DECLARACIÓN DE PRÁCTICAS SERVICIOS DE VALOR AÑADIDO

CONTENIDO

1. INTRODUCCIÓN

SOFT & NET SOLUTIONS es una empresa peruana, con más de siete años de experiencia en Tecnologías de la Información y soporte nacional e internacional en temas de seguridad de tecnología de clave pública, provee soluciones de firma digital, encriptación, y autenticación; a través de su Unidad de Negocios de Identidad Digital, y es representante comercial de una gama de proveedores de tecnología PKI.

2. OBJETIVO DEL DOCUMENTO

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza Soft&Net Solutions para la administración de sus servicios como Prestador de Servicios de Valor Añadido tipo Sistema de Intermediación Digital, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Prestadores de Servicios de Valor Añadido (SVA)" establecida por el INDECOPI.

3. OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación del Sistema de Intermediación Digital de SOFT & NET SOLUTIONS en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Prestadores de Servicios de Valor Añadido (SVA)" establecida por el INDECOPI, comprende la representación de las siguientes plataformas:

- Pegasus – Sistema de Intermediación Digital

SOFT & NET SOLUTIONS es responsable de exigir el cumplimiento de los requisitos establecidos por la Autoridad Adminitrativa de la IOFE a sus proveedores y es responsable ante sus clientes de la calidad y seguridad de los servicios brindados.

Los proveedores por si mismos no se encuentran amparados por la presente acreditación, sino solamente a través del control de calidad y seguridad que exige SOFT & NET SOLUTIONS a sus proveedores.

4. DEFINICIONES Y ABREVIACIONES

Prestador de Servicios de Valor Añadido:	SVA: Entidad que presta servicios que implican el uso de firma digital en el marco de la regulación establecida por la IOFE.
Servicios de valor añadido:	Servicios compuestos por tecnología y sistemas de gestión que utilizan certificados digitales garantizando la autenticidad e integridad de los mismos durante su aplicación.
Política de servicios de valor añadido:	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
Suscriptor:	Entidad que requiere los servicios provistos por el SVA de Soft&Net Solutions y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
Tercero que confía:	Persona que recibe un documento, log, o notificación electrónica generada durante la ejecución de los servicios de valor añadido, y que confía en la validez de las transacciones realizadas.

5. COMUNIDAD DE USUARIOS

Soft&Net brinda sus servicios de valor añadido a personas jurídicas del sector privado y gubernamental.

6. TERCEROS QUE CONFÍAN

Los terceros que confían son todas aquellas personas naturales y jurídicas, incluyendo entidades de otras infraestructuras además de la IOFE, que requieren evaluar la validez de una transacción electrónica, un documento firmado o un certificado utilizado o generado en los servicios brindados por los servicios brindados por el SID de Soft&Net.

7. PEGASUS – SISTEMA DE INTERMEDIACIÓN DIGITAL

Aplicación web para la definición y ejecución de flujos de trabajo de firma electrónica, como por ejemplo:

- Gestión de usuarios y cargos
- Definición y ejecución de flujos de aprobación de documentos
- Firma de documentos como parte de los flujos definidos
- Generación de cargos y reportes de auditorías de los flujos de aprobación

8. CERTIFICACIÓN ISO 27001

Los servicios entregados por los proveedores que brindan los servicios del Sistema de Intermediación Digital de SOFT & NET SOLUTIONS utilizan los marcos de seguridad conforme al estándar ISO / IEC 27001:2005, certificado por auditores independientes.

El estándar ISO 27001 define cómo implementar, monitorear, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

9. RESPONSABILIDADES DE SOFT & NET SOLUTIONS

SOFT & NET SOLUTIONS exige a sus proveedor la implementación de los controles de seguridad y privacidad necesarios para proteger la información de sus clientes, conforme a lo declarado en el presente documento.

El detalle de las limitaciones de responsabilidad son definidas en los respectivos contratos, según la normatividad y acuerdos con cada cliente.

10. RESPONSABILIDADES Y OBLIGACIONES DEL SUSCRIPTOR

El suscriptor es la entidad que contrata el servicio del Sistema de Intermediación Digital, Pegasus, y tiene las siguientes responsablilidades y obligaciones.

