SEXTO SUPLEMENTO

REGISTRO OFICIAL

ÓRGANO DE LA REPÚBLICA DEL ECUADOR

SUMARIO:

Págs.

Año II - Nº 509 - 184 páginas
Quito, miércoles 4 de agosto de 2021

Oficio Nro. SENAE-DSG-2021-0145-OF

Guayaquil, 22 de mayo de 2021

Asunto: SOLICITUD DE PUBLICACIÓN EN EL R.O DE LA RESOLUCIÓN SENAE-SENAE-2021-0080-RE

Señor Ingeniero
Hugo Del Pozo Berrazueta
REGISTRO OFICIAL DEL ECUADOR
En su Despacho

De mi Consideración:

Con un atento saludo, solicito a usted comedidamente vuestra colaboración, para que se sirva requerir a quien corresponda la publicación en el Registro Oficial, de la Resolución Nro. **SENAE-SENAE-2021-0080-RE,** suscrita por la Mgs. Andrea Colombo Cordero, Directora General del Servicio Nacional de Aduana del Ecuador, del siguiente acto administrativo:

No. Resolución	Asunto:	Páginas
SENAE-SENAE-2021-0080-RE	***"(…) RESUELVE:*** *Artículo Único- Expedir el procedimiento documentado denominado: "SENAE-ME-2-1-001-V1 MANUAL ESPECÍFICO PARA USO DEL ISOLOGOTIPO – PROGRAMA OPERADOR ECONÓMICO AUTORIZADO (OEA)".(...)"*	**02**

Agradezco anticipadamente la pronta publicación de la referida Resolución, no sin antes reiterarle mis sentimientos de distinguida consideración y estima.

Atentamente,

Oficio Nro. SENAE-DSG-2021-0145-OF

Guayaquil, 22 de mayo de 2021

Documento firmado electrónicamente

Lcda. Maria Lourdes Burgos Rodriguez
DIRECTORA DE SECRETARIA GENERAL

Anexos:
- senae-senae-2021-0080-re.pdf

Copia:
Señorita Magíster
Amada Ingeborg Velasquez Jijon
Subdirectora General de Normativa Aduanera

Señor
Manuel Eduardo Villa Asencio
Tecnico en Archivo

Firmado electrónicamente por:
MARIA LOURDES BURGOS RODRIGUEZ

Resolución Nro. SENAE-SENAE-2021-0080-RE

Guayaquil, 21 de mayo de 2021

SERVICIO NACIONAL DE ADUANA DEL ECUADOR

LA DIRECCIÓN GENERAL

CONSIDERANDO:

Que, el numeral 3 del artículo 225 de la Constitución de la República del Ecuador expresamente señala que son entidades del Sector Público, los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado.

Que, el artículo 227 de la Constitución de la República del Ecuador señala que la administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.

Que, en el Capítulo I, Naturaleza y Atribuciones, Título IV de la Administración Aduanera, regulado en el Código Orgánico de la Producción, Comercio e Inversiones, publicado en el Suplemento del Registro Oficial No. 351 del 29 de diciembre de 2010, se señala: "*El servicio de aduana es una potestad pública que ejerce el Estado, a través del Servicio Nacional de Aduana del Ecuador, sin perjuicio del ejercicio de atribuciones por parte de sus delegatarios debidamente autorizados y de la coordinación o cooperación de otras entidades u órganos del sector público, con sujeción al presente cuerpo legal, sus reglamentos, manuales de operación y procedimientos, y demás normas aplicables…"*

Que, dentro de las competencias y atribuciones que tiene el Director General del Servicio Nacional de Aduana del Ecuador, se encuentra determinado en el literal l) del Art. 216 del Código Orgánico de la Producción, Comercio e Inversiones, que establece *"... Expedir, mediante resolución los reglamentos, manuales, instructivos, oficios circulares necesarios para la aplicación de aspectos operativos, administrativos, procedimentales, de valoración en aduana y para la creación, supresión y regulación de las tasas por servicios aduaneros, así como las regulaciones necesarias para el buen funcionamiento de la administración aduanera y aquellos aspectos operativos no contemplados en este Código y su reglamento…"*

Que, mediante Decreto Ejecutivo Nº 312 de fecha 2 de febrero de 2018, el Presidente de la República declara al Programa Operador Económico Autorizado como parte de la política de Facilitación del Comercio Exterior y en su artículo 13 señala el ***"Uso del sello distintivo OEA para efectos de la publicidad de su empresa"*** como uno de los beneficios de los Operadores Económicos Autorizados.

Que, según el Artículo 15 del *REGLAMENTO PARA OBTENER O RENOVAR LA CALIFICACIÓN DE OPERADOR ECONÓMICO AUTORIZADO (OEA)*, expedido mediante Resolución SENAE-SENAE-2019-0063-RE señala que el OEA, de acuerdo a su eslabón, tendrá como uno de los beneficios el ***"Uso del sello distintivo OEA para efectos de la publicidad de su empresa".***

Que, mediante Decreto Ejecutivo Nº 1105 de fecha 21 de julio de 2020, la Mgs. Andrea Paola Colombo, fue designada Directora General del Servicio Nacional de Aduana del Ecuador, de conformidad con lo establecido en el artículo 215 del Código Orgánico de la Producción, Comercio e Inversiones; y, en tal virtud, la Directora General del Servicio Nacional de Aduana del Ecuador, en ejercicio de la atribución y competencia dispuesta en el literal l) del artículo 216 del Código Orgánico de la Producción, Comercio e

Resolución Nro. SENAE-SENAE-2021-0080-RE

Guayaquil, 21 de mayo de 2021

Inversiones, publicado en el Suplemento del Registro Oficial No.351 del 29 de diciembre de 2010.

RESUELVE

Artículo Único- Expedir el procedimiento documentado denominado:

- **"SENAE-ME-2-1-001-V1 MANUAL ESPECÍFICO PARA USO DEL ISOLOGOTIPO – PROGRAMA OPERADOR ECONÓMICO AUTORIZADO (OEA)".**

DISPOSICIONES FINALES

PRIMERA.- La presente resolución entrará en vigencia a partir del día siguiente al de su publicación en el Registro Oficial.

SEGUNDA.-Notifíquese del contenido de la presente Resolución a las Subdirecciones Generales, Direcciones Nacionales, Direcciones Distritales del Servicio Nacional de Aduana del Ecuador.

TERCERA.- Publíquese en la Página Web del Servicio Nacional de Aduana del Ecuador el referido manual y encárguese a la Dirección de Secretaría General del Servicio Nacional de Aduana del Ecuador el formalizar las diligencias necesarias para la difusión y publicación de la presente resolución junto con el referido "**SENAE-ME-2-1-001-V1: MANUAL ESPECÍFICO PARA USO DEL ISOLOGOTIPO – PROGRAMA OPERADOR ECONÓMICO AUTORIZADO (OEA)**" en el Registro Oficial.

