Firmado digitalmente por :
SALAZAR QUICANA KELLY
LORENA FAU 20509645150 HARD
Motivo : Doy VB
Fecha :
07/03/2024 15:51:43

Firmado digitalmente por :
STEIN LAVARELLO ISRAEL
FAU 20509645150 HARD
Motivo : Doy VB
Fecha :
07/03/2024 16:04:59

Firmado digitalmente por :
REVILLA ARREDONDO JOSE
ANTONIO FAU 20509645150 HARD
Motivo : Doy VB
Fecha :
07/03/2024 17:37:43

REPUBLICA DEL PERU

Firmado digitalmente por :
MOLINA BARRUTIA CARLOS
RODOLFO FAU 20509645150 HARD
Motivo : Soy el Autor
Fecha : 07/03/2024 17:38:56

Resolución de Gerencia General

N° 0160-2024-APN-GG

Callao, 7 de marzo de 2024

VISTO:

El Informe N° 0035-2024-APN-OGA, de fecha 5 de marzo de 2024 de la Oficina General de Administración de la Autoridad Portuaria Nacional;

CONSIDERANDO:

Que, mediante Ley Nº 27943, Ley del Sistema Portuario Nacional (en adelante, LSPN), se creó la Autoridad Portuaria Nacional (APN) como un Organismo Público Descentralizado (ahora, Organismo Técnico Especializado, de acuerdo a lo establecido en la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo y el Decreto Supremo N° 058-2011-PCM), encargado del Sistema Portuario Nacional, adscrito al Ministerio de Transportes y Comunicaciones, dependiente del Ministro, con personería jurídica de derecho público interno, patrimonio propio y con autonomía administrativa, funcional, técnica, económica, financiera y facultad normativa por delegación del Ministro de Transportes y Comunicaciones;

Que, mediante Resolución Ministerial N° 004-2016-PCM, se aprobó el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2004 tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª. Edición”, en todas las entidades integrantes del Sistema Nacional de Información;

Que de acuerdo con lo establecido en el artículo 3 de la Resolución Ministerial Nº 19-2011-PCM, la APN se encuentra sujeta al Sistema Nacional de Informática, por tanto, le resulta de aplicación la resolución ministerial antes mencionada;

Que, mediante Resolución de Gerencia General N° 431-2016-APN/GG de fecha 15 de setiembre del 2016, se aprobó la Política, la Directiva y el Manual del Sistema de Gestión de Seguridad de la Información (en adelante SGSI) de la APN;

Que, mediante Resolución de Gerencia General N° 657-2019-APN/GG, de fecha 8 de agosto del 2019, se aprobó la actualización de documentos del SGSI;

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación:**4HHIn8m**

Que, mediante informe del visto, el Director de la OGA señala que resulta necesario actualizar los documentos del SGSI, y aprobar la versión actualizada de los documentos del SGSI: i) SGSI-PO-05 Política de Adquisición, desarrollo, mantenimiento de Sistemas ii) SGSI-PO-09 Política de Ingeniería de Software, los mismos que adjunta para su aprobación;

Que, mediante Resolución de Acuerdo de Directorio Nº 089-2023-APN/DIR de fecha 20 de diciembre de 2023, el Directorio de la APN resolvió delegar en la Gerencia General la aprobación de las directivas y lineamientos para su aplicación en todas las direcciones, unidades y oficinas de la APN;

Que, en ese contexto, resulta necesario emitir el acto de gestión, destinado a aprobar los documentos del Sistema de Gestión de Seguridad de la Información de la APN, actualizados conforme a la Norma Técnica Peruana vigente;

De conformidad con la Ley N° 27943 – Ley del Sistema Portuario Nacional, Ley N° 29733, Ley de Protección de Datos Personales, el Decreto Legislativo N° 1353, así como el Reglamento de Organización y Funciones - ROF de la APN, aprobado con Decreto Supremo N° 034-2004-MTC.

