Pautas de acreditación de proveedores tecnológicos para carpeta de despacho electrónica.

Abril de 2012

1. Introducción. 1
2. Metodología de evaluación 1
2.1. Objetivos evaluación. 1
2.2. Esquema de evaluación 1
2.3. Escala de evaluación. 5
2.4. Consideraciones Generales de validación. 5
2.5. Presentación de Antecedentes 6
3. Evaluación de admisibilidad 7
3.1. Requerimientos Legales y financieros requeridos para Agentes de Aduana. 7
3.2. Requerimientos Legales y financieros requeridos para empresas Prestadoras de Servicios de Carpetas de Despacho Electrónicas. 7
4. Requisitos de Acreditación 8
4.1. Requisitos de la aplicación. 8
4.2. Requisitos Generales de Infraestructura 9
4.2.1. Site 9
4.2.2. Suministro eléctrico. 9
4.2.3. Plataforma de diseño de operación 10
4.2.4. Plataforma de Almacenamiento 10
4.2.5. Plataforma de Comunicaciones. 10
4.2.6. Plataforma de Soporte a usuarios. 10
4.3. Requisitos Generales de Servicio 11
4.4. Requisitos de seguridad 12
5. Evaluación de Requisitos 13
5.1. Revisión documental 13
5.2. Etapa de revisión “Prueba de aplicación: aspectos técnicos y casos de uso”. 13
5.3. Etapa de revisión visita de verificación. 14
6. Anexos 15
6.1. ANEXO 1: Formulario de Postulación a PSR. 15
6.2. ANEXO 2: 16
6.3. ANEXO 3: 32

1. Introducción.

Este documento tiene como objetivo dar las pautas necesarias para acceder a la acreditación para proveer los servicios de repositorio de carpeta de despacho electrónica. Esta pauta asume el nivel básico de seguridad de documentos electrónicos, de acuerdo a las definiciones del Decreto Supremo N° 83 del 3 de junio de 2004 sobre "Normas técnicas sobre seguridad y confidencialidad del documento electrónico" y las prácticas señaladas en la norma chilena Nch-ISO 27002 - Of.2009 sobre "Código de prácticas para la gestión de la seguridad de la información".

El desglose del documento considera los siguientes elementos:

- Metodología de evaluación.
- Requisitos de Admisibilidad.
- Requisitos de Acreditación.
- Evaluación de requisitos.
- Anexos.

2. Metodología de evaluación

Esta sección expone el método mediante el cual el Servicio Nacional de Aduanas entregará la acreditación a las empresas interesadas en proveer el servicio de repositorio de carpeta de despacho electrónica.

2.1. Objetivos evaluación.

El objetivo general de la evaluación es acreditar que se ha implementado una infraestructura y procedimientos operacionales que permitirán proveer el servicio de carpeta de despacho electrónico, bajo parámetros de seguridad, confianza y durabilidad definidos por el Servicio Nacional de Aduanas.

2.2. Esquema de evaluación

El proceso de acreditación se efectuará por medio de la verificación de cumplimiento de los requisitos según el siguiente procedimiento:

a) Verificación de antecedentes y evaluación de admisibilidad.

Evaluación de los antecedentes presentados para determinar el cumplimiento de los requisitos legales y financieros, para definir la admisibilidad del postulante al proceso.

b) Evaluación de antecedentes de infraestructura y modelo operacional.

La evaluación se efectuará conforme a escala indicada en punto 2.3 y los requisitos

establecidos en el punto 3 del presente documento.

c) Visitas de auditoría.

Conforme a las pautas de auditoría en estas materias, la parte evaluadora podrá verificar los antecedentes por medio de una visita. De igual forma, podrá solicitar antecedentes in-situ para verificar el cumplimiento de los requisitos.

d) Observaciones.

Aquellos aspectos que fueran calificados con A-, según escala de evaluación, tendrán un plazo de 10 días para presentar un Plan Correctivo, que indique el modo en que serán en mediano plazo subsanadas las observaciones.

e) Elaboración de resolución de acreditación.

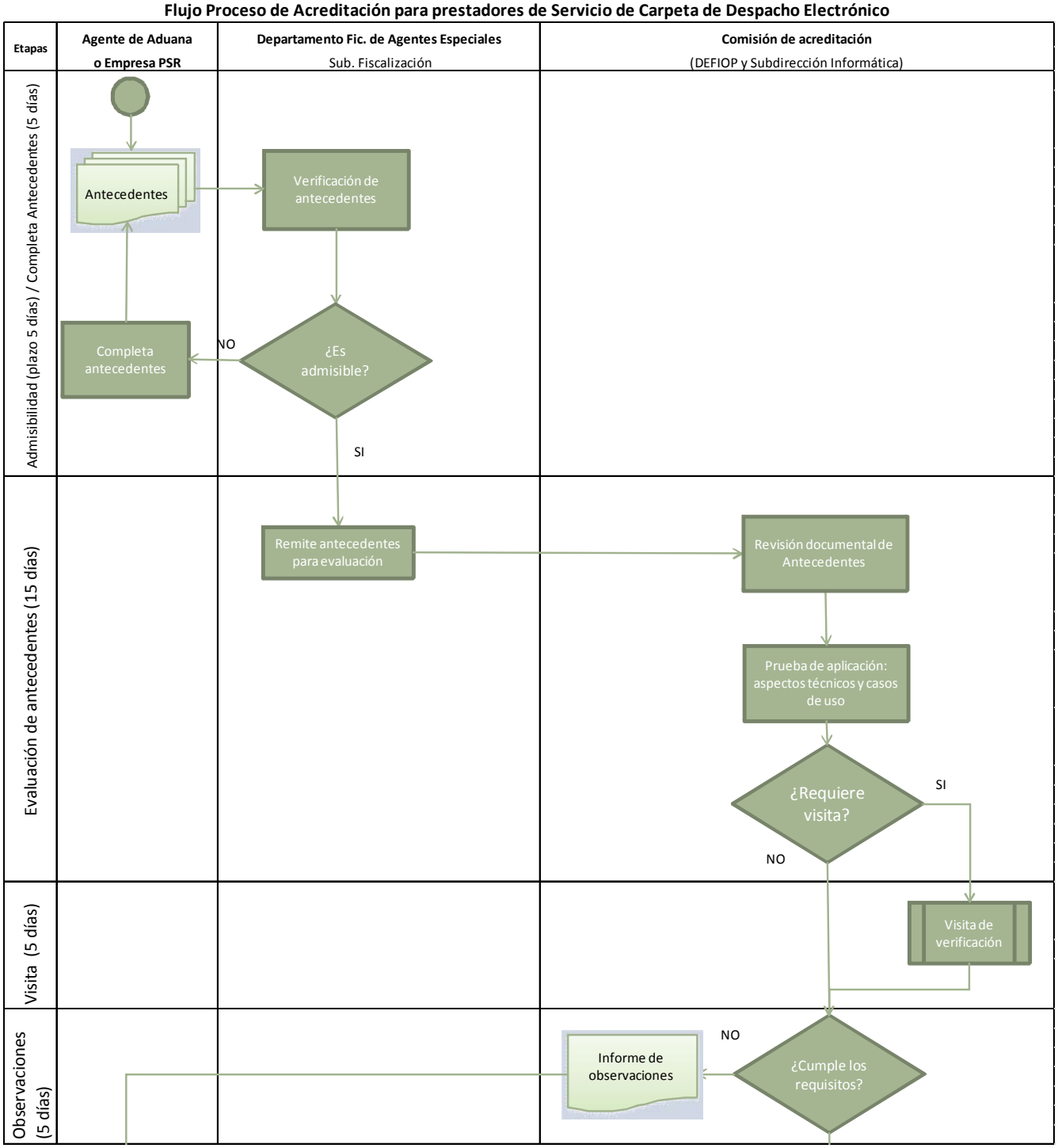
Una vez emitido favorablemente los informes de evaluación de los requisitos establecidos en las presentes pautas, la resolución de acreditación es el instrumento mediante el cual el postulante quedará habilitado para proveer el servicio de de repositorio de carpeta de despacho electrónica.