Dado y firmado en el Despacho Principal de la Dirección General del Servicio Nacional de Aduana del Ecuador, en la ciudad de Santiago de Guayaquil.

Documento firmado electrónicamente

Mgs. Andrea Paola Colombo Cordero
DIRECTORA GENERAL

Anexos:
- manual_especifico_para_uso_de_isologotipo_-_programa_operador_econÓmico.pdf

Copia:
Señorita Magíster
Amada Ingeborg Velasquez Jijon
Subdirectora General de Normativa Aduanera

Señora Magíster
Angelita Karoly Santistevan Torres
Subdirectora General de Operaciones

Señora Economista
Alba Alegria Villamar Andrade
Subdirectora General de Gestión institucional

wfaz/menr/av

Firmado electrónicamente por:
ANDREA PAOLA COLOMBO CORDERO

SENAE-ME-2-1-001-V1

MANUAL ESPECÍFICO PARA USO DEL ISOLOGOTIPO - PROGRAMA OPERADOR ECONÓMICO AUTORIZADO (OEA)

ABRIL 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento detalla el procedimiento para el uso del sello distintivo del Operador Económico Autorizado (OEA) por parte de los Operadores de Comercio Exterior que ostenten la calificación de OEA otorgada por el Servicio Nacional de Aduana del Ecuador (SENAE).		
Objetivo:		
Establecer el procedimiento que permita estandarizar el manejo del isologotipo del Programa OEA como beneficio, con la finalidad de poner en conocimiento del usuario las condiciones, responsabilidades, prohibiciones y su correcto uso.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
X Firmado electrónicamente por: WILSON FABRICIO ALCIVAR ZAVALA Mgp. Wilson Fabricio Alcívar Zavala Especialista en Cooperación Internacional Adu...	Programa OEA	Elaboración
X Firmado electrónicamente por: XAVIER ANDRES SAENZ DE VITERI CAMACHO Lcdo. Xavier Andrés Sáenz de Viteri Camacho Director de Relaciones Aduaneras Internacion...	Dirección de Relaciones Aduaneras Internacionales	Revisión
X Firmado electrónicamente por: MARIA EUGENIA NAVARRETE PEREZ Sra. Maria Eugenia Navarrete Perez Directora de Comunicación	Dirección de Comunicación	Revisión
X Firmado electrónicamente por: AMADA INGEBORG VELASQUEZ JIJON Ab. Amada Ingerborg Velásquez Jijón Subdirectora General de Normativa Aduanera	Subdirección General de Normativa Aduanera	Aprobación

Actualizaciones / Revisiones / Modificaciones:			
Versión	**Fecha**	**Razón**	**Responsable**
1	Abril 2021	Versión Inicial	Mgp. Fabricio Alcívar

ÍNDICE

1. OBJETIVO

Describir las actividades que debe tener en cuenta un OCE calificado como **Operador Económico Autorizado (OEA)** para usar el sello distintivo que compone la identidad visual del Programa OEA, así como determinar las pautas y condiciones según las cuales una empresa calificada pueda utilizar el isologotipo OEA.

2. ALCANCE

Está dirigido a todos los Operadores de Comercio Exterior (OCE) que hayan sido calificados como OEA. Este manual establece las directrices del uso del isologotipo del Programa OEA, y no comprende el proceso de obtención de la calificación OEA en sus etapas de condiciones y requisitos.

3. RESPONSABILIDAD

Los Operadores Económicos Autorizados no deberán descomponer, alterar el orden de los textos o alterar de ninguna otra forma el isologotipo OEA, debiendo permanecer junto a los textos como una sola imagen.

Los Operadores Económicos Autorizados, serán responsables de cumplir con las consideraciones generales, condiciones de uso y las especificaciones técnicas sobre el área de protección y tamaño mínimo establecidas en el presente documento, y proporcionar la información o documentación que sea requerida por los especialistas del Programa OEA.

Los especialistas del Programa OEA son los responsables de analizar, verificar y comprobar la correcta aplicación del presente manual.

Los especialistas del Programa OEA y la Dirección General de Secretaria, son responsables de realizar y gestionar los cambios que fueren necesarios en este manual, para su actualización y su difusión.

4. NORMATIVA VIGENTE

- Decreto Ejecutivo No. 312 del 02 de febrero del 2018.
- Código Orgánico de la Producción, Comercio e Inversiones, publicado en el Suplemento Registro Oficial No. 351, del 29 de diciembre del 2010.
- Reglamento al Código Orgánico de la Producción, Comercio e Inversión publicado en Registro Oficial No. 452, del 19 de mayo del 2011.
- Resolución No. SENAE-SENAE-2019-0063-RE del 06 de agosto del 2019 publicado en Registro Oficial Edición Especial 34 del 16 de agosto del 2019.
- Resolución No. SENAE-SENAE-2019-0064-RE del 06 de agosto del 2019 publicado en Registro Oficial Edición Especial 34 del 16 de agosto del 2019.

- Resolución No. SENAE-SENAE-2019-0086-RE del 24 de septiembre del 2016 publicado en Registro Oficial Edición Especial No. 111, martes 22 de octubre 2019.

5. CONSIDERACIONES GENERALES

5.1 Con el propósito de que se apliquen los términos de manera correcta, a continuación se presentan algunas definiciones inherentes al presente documento:

Calificación OEA: Es la calidad otorgada al operador de comercio exterior que cumple con las condiciones y requisitos, establecidos en el Programa Operador Económico Autorizado, la misma que tendrá validez de tres (3) años a partir de la resolución expedida por la máxima autoridad de la administración aduanera.

Especialista OEA: Es el funcionario aduanero encargado de realizar las validaciones documentales y de campo a los postulantes, elaborar los informes de aceptación o rechazo de la postulación del operador de comercio exterior en análisis, así como las demás actividades establecidas para el cumplimiento de su gestión.

Isologotipo OEA: Es el identificador gráfico que sirve para identificar al operador de comercio exterior calificado como OEA, formado por la unión del símbolo gráfico del SENAE y el texto Operador Económico Autorizado.

Operador Económico Autorizado OEA: Es la persona natural o jurídica involucrada en el movimiento internacional de mercancías, cualquiera que sea la función que haya asumido, que cumpla con las normas equivalentes de seguridad de la cadena logística establecidas por el Servicio Nacional de Aduana del Ecuador, para acceder a facilidades en los trámites aduaneros. Los Operadores Económicos Autorizados incluyen, entre otros, a fabricantes, importadores, exportadores, transportistas, consolidadores, desconsolidadores, agentes de carga internacional, puertos, aeropuertos, depósitos aduaneros, depósitos temporales, courier, operadores de terminales, y se regularán conforme las disposiciones que para el efecto emita la Directora o el Director General.