- No compartir sus credenciales de acceso a la plataforma.
- Contar con certificados vigentes emitidos por una Entidad de Certificación Acreditada.
- Diseñar los flujos de firma de documentos de manera apropiada.
- Leer los documentos antes de firmarlos.
- Cumplir los acuerdos suscritos en los contratos con SOFT & NET SOLUTIONS.

11. RESPONSABILIDADES Y OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Los terceros que confían son todas aquellas personas naturales o jurídicas, que requieren evaluar la validez de una transacción electrónica, realizada a través del uso de la plataforma del Sistema de Intermediación Digital, Pegasus. Estos son responsables de:

• Verificar la validez de los certificados digitales de los documentos generados por el Sistema de Intermediación Digital Pegasus.
• Tomar en cuenta cualquier limitación en el uso de los sistemas considerados en la presente declaración de prácticas.
• Tomar en cuenta cualquier otra precaución prescrita en los acuerdos u otra parte.

12. ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS NORMATIVOS

SOFT & NET SOLUTIONS administra los documentos de Declaración de Prácticas, y todos los documentos normativos del SVA.

Para cualquier consulta contactar:

- Nombre: **Ing. Leonel García Jáuregui**
- Cargo: **Representante de la ID de SOFT & NET SOLUTIONS**
- Dirección de correo electrónico: **lgarcia@soft-net.com.pe**

13. PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Declaración de Prácticas de Servicios de Valor Añadido de SOFT & NET SOLUTIONS, la Política y Plan de Privacidad y otra documentación relevante son publicados en la siguiente dirección: http://www.soft-net.com.pe.

Todas las modificaciones relevantes serán comunicadas al INDECOPI y las nuevas versiones del documento, una vez aprobadas, serán publicadas en el mismo sitio web.

El presente documento es firmado por el Representante de la ID antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas. Las versiones cambian conforme son presentadas y aprobadas por el INDECOPI.

14. GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES

14.1. GENERACIÓN DE LAS CLAVES

La generación del par de claves para firma del agente automatizado del SID de SOFT&NET se debe realizar en un ambiente provisto de las medidas de seguridad apropiadas, por personal designado que ocupe roles de confianza dentro de la entidad, empleando al menos un control de acceso dual y con los permisos limitados al cumplimiento de esta tarea.

Respecto al dispositivo criptográfico, se empleará un HSM con certificación FIPS 140-2 nivel 3 mínimo.

Los detalles y procedimientos empleados en la generación de las claves se encontrarán debidamente documentados indicando entre otras cosas la identificación del personal que fuera encargado, la identificación del dispositivo criptográfico y los detalles de las claves generadas (algoritmo de generación de claves, tamaño de claves, y algoritmo de firma de su certificado).

14.2. PROTECCIÓN DE LA CLAVE PRIVADA

El SID de SOFT&NET almacena y protege la clave privada de sus agentes automatizados en módulos criptográficos que cuenten con certificación FIPS 140-2 nivel 3, mínimo.

El SID de SOFT&NET no realiza copia de respaldo (backup) de sus claves privadas. De requerirse, esta actividad será realizada dentro de un ambiente protegido mediante controles de acceso físico. Dicha actividad deberá requerir de la participación de personal que ocupe roles de confianza empleando al menos un control de acceso de dos personas. El personal autorizado para realizar estas funciones debe estar limitado para realizar esta tarea conforme a los procedimientos del SVA.

Cualquier copia de la clave deberá ser protegida por la clave secreta del módulo criptográfico antes de ser almacenada fuera del dispositivo.

14.3. DISTRIBUCIÓN DE LA CLAVE PÚBLICA

La clave pública de firma del agente automatizado estará disponible para los terceros que confían a través de su certificado de clave pública.

El certificado debe ser emitido por una EC reconocida por la IOFE y bajo una política que provea un nivel de seguridad equivalente o superior a la DPSVA.

Este certificado debe ser reconocido por la IOFE para lo cual la EC emisora del mismo debe estar acreditada.