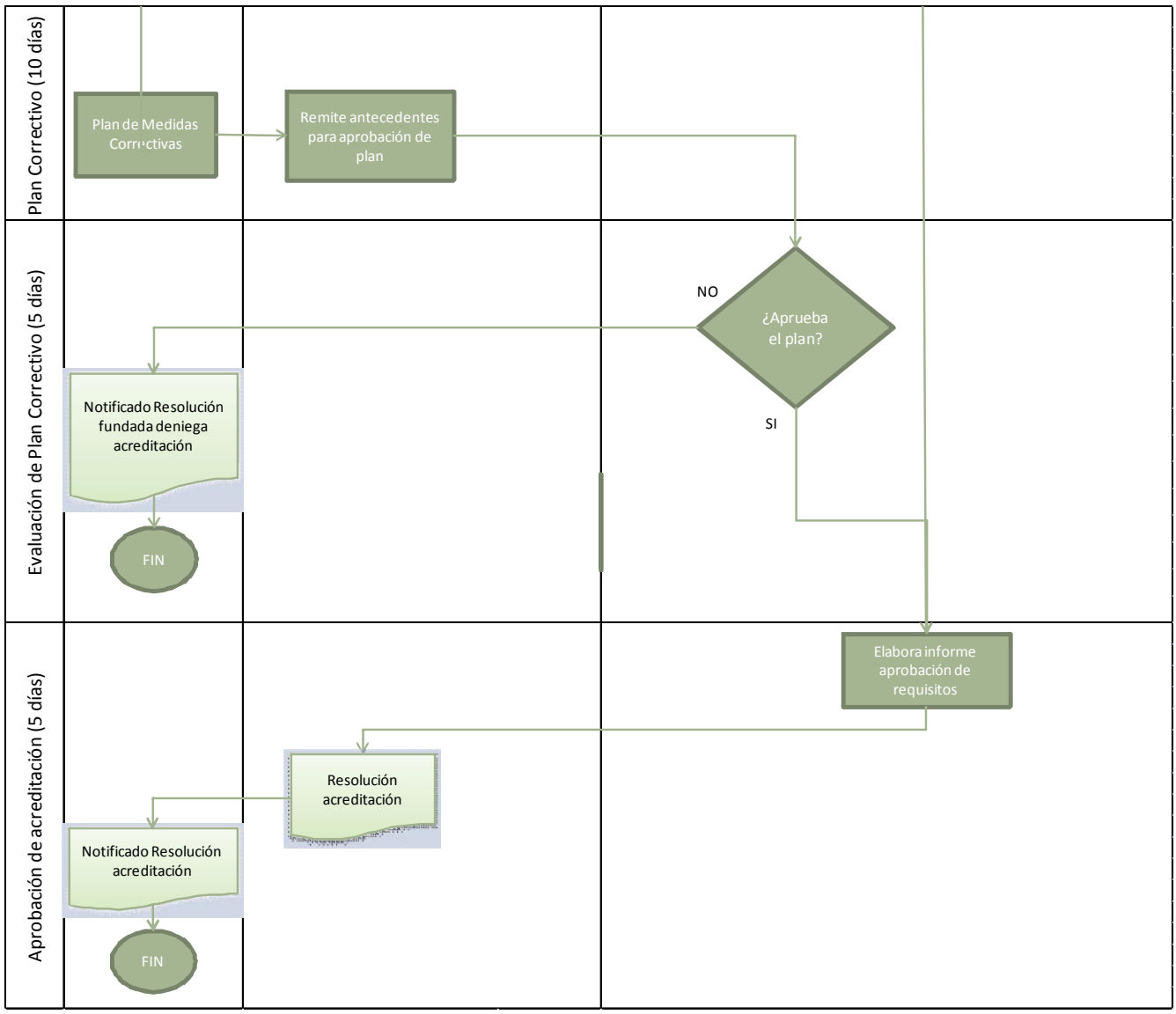
A continuación se entrega un detalle de los plazos máximos para la realización de cada una de las fases del proceso de acreditación. Como se puede observar, el plazo máximo del proceso es de 55 días hábiles.

Nombre de la Etapa	Plazos
Verificación de antecedentes y evaluación de admisibilidad	5 días
Plazo para completar presentación de antecedentes	5 días
Evaluación de antecedentes de infraestructura y modelo operacional.	15 días
Visitas de auditoría	5 días
Formulación de observaciones	5 días
Plazo para presentar Plan Correctivo	10 días
Evaluación de Plan Correctivo	5 días
Elaboración de resolución de acreditación	5 días

A continuación se presenta un diagrama del proceso de acreditación.

Flujo Proceso de Acreditación para prestadores de Servicio de Carpeta de Despacho Electrónico




Plan Correctivo (10 días)
Evaluación de Plan Correctivo (5 días)
Aprobación de acreditación (5 días)
Plan de Medidas Correctivas
Remite antecedentes para aprobación de plan
¿Aprueba el plan?
NO
SI
Notificado Resolución fundada deniega acreditación
FIN
Elabora informe aprobación de requisitos
Resolución acreditación
Notificado Resolución acreditación
FIN

2.3. Escala de evaluación.

Cada requisito será evaluado en conformidad con la siguiente escala:

Calificación	Descripción
A	EL postulante cumple totalmente el requisito exigido.
A-	EL postulante no cumple totalmente el requisito, pero se determina que el cumplimiento es subsanable y no afecta el correcto funcionamiento del sistema ni los fines previstos en las normativas definidas por el Servicio Nacional de Aduanas. En estos casos el postulante debe presentar una propuesta de trabajo según formato anexo 3.
B	EL postulante no cumple totalmente el requisito y no es subsanable y afecta el correcto funcionamiento del sistema y los fines previstos en las normativas definidas por el Servicio Nacional de Aduanas.

El objetivo de la calificación A-, es permitir que el PSR pueda modificar los aspectos negativos que son subsanables en un corto periodo de tiempo y así optar a la acreditación durante su primera postulación.

Las postulaciones que poseen calificación B no podrán acceder a la acreditación. En caso de subsanar los incumplimientos, deberá iniciar un nuevo proceso de acreditación.

2.4. Consideraciones Generales de validación.

Las consideraciones generales con las que se realizará la comprobación del buen funcionamiento de los servicios son las siguientes:

- **Transparencia**: El proceso de acreditación pondrá a disposición pública toda la información necesaria requerida para conocer el estado del sistema de prestación de servicio de carpeta electrónica acreditado, con el propósito de entregar confianza a los usuarios y generar las condiciones y los acuerdos necesarios para el desarrollo de la actividad en conformidad a normas y acuerdos internacionales que se celebren. En este sentido, se considera necesaria la información que muestre el cumplimiento de los requisitos mínimos, manteniéndose reserva de cumplimientos de valor agregado que signifiquen una diferenciación entre un prestador y su competencia, en la medida que sea posible separar dichas informaciones.
- **Gradualidad**: Los niveles de exigencia del proceso de acreditación serán graduales y se irán adaptando desde un estado inicial en que las exigencias apuntarán a cumplir estándares suficientes que provean confianza en el sistema y compatibles con la realidad nacional, hasta el cumplimiento estricto de los estándares internacionales a medida que el desarrollo de la actividad lo requiera.

- **Privacidad**: El proceso de acreditación, requiere de información estratégica de parte de los Prestadores. Por lo anterior, la entidad acreditadora se compromete a no divulgar ni usar la información entregada por los Prestadores, más que para el proceso y fin del propio procedimiento de acreditación.

2.5. Presentación de Antecedentes

Los antecedentes deberán ser presentados en la Subdirección Jurídica del Servicio Nacional de Aduanas.

El formato de los antecedentes podrá ser entregado en formato digital, papel o combinación de ellos.