Programa OEA: El Programa de Operador Económico Autorizado es una iniciativa impulsada por la OMA, normada mediante el Marco SAFE, cuyo objetivo es garantizar la seguridad en la cadena logística y la facilitación del comercio internacional.

Solicitante: Se refiere a la empresa calificada como OEA así como a su representante legal o a quien a su vez él delegue como representante de la empresa calificada, por ejemplo el Gerente de Logística, Gerente de Comercio Exterior, etc.

5.2 El *"Uso del sello distintivo OEA para efectos de la publicidad de su empresa."* es uno de los beneficios de los Operadores Económicos Autorizados estipulado mediante el Decreto Ejecutivo 312 y mediante la Resolución No. SENAE-SENAE-2019-0063-RE

5.3 El solicitante deberá utilizar el isologotipo OEA únicamente del modo y por el periodo autorizado por la administración aduanera, siendo objeto de control en las revalidaciones

5.4 La autorización para utilizar el isologotipo OEA no confiere ningún derecho exclusivo para su uso, ni tampoco significa que se permita inscribir el símbolo o una imitación del mismo en una marca o en cualquier otro derecho de propiedad intelectual.

5.5 El uso indebido del isologotipo OEA, podrá ser objeto de control de conformidad a lo establecido en el en el Decreto Ejecutivo No. 312, y causal de suspensión según se establece en el "*Reglamento Para Obtener o Renovar la Calificación de Operador Económico Autorizado (OEA)*".

5.6 Tras la suspensión o revocatoria de la Calificación OEA, el solicitante debe retirar el uso de todo material publicitario que contenga una referencia al isologotipo OEA. En caso de que la administración aduanera identifique que un OCE hace uso del isologotipo OEA después de la revocatoria de su calificación, se procederá con la falta reglamentaria correspondiente.

5.7 Todos los cambios o actualizaciones del presente manual se publicarán en la página web del Servicio Nacional de Aduana del Ecuador.

6. CONDICIONES DE USO

El isologotipo OEA podrá ser utilizado por los solicitantes tanto y cuanto se cumplan las siguientes condiciones:

6.1 El isologotipo OEA siempre deberá estar acompañada de la imagen institucional del solicitante, en ningún caso podrá exhibirse el sello distintivo OEA en forma independiente con la especificación "Operador Económico Autorizado" y "Servicio Nacional de Aduanas del Ecuador".

6.2 No debe haber ambigüedad, con el isologotipo OEA o en el texto que lo acompaña. No debe darse a entender que la calificación OEA aplique a varias actividades del comercio exterior que pudiera tener el OCE, únicamente su uso irá ligado al eslabón calificado por la administración aduanera por ejemplo: OEA importador; OEA exportador.

6.3 El isologotipo OEA debe ser utilizado para promocionar la calificación del solicitante y podrá ser utilizado dentro del período de validez de la calificación OEA.

6.4 Para efectos del uso del isologotipo OEA, se aplicarán los colores especificados por el Servicio Nacional de Aduana del Ecuador, sin embargo se permitirá ampliaciones o reducciones sin alterar la forma del isologotipo.

6.5 El isologotipo OEA se podrá utilizar en los documentos (hojas membretadas, tarjetas de presentación, sobres, carpeta institucional) del solicitante.

6.6 El solicitante puede utilizar el isologotipo OEA con fines publicitarios bajo el compromiso de no modificarlo.

6.7 El solicitante deberá solicitar el uso del isologotipo OEA por la vía formal, mediante una carta dirigida a la máxima autoridad del Servicio Nacional de Aduana del Ecuador, suscrita de forma electrónica por el representante legal e ingresada a través de los canales electrónicos autorizados por la institución para la recepción de documentos.

6.8 Conforme las atribuciones del Servicio Nacional de Aduana del Ecuador, se autorizará al solicitante el uso del isologotipo OEA, como parte de los beneficios reconocidos en la normativa vigente.

6.9 La autorización de uso podrá concederse siempre que el isologotipo OEA no se utilice de forma que pueda inducir al público a creer erróneamente que los servicios o bienes que elabora o realiza el solicitante son auspiciados por el Servicio Nacional de Aduana del Ecuador.

6.10 El isologotipo OEA no podrá ser utilizado de modo que pueda causar descrédito, perjudicar la reputación o dañar la imagen del Programa OEA, y en consecuencia del Servicio Nacional de Aduana del Ecuador.

6.11 En caso de suspensión o revocatoria, el solicitante deberá eliminar el isologotipo OEA asociado a su logotipo empresarial como publicidad de su calificación, esto con el fin de evitar el uso de isologotipo de manera engañosa, y que pueda confundir al consumidor o traer descredito al programa OEA o al Servicio Nacional de Aduana del Ecuador.

6.12 El uso del isologotipo OEA por parte del solicitante, debe ir siempre acompañado del nombre de la empresa.

7. ESPECIFICACIONES TÉCNICAS – ÁREA DE PROTECCIÓN Y TAMAÑO MÍNIMO

7.1 El isologotipo OEA original está creado en ilustración 100% vertical, por lo que puede escalarse a cualquier tamaño sin pérdida de definición o calidad. Las versiones rasterizadas o en píxeles son derivaciones de la original vectorial.

7.2 El tamaño mínimo de aplicación del isologotipo OEA para medios impresos y medios digitales depende de la calidad y la resolución de cada medio, de manera que se garantice una lectura clara de sus detalles.

7.3 En el caso de medios digitales, el isologotipo OEA no debe de ser aplicado a tamaños inferiores a 100 píxeles de ancho.

7.4 Alrededor del isologotipo OEA tiene que aparecer un espacio libre de al menos una unidad básica de altura y anchura en X. En esta área no deberán colocarse otros elementos gráficos o logos. Asimismo, esta zona debe respetarse a la hora de establecer la distancia respecto a los márgenes de la página. Este espacio libre es el mínimo espacio que debe incluirse; se recomienda aumentarlo siempre que sea posible.

7.5 El solicitante debe asegurar la legibilidad del isologotipo OEA en todo momento. En base a esta premisa, se generará un marco de protección que no debe ser invadido por ningún elemento externo. El isologotipo está enmarcado en una cuadricula de 9 x 7.

7.6 Con el fin de garantizar su consistencia y legibilidad, el isologotipo OEA no debe ser aplicado en un tamaño menor a 12 mm, no obstante, el isologotipo OEA se puede ampliar proporcionalmente tanto en alto como en ancho sin alterar la imagen.