14.4. RE-EMISIÓN DE LA CLAVE

En caso la EC que emite el certificado de agente automatizado soporte la re-emisión de certificado, el tiempo de vigencia del mismo no debe ser mayor que el periodo de vigencia de los algoritmos y tamaños de claves, conforme al reconocimiento de la IOFE.

14.5. TÉRMINO DEL CICLO DE VIDA DE LA CLAVE PRIVADA

Las operaciones del SID de SOFT&NET se realizarán en plena vigencia de los certificados digitales de agente automatizado empleados. El SID de SOFT&NET emplea un software de firma acreditado que rechazará cualquier intento de empleo de un certificado si su clave privada de firma ha expirado o ha sido revocada.

Una clave privada llega al final de su ciclo de vida si:

- El certificado asociado a expirado.
- El certificado asociado ha sido revocado. Esto puede haber sido motivado debido a que la clave se ha visto comprometida, o se han detectado debilidades en su algoritmo de firma, en su algoritmo hash o en el tamaño de clave.

Cuando el certificado digital de agente automatizado llegue a su fin se realizarán las siguientes acciones:

- Se procederá a desactivar el certificado del SID de SOFT&NET.
- Se programará el procedimiento de destrucción segura de la clave de dicho certificado. En caso de haberse generado backup de dicha clave también deberá realizarse el borrado seguro de dicha copia.
- En paralelo podrá gestionarse la emisión de un nuevo certificado.

Para la destrucción segura de una clave privada de agente automatizado se seguirán las instrucciones propias del fabricante para el módulo de seguridad de hardware (HSM) empleado. Los procedimientos serán llevados a cabo por personal adecuado según los roles de confianza.

15. CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO

SOFT&NET es responsable de la seguridad del hardware criptográfico a lo largo de su ciclo de vida. Particularmente se garantiza que:

- El hardware del módulo criptográfico no debe ser manipulado durante su transporte.
- El hardware del módulo criptográfico no debe ser manipulado durante su almacenamiento.
- La instalación, activación y duplicación de la clave de firma en el hardware del módulo criptográfico debe ser realizado sólo por personal que ocupa roles de confianza, usando al menos un control de acceso de dos personas en un ambiente físico seguro.
- El hardware del módulo criptográfico funciona correctamente.
- Las claves de firma que son almacenadas en un módulo criptográfico son borradas antes de que el dispositivo sea retirado y su certificado revocado de ser el caso.

16. AUTENTICACIÓN

Se emplea autenticación mediante usuario y contraseña. Se prevé que el futuro se empleará autenticación mediante certificado digital en cuyo caso se deberá verificar la validez del mismo antes de autorizar su acceso, esto es:

- El sistema deberá verificar que el certificado corresponde a una Entidad de Certificación reconocida por la IOFE, de no ser exitosa la verificación, el sistema no debe permitir el acceso.
- El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación no hayan expirado y no se encuentran revocados. La verificación de revocación se puede realizar mediante los mecanismos CRL u OCSP. En caso de ser CRL, se deberá verificar la vigencia y autenticidad de la CRL.
- El sistema deberá verificar que el certificado del usuario final tiene como propósito autenticación, conforme a la RFC 5280.

17. CIFRADO

El SID de SOFT&NET no realiza funciones de cifrado de datos mediante certificados digitales.

18. CANALES SSL

- Al momento de descifrar la información, el sistema no debe copiar la clave privada sin cifrar fuera del módulo criptográfico. La clave privada siempre se mantiene dentro del módulo criptográfico.

- El sistema debe verificar que el certificado corresponde a una Entidad de Certificación reconocida por la IOFE, de no ser exitosa la verificación, el sistema no permite el acceso.
- El sistema debe verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación no hayan expirado y no se encuentren revocados. La verificación de revocación se puede realizar mediante los mecanismos CRL u OCSP. En caso de ser CRL, se verifica la vigencia y autenticidad de la CRL.
- El sistema debe verificar que el certificado del usuario final tiene como propósito de cifrado de clave, conforme a la RFC 5280.