El postulante deberá presentar:

a) Formulario de postulación indicado en Anexo 1.

b) Matriz de evidencia, completada según instrucciones indicadas en Anexo 2 (formato digital).

c) Antecedentes legales y financieros indicados en Anexo 3.

d) Declaración simple que autorice al Servicio Nacional de Aduanas para que, en cualquier momento, pueda efectuar fiscalizaciones con el objeto de verificar el cumplimiento de las normas que regulan a las Prestadoras de Servicios de Carpetas de Despacho Electrónicas, pudiendo solicitarle información documental o efectuar visitas a las instalaciones.

e) Designación de persona natural en calidad de contacto con el Servicio Nacional de Aduanas. Esta persona deberá estar en posesión de, a lo menos, un título técnico de nivel superior. Indicar en Anexo 1.

La entrega de los antecedentes deberá contar con un índice guía de los antecedentes conforme al capítulo de requerimientos. De igual forma, los antecedentes proporcionados en formato digital deberán estar contenidos y ordenados en carpetas cuyos nombres indiquen el requerimiento respectivo.

3. Evaluación de admisibilidad

La evaluación de admisibilidad corresponde a la etapa mediante la cual se podrá identificar si las empresas han puesto a disposición la totalidad de los documentos solicitados en el punto 2.5 presentación de antecedentes y el cumplimiento de los requerimientos legales y financieros establecidos en la resolución que entrega el marco general de Carpeta de Despacho Electrónico.

La no presentación de los anexos solicitados en las presentes pautas de acreditación, serán causal de inadmisibilidad de la solicitud de acreditación presentada.

3.1. Requerimientos Legales y financieros requeridos para Agentes de Aduana.

No se efectuará evaluación de los requerimientos legales y financieros para el caso de los Agentes de Aduana que se auto preverán el servicio, debido a que los requisitos establecidos en esta área son equivalentes a los dispuestos para ostentar la calidad de Agente.

Para comprobar el cumplimiento del requisito se verificará que en la fecha de ingreso de su solicitud de acreditación este se encuentre vigente en la ficha única de registro, disponible en el Departamento de Agentes Especiales.

3.2. Requerimientos Legales y financieros requeridos para empresas Prestadoras de Servicios de Carpetas de Despacho Electrónicas.

Corresponden a todos los elementos de carácter legal y financieros que debe presentar el postulante con lo cual formaliza su solicitud y establece el cumplimiento del marco jurídico que lo constituye como empresa y prestador de servicios.

Se validará el cumplimiento de los siguientes elementos, siendo responsabilidad del postulante presentar con antecedentes necesarios para su validación:

- El postulante PSR deberán estar constituidas como personas jurídicas, teniendo por objeto principal la creación, modificación, conservación y administración de documentos electrónicos y digitales.
- Su capital social pagado, no podrá ser inferior a 2.500 Unidades de Fomento a la fecha de su autorización.

4. Requisitos de Acreditación

Los requisitos mínimos que debe cumplir un postulante para prestar el servicio de Repositorio de Carpetas de Despacho Electrónicas, se agrupan en función de la protección de la información y el proceso de negocio.

Para optimizar la entrega de información y evaluación posterior de la misma, las empresas y agentes de aduana interesados en participar del proceso de acreditación deberán llenar la Matriz de Evidencia (descrita en anexo 2). Dicha matriz contempla la auto evaluación del nivel de cumplimiento de los requisitos expuestos a continuación, una descripción de las brechas existentes entre los requisitos y el estado actual, y la identificación de los documentos o evidencias que permitirán comprobar la auto evaluación.

4.1. Requisitos de la aplicación.

La solución requerida establece el desarrollo de servicios e interfaces para el uso de los Agentes de Aduanas y personal del Servicio Nacional de Aduana.

El desarrollo de software deberá estar sujeto a los siguientes requerimientos:

4.1.1 Se deberán cumplir los requerimientos de desarrollo y estándares indicados en el documento de “Especificaciones del Modelo Operacional y Tecnológico de Carpeta de Despacho Electrónica”.

4.1.2 Las aplicaciones deben correr sobre Browser Explorer 8 o superior y Mozilla Firefox 3.6 o superior.

El postulante a PSR deberá proporcionar los siguientes elementos para evaluar el cumplimiento de los requisitos:

a) Flujo grama del proceso indicando aplicaciones y funcionalidades.

b) Especificaciones de la tecnológica utilizada para implementar las aplicaciones y servicios (Software básico, software aplicativo) y modelo operacional.

c) Descripción de la plataforma operativa.

d) Especificaciones del proceso de desarrollo y calidad.

e) Descripción de XML, XLS y XSD utilizadas según definiciones establecidas en el Modelo Operacional.

f) Procedimiento y descripción de firma digital de documentos.

g) URL del sitio web (acceso).

h) Procedimiento de digitalización

4.2. Requisitos Generales de Infraestructura

Se deberá proporcionar los antecedentes de la arquitectura tecnológica empleada.

La plataforma que soporta los procesos de solicitud, consulta, intercambio, carga y almacenamiento de las carpetas electrónicas deben cumplir con los siguientes requerimientos:

4.2.1. Site

Las dependencias donde residen los servidores y se almacena la información debe contar con las siguientes características:

a) Las instalaciones deberán contar con sistema de temperatura controlada entre 18° y 24° Celsius (climatización).

b) La humedad del centro de proceso y almacenamiento deberá estar controlada.

c) Control de acceso a las instalaciones, seguridad y control perimetral.

d) Construcción antisísmica.

e) Alejado de lugares con riesgo de naturaleza (desbordes de ríos, desmoronamientos, aluviones, maremotos, etc.) o actos vandálicos.

f) No ubicado en subterráneos o directamente sobre estacionamientos.

g) No haber adyacentes tuberías de gas, agua u otro tipo de elementos que pongan en riesgo las instalaciones.

h) Sistema de detección de incendios.

i) Elementos para extinción manual de incendios.

4.2.2. Suministro eléctrico.

La plataforma deberá contar a lo menos con las siguientes características:

a) Contener canalización separada de corrientes fuertes y débiles.

b) Energía eléctrica no interrumpida con disponibilidad de 99,5%. Eso implica contar con:

c) Sistema de UPS de auto respaldo.

d) Sistema de continuidad en el suministro eléctrico (grupo electrógeno), para equipos y sistema de climatización.

e) Alimentación 220 volts +/- 5%.

f) Frecuencia 50 HZ +/- 0.5%

g) Tierra de Servicio.

4.2.3. Plataforma de diseño de operación

La plataforma que sustenta los servicios de carga, publicación, consulta, transacción y administración de documentos y carpeta electrónica debe contar con los siguientes requerimientos:

a) Plataforma de alta disponibilidad.

b) Servidores con componentes redundantes.

c) Redundancia en plataforma de servidores y equipos de comunicación.

d) Acceso a red de comunicaciones para distintos proveedores.

e) Servicio de soporte y mantención para todo el equipamiento involucrado.

f) Disponibilidad de 99,5% anual.

4.2.4. Plataforma de Almacenamiento

En lo que respecta al proceso de almacenamiento de información, se requiere:

a) Contar con Política y procedimientos de respaldo.

b) Política de % mínimo libre de espacio en sistema principal.

c) Plataforma de almacenamiento redundante.

d) Procedimientos de recuperación de datos y sistemas.

4.2.5. Plataforma de Comunicaciones.

La plataforma de comunicaciones deberá cumplir con:

a) Sistema redundante de enlace.

b) Hardware de comunicaciones en conformación redundante.

c) Disponibilidad de 99,5%

d) Reglas sobre prácticas de recepción, envío y almacenaje de documentos que sean objetivas y no discriminatorias.

4.2.6. Plataforma de Soporte a usuarios.

Para proporcionar soporte a los usuarios se deberá cumplir con los siguientes requerimientos:

a) Disponer de sistema de monitoreo.

b) Niveles de escalamiento, ante alarmas y eventos.

c) Sistema de registro de solicitudes de atención.

d) Servicio mínimo de 7x12.

e) Teléfono de contacto y casilla e-mail.

El postulante a PSR podrá proporcionar los siguientes elementos para evaluar el cumplimiento de los requisitos, u otros que antecedente que permitan demostrar el cumplimiento. Un ejemplo de los documentos que podrán presentar son los siguientes:.

