datos reales de producción para ambientes de desarrollo o certificación. Todas las pruebas funcionales son ejecutadas de forma exclusiva utilizando datos sintéticos creados para tal fin.

- Monitoreo de actividades anómalas

CSMS2000.3.6. Comunicación con el titular de los datos

En su calidad de encargado del tratamiento, Indexa no destina los datos personales de los titulares para originar o mantener comunicaciones independientes en el marco del servicio prestado. Cualquier flujo de comunicación automatizado o gestionado a través de nuestra infraestructura se ejecuta de manera estricta bajo las instrucciones y requerimientos de la institución financiera contratante, de conformidad con la normativa vigente en materia de protección de datos personales.

CSMS2000.3.7. Requerimiento de información

Atendido el rol de la organización como encargado en la administración de los datos, cualquier requerimiento relativo a los derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad (ARCOP) interpuesto por un titular final de datos debe ser canalizado, resuelto y gestionado directamente por la Institución Financiera en su condición de responsable del Tratamiento.
En caso de que un titular remita una solicitud directamente a Indexa, se activará protocolo de redirección inmediata, remitiendo el caso formalmente al banco respectivo en un plazo no superior a 24 horas hábiles, mismo alcance realizado en Política Global de protección de datos personales[2]..

CSMS2000.3.8. Canal para reclamaciones

Empresas Indexa ha establecido un canal oficial para la atención de requerimientos sobre datos personales, garantizando la privacidad y el pleno ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad (derechos ARCOP) de los titulares, en estricto cumplimiento de la legislación vigente en materia de protección de datos, el que ha sido definido a través del Procedimiento de gestión de requerimientos de datos personales. [3]

CSMS2000.3.9. Retención y destrucción segura

Los datos personales serán mantenidos única y estrictamente durante la vigencia del contrato de servicios SaaS. Una vez concluida la relación comercial, y a elección de la entidad financiera, toda la información será devuelta de forma íntegra o destruida mediante metodologías de borrado seguro certificadas, emitiendo un acta formal que acredite la imposibilidad de recuperación de los registros.
Para más detalle refiérase a: *CSMS1900_PI_Política global de protección de datos personales*

CSMS2000.3.10. Medición

El comité de seguridad de la información debe evaluar el cumplimiento de esta política, bajo los lineamientos de seguridad definidos en el marco normativo de Indexa S.A, a fin de asegurar la efectividad de los controles desarrollados por los propietarios y custodios de información, según los indicadores que ellos establezcan en cada uno de los procesos y/o servicios en alcance a su gestión. Asimismo, el comité es responsable de garantizar la efectividad de este documento y de evitar infracciones en materia de protección de datos y privacidad.

CSMS2000.3.11. Monitoreo y control

De conformidad con la normativa vigente, Indexa S.A, adoptara todas las medidas necesarias para el resguardo de la seguridad de los datos personales y la privacidad de las personas, asegurando la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos; así como evitar su alteración, destrucción, pérdida, tratamiento o acceso no autorizado.

El espíritu de estas medidas se encuentra en la "Política de Seguridad de la Información” y “Politica de Ciberseguridad de la Organización” y marco normativo vigente de la empresa.

Independiente de lo anterior, cada gerencia dentro de su área de responsabilidad deberá coordinar, controlar y monitorear las medidas de resguardo, definidas en el alcance de su función, para preservar la confidencialidad e integridad de los datos personales en el tratamiento y almacenamiento de los mismos.

[2] CSMS1900_PI_Política global de protección de datos personales
[3] CSPS1950_P_Procedimiento de gestión de requerimientos de datos personales

El comité de seguridad de la información en conjunto con el delegado de protección de datos deben solicitar a los custodios y propietarios de información, según la frecuencia que estimen conveniente, detalles de los indicadores y controles utilizados en el resguardo y administración de los datos. Del resultado de esta gestión, se entregarán reportes a las unidades involucradas para que realicen las acciones correctivas, si amerita.

CSMS2000.4. AUDITORÍAS EXTERNAS Y CUMPLIMIENTO

Indexa reconociendo el carácter crítico de los procesos llevados a cabo, adopta un modelo de transparencia irrestricta frente a los entes de control:

- **Facultades de la CMF:** Disposición absoluta para atender requerimientos de información, inspecciones o fiscalizaciones especiales derivadas del marco de supervisión de la CMF.