19. PETICIÓN DE SELLOS DE TIEMPO

Se deben cumplir requisitos que garanticen su confiabilidad:

- El formato de petición debe estar conforme a la RFC 3161.
- El sistema debe verificar que el certificado con el que se firma el sello de tiempo corresponde a una Entidad de Certificación reconocida por la IOFE.
- El sistema debe verificar que el certificado con el que se firman los sellos de tiempo no se encuentre revocado.
- El sistema debe verificar que el certificado con el que se firman los sellos de tiempo no se encuentre expirado.
- El sistema debe verificar la firma del sello de tiempo para corroborar que los datos son íntegros.

20. CONTROLES EN LAS INSTALACIONES, GESTION Y OPERACIONALES

20.1. CUMPLIMIENTO

Anualmente los servicios brindados por las plataformas que componen el SID de SOFT & NET SOLUTIONS, son sometidos a auditorías de terceros por parte de auditores reconocidos internacionalmente y autorizados para el logro de la certificación ISO 27001.

20.2. EVALUACIÓN DE RIESGOS

Anualmente, los proveedores de SOFT & NET SOLUTIONS llevan a cabo un análisis de riesgo de seguridad de la información. El análisis incluye:

- La identificación de las amenazas relacionadas con los procesos de intercambio de información y firma digital.
- Una estrategia aprobada de gestión para la mitigación de las amenazas significativas identificadas.

20.3. CONTROL DE ACCESO A LOS AMBIENTES

El acceso a todas las instalaciones de los provedores de Soft&Net Solutions donde se ejecuta la soluciones del Sistema de Intermediación Digitala está controlado. Existen perímetros claramente definidos y personal encargado de supervisar la recepción para realizar la identificación de los empleados de tiempo completo o contratistas autorizados que no cuentan con tarjetas de identificación. Todos los visitantes son requeridos a usar identificadores y ser escoltados por personal autorizado de Soft&Net Solutions.

20.4. CONTROL DE ACCESOS ACCESO DE USUARIOS

El sistema de Intermediación digital cuenta con controles y sistemas adecuados para monitorear el acceso a los sistemas de software y hardware físico dentro de los centros de datos, y todo ese acceso está estrechamente controlado y gestionado.

El acceso está restringido según la función de trabajo de cada rol de manera que sólo el personal esencial puede recibir autorización para administrar aplicaciones y servicios de los clientes.

20.5. AUTORIZACIÓN PARA RETIRAR EQUIPOS O SISTEMAS FUERA DEL LOCAL

Los procedimientos de protección de activos proporcionan una guía normativa en torno a la protección de los datos lógicos y físicos e incluyen instrucciones que dirigen la reubicación de datos, software, hardware fuera de las instalaciones.

20.6. GESTIÓN DE ACTIVOS

Los activos son contabilizados y son asignados a un propietario. Se mantiene un inventario de los principales activos de hardware utilizados en los servicio que componen el SID.

20.7. SEGURIDAD DE LOS RECURSOS HUMANOS

El personal de los proveedores de Soft&Net Solutions son requeridos a completar satisfactoriamente una verificación de antecedentes estándar como parte del proceso de su contratación a fin de validar el empleo anterior, educación, antecedentes penales.

El personal de los proveedores de Soft&Net Solutions es requerido a tomar algún tipo de formación que se considere conveniente a los servicios que prestan y el rol que desempeñan.

La Política Corporativa de Recursos Humanos Soft&Net Solutions dirige los procesos de terminación de los empleados.

20.8. GESTIÓN DE INCIDENTES

Como parte de sus servicios, Soft&Net Solutions realiza los procesos de detección e investigación de todas las incidencias reportadas por sus clientes.

20.9. SEGURIDAD DE LA INFORMACIÓN – ANTIVIRUS/SOFTWARE MALICIOSO

Los sistemas servidores de los proveedores de Soft&Net Solutions cuentan con software anti-virus para asegurar la protección contra software malicioso común.