- Descripción de infraestructura donde alojan los equipos y servicios principales.
- Descripción, capacidad y características del sistema de detección y extinción de incendios.
- Descripción del sistema de protección perimetral del Site.
- Descripción del esquema de alta disponibilidad.
- Especificaciones de la plataforma de servidores y equipos de respaldo.
- Política y procedimientos de respaldo.
- Contratos y SLA de servicios de comunicación contratados.
- SLA y procedimientos de atención a usuarios.
- En caso de contar con servicios externos de Housing, hosting u otro, se deberá adjuntar los contratos, SLA correspondientes, características específicas del servicio e infraestructura contratada, adjuntando los mismos antecedentes indicados en los numerales anteriores.

4.3. Requisitos Generales de Servicio

Corresponde a:

- Contratos con terceros que mantengan la operatividad tecnológica.
- SLA's de la plataforma tecnológica y los servicios.

En caso de subcontratar servicios, se debe adjuntar contratos, SLA contratados y aspectos técnicos de la plataforma y servicios externos.

Los estándares de servicio mínimo son los indicados en el documento “Especificaciones del Modelo Operacional y Tecnológico de Carpeta de Despacho Electrónica”, entre otros:

a) Tiempo máximo de interrupción del servicio (tiempo de desconexión): 2 horas continuas.

b) Tiempo de respuesta: hasta 5 segundos en el peor caso, inferior a 2 segundos para el 95% de las transacciones.

c) Acceso a bitácoras para registros de los últimos 5 años: hasta 5 segundos en el peor caso, inferior a 2 segundos para el 95% de las transacciones.

d) Acceso a bitácoras para registros de carpetas disponibilizadas, aunque tengan más de 5 años: hasta 5 segundos en el peor caso, inferior a 2 segundos para el 95% de las transacciones.

e) Frecuencia y procedimientos de respaldos: a definir por parte de entidad acreditadora para velar por el cumplimiento de tiempos de disponibilización de carpetas.

f) Tiempo durante el cual una carpeta disponibilizada estará accesible para el Servicio Nacional de Aduanas: al menos 15 días.

g) Ancho de banda disponible: no inferior a 5 Mbps para tráfico entre el Servicio Nacional de Aduanas y el PSR.

h) Latencia de conexión: inferior a 200 ms.

i) Jitter o variabilidad de la conexión: inferior a 150 ms.

j) Pérdida de paquetes en conexión: inferior a 1%.

k) Digitalización de documentos de origen papel: mínimo resolución de 200 ppi, 256 tonos de gris en general, 256 colores para documentos que requieren color.

4.4. Requisitos de seguridad

Son aquellos requisitos que permiten determinar los servicios de seguridad que dispone el PSR para presentar sus servicios. Están relacionados con la valorización de riesgos y amenazas, según las prácticas señaladas en las definiciones del Decreto Supremo N° 83 del 3 de junio de 2004 sobre "Normas técnicas sobre seguridad y confidencialidad del documento electrónico" y las prácticas señaladas en la norma chilena Nch-ISO 27002 - Of.2009 sobre "Código de prácticas para la gestión de la seguridad de la información".

El conjunto de requisitos asociados a la Nch-ISO 27002 que serán solicitados, tanto como las evidencias que deberán ser presentadas, son especificadas en el anexo 2 del presente documento correspondientes a la Matriz de evidencia para la auto evaluación.

5. Evaluación de Requisitos

Se generará una validación por cada una de las ramas especificadas como parte del diseño del sistema. La mejor práctica de validación de la plataforma tecnológica es basada en los estándares ya conocidos, como por ejemplo: TIA/EIA-942 para temas de estructura de Data Center, ITIL, para el manejo y manipulación de la plataforma ya en producción, y otros estándares que hacen mención a lo relacionado a comunicaciones (HTTP o HTTPS), etc.

Para las fases de desarrollo, mantención, explotación y gestión del sistema de registros de carpeta electrónica deberán estar basadas, a lo menos en el marco ITSM (IT Service management) adscribiéndose a algún estándar o patrón de recomendaciones tales como ITIL, MOF, CMMI, ISO 27001, ISO 9000, COBIT, etc.

5.1. Revisión documental

La revisión documental de los antecedentes o evidencia, se realizará a partir de la información provista en el anexo 2 del presenta documento.

5.2. Etapa de revisión “Prueba de aplicación: aspectos técnicos y casos de uso”.

La etapa de revisión de los aspectos técnicos y casos de uso descritos en el documento denominado “Modelo operacional y tecnológico”, se llevarán a cabo en los plazos señalados en el flujo del proceso de acreditación y entre otros considerarán las siguientes acciones:

- Revisión de la funcionalidad de los casos de uso descritos en el documento “Modelo operacional y tecnológico”.
- Configuración del tiempo oficial de Chile para los equipos que compongan la solución y que a lo más exista una diferencia de 0,5 segundos.
- Validar zona horaria, como por ejemplo desfase de no más de 0,5 segundos.
- Realizar visualización de los 3 tipos de documentos definidos. Según el esquema entregado por el Servicio Nacional de Aduanas, la validación de la visualización de los diversos tipos de documentos que contenga una carpeta, es a través del protocolo de visualización en XHTML, donde su estándar está definido y se podrá obtener resultados esperados en las funcionalidades de visualización, no obstante también debe

considerarse visualizar un documento mediante el formato PDF.

- Actividades de notificación de eventos.

5.3. Etapa de revisión visita de verificación.

Finalmente para efectuar la revisión de los requisitos de acreditación se ha contemplado la visita de verificación a las instalaciones de las empresas o agentes de aduana. El detalle de los aspectos a revisar serán definidos por los auditores que componen la comisión de acreditación, en base a los antecedentes entregados por los interesados.

Entre otros podrán realizarse las siguientes verificaciones:

- Controles de paso a Producción.
- Normas para cumplir respecto a Data Center.
- Conectividad o aseguramiento de acceso.
- Validar el tipo de conexión contratado y su uptime de conexión establecido.
- Ambientes de Testing y Producción separados y con restricciones independientes para los usuarios que pueden acceder a cada una.
- Validar redundancia, como por ejemplo: redundancia en fuentes de poder, UPS.
- Realizar distintas acciones y medir tiempos de respuestas.

6. Anexos

6.1. ANEXO 1: Formulario de Postulación a PSR.

	FORMULARIO DE POSTULACIÓN PARA ACREDITACIÓN DE SERVICIOS DE CARPETA ELECTRONICA	
Empresa		
Nombre:		RUT:
Dirección:		
Giro:		
Representante Legal		
Nombre: Nombres / Apellido Paterno / Apellido Materno		RUT:
Dirección:		
Teléfono Fijo:	Teléfono móvil:	e-mail:
Contacto Administrativo		
Nombre: Nombres / Apellido Paterno / Apellido Materno		RUT:
Cargo y Título profesional:		
Dirección:		
Teléfono Fijo:	Teléfono móvil:	e-mail:
Contacto Técnico		
Nombre: Nombres / Apellido Paterno / Apellido Materno		RUT:
Cargo y Título profesional:		
Dirección:		
Teléfono Fijo:	Teléfono móvil:	e-mail:
Dirección de Site / Laboratorios / Servicios:		
Dirección de Site / Laboratorios / Servicios:		
Firma Representante: Solicita : Nombre/ Firmas / timbres / Fecha		Recepción: Firmas / timbres / Fecha

6.2. ANEXO 2:

La planilla se separa por dominios conforme a norma vigente y exigencias particulares de este proyecto.

Se debe completar la condición de cumplimiento (Sí/No) e indicar la evidencia o informe que señale la condición de cumplimiento. La planilla sugiere evidencia a entregar. El postulante deberá entregar la evidencia conforme a sus procesos y estándares.

En el caso de tener servicios externalizados, se deberán proveer los antecedentes de validación que permitan establecer el cumplimiento del tercero.