SE RESUELVE:

Artículo 1.- Aprobar la actualización de los siguientes documentos del Sistema de Gestión de Seguridad de la Información (SGSI), que en anexos adjuntos forman parte de la presente Resolución, los mismos que son:

1. SGSI PO-05 Política de Adquisición, desarrollo, mantenimiento de Sistemas
2. SGSI-PO-09 Política de Ingeniería de Software

Articulo 2.- Notificar la presente Resolución a todas las Direcciones, Unidades y Oficinas de la Autoridad Portuaria Nacional, para su conocimiento y cumplimiento.

Regístrese y Comuníquese

(Firmado digitalmente por)
Carlos Rodolfo Molina Barrutia
Gerente General (e)
Autoridad Portuaria Nacional

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación:**4HHIn8m**

POLÍTICA
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación:**4HHIn8m**

Con Punche Perú

CONTENIDO

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación:**4HHIn8m**

1. OBJETIVO

Garantizar que la seguridad de la información sea parte integral de los sistemas de información en todo el ciclo de vida. Incluyendo los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

2. ALCANCE

La presente política se aplica al personal interno y externo que mantenga vínculo laboral o contractual alguno con la Autoridad Portuaria Nacional; y que participa en la adquisición, desarrollo, actualización o mantenimiento de los aplicativos y sistemas de información.

3. POLÍTICA

3.1. Requisitos de Seguridad de los Sistemas de Información

3.1.1. Análisis y Especificación de los Requisitos de Seguridad de la Información

a) La APN cuenta con Políticas para el Desarrollo de Sistemas de Información: PLT-GP-GestiónProyectos-V1.0, PLT-IP-IngenieriaProyectos-V1.0, PLT-IP-SoporteProyectos-V1.0, donde se establecen directrices, reglas y obligaciones a seguir y acatar por las personas que forman parte de los proyectos, los mismos que son desarrollados utilizando el Método de Trabajo de Desarrollo de Software (MTDS).

b) El Área de Sistemas de Información cuenta con el documento FRM-AREQM04-Especif-Req-SW, en donde se define y aprueban los requerimientos a ser desarrollados en el sistema, especificando el alcance, restricciones y demás características de los mismos; en dicho formato también se han de definir los requisitos de seguridad de la información.

c) Para todos los sistemas desarrollados por o para APN, se deben determinar los requisitos de seguridad de información antes de comenzar la fase de desarrollo de la aplicación, con el fin de evitar o minimizar fallas de seguridad en los sistemas de información a desarrollar, esto lo determina los especialistas de sistemas de información.

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación:**4HHIn8m**

Con Punche Perú

d) Estos requisitos deben ser incorporados en cada fase del ciclo de desarrollo como son: Análisis de Requerimientos, Diseño, Construcción, Pruebas e Implantación.

e) El área de Sistemas de información define los requisitos de seguridad en el documento FRM-AREQM04-Especif-Req.

f) En coordinación con el Oficial de Seguridad de la Información se valida el cumplimiento de los requisitos de seguridad establecidos.

3.1.2. Aseguramiento de los Servicios de Aplicación en las Redes Públicas

a) La información involucrada en los servicios de aplicación que pasan a través de redes públicas es protegida de acuerdo con los requisitos de seguridad definidos en el punto anterior.

3.1.3. Protección de las Transacciones de los Servicios de Aplicación

b) La información implicada en las transacciones de los servicios de aplicación se protege para prevenir la transmisión incompleta, la omisión de envío, la alteración del mensaje, la divulgación, la duplicación o repetición del mensaje no autorizados.

3.2. Seguridad en los Procesos de Desarrollo y Soporte

3.2.1. Política de Desarrollo Seguro

a) Se han contemplado los principios para el desarrollo seguro en el documento SGSI-PO-09 Política Ingeniería de Software.

b) Los requerimientos de seguridad se validan en el documento FRM-AREQM04-Especif-Req-SW, en cada fase de desarrollo, cambio o mantenimiento a los sistemas.

3.2.2. Procedimiento de Control de Cambio del Sistema

a) Se ha determinado que se realiza el versionamiento en el ambiente de integración antes de pasar los cambios al ambiente de pruebas. Esta actividad permite gestionar y controlar los cambios realizados que finalmente modifican el ambiente productivo siendo un requerimiento fundamental para realizar dichas modificaciones. Dicha

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación:**4HHIn8m**

Con Punche Perú

actividad se hace efectiva de acuerdo a lo establecido en el documento MT-MTDS Método de Trabajo de Desarrollo de Software.

b) Se deben realizar las revisiones de la funcionalidad con respecto a seguridad de la información en la fase de pruebas y además en la fase de mantenimiento.

3.2.3. Revisión Técnica de Aplicaciones después de Cambios en la Plataforma Operativa

a) Se debe verificar y garantizar que los cambios realizados no tengan un impacto adverso en las actividades y operaciones críticas del negocio.

b) Se deben realizar pruebas con la finalidad de evidenciar posibles inconvenientes, con la finalidad de evidenciar el cumplimiento de los requisitos de seguridad de la información solicitados y determinar si estos cumplen con los criterios de aceptación definidos en la etapa de análisis.

c) En caso las funcionalidades no satisfagan los requerimientos mínimos de seguridad, OTI debe emitir un informe que especifique las deficiencias de seguridad encontradas y recomendar los controles compensatorios en caso fuesen identificados, para que éstas sean aprobadas por la gerencia del área usuaria aceptando los riesgos encontrados.

3.2.4. Restricciones en Cambios a Paquetes de Software

a) Las modificaciones a paquetes de software deben desalentarse, limitarse solo a cambios necesarios y todos los cambios deberían ser estrictamente controlados.

b) Se debe considerar el impacto ocasionado, si la APN se hace responsable por el futuro mantenimiento del software como consecuencia de los cambios y la compatibilidad con otro software en uso.

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación:**4HHIn8m**

Con Punche Perú

3.2.5. Entorno de Desarrollo Seguro

a) Se ha determinado un ambiente seguro de Desarrollo; solo las personas autorizadas podrán tener acceso a dicho ambiente, de acuerdo con las funciones o actividades asignadas.

3.2.6. Desarrollo Subcontratado

a) La APN supervisa y realiza el seguimiento de las actividades de desarrollo de sistemas subcontratados, considerando:

- ✓ El acuerdo de licencias, la propiedad del código y los derechos de propiedad intelectual relacionado con el contenido de terceros.
- ✓ Los requisitos contractuales para el diseño, la codificación y las pruebas seguros.
- ✓ Las pruebas de aceptación para la calidad y precisión de los entregables.
- ✓ La presentación de pruebas de que se probaron los requisitos de seguridad para establecer los niveles mínimos aceptables de seguridad y calidad.

3.2.7. Pruebas de Seguridad de Sistemas y Pruebas de Aceptación de Sistemas

a) El Área de Sistemas de Información es responsable del desarrollo de pruebas en base a los casos de prueba definidos para validar el cumplimiento de los requerimientos establecidos por la necesidad del usuario. Si el resultado de estas pruebas es satisfactorio, el Área de Sistemas de Información convoca al Usuario Líder para realizar las pruebas de aceptación de usuario. Con la confirmación de dichas pruebas el Usuario Líder brinda la aprobación correspondiente para que el cambio realizado al sistema de información pase al ambiente de Producción.

b) El Área de Sistemas de Información cuenta con el documento OTI-FMT-Acta de Pase a Producción, para realzar el pase del ambiente de pruebas al ambiente de desarrollo.

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación:**4HHIn8m**

Con Punche Perú

3.3. Datos de Prueba

3.3.1. Protección de los Datos de Prueba

a) Se tiene establecido el uso de mecanismos de protección de datos para el caso en que se requiera migrar datos del ambiente de producción hacia el ambiente de desarrollo o pruebas, con la finalidad de utilizarlos en las diversas etapas de los proyectos del Área de Sistemas de Información. Esta actividad se realiza a demanda y para ello el responsable del proyecto deberá solicitar autorización al Oficial de Seguridad, registrando en un documento la solicitud que deberá contener como mínimo el nombre y cargo del solicitante, fecha, nombre del sistema, descripción de información requerida y motivo, autorizaciones correspondientes para la extracción de la información especificada. La tarea solicitada debe incluir el enmascaramiento de la misma antes de ser replicada en el ambiente de pruebas.

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación:**4HHIn8m**

Historial de Cambios del Documento

Fecha	Versión	Descripción	Autor
15.09.16	V 1.0	• Aprobación de la Política.	GG[1]
19.10.16	V 2.0	• Se adicionó el historial de cambios al documento.	OSI[2]
26.09.18	V 3.0	• Se modificó el numeral 3.1.1 análisis y especificación de los requisitos de seguridad de la información, incluyendo las políticas referidas al Método de Trabajo de Desarrollo de Software.	OSI[2]
23.02.24	V 4.0	• Se modificó el numeral 3.1.1, análisis y especificación de los requisitos de seguridad de la información. En el punto c), se adicionó al final: "esto lo determina los especialistas de sistemas de información".	OSI[2]

[1] Gerencia General
[2] Oficial de Seguridad de la Información

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación: **4HHIn8m**

POLÍTICA

INGENIERIA DE SOFTWARE

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación:**4HHIn8m**

Con PUNCHE Perú

CONTENIDO

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación: **4HHIn8m**

1. OBJETIVO

Garantizar que el desarrollo de las aplicaciones de la APN, cuenten con lineamientos de ingeniería de software para el desarrollo seguro.

2. ALCANCE

La presente política se aplica al personal interno y externo que mantenga vínculo laboral o contractual alguno con la Autoridad Portuaria Nacional; y que participa en la adquisición, desarrollo, actualización o mantenimiento de los aplicativos y sistemas de información.

3. POLÍTICA

Es política de APN, ejecutar los proyectos de desarrollo en base a un proceso de ingeniería definido que considere los siguientes lineamientos:

3.1. Recolectar las necesidades, expectativas, restricciones de los usuarios para el desarrollo de sus requerimientos; se deben establecer los requisitos del producto, identificando las interfaces; componentes, los que deben ser analizados y validados (necesarios y suficientes); a fin de asegurar la funcionalidad del producto.

3.2. La solución debe ser el resultado del análisis bajo criterios establecidos, que siguió el proceso descrito en el Método de Trabajo de Desarrollo de Software de la APN. El diseño del producto debe incluir el diseño de las interfaces, así como un análisis de lo que debe desarrollarse, adquirirse o reutilizarse.

3.3. La implementación de principios y mejores prácticas en el desarrollo seguro de software debe ser guiada por los requisitos y metodologías que el responsable de sistemas de información considere, pudiendo ser OWASP, CWE, entre otros. Este proceso debe ser exhaustivamente documentado para garantizar la transparencia y trazabilidad de las decisiones tomadas en el ciclo de desarrollo.

3.4. Se debe verificar el producto con la finalidad de asegurar que satisface los requerimientos especificados, para lo cual se deben seleccionar los productos a verificar, establecer el ambiente donde el producto será verificado y realizar la verificación respectiva, siguiendo los procedimientos y criterios establecidos, los resultados de la verificación deben ser analizados.

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación:**4HHIn8m**

Con Punche Perú

Historial de Cambios del Documento

Fecha	Versión	Descripción	Autor
26.09.2018	V 1.0	• Aprobación de la Política.	GG[1]
21.10.2020	V 2.0	• Se ha de considerar principios y mejores prácticas como (OWASP).	GG[1]
22.12.2023	V 3.0	• Se ha de considerar mejores prácticas de desarrollo seguro para el desarrollo de los software.	GG[1]

[1] Gerencia General

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Autoridad Portuaria Nacional, Aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web http://consultadoc.apn.gob.pe/ e ingresando el siguiente código de verificación:**4HHIn8m**