21. REGISTRO DE AUDITORÍA

El sistema debe permitir registrar los eventos críticos

21.1. EVENTOS REGISTRADOS

Los eventos que son registrados están relacionados a las transacciones de autenticación y generación de firma digital.

21.2. PROTECCIÓN DE LOS REGISTROS

Los eventos son registrados de tal forma que ellos no puedan ser borrados o destruidos dentro del periodo de tiempo que son requeridos como evidencia (excepto si son transferidos a medios de almacenamiento de largo plazo).

21.3. EVENTOS SIGNIFICATIVOS

Son registrados las solicitudes o transacciones de autenticación, firma digital o cifrado (en caso se implemente). Se consideran como eventos significativos para el SID:

- Fecha y hora de autenticación de los usuarios
- Fecha y hora de despacho de notificación
- Fecha y hora de generación de notificación
- Fecha y hora de registro de depósito de notificación en domicilio electrónico
- Fecha y hora de cambio en la configuración de usuarios
- Fecha y hora de cambio en la configuración del sistema

22. AUDITORÍA

SOFT6NET debe ser auditado anualmente por la AAC, respecto a la correcta operación de los servicios de registro.

Como parte de dicha auditoría anual se revisan los registros, el archivo, los procedimientos y controles implementados.

El auditor debe cumplir con los siguientes requisitos:

- Estar autorizado por la AAC.
- Ser independiente de ONPE y no haber realizado trabajos para ella dentro de los dos años anteriores a la ejecución de la auditoría.

23. DERECHOS DE PROPIEDAD INTELECTUAL

De ser requerido y en caso de aplicar, se deberán declarar cláusulas contractuales respecto de obligaciones y derechos relacionados a la propiedad intelectual.

24. NOTIFICACIONES Y COMUNICACIONES ENTRE PARTICIPANTES

Para todos los efectos de las comunicaciones entre el PSVA, los suscriptores y terceros que confían, se tendrá como referencia el domicilio real o electrónico que hubieren señalado, en donde se tendrán por válidamente realizadas todas las comunicaciones que pudieran serles cursadas.

25. POLÍTICA DE REEMBOLSO

Las condiciones de reembolso, de aplicar, serán definidas con cada cliente en los respectivos contratos (u otro documento empleado para establecer la relación contractual con SOFT&NET), de acuerdo al tipo de servicio, contrato y cliente.

26. RESPONSABILIDAD FINANCIERA, REPRESENTACIONES Y GARANTÍAS

La cobertura de seguro, las provisiones de garantía y responsabilidad, así como las indemnizaciones pueden ser definidas en los contratos con los clientes, de acuerdo al tipo de servicio, contrato y cliente.

Los seguros son provistos por los proveedores de Soft&Net Solutions y dan cobertura cada uno a sus servicios.

27. ENMENDADURAS

Los procedimientos para la resolución de enmendaduras podrán ser definidas en los contratos con las organizaciones clientes, de acuerdo al tipo de servicio, contrato y cliente.

28. RESOLUCIÓN DE DISPUTAS

Los procedimientos para la resolución de disputas están definidos en la Política de Gestión de Disputas y en su procedimiento. Estas podrán ser definidas en los contratos con las organizaciones clientes, de acuerdo al tipo de servicio, contrato y cliente.

En caso de presentarse cualquier disputa o reclamo en relación a los derechos u obligaciones que se alude en el presente documento, el interesado deberá presentar dicho reclamo a través del Sistema de Gestión de Incidentes, elaborando un resumen de los aspectos más relevantes de la reclamación y acompañando los documentos sustentatorios correspondientes. SOFT&NET resolverá en primera instancia el aludido reclamo.

Agotada la vía anteriormente indicada y en caso el reclamante no se encontrara conforme, se podrá recurrir en vía administrativa ante la Autoridad Administrativa Competente.

29. EXENCIÓN DE GARANTÍAS

SOFT&NET no realizará pago de indemnización alguna, salvo lo correspondiente a las obligaciones derivadas de la ejecución del seguro por responsabilidad que corresponde contratar de conformidad con lo que disponga para dichos efectos la Autoridad Administrativa Competente.