4.1 Requisitos de la Aplicación

4.3	Requisito	cumple (Si/NO/ No aplica)	Antecedente de cumplimiento y descripción / referencias al documento descriptivo y evidencia.	NIVEL TOLERANCIA A / A-
	Aplicación corre sobre Explorer 8 o sup. y Firefox 3.6 o sup.		Indicar el Browser utilizados. Se verifica al ejecutar ciclo de prueba.	A
a)	Flujograma del proceso indicando aplicaciones y funcionalidades		Entrega de documento técnico con la descripción de la aplicación	A
b)	Especificaciones tecnológicas de aplicativos y sw básico asociado + modelo operacional			A
c)	Descripción Plataforma Operativa		Entrega documento con descripción técnica de la plataforma que soporta la aplicación	A
d)	Especificaciones del proceso de desarrollo y calidad.		Entrega de documento de descripción del proceso para asegurar calidad del producto.	A
e)	Descripción de XML, XLS y XSD utilizadas según definiciones establecidas en el Modelo Operacional.		Entrega de documento XML, XLS y XSD, según lo descrito en el Modelo Operacional.	A
f)	Procedimiento y descripción de firma digital de documentos.		Entrega documento que contenga procedimiento descriptivo del uso de la firma digital.	A
g)	URL al sitio WEB de acceso		Indicar dirección de acceso	A
h)	Procedimiento de digitalización		Entregar documento con descripción del modelo	A-

4.2 Requisitos Generales Infraestructura

UBICACIÓN DEL SITE PRINCIPAL	
UBICACIÓN DEL SITE SECUNDARIO (CONTINGENCIA)	

SITE

4.2.1	Requisito	SITE Principal (Si/NO)	SITE Contingencia (SI/NO)	Antecedente de cumplimiento y descripción / referencia al documento	NIVEL TOLERANCIA A / A-
a	Las instalaciones deberán contar con sistema de temperatura controlada entre 18° y 24° Celsius (climatización).				A
b	La humedad del centro de proceso y almacenamiento deberá estar controlada.				A
c	Control de acceso a las instalaciones, seguridad y control perimetral.				A
d	Construcción Antisísmica				A
e	Alejado de lugares con riesgo de naturaleza (desbordes de ríos, desmoronamientos, aluviones, maremotos, etc.) o actos vandálicos.				A
f	No ubicado en subterráneos o directamente sobre estacionamientos.				A
g	No haber adyacentes tuberías de gas, agua u otro tipo de elementos que pongan en riesgo las instalaciones.				A
h	Sistema de detección de incendios.				A
i	Elementos para extinción manual de incendios.				A
	Certificaciones				
	Contratos Asociados				
	Descripción de infraestructura donde alojan los equipos y servicios.				

Suministro Eléctrico

4.2.2.	Requisito	SITE Principal (Si/NO)	SITE Contingencia (SI/NO)	Antecedente de cumplimiento y descripción / referencia al documento	NIVEL TOLERANCIA A / A-
a	Contener canalización separada de corrientes fuertes y débiles.				A
b	Energía eléctrica no interrumpida con disponibilidad de 99,5%.				A
c	Sistema de UPS de auto respaldo.				A
d	Sistema de continuidad en el suministro eléctrico (grupo electrógeno) para equipos y sistemas de climatización.				A
e	Alimentación 220 volts +/- 5%				A
f	Frecuencia 50 HZ +/- 0.5%				A
g	Tierra de Servicio				A
	Certificaciones				
	Contratos Asociados				

Plataforma de Operación

4.2.3.	Requisito	SITE Principal (Si/NO)	SITE Contingencia (SI/NO)	Antecedente de cumplimiento y descripción / referencia al documento	NIVEL TOLERANCIA A / A-
a	Plataforma de alta disponibilidad.				A
b	Servidores con componentes redundantes.				A
c	Redundancia en Plataforma de Servidores y Equipo de Comunicación.				A
d	Acceso a red de comunicaciones para distintos proveedores.				A
e	Servicio de soporte y mantención para todo el equipamiento involucrado.				A
f	Disponibilidad 99,5% anual.				A
	Esquema de alta Disponibilidad				
	Certificaciones				
	Contratos Asociados				
	SLAs				

Plataforma de Almacenamiento

4.2.4.	Requisito	SITE Principal (Si/NO)	SITE Contingencia (SI/NO)	Antecedente de cumplimiento y descripción / referencias al documento descriptivo y evidencia.	NIVEL TOLERANCIA A / A-
a	Contar con Política y procedimientos de respaldo.				A
b	Política de % mínimo libre de espacio en sistema principal.				A
c	Plataforma de almacenamiento redundante.				A
d	Procedimientos de recuperación de datos y sistemas.				A
	Certificaciones				
	Contratos Asociados				
	SLAs				

Plataforma de Comunicaciones

4.2.5.	Requisito	SITE Principal (Si/NO)	SITE Contingencia (SI/NO)	Antecedente de cumplimiento y descripción / referencias al documento descriptivo y evidencia.	NIVEL TOLERANCIA A / A-
a	Sistema redundante de enlace				A
b	Hardware de comunicaciones en conformación redundante.				A
c	Disponibilidad de 99,5%				A
d	Reglas sobre recepción, envío y almacenaje de documentos a los usuarios finales				A-
	Descripción de plataforma de comunicaciones.				
	Certificaciones				
	SLAs				

Plataforma de Soporte a Usuarios

4.2.6.	Requisito	(Si/NO)		Antecedente de cumplimiento y descripción / referencias al documento descriptivo y evidencia.	NIVEL TOLERANCIA A / A-
a	Disponer de sistema de monitoreo				A-
b	Niveles de escalamiento, ante alarmas y eventos				A
c	Sistema de registro de solicitudes de atención				A-
d	Servicio mínimo de 7x12.				A-
e	Teléfono de contacto y casilla e-mail				A
	Descripción del modelo de soporte a usuarios				
	SLA y procedimientos de atención a usuarios				
	Ubicación del lugar donde operan los servicios de soporte				
	Certificaciones asociadas a soporte de usuarios				
	Contratos de Servicio externalizados				

4.3 Requisitos Generales de Servicio

Estándares de servicio mínimo

4.3	Requisito	cumple (Si/NO)	Antecedente de cumplimiento y descripción / referencias al documento descriptivo y evidencia.	NIVEL TOLERANCIA A / A-
a	Tiempo máximo de interrupción del servicio (tiempo de desconexión): 2 horas continuas.			A
b	Tiempo de respuesta: hasta 5 segundos en el peor caso, inferior a 2 segundos para el 95% de las transacciones.			A
c	Acceso a bitácoras para registros de los últimos 5 años: hasta 5 segundos en el peor caso, inferior a 2 segundos para el 95% de las transacciones.			A
d	Acceso a bitácoras para registros de carpetas disponibilizadas, aunque tengan más de 5 años: hasta 5 segundos en el peor caso, inferior a 2 segundos para el 95% de las transacciones.			A
e	Frecuencia y procedimientos de respaldos			A
f	Tiempo durante el cual una carpeta disponibilizada estará accesible para el Servicio Nacional de Aduanas: al menos 15 días.			A
g	Ancho de banda disponible: no inferior a 5 Mbps para tráfico entre el Servicio Nacional de Aduanas y el PSR.			A
h	Latencia de conexión: inferior a 200 ms.			A
i	Jitter o variabilidad de la conexión: inferior a 150 ms.			A
j	Pérdida de paquetes en conexión: inferior a 1%.			A
k	Digitalización de documentos de origen papel: mínimo resolución de 200 ppi, 256 tonos de gris en general, 256 colores para documentos que requieren color.			A