7.7 El isologotipo OEA deberá ir acompañado por el logotipo del solicitante.

7.8 COLORES E IMPRESIÓN DEL SIMBOLO:

7.8.1 Los códigos de color establecidos para el texto "Operador Económico Autorizado" en el isologotipo OEA es azul (Pantone - C) y el texto "Aduana del Ecuador" es negro 100%. Para su correcta aplicación en medios físicos y digitales, existen algunas variantes que se presentan más adelante. El texto en ningún caso se podrá utilizar independientemente del símbolo.

7.8.2 Los colores del isologotipo son basados en la cromática institucional del Servicio Nacional de Aduana del Ecuador manteniendo los tonos amarillo azul y rojo centrales de la marca en este caso se aplica también al isologotipo OEA, el tono del isologotipo es azul oscuro. La cromática está definida de la siguiente manera.

7.8.3 Por funciones prácticas, se define una versión especial la cual debe ser usada únicamente cuando las limitantes técnicas de producción como impresiones monocromáticas, o cualquier otra aplicación que impida el uso de la versión principal de la identidad visual.

7.8.4 En el caso que la impresión sea en blanco y negro (por ejemplo, avisos pequeños de prensa). La opción por lo tanto tiene que ser limitada a blanco y negro:

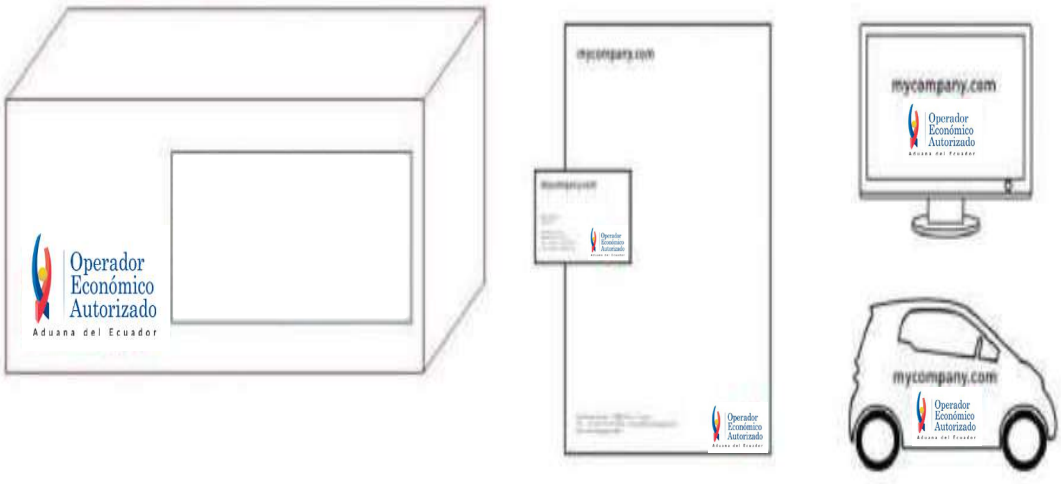
8. NOTAS SOBRE EL ISOLOGOTIPO OEA

8.1 El isologotipo OEA estará disponible en dos formatos: jpeg e Illustrator.

8.2 En ningún caso un solicitante puede permitir que se use su isologotipo OEA asociándolo a otras empresas y marcas que no han sido calificadas como OEA.

8.3 El uso del isologotipo OEA no es obligatorio para los solicitantes, sin embargo, en caso de implementarlo, se debe realizar siguiendo estos tres aspectos:

Ejemplos de uso del isologotipo OEA:



Descripción del Requisito	Operador Económico Autorizado Aduana del Ecuador	Operador Económico Autorizado Aduana del Ecuador **Con la declaración del producto**
Exclusivamente en los siguientes materiales de papelería: Hoja membretada, sobres, carpeta institucional, tarjetas de presentación.	Permitido	Permitido
Exclusivamente en los siguientes materiales publicitarios: Stands, banners, publicaciones en redes sociales y páginas webs, carteleras físicas y digitales, anuncios en medios de comunicación digital o escrito.	Permitido	Permitido
En panfletos, sitio web o publicidad.	Permitido	Permitido

8.4 El isologotipo se puede aplicar de las siguientes formas: en la literatura, folletos, en la publicidad corporativa y página web; en vehículos de la empresa, tales como camiones y furgonetas; en la empresa dentro de los pendones utilizados; en la exposición de equipos y pantallas de la compañía; y, otras afines a las antes descritas.

8.5 En caso de que el solicitante requiera una declaración sobre la calificación de su representada esta deberá ser: *"Este servicio ha sido provisto bajo los estándares de la Calificación OEA bajo los controles establecidos por el Servicio Nacional de Aduana del Ecuador"*. La declaración no implicará en modo alguno que el producto, proceso o servicio esté certificado por la administración aduanera.

8.6 Al utilizar el isologotipo OEA se deberá prestar atención a que no se infrinjan las condiciones generales de uso del presente manual expedido por el Servicio Nacional de Aduana del Ecuador.

8.7 Está prohibida la utilización del isologotipo OEA en informes de pruebas de laboratorio, calibración o inspección, certificados de labores o trabajo, certificados de competencias, certificados de aprobación de productos, estudios, recomendaciones, entre otros que sean ajenos a la operación certificada; pues, se considera que dicha información son productos en este contexto.

8.8 El solicitante está autorizado a exhibir su calificación OEA de aprobación en su lugar de trabajo o en cualquier aviso publicitario, promocional o impreso, teniendo en cuenta el cumplimiento de las condiciones expresadas en el presente manual. Adicionalmente está autorizado a exhibir el isologotipo OEA en su papelería y en cualquier otro impreso promocional, así como en presentaciones de la empresa.