- **Auditorías de Clientes Financieros:** Derecho contractual a los bancos clientes para realizar auditorías de seguridad, revisiones documentales, ethical hacking y visitas técnicas presenciales guiadas a los perímetros de Housing contratados.

CSMS2000.5. POLÍTICAS

Es política del grupo de empresas indexa establecer los siguientes principios, que deben ser respetados y seguidos por todos los funcionarios que participen o interactúen en el tratamiento y/o almacenamiento de datos personales.

Acceso
Toda información derivada de datos personales debe garantizar el acceso sólo a los titulares de la información o a las personas debidamente autorizadas por este último.

Durabilidad
La conservación de los datos personales no se extenderá más allá del plazo necesario para conseguir los fines que originaron su recolección o el tiempo señalado en la ley.

Finalidad
Todo dato personal debe ser empleado para los fines explícitos, lícitos y específicos que originaron su autorización. Si se utilizan para otros propósitos distintos a los informados al momento de su recepción, se debe solicitar autorización *(previa)* del titular de la información para este efecto.

Gratuidad
Todo acceso a los datos personales por parte de los titulares de la información será gratuito acorde a las leyes y el ordenamiento jurídico.

Inviolabilidad
Toda persona que administre, trate, almacene, controle o interactúe con datos personales conferidos a la empresa, debe garantizar su confidencialidad incluso, al terminar las relaciones laborales según las disposiciones legales que regulan esta materia.

Licitud
Todo dato personal almacenado y tratado por la empresa debe estar debidamente autorizado por el titular de la información y debe contar con su autorización expresa para este efecto.

Información
Toda incidencia, evento y/o problema de carácter personal debe ser informado a los entes interesados *(cliente, alta dirección y órganos reguladores)* según sus características, consecuencias e impactos.

Indexa comunicará, a los clientes afectados, las incidencias de datos personales considerando todo su ciclo de vida. Además de las medidas de contención utilizadas *(temporales o definitivas)* para superar la emergencia.

Toda comunicado enviado por indexa debe estar alineado a la exigencias regulatorias que norman el tratamiento de datos o leyes aplicables, según sus características técnicas.

Indexa informará la incidencias a los clientes implicados, lo antes posibles, según su prioridad de atención o plazos establecidos en la normativa vigente.

Legalidad
El tratamiento de los datos personales debe estar acorde de las exigencias del ordenamiento jurídico vigente y su tratamiento debe estar sujeto a sus disposiciones.

Indexa aplicará el principio de responsabilidad proactiva, debiendo no solo cumplir con la normativa de protección de datos personales, sino también ser capaz de demostrar dicho cumplimiento mediante la implementación de controles, registros, evaluaciones y mecanismos de supervisión continua.

indexa debe velar que los países receptores de información de carácter personal tengan un nivel de protección de datos adecuados en conformidad a la normativa nacional vigente. No obstante, si existen garantías contractuales aprobadas y consentimiento expreso del titular de la información se efectuará la transmisión de datos de forma segura.

Responsabilidad
Indexa y todo funcionario que administre, controle, manipule, almacene, trate y/o interactúe con datos personales o sensibles, son responsables de mantener la confidencialidad, integridad e inviolabilidad de la información tratada y almacenada bajo los lineamientos de esta política y la legislación vigente.

Seguridad
La información de carácter personal y sensible será manejada con todas las medidas técnicas, administrativas y humanas que garanticen la seguridad de los datos, a fin de disminuir y evitar cualquier tipo de adulteración, perdida, consulta, robo, uso y acceso no autorizado.

Veracidad
La información obtenida de datos personales y sujeta a tratamiento, debe ser exacta, actual y comprobable. En caso contrario, deberá ser suprimida o rectificada.

Prevención de uso indebido de información

El tratamiento de datos personales deberá realizarse evitando cualquier uso indebido de la información, acceso no autorizado o utilización con fines distintos a los establecidos, en conformidad con el Modelo de Prevención de Delitos de la organización y la normativa vigente.

CSMS2000.6. REPORTE DE INCIDENTES O QUIEBRES

Es responsabilidad de todos los funcionarios de indexa el informar cualquier sospecha o confirmación de quiebre a esta política u otra normativa de seguridad, a fin de minimizar el grado de exposición de la información y optimizar los tiempos de respuestas a la incidencia.