4.4 Requisitos de Seguridad

DOMINIO	CONTROL ISO 27002	REF. DS-83	AMBITO	CONTROL	ENTREGABLE	NIVEL DE CUMPLIMIENTO	NIVEL TOLERANCIA
						0	
Política de Seguridad	A.5.1.1	Art. 11	Documento de la política de seguridad de la información	¿Existe un documento denominado Política de Seguridad de la información, oficializado, y que refleja claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad?	Política General de Seguridad		A
		Art. 11 a		El documento Política de Seguridad: ¿contiene una definición de seguridad de los activos de información, sus objetivos globales, alcance e importancia?	Política General de Seguridad		A-
	A.5.1.1			En la actualidad, el documento Política de Seguridad: ¿se publica y se comunica a todos los funcionarios y partes externas relevantes?	Pantallazo Intranet, correo institucional, documento o el medio por el cual se publique según sea el caso.		A-
Organización de la Seguridad de la Información	A.6.1.1	Art. 12	Compromiso de la dirección con la seguridad de la información	¿ha designado formalmente un Encargado de Seguridad de la Información?	Documento de Nombramiento		A
	A.6.1.3	Art. 12 a	Asignación de las responsabilidades de la seguridad de la información	En el nombramiento del Encargado de Seguridad de la Información: ¿se encuentra explicitada la función: "Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de su organización y el control de su implementación, y velar por su correcta aplicación"?	Documento de Nombramiento		A-
		Art. 12 b		En el nombramiento del Encargado de Seguridad de la Información: ¿se encuentra explicitada la función: "Coordinar la respuesta a incidentes que afecten a los activos de información institucionales"?	Documento de Nombramiento		A-
	A.6.1.6		Contacto con las autoridades	En la actualidad: ¿existe un procedimiento que especifique cuándo y qué autoridades deben ser contactadas (bomberos, carabineros, PDI, proveedor de Internet, etc)?	Procedimiento		A-

Organización de la Seguridad de la Información	A.6.1.4		Proceso de autorización para medios de procesamiento de información.	En la actualidad: ¿existe un procedimiento de autorización para instalar nuevos medios de procesamiento de información?	Procedimiento de autorización		A
	A.6.1.5		Acuerdos de confidencialidad	En la actualidad: ¿existen acuerdos o contratos de confidencialidad o no-divulgación que reflejen las necesidades de protección de la información?	Acuerdo o contrato con clausula de confidencialidad o no divulgación		A
	A.6.2.1	Art. 10 Letra a	Identificación de los riesgos relacionados con los grupos externos	En la actualidad: ¿Identifica el riesgo para la información y sus medios de procesamiento que surge al involucrar a entidades externas en los procesos de negocio?	Registro de incidentes de seguridad		A
	A.6.2.2	Art. 10 Letra a-b-c	Tratamiento de la seguridad cuando se lidia con terceros	En la actualidad: ¿se abordan todos los requerimientos de seguridad antes de entregar acceso a los activos de información a sus clientes/usuarios/beneficiarios?	Registro de incidentes de seguridad		A
	A.6.2.3	Art. 10 Letra a-b-c	Tratamiento de la seguridad en acuerdos con terceros	En la actualidad: ¿los contratos con terceros que involucren acceso, procesamiento, comunicación o manejo de la información o medios de procesamiento de información, o los contratos que impliquen agregar productos o servicios a los medios de procesamiento de información, abarcan todos los requerimientos de seguridad relevantes?	Registro de incidentes de seguridad		A-
Gestión de Activos	A.7.1.1	Art. 13	Inventario de los activos	¿se identifican los activos de información y se elabora un inventario de ellos?	Inventario de Activos de Información dentro del alcance del proyecto.		A
	A.7.1.2	Art. 14	Propiedad de los activos	¿se ha designado un responsable por los activos de información?	Documento, inventario de Activos de Información con nominaciones, Acta de Acuerdos. Dentro del alcance del proyecto.		A-
	A.7.1.3	Art 15	Uso aceptable de los activos	¿existen normas para el Copiado de los activos de información?	Procedimiento de manipulación. Dentro del alcance del proyecto.		A
				¿existen normas para el Almacenamiento de los activos de información?	Procedimiento de manipulación, dentro del alcance del proyecto.		A
				¿existen normas para Transmisión por correo electrónico de los activos de información?	Procedimiento de manipulación, dentro del alcance del proyecto.		A
				¿existen normas para la Destrucción de los activos de información?	Procedimiento de manipulación, dentro del alcance del proyecto.		A
	A.7.2.2	Art. 15 Art. 16	Etiquetado y manejo de la información	¿existen procedimientos de etiquetado y manejo de los activos de información que consideren dicha clasificación?	Procedimiento de manipulación, dentro del alcance del proyecto.		A-

Seguridad de recursos humanos	A.8.1.1		Roles y responsabilidades	En la actualidad: ¿cuenta con una definición de roles de los funcionarios, tanto contrata, planta como personal a honorarios, que especifiquen su responsabilidad en temas de seguridad de la información?	Manual de RRHH con definición de roles, dentro del alcance del proyecto.		A-
	A.8.1.2		Investigación de antecedentes	En la etapa de selección: ¿Se lleva a cabo la verificación de antecedentes legales, comportamientos éticos, y otros antecedentes de relevancia según la clasificación de la información a la cual va a tener acceso, de todos los candidatos a un cargo, sea de planta, contrata o personal a honorarios?	Check list - Manual RRHH para actuaciones en un proceso de selección dentro del alcance del proyecto.		A
	A.8.2.1	Art. 20 Letra a	Responsabilidades de la dirección	¿ha impartido instrucciones sobre el uso de sistemas informáticos, con énfasis en prohibición de instalación de software no autorizado, documentos y archivos guardados en el computador?	Procedimiento o instrucción dentro del alcance del proyecto		A
		Art. 20 Letra b		¿ha impartido instrucciones sobre el uso de la red interna, uso de Internet, uso del correo electrónico, acceso a servicios públicos, recursos compartidos, servicios de mensajería y comunicación remota?	Procedimiento o instrucción dentro del alcance del proyecto		A
		Art. 20 Letra c		¿ha impartido instrucciones sobre la generación, transmisión, recepción, procesamiento y almacenamiento de activos de información?	Procedimiento o instrucción dentro del alcance del proyecto		A
		Art. 20 Letra d		¿ha impartido procedimientos para reportar incidentes de seguridad?	Procedimiento o instrucción dentro del alcance del proyecto		A
	A.8.3.3		Retiro de los derechos de acceso	¿existe un procedimiento para eliminar los derechos de acceso a los medios de procesamiento de la información de todo el personal, al término de sus funciones o de su contrato, o para ajustarlos según el cambio de funciones?	Procedimiento o instrucción dentro del alcance del proyecto		A-

Seguridad Física y Ambiental	A.9.1.1	Art. 17	Perímetro de seguridad física	¿se utilizan perímetros de seguridad (paredes, rejas controladas por tarjetas o recepcionistas, u otros similares) para proteger las áreas que contienen información y sus medios de procesamiento?	Descripción de la medida de seguridad		A
	A.9.1.2	Art. 17	Controles de ingreso físico	¿se han impartido instrucciones para que sólo acceda personal autorizado a las áreas seguras?	Política o procedimiento dentro del alcance del proyecto.		A
	A.9.1.4	Art. 17	Protección contra amenazas externas e internas	¿Cuenta con protección contra daños causados por fuego?	Descripción de la medida de seguridad		A
		Art. 17		¿Cuenta con protección contra daños causados por inundación?	Descripción de la medida de seguridad		A
				¿Cuenta con protección contra daños causados por terremoto?	Descripción de la medida de seguridad		A
				¿Cuenta con protección contra daños causados por explosión?	Descripción de la medida de seguridad		A
				¿Cuenta con protección contra daños causados por revuelta civil?	Descripción de la medida de seguridad		A
		Art. 17		¿Cuenta con protección contra otras formas de desastres naturales o por causa humana?	Descripción de la medida de seguridad		A
	A.9.1.6	Art. 17	Áreas de acceso público, entrega y carga	¿Ha impartido instrucciones respecto al control de las áreas de acceso público, entrega y carga?	Política o procedimiento dentro del alcance del proyecto.		A-
	A.9.2.1	Art. 17	Ubicación y protección del equipo	¿El equipamiento está ubicado o protegido de forma que se reduzcan las amenazas y peligros ambientales y acceso no autorizado?	Política o procedimiento dentro del alcance del proyecto.		A
		Art. 18 letra a		¿La autoridad ha impartido instrucciones relativas al consumo de alimentos, bebidas y tabaco en las cercanías de los medios de procesan y soportan información?	Política o procedimiento dentro del alcance del proyecto.		A-
	A.9.2.2	Art. 17	Servicios públicos de soporte	¿el equipamiento está protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios básicos de soporte?	Contrato, factura, resolución o informe técnico.		A
	A.9.2.3	Art. 10 Letra a	Seguridad del cableado	¿la autoridad ha impartido instrucciones para proteger contra intercepción o daño el cableado usado para energía y las telecomunicaciones para transmisión de datos o soportan los servicios de información?	Contrato, factura, resolución o informe técnico.		A-
	A.9.2.4		Mantenimiento de equipo	¿se han impartido instrucciones para asegurar que se haga mantenimiento del equipamiento?	Procedimiento dentro del alcance del proyecto o contrato de mantención		A