30. INDEMNIZACIONES

Las indemnizaciones a las cuales pudiera estar sujeta SOFT&NET en su condición de Prestador de Servicio de Valor Añadido, se sujetará a lo detallado en la póliza de Seguro de Responsabilidad Civil que deberá adquirir de conformidad con lo detallado para dichos efectos por la Autoridad Administrativa Competente.

31. ACUERDO ÍNTEGRO, SUBROGACIÓN Y DIVISIBILIDAD

Las cláusulas de acuerdo íntegro, subrogación y divisibilidad podrán ser definidas en los contratos con las organizaciones clientes, de acuerdo al tipo de servicio, contrato y cliente.

32. FUERZA MAYOR Y OTRAS PROVISIONES

Las cláusulas de fuerza mayor y otras provisiones aplicables a la entrega de los servicios de valor añadido podrán ser definidas en los contratos con las organizaciones clientes, de acuerdo al tipo de servicio, contrato y cliente.

33. TARIFAS

Las tarifas por los servicios serán definidas en los contratos con las organizaciones clientes, de acuerdo al tipo de servicio, contrato y cliente.

34. FINALIZACIÓN DEL SVA

Antes de que el SVA termine sus servicios realizará las siguientes medidas:

- De ser aplicable, con 30 días de anticipación se informará a todos clientes y suscriptores, la finalización de las operaciones del SVA.
- Se pondrá a disponibilidad de todas las organizaciones cliente la información concerniente a su terminación y las limitaciones de responsabilidad.
- Se concluirán los permisos de autorización de funciones de todos los subcontratados para actuar en nombre del SVA
- Se mantendrán o transferirán a los terceros que confían sus obligaciones de verificar los documentos generados.
- Las provisiones sobre término y terminación, así como las cláusulas de supervivencia serán definidas en los contratos de los clientes. Además, las modificaciones realizadas deben ser comunicadas a los suscriptores, titulares y terceros que confían.
-

35. CONFORMIDAD CON LA LEY APLICABLE

Soft&Net Solutions es afecta y cumple con las obligaciones establecidas por la IOFE, a los requerimientos de la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados

Digitales -Ley27269, para el reconocimiento legal de los servicios de valor añadido emitidos bajo las directrices definidas en el presente documento.

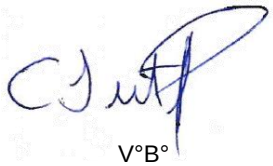
36. BIBLIOGRAFÍA

a) Guía de Acreditación de Prestadores de Servicios de Valor Añadido, INDECOPI
b) Ley de Firmas y Certificados Digitales –Ley 27269
c) Decreto Supremo 052-2008
d) Decreto Supremo 070-2011
e) Decreto Supremo 105-2012

37. HISTORIAL DE CAMBIOS

Generales			
Propietario del Documento	*Leonel Garcia Jauregui*	**Clasificación**	*Privada*
Aprobado por:	*Leonel Garcia Jauregui*	**Fecha aprobación inicial**	*10/02/2018*

Fecha	***Versión***	***Descripción***	***Autor***
10/02/2018	*1.0*	*Documento Inicial*	*Coordinador de la seguridad de la Informacion*
10/02/2018	*1.0*	*Revision de Documentos*	*Gerente de Operaciones*
10/02/2018	*1.1*	*Ajuste en la denominación del tipo de SGID como servicio realizado como parte del proceso de acreditación ante INDECOPI*	*Coordinador de la seguridad de la Informacion*
25/03/2019	*1.2*	*Actualización y descripción de procedimientos para la auditoría de seguimiento del 2019*	*Coordinador de la seguridad de la Informacion*
28/10/2020	*1.2*	*Revision de Docuementos*	*Gerente de Productos y Servicios*

Elaborado por: Pedro Rivera Pérez.	Revisado por: Christian Gutierrez Pérez.	Revisado y Aprobado por: Leonel Garcia Jauregui.
 V°B°	 V°B°	 V°B°
Cargo: Coordinador de Seguridad de la Información	Cargo: Gerente de Productos y Servicios	Cargo: Representante de la ID