Si el funcionario identifica fallas y/o anormalidades en los controles, sistemas, servicios, herramientas o elementos utilizados en el desarrollo de sus funciones que pueda constituir un riesgo de seguridad, debe informar inmediatamente el hecho al comité de seguridad de la información *(por medio del email CSI@indexa.cl)*, para que establezca las pautas de trabajo y genere las acciones correctivas pertinentes y/o ejecutar procedimiento gestión de incidentes

En caso de incidentes que puedan comprometer obligaciones regulatorias, la organización deberá activar los procedimientos comunicacionales según alcance *(gestión de crisis o incidentes)* informando a: entes interesados, autoridades regulatorias en conformidad a los protocolos y normativas aplicables.

CSMS2000.7. CUMPLIMIENTO LEY MARCO DE CIBERSEGURIDAD (LEY N° 21.663)

En cumplimiento de las regulaciones de la Agencia Nacional de Ciberseguridad (ANCI) y considerando la condición de Indexa como responsable o encargado del tratamiento y administración de la información, se establecen los siguientes alcances en materia de seguridad y protección de datos:

Deber de Alerta Temprana y Notificación de Incidentes (Ventana Crítica de 3 Horas): Ante cualquier brecha de seguridad confirmada, acceso no autorizado, malware o incidente de ciberseguridad que afecte a los servidores en los racks y comprometa la confidencialidad, integridad o privacidad de los datos, Indexa notificará de forma oportuna al área de Ciberseguridad del Banco en un plazo máximo de tres (3) horas desde su detección. Esta diligencia permite al Banco dar cumplimiento oportuno a sus obligaciones de reporte ante la ANCI y la autoridad de protección de datos dentro de los plazos legales.

Ciclo de Desarrollo Seguro y Privacidad desde el Diseño (SecDevOps): Todo desarrollo, actualización o parche implementado en la infraestructura se rige de manera estricta por principios de seguridad y privacidad desde el diseño y por defecto. Este proceso está orientado a mitigar riesgos de filtración de información y prevenir las vulnerabilidades críticas descritas en marcos internacionales de referencia (OWASP o equivalentes).

Nota: dependiendo del alcance de la incidencia indexa reportara al ente regulador en alcance (agencia nacional de protección de datos, agencia nacional de ciberseguridad, entre otros entes reguladores, según procedimientos, marco regulatorio interno y leyes aplicable)

CSMS2000.8. ACCIONES DISCIPLINARIAS

Indexa podrá ejercer las acciones disciplinarias y legales cuando corresponda por el no cumplimiento con lo estipulado en esta política y/o en el manual de seguridad de la empresa.

Las acciones disciplinarias, dependencia de la gravedad de los hechos, consideran: amonestaciones, multas y el término inmediato del contrato de trabajo conforme a lo dispuesto en el reglamento interno de orden higiene y seguridad.

CSMS2000.9. DOCUMENTOS Y REFERENCIAS

- Norma chilena NCH-ISO27001.
- Norma chilena NCH-ISO27002.
- Ley 19.628
- Ley 21.719
- Modelo de Prevención de Delitos de la organización
- CNMC0000_PI_Política de continuidad de negocio.
- CSMS0000_PI_Política Global de seguridad de la información.
- ROGR001_PI_Política de Riesgo Operacional.
- CSMS0000_PI_Política de Gestión de Incidentes Tecnológicos.
- CSMS0700_PI_Política Global de Cifrados.
- CSMS0600_PI_Política global de ciberseguridad
- CSMS1000_N_Seguridad física y Medioambiental.
- CSMS1100_N_Norma de Seguridad física de la sala de servidores y equipamiento.
- CSMS3100_N_Respaldo de información.
- CSMS3000_N_Norma de clasificación y manejo de la información.
- CSMS0500_N_Administración de cuentas de usuario y claves de acceso.
- CSMS2500_N_Monitoreo y manejo de incidentes de seguridad.

- CSMS2600_N_Prevención de virus.
- CSPS2500_P_Procedimiento de Gestión de Incidentes.
- CSPS0500_P_Procedimiento de administración de cuentas de usuario y claves de acceso
- CSPS3100_P_Procedimiento de eliminación de información.
- CSPS3000_P_Procedimiento de clasificación de información
- [1] CSMS1900_PI_Política global de protección de datos personales V 1.0
- 1 CSPS1950_P_Procedimiento de gestión de requerimientos de datos personales V 1.0

Historia de revisiones					
Cambio	**Descripción del cambio**	**Realizado por**	**Aprobado por**	**Identificación**	**Vigencia**
PRM01SP2026	Versión Inicial	SP	CSI	CSMS2000 V 0.0	22Septiembre2026