Seguridad Física y Ambiental	A.9.2.5		Seguridad del equipo fuera de las localidades	¿ha impartido instrucciones para que se aplique seguridad al equipamiento fuera de las dependencias de la institución?	Procedimiento dentro del alcance del proyecto o medida		A-
	A.9.2.6	Art. 26 Letra e	Seguridad de la eliminación o re-uso del equipo	¿se ha establecido que se debe chequear el equipamiento que contiene información para asegurarse que se haya retirado o sobre-escrito cualquier dato confidencial o licencia antes de su eliminación?	Procedimiento dentro del alcance del proyecto o medida		A-
	A.9.2.7		Retiro de propiedad	¿En el servicio se ha previsto que haya una autorización antes del retiro de equipamiento, información o software?	Procedimiento dentro del alcance del proyecto o medida		A-
Gestión de las comunicaciones y operaciones	A.10.1.1	Art. 7 Letra b-c	Procedimientos de operación documentados	Los procedimientos de operación, ¿están documentados, al día y puestos a disposición de todos los usuarios que los necesiten?	Procedimientos formalizados, con control de cambios, para el alcance del proyecto		A-
	A.10.1.2		Gestión del cambio	¿Se controlan los cambios en los medios y sistemas de procesamiento de la información?	Procedimientos de operación, formalizados, para el alcance del proyecto.		A-
	A.10.1.3	Art. 7 Letra f	Segregación de los deberes	Los deberes y áreas de responsabilidad, ¿son segregados de manera de reducir las oportunidades de una modificación no-autorizada o mal uso no-intencional o mal uso de los activos de la institución?	Entregar pantallazo de la aplicación de proyecto, con lista de perfiles de administración.		A
	A.10.1.4		Separación de los medios de desarrollo, prueba y operación	Los medios de desarrollo, prueba y operación, ¿están separados de manera de reducir los riesgos de acceso no-autorizado o cambios en el sistema operacional?	Esquema de desarrollo mostrando arquitectura y diferenciación de los ambientes, de la aplicación del proyecto. Demostrando que operación se encuentra en un ambiente separado de los otros ambientes.		A
	A.10.2.1		Entrega del servicio	¿Se aseguran que los controles de seguridad, definiciones del servicio y niveles de entrega incluidos en el acuerdo de entrega del servicio de terceros se implementen, operen y mantengan?	Acuerdo de niveles de servicio con terceros (contrato, procedimientos, políticas, etc), dentro del alcance del proyecto.		A-
	A.10.2.2		Monitoreo y revisión de los servicios de terceros	Los servicios, reportes y registros provistos por terceros, ¿son monitoreados y revisados regularmente?	Procedimiento de revisión de los niveles de servicio, dentro del alcance del proyecto.		A-
	A.10.2.3		Manejo de cambios en los servicios de terceros	¿Se manejan los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta el grado crítico de los sistemas y procesos del negocio involucrados y la re-evaluación de los riesgos?	Procedimientos de operación para el control de cambios en arquitectura tecnológica, formalizados, dentro del alcance del proyecto.		A

Gestión de las comunicaciones y operaciones	A.10.3.1		Gestión de la capacidad	¿Se monitorea y afina el uso de los recursos?	Reporte de monitoreo en infraestructura dentro del alcance del proyecto.		A-
				¿Se realizan proyecciones de los requerimientos de capacidad futura para asegurar el desempeño requerido del sistema?	Procedimiento de generación de reporte de análisis de capacidad, en infraestructura para el alcance del proyecto.		A-
	A.10.3.2		Aceptación del sistema	¿Se establece el criterio de aceptación de los sistemas de información nuevos, actualizaciones o versiones nuevas?	Procedimientos de operación para el control de cambios en sistemas, formalizados para el alcance del proyecto.		A
	A.10.4.1	Art. 22 Letra c Art. 26	Controles contra códigos maliciosos	¿ Existen controles de detección, prevención y recuperación para proteger contra códigos maliciosos?	Pantallazo de sistemas de prevención de códigos maliciosos (antivirus, antispyware, etc).		A
	A.10.5.1	Art. 24 Letra a-b-c-d-e-f-g	Respaldo de información	¿Se realizan copias de respaldo de la información y software? y	Política de respaldo, procedimiento y evidencia de su ejecución, dentro del alcance del proyecto.		A-
	A.10.6.1		Controles de redes	Las redes, ¿son adecuadamente manejadas y controladas para poder proteger la información y mantener la seguridad de los sistemas y aplicaciones, incluyendo la información en tránsito?	Diagrama de arquitectura de la red.		A-
	A.10.6.2		Seguridad de los servicios de la red	En todo contrato de redes, ¿se identifican e incluyen las características de seguridad?,	Identificación de cláusula de seguridad en contrato de redes con terceros y niveles de servicios.		A-
				¿los niveles de servicio? Y	Identificación de cláusula de seguridad en contrato de redes con terceros y niveles de servicios.		A-
				¿los requerimientos de gestión de todos los servicios de red, ya sea que estos servicios sean provistos interna o externamente?	Identificación de cláusula de seguridad en contrato de redes con terceros y niveles de servicios.		A-
	A.10.7.1	Art. 24 Letra e	Gestión de medios removibles	¿Existen procedimientos para la gestión de los medios removibles?	Procedimiento formalizado para gestión de medios removibles, dentro del alcance del proyecto.		A
	A.10.7.2	Art. 15 Letra b	Procedimientos para el manejo de información	¿Se establecen los procedimientos para el manejo y almacenaje de información para proteger esta información de una divulgación no-autorizada o mal uso?	Procedimiento formalizado para manejo de información, dentro del alcance del proyecto.		A
	A.10.7.3	Art. 15 Letra b	Seguridad de la documentación del sistema	¿Se protege la documentación del sistema de accesos no-autorizados?	Descripción del método de protección de la información.		A

Gestión de las comunicaciones y operaciones	A.10.8.1	Art. 9 Art. 10 Letra a	Políticas y procedimientos de intercambio de información	¿Se establecen políticas, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación?	Política o procedimiento de seguridad de intercambio de información, sancionada.		A
	A.10.8.3		Medios físicos en tránsito	Los medios que contienen información, ¿son protegidos contra accesos no-autorizados, mal uso o corrupción durante el transporte más allá de los límites físicos de una institución?	Política o procedimiento de seguridad de medios físicos en tránsito, sancionada.		A-
	A.10.9.2		Transacciones en-línea	¿Se protege la información involucrada en las transacciones en-línea para evitar una transmisión incompleta, routing equivocado, alteración no-autorizada del mensaje, divulgación no-autorizada, duplicación o repetición no-autorizada del mensaje?	Política de seguridad y/o pantallazo de configuración de seguridad en servicios conectados en redes públicas (uso de certificados SSL, etc).		A
	A.10.9.3	Art. 26 Letra b	Información públicamente disponible	¿Se protege la integridad de la información puesta a disposición en un sistema públicamente disponible para evitar una modificación no-autorizada?	Política de seguridad y/o pantallazo de configuración de seguridad en servicios conectados en redes públicas (uso de certificados SSL, etc).		A
	A.10.10.1	Art. 23	Registro de auditoría	¿Se producen y mantienen registros de auditoría de las actividades, excepciones y eventos de seguridad de la información durante un período acordado para ayudar en investigaciones futuras?	Pantallazo de registros de logs de auditoría		A-
				¿Se monitorea el control de acceso?	Procedimiento formalizado de monitoreo de control de acceso.		A
	A.10.10.4		Registros del administrador y operador	¿Se registran las actividades del administrador del sistema? y	Pantallazo de registros de logs de auditoría		A-
				¿Del operador del sistema?	Pantallazo de registros de logs de auditoría		A-
	A.10.10.5		Registro de fallas	¿Se registran y analizan las fallas?, y	Procedimiento formalizado de registro de fallas y respuestas.		A-
				¿Se toman las acciones necesarias?	Procedimiento formalizado de registro de fallas y respuestas.		A-
	A.10.10.6		Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad, ¿Se sincronizan con una fuente que proporcione la hora exacta acordada?	Procedimiento o pantallazo de la sincronización de relojes de los servidores.		A