9. PROCEDIMIENTO

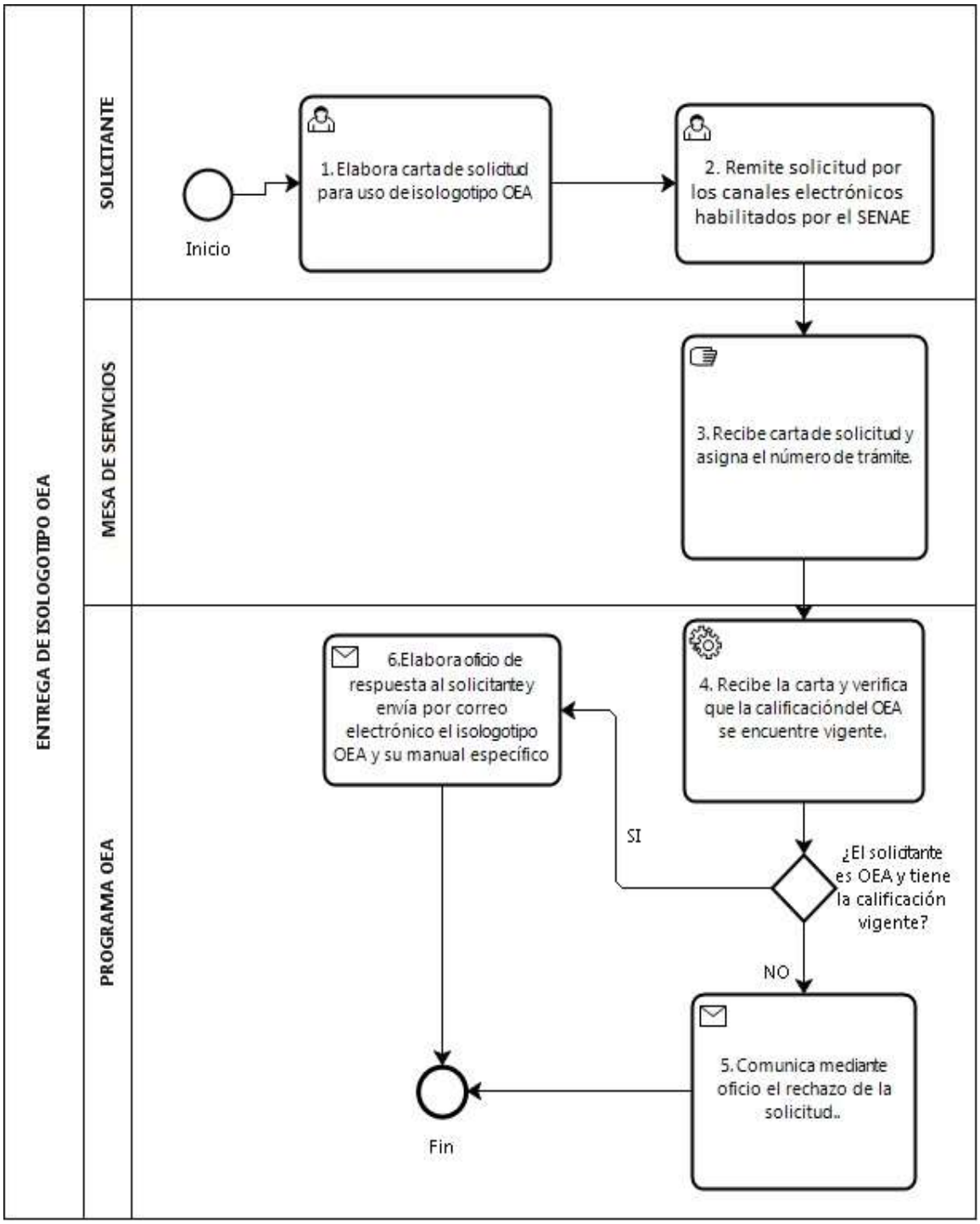
9.1 Para la entrega de isologotipo OEA:

N°	Actividad	Producto de Entrada	Descripción de Actividad	Responsable	Producto de Salida
1	Elabora la solicitud para uso de isologotipo OEA	Carta, Ruc, Cédula, Nombramiento y Resolución Autorización OEA	El solicitante elabora una carta firmada por el Representante Legal, en la cual expresa su deseo de utilizar el beneficio del uso isologotipo OEA	Solicitante	Carta de solicitud de uso isologotipo OEA con fines publicitarios
2	Remite la solicitud por los canales electrónicos habilitados por el SENAE	Carta, Ruc, Cédula, Nombramiento y Resolución autorización OEA	El solicitante remite la solicitud a través del correo electrónico: mesadeservicios@aduana.gob.ec	Solicitante	Carta de solicitud de uso isologotipo OEA con fines publicitarios

N°	Actividad	Producto de Entrada	Descripción de Actividad	Responsable	Producto de Salida
3	Recibe carta de solicitud y asigna el número de trámite	Carta, Ruc, Cédula, Nombramiento y Resolución autorización OEA	Mesa de Servicios asigna un número de trámite para su seguimiento. Posteriormente, esta documentación es remitida y derivada al Programa OEA	Mesa de Servicios	Carta de solicitud de uso de isologotipo OEA con fines publicitarios con número asignado
4	Recibe la solicitud y verifica que la calificación del OEA se encuentre vigente	Carta de solicitud de uso de isologotipo OEA con fines publicitarios con número asignado	Una vez recibida la solicitud se revisa que la calificación se encuentre vigente y continúa con el paso 6; caso contrario continúa con la actividad 5	Programa OEA	Análisis de la vigencia de la Calificación OEA
5	Comunica mediante oficio el rechazo de la solicitud	Análisis preliminar de la documentación	El Programa OEA en un plazo no mayor a 5 días elabora un oficio dirigido al solicitante a través del cual se comunica que no procede su solicitud	Programa OEA	Oficio del Programa OEA
6	Elabora oficio de respuesta al solicitante y envía por correo electrónico el isologotipo OEA y su manual específico	Oficio del Programa OEA dirigido al solicitante	El Programa OEA elabora un oficio dirigido al solicitante autorizando uso de isologotipo. Adicionalmente, a través de correo electrónico adjunta el isologotipo OEA y el manual específico	Programa OEA	Oficio enviado al usuario y el isologotipo OEA mediante correo electrónico en formatos: JPEG e Illustrator

10. FLUJOGRAMA

10.1 El flujograma del proceso a seguir para la entrega de isologotipo OEA se muestra a continuación:



Oficio Nro. SENAE-DSG-2021-0147-OF

Guayaquil, 22 de mayo de 2021

Asunto: SOLICITUD DE PUBLICACIÓN EN EL R.O. DE LA RESOLUCIÓN SENAE-SENAE-2021-0082-RE.

Señor Ingeniero
Hugo Del Pozo Berrazueta
REGISTRO OFICIAL DEL ECUADOR
En su Despacho

De mi Consideración:

Con un atento saludo, solicito a usted comedidamente vuestra colaboración, para que se sirva requerir a quien corresponda la publicación en el Registro Oficial, de la Resolución Nro. **SENAE-SENAE-2021-0082-RE,** suscrita por la Mgs. Andrea Colombo Cordero, Directora General del Servicio Nacional de Aduana del Ecuador, del siguiente acto administrativo:

No. Resolución	Asunto:	Páginas
SENAE-SENAE-2021-0082-RE	*"(…) **RESUELVE:** Artículo Único: Expedir las siguientes políticas de seguridad de la información, denominadas:(....)"*	**06**

Agradezco anticipadamente la pronta publicación de la referida Resolución, no sin antes reiterarle mis sentimientos de distinguida consideración y estima.

Atentamente,

Documento firmado electrónicamente

Lcda. Maria Lourdes Burgos Rodriguez
DIRECTORA DE SECRETARIA GENERAL

Anexos:
- senae-senae-2021-0082-re0923413001621721110.pdf

Oficio Nro. SENAE-DSG-2021-0147-OF

Guayaquil, 22 de mayo de 2021

Copia:
Señorita Magíster
Amada Ingeborg Velasquez Jijon
Subdirectora General de Normativa Aduanera

Señor
Manuel Eduardo Villa Asencio
Tecnico en Archivo

Firmado electrónicamente por:
MARIA LOURDES BURGOS RODRIGUEZ

Resolución Nro. SENAE-SENAE-2021-0082-RE

Guayaquil, 22 de mayo de 2021

SERVICIO NACIONAL DE ADUANA DEL ECUADOR

LA DIRECCIÓN GENERAL

CONSIDERANDO

Que, el numeral 3 del artículo 225 de la Constitución de la República del Ecuador expresamente señala: *"Los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado";*

Que, el artículo 227 de la Constitución de la República del Ecuador señala que la *"La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación";*

Que, en el Capítulo I, Naturaleza y Atribuciones, Título IV de la Administración Aduanera, regulado en el Código Orgánico de la Producción, Comercio e Inversiones, publicado en el Suplemento del Registro Oficial No. 351 del 29 de diciembre de 2010, se señala: *" El servicio de aduana es una potestad pública que ejerce el Estado, a través del Servicio Nacional de Aduana del Ecuador, sin perjuicio del ejercicio de atribuciones por parte de sus delegatarios debidamente autorizados y de la coordinación o cooperación de otras entidades u órganos del sector público, con sujeción al presente cuerpo legal, sus reglamentos, manuales de operación y procedimientos, y demás normas aplicables...";*

Que, de conformidad a las competencias y atribuciones que tiene el Director General del Servicio Nacional de Aduana del Ecuador, se encuentra determinado en el literal l) del Art. 216 del Código Orgánico de la Producción, Comercio e Inversiones, *"l) Expedir, mediante resolución los reglamentos, manuales, instructivos, oficios circulares necesarios para la aplicación de aspectos operativos, administrativos, procedimentales, de valoración en aduana y para la creación, supresión y regulación de las tasas por servicios aduaneros, así como las regulaciones necesarias para el buen funcionamiento de la administración aduanera y aquellos aspectos operativos no contemplados en este Código y su reglamento...";*

Que, mediante Acuerdo-Ministerial-No. 025-2019 del Ministerio de Telecomunicaciones y de la Sociedad de la Información se acuerda: "*Expedir el Esquema Gubernamental de Seguridad de la Información -EGSI-, el cual es de implementación obligatoria en las instituciones de la Administración Pública Central, Institucional y que dependen de la*

Resolución Nro. SENAE-SENAE-2021-0082-RE

Guayaquil, 22 de mayo de 2021

Función Ejecutiva", con lo cual se actualiza la normativa sobre seguridad informática;

Que, en el Acuerdo Nro. 039 de la Contraloría General del estado, publicado en el Registro Oficial 78 de fecha 1 diciembre de 2009, sección 410-04 *"Políticas y procedimientos",* se indica: *"La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria";*

Que, es menester actualizar las políticas de seguridad de la información de aplicación interna, para garantizar de que cumplan con las normas técnicas vigentes, los cuales serán de aplicación a nivel nacional y con carácter obligatorio; y

Que, mediante Decreto Ejecutivo Nro. 1105 de fecha 21 de julio de 2020, la Ing. Andrea Colombo Cordero fue designada Directora General del Servicio Nacional de Aduana del Ecuador, de conformidad con lo establecido en el artículo 215 del Código Orgánico de la Producción, Comercio e Inversiones; y el artículo 11, literal d) del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva;

En tal virtud, la Directora General del Servicio Nacional de Aduana del Ecuador, en ejercicio de la atribución y competencia dispuesta en el literal l) del artículo 216 del Código Orgánico de la Producción, Comercio e Inversiones, publicado en el Suplemento del Registro Oficial No. 351 del 29 de diciembre de 2010.

RESUELVE:

Artículo Único: Expedir las siguientes políticas de seguridad de la información, denominadas:

Codificación	Nombre de Documento
SENAE-PI-3-2-001-V2	POLÍTICAS INSTITUCIONALES PARA EL ACCESO Y USO DEL INTERNET.
SENAE-PI-3-2-002-V2	POLÍTICAS INSTITUCIONALES PARA EL USO DEL CORREO ELECTRÓNICO.
SENAE-PI-3-2-003-V2	POLÍTICAS INSTITUCIONALES DEL PROCEDIMIENTO FORMAL PARA EL REPORTE ESCALADA Y RESPUESTA ANTE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Resolución Nro. SENAE-SENAE-2021-0082-RE

Guayaquil, 22 de mayo de 2021

SENAE-PI-3-2-004-V3	POLÍTICAS INSTITUCIONALES DE LOS REQUERIMIENTOS MÍNIMOS DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
SENAE-PI-3-2-005-V2	POLÍTICAS INSTITUCIONALES PARA EL ACCESO A SISTEMAS DE INFORMACIÓN.
SENAE-PI-3-2-006-V3	POLÍTICAS INSTITUCIONALES DE LOS REQUERIMIENTOS DE SEGURIDAD PARA RESPALDOS DE LA INFORMACIÓN.
SENAE-PI-3-2-007-V2	POLÍTICAS INSTITUCIONALES DEL CATALOGO DE PERFILES DE ACCESO PARA CUENTAS DE USUARIOS.
SENAE-PI-3-2-008-V2	POLÍTICAS INSTITUCIONALES PARA EL USO DE LOS SISTEMAS DE VIDEOCONFERENCIA.
SENAE-PI-3-2-009-V2	POLÍTICAS INSTITUCIONALES DE LOS REQUERIMIENTOS MÍNIMOS DE SEGURIDAD PARA ESTACIONES DE TRABAJO Y EQUIPOS DE CENTRO DE CÓMPUTO.
SENAE-PI-3-2-010-V2	POLÍTICAS INSTITUCIONALES DEL PROCEDIMIENTO DE BORRADO SEGURO EN LOS DISPOSITIVOS DE ALMACENAMIENTO DE LAS ESTACIONES DE TRABAJO.
SENAE-PI-3-2-011-V2	POLÍTICAS INSTITUCIONALES DE SEGURIDAD PARA LOS EQUIPOS INFORMÁTICOS
SENAE-PI-3-2-012-V2	POLÍTICAS INSTITUCIONALES PARA EL PROCEDIMIENTO DE GESTIÓN DE PARCHES DE SOFTWARE
SENAE-PI-3-2-013-V2	POLÍTICAS INSTITUCIONALES PARA EL CONTROL DE CAMBIOS A LOS PROCESOS OPERATIVOS DE LA JEFATURA DE INFRAESTRUCTURA TECNOLÓGICA
SENAE-PI-3-2-014-V2	POLÍTICAS INSTITUCIONALES PARA LA PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Resolución Nro. SENAE-SENAE-2021-0082-RE

Guayaquil, 22 de mayo de 2021

SENAE-PI-3-2-015-V2	POLÍTICAS INSTITUCIONALES PARA LA CLASIFICACIÓN Y ENTREGA DE INFORMACIÓN
SENAE-PI-3-2-016-V2	POLÍTICAS INSTITUCIONALES PARA LA ADMINISTRACIÓN DE LAS CLAVES DE LAS CUENTAS DE USUARIOS PRIVILEGIADOS DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

DISPOSICIÓN DEROGATORIA

Única: Dejar sin efecto las siguientes políticas de seguridad de la información, denominadas:

Codificación	Resolución
SENAE-PI-3-2-001-V1	SENAE-DGN-2015-0591-RE
SENAE-PI-3-2-002-V1	SENAE-DGN-2015-0590-RE
SENAE-PI-3-2-003-V1	SENAE-DGN-2015-0627-RE
SENAE-PI-3-2-004-V2	SENAE-SENAE-2021-0052-RE
SENAE-PI-3-2-005-V1	SENAE-DGN-2015-0629-RE
SENAE-PI-3-2-006-V2	SENAE-SENAE-2017-0346-RE
SENAE-PI-3-2-007-V1	SENAE-DGN-2015-0633-RE
SENAE-PI-3-2-008-V1	SENAE-DGN-2015-0634-RE
SENAE-PI-3-2-009-V1	SENAE-DGN-2015-0635-RE
SENAE-PI-3-2-010-V1	SENAE-DGN-2015-0802-RE
SENAE-PI-3-2-011-V1	SENAE-DGN-2016-1025-RE
SENAE-PI-3-2-012-V1	SENAE-DGN-2016-1026-RE
SENAE-PI-3-2-013-V1	SENAE-DGN-2016-1027-RE
SENAE-PI-3-2-014-V1	SENAE-DGN-2016-1028-RE
SENAE-PI-3-2-015-V1	SENAE-DGN-2016-1029-RE
SENAE-PI-3-2-016-V1	SENAE-DGN-2016-0698-RE

DISPOSICIONES FINALES

Resolución Nro. SENAE-SENAE-2021-0082-RE

Guayaquil, 22 de mayo de 2021

PRIMERA.- La presente Resolución entrará en vigencia a partir del día siguiente al de su publicación en el Registro Oficial.

SEGUNDA.- Encárguese a la Dirección de Secretaría General del Servicio Nacional de Aduana del Ecuador la notificación del contenido de la presente Resolución y sus anexos a las Subdirecciones Generales, Direcciones Nacionales y Direcciones Distritales del Servicio Nacional de Aduana del Ecuador.

TERCERA.- Encárguese a la Dirección de Secretaría General del Servicio Nacional de Aduana del Ecuador el formalizar las diligencias necesarias para la difusión y publicación de la presente en el Registro Oficial.

CUARTA.- Encárguese a la Dirección Nacional de Mejora Continua y Tecnologías de la Información del Servicio Nacional de Aduana del Ecuador, la publicación de la presente resolución junto con los referidos documentos en el Sistema de Administración del Conocimiento (SAC).

Dado y firmado en el despacho de la Dirección General del Servicio Nacional de Aduana del Ecuador, en la ciudad de Santiago de Guayaquil.

Documento firmado electrónicamente

Mgs. Andrea Paola Colombo Cordero
DIRECTORA GENERAL

Anexos:
- perfiles_-_complementario01372690016215441 87.xls
- perfiles_-_directores04855370016215441 87.xls
- perfiles_-_jefes.xls
- perfiles_-_operativos.xls
- senae-pi-3-2-016-v2-signed-signed-signed-signed.pdf
- senae-pi-3-2-015-v2-signed-signed-signed-signed.pdf
- senae-pi-3-2-014-v2-signed-signed-signed-signed.pdf
- senae-pi-3-2-013-v2-signed-signed-signed-signed.pdf
- senae-pi-3-2-012-v2-signed-signed-signed-signed.pdf
- senae-pi-3-2-011-v2-signed-signed-signed-signed.pdf
- senae-pi-3-2-010-v2-signed-signed-signed-signed.pdf
- senae-pi-3-2-009-v2-signed-signed-signed-signed.pdf
- senae-pi-3-2-008-v2-signed-signed-signed-signed.pdf
- senae-pi-3-2-007-v2-signed-signed-signed-signed.pdf
- senae-pi-3-2-006-v3-signed-signed-signed-signed.pdf
- senae-pi-3-2-005-v2-signed-signed-signed-signed.pdf
- senae-pi-3-2-004-v3-signed-signed-signed-signed.pdf
- senae-pi-3-2-003-v2-signed-signed-signed-signed.pdf

Resolución Nro. SENAE-SENAE-2021-0082-RE

Guayaquil, 22 de mayo de 2021

- senae-pi-3-2-002-v2-signed-signed-signed-signed.pdf
- senae-pi-3-2-001-v2-signed-signed-signed-signed.pdf

Copia:

Señorita Magíster
Amada Ingeborg Velasquez Jijon
Subdirectora General de Normativa Aduanera

Señora Licenciada
Maria Lourdes Burgos Rodriguez
Directora de Secretaria General

Señor Ingeniero
Nelson Gabriel Rodriguez Martinez
Director Nacional de Mejora Continua y Tecnologías de la Información, Encargado

Señora Magíster
Patricia Coronado Dominguez
Oficial de Seguridad de la Información

drms/nr/av

Firmado electrónicamente por:
ANDREA PAOLA COLOMBO CORDERO

SENAE-PI-3-2-001-V2

POLÍTICAS INSTITUCIONALES PARA EL ACCESO Y USO DEL INTERNET

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona las directrices a seguir para el buen uso en el servicio de Internet institucional del Senae.		
Objetivo:		
Establecer normas y procedimientos para el uso adecuado del uso en el servicio de Internet institucional, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
Firmado electrónicamente por: CARLA MARGARITA ORTUNO DELGADO Ing. Carla Ortuno Analista Informático	Seguridad Informática	Elaboración
X Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA Ing. Hugo Robayo Jefe de Infraestructura Tencologica	Jefatura de Infraestructura Tecnológica	Revisión
X Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ Lsi. Diego Maldonado Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
X Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ Ing. Nelson Rodriguez Director de Tecnologías de la Información	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:			
Versión	**Fecha**	**Razón**	**Responsable**
1	Junio 2015	Versión Inicial	Ing. Mario Barragán J.
2	Abril 2021	Inclusión sobre normativa vigente	Ing. Carla Ortuño D.

ÍNDICE

1. OBJETIVO

Establecer normas, procedimientos y lineamientos para el uso adecuado del servicio de internet institucional, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información, de manera que se garantice una utilización eficiente del recurso.

2. ALCANCE

Está dirigido a todos los usuarios internos que utilicen el servicio de internet institucional del Senae.

Es necesario que todos los usuarios estén enterados y conscientes de los compromisos, normas y lineamientos que han adquirido para el uso del Internet, tomando todas las medidas que correspondan para que estas directrices se respeten y se cumplan.

La Dirección Nacional de Mejora Continua y Tecnologías de la Información proporcionará accesos a Internet para que los usuarios puedan utilizar este servicio como una herramienta de trabajo más, proporcionada por el Senae. Todos los usuarios que utilicen el servicio de internet institucional están sujetos a esta política y a los términos de este manual, y a una actuación con altos principios morales y éticos al utilizar este recurso, el uso inapropiado del servicio de Internet Institucional puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de los usuarios que requieran utilizar el servicio de internet institucional del Senae.

3.2. La actualización y mejoramiento del presente documento le corresponde al área de Seguridad de la Información perteneciente a la Jefatura de Infraestructura Tecnológica de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.

- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.
- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto de que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al servicio de Internet institucional:

5.1.1. Usuario: persona que recibe un producto o servicio de un proceso que pertenece al Senae.

5.1.2. Navegador de páginas en internet: os navegadores utilizados por el Senae son: Microsoft Internet Explorer, Mozilla Firefox y Google Chrome.

5.1.3. Internet normal: sitios de internet que encuentren enmarcados dentro de las políticas establecidas en el presente manual y que sirven como una herramienta directa para los intereses del Senae.

5.1.4. Consulta de valor: sitios de Internet con información de precios de todo tipo de mercancías, sean directamente del fabricante, como de terceros o intermediarios; y que se encuentren enmarcados dentro de las políticas establecidas en el presente manual.

5.2. La Dirección Nacional de Mejora Continua y Tecnologías de la Información tiene la facultad de bloquear o limitar el acceso y uso de Internet al usuario que utilice el presente servicio.

6. NAVEGACIÓN EN INTERNET

El uso de internet debe estar destinado exclusivamente a la ejecución de las actividades del Senae y deben ser utilizados por el usuario para realizar las funciones establecidas para su cargo, por lo cual la Dirección Nacional de Mejora Continua y Tecnologías de la Información definió los siguientes parámetros para su uso:

6.1. DESCARGAS:

6.1.1. El usuario debe abstenerse de descargar programas no autorizados y para su posterior instalación.

6.1.2. El usuario debe abstenerse de descargar programas no autorizados que realicen conexiones automáticas.

6.1.3. El usuario debe abstenerse de descargas programas que realicen conexiones automáticas en sitios clasificados como pornográficos, así como la utilización de los recursos del Senae para la distribución o reproducción de este tipo de material.

6.1.4. Está prohibido descargar música y videos, con fines no laborales.

6.1.5. Está prohibido realizar descargas de información de gran tamaño en horarios laborales. Cualquier descarga que sobrepase los 10 MB de información deberán realizar fuera de dichos horarios.

6.2. ACCESOS:

6.2.1. Abstenerse de usar sitios web que salten la seguridad del servidor proxy de acceso a Internet.

6.2.2. Abstenerse del uso de este servicio con fines comerciales, políticos, particulares o cualquier otro que no sea el laboral.

6.2.3. Abstenerse de acceder a informaciones sensacionalistas, violentas, inmorales o ilegales y de contenido impropio que son consideradas como falta a la moral.

6.2.4. Está prohibida la obtención de acceso no autorizado sobre otras computadoras pertenecientes a cualquier otra organización o entidad, así como las del Senae mismo.

6.3. CONTENIDO:

6.3.1. Evitar compartir el acceso a Internet con otros usuarios del Senae. El acceso a internet institucional es estrictamente personal.

6.3.2. Abstenerse de enviar, descargar o solicitar información que pueda tener implicaciones contractuales o legales para el Senae, a menos que sea para efectos específicos autorizados y mediante codificación aprobada por la Dirección Nacional de Mejora Continua y Tecnologías de la Información, a través de un correo electrónico.

6.3.3. Abstenerse de enviar, descargar o solicitar información (incluyendo software) que pueda infringir derechos de autor y otros derechos de propiedad intelectual.

6.3.4. Cuando exista la necesidad de compartir información en nube se deberá utilizar la aplicación propia del Senae.

6.3.5. Se podrá utilizar tecnologías de computación en nube, previamente autorizado por la Dirección Nacional de Mejora Continua y Tecnologías de la Información. El usuario deberá solicitar autorización de su requerimiento vía correo electrónico a su director inmediato, indicando los justificativos laborables del caso, el tipo de información y la ruta respectiva. El director enviará su requerimiento al Director Nacional de Mejora Continua y Tecnologías de la Información. Posteriormente se realizará una verificación de la información indicada. El acceso también puede ser solicitado a través de la solicitud de privilegios justificando el uso y con la respectiva autorización del director inmediato.

6.3.6. Está prohibida la participación en cualquier actividad ilegal o criminal.

6.3.7. Está prohibida la solicitud de dinero o la operación de negocios personales.

6.4. ACCIONES:

6.4.1. No deje el navegador abierto cuando no esté utilizando Internet, cierre la sesión; de esta manera evitará consumo de ancho de banda innecesario.

6.4.2. **6.4.2.** Informar inmediatamente al buzón de Mesa de Servicios, sobre cualquier ocurrencia inusual que suceda en el uso de este servicio.

7. CATÁLOGO DE CATEGORÍAS DE ACCESO A INTERNET

Para el acceso a Internet, se ha establecido grupos o categorías, que están relacionadas con el cargo de cada usuario.

Cada usuario tendrá asociado una categoría de navegación, que le permitirá tener una cobertura distinta de acceso a Internet, de acuerdo con la actividad que realiza.

El usuario que requiera por motivos laborales acceso a uno de los servicios y que por su categoría no los tenga, deberá solicitar autorización de su director inmediato, indicando la vigencia del acceso. Seguir el instructivo de trabajo (SENAE-IT-03-2-005) para el registro de datos en el formulario de solicitud de accesos a cuentas de usuarios.

Se establecen 6 categorías, con el siguiente detalle:

7.1. CATÁLOGO DE ACCESO PARA NAVEGACIÓN DE INTERNET

CAT-I1	**INTERNET_DIRECTIVOS:** Categoría establecida para el Director General, Subdirectores Generales, Directores Nacionales, Directores Distritales, Directores de Área, Coordinador general de control disciplinario y Asesores; y tendrá una cobertura de navegación a Internet en los siguientes servicios: - Internet normal - Redes sociales - Correos electrónicos gratuitos - Prensa en línea (periódicos) - Consultas de valor - YouTube - Skype
CAT-I2	**INTERNET_CONTROL:** Categoría establecida para los Jefes de control de procesos operativos y procesos de campo, jefe de control posterior, jefe de evaluación de agentes de comercio exterior