Control de acceso	A.11.2.1	Art. 27 Art. 28 Art. 29	Registro del usuario	¿Existe un procedimiento formal para el registro y des-registro del usuario para otorgar y revocar el acceso a todos los sistemas y servicios de información?	Procedimiento formalizado de administración de usuarios		A
	A.11.2.2	Art. 30	Gestión de privilegios	¿Se restringe y controla la asignación y uso de privilegios?	Procedimiento formalizado que contenga gestión de privilegios		A
	A.11.2.3	Art. 32	Gestión de las contraseñas de los usuarios	La asignación de contraseñas, ¿Se controla a través de un proceso de gestión formal?	Procedimiento formalizado que contenga gestion de contraseñas de los usuarios		A
	A.11.3.1	Art. 27	Uso de Contraseñas	¿Se requiere a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de contraseñas?	Política o procedimiento formalizado		A-
	A.11.4.7		Control de routing de la red	¿Se implementan controles de routing en las redes para asegurar que las conexiones de la computadora y los flujos de información no violen la política de control de acceso de las aplicaciones de negocio?	Pantallazo de reglas de Firewall o routing		A
	A.11.5.2	Art. 27	Identificación y autenticación del usuario	¿Todos los usuarios tienen un identificador único (ID de usuario) para su uso personal?, y	Regla de verificación de cuentas de usuario		A
				¿Se escoge una técnica de autenticación adecuada para sustanciar la identidad de un usuario?	Regla de autenticación de usuario		A
	A.11.5.4		Uso de las utilidades del sistema	¿Se restringe y controla estrechamente el uso de los programas de utilidad que podrían ser capaces de superar los controles del sistema y la aplicación?	pantallazo de políticas que restrinjan la instalación de software en el usuario		A
	A.11.5.5	Art. 31 Letra b	Cierre de una sesión por inactividad	Las sesiones inactivas, ¿son cerradas después de un período de inactividad definido?	Procedimiento formalizado, pantallazo de política automatizada		A-
	A.11.5.6		Limitación del tiempo de conexión	¿Se utilizan restricciones sobre los tiempos de conexión para proporcionar seguridad adicional para las aplicaciones de alto riesgo?	Procedimiento formalizado, pantallazo de política automatizada		A-
	A.11.7.1	Art. 7 Letra a Art. 9	Computación y comunicaciones móviles	¿Se establece una política y se adoptan las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móvil?	Politica de seguridad formalizada		A-

Adquisición, desarrollo y mantenimiento de los Sistema de Información	A.12.2.1	10.2.1	Validación de la data de entrada	¿Se valida la input data para las aplicaciones para asegurar que esta data sea correcta y apropiada?	Política o procedimiento formalizado; pantallazo de ejemplo de las reglas de validación de entrada		A
	A.12.2.4	10.2.4	Validación de la data de salida	¿Se validan los datos de salida de una aplicación, para asegurar que el procesamiento de la información almacenada sea el correcto y el apropiado para las circunstancias?	Política o procedimiento formalizado; pantallazo de ejemplo de las reglas de validación de salida		A
	A.12.4.1	10.4.1	Control del software operacional	¿Se establecen procedimientos para el control de la instalación del software en los sistemas operacionales?	Política o procedimiento formalizado de control de instalación del software en los sistemas operacionale		A
	A.12.4.3	10.4.3	Control de acceso al código fuente del programa	¿Se restringe el acceso al código fuente del programa?	Pantallazo del acceso al equipo donde se ubica el código fuente.		A
	A.12.5.1	10.5.1	Procedimientos del control del cambio	¿Se controla la implementación de los cambios mediante el uso de procedimientos formales para el control del cambio?	Política o procedimiento formalizado de control de cambios		A
	A.12.5.2	10.5.2	Revisión técnica de la aplicación después de cambios en el sistema	Cuando se cambian los sistemas de operación, ¿se revisan y prueban las aplicaciones de negocio críticas para asegurar que no exista un impacto adverso sobre las operaciones institucionales o en la seguridad?	Política o procedimiento formalizado de control de cambios		A
	A.12.5.3	10.5.3	Restricciones sobre los cambios en los paquetes de software	Las modificaciones a paquetes de software, ¿Se limitan a los cambios necesarios? Y	Política o procedimiento formalizado de control de cambios		A
				¿Todos los cambios son estrictamente controlados?	Política o procedimiento formalizado de control de cambios		A-
	A.12.5.4	10.5.4	Filtración de información	¿Se evitan las oportunidades para el filtrado de información?	Política o procedimiento formalizado sobre filtración de información.		A
	A.12.5.5	10.5.5	Desarrollo de software abastecido externamente	El desarrollo del software abastecido externamente, ¿es supervisado y monitoreado?	Política o procedimiento formalizado sobre desarrollo de software abastecido externamente.		A
						0	
Gestión de un incidente en la seguridad de la información	A.13.1.1	Art. 12 Letra b	Reporte de eventos en la seguridad de la información	En la actualidad: ¿cuenta con un procedimiento de reporte de eventos que afecten a la seguridad de la información?	Procedimiento o instrucción		A-
	A.13.2.1	Art. 12 Letra b	Responsabilidades y procedimientos	En la actualidad: ¿cuenta con procedimientos para manejar diversos tipos de incidentes de seguridad de la información de forma rápida, eficaz y ordenada?	Procedimiento o instrucción		A-

Gestión de la continuidad del negocio	A.14.1.1		Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio	¿se ha establecido un proceso para gestionar la continuidad del negocio?	Política o procedimiento		A-
	A.14.1.2	Art. 7 Letra d Art. 8	Continuidad del negocio y evaluación del riesgo	¿ha identificado los eventos que pueden causar interrupciones?	Política o procedimiento		A-
				¿Se ha identificado la probabilidad de ocurrencia, el impacto y consecuencias de dichas interrupciones?	Política o procedimiento		A-
	A.14.1.3	Art. 35	Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información	¿hay planes de continuidad de negocio que incluyan la seguridad de la información (disponibilidad en nivel y escala de tiempo después de la falla)?	Política o procedimiento		A-

6.3. ANEXO 3:

A continuación se entrega plantilla para presentar plan de acciones correctivas. Este plan podrá ser propuesto al momento de presentar la solicitud, si en el proceso de autoevaluación la empresa o agente de aduana ha evaluado que no cumple el requisito propuesto y dicho requisito contempla un nivel de tolerancia calificado con A- en el anexo 2.

Este mismo formato deberá ser utilizado si en el proceso de evaluación de antecedentes realizado por el Servicio Nacional de Aduanas, la empresa o agente de aduana es calificada con un A- producto de la revisión de la evidencia presentada.

FORMULARIO DE MEDIDAS CORRECTIVAS Acreditación de proveedores tecnológicos para carpeta de despacho electrónica				
Identificación del requisito	**Descripción de la brecha**	**Descripción de la medida comprometida para subsanar la brecha**	**Plazos**	**Responsable de la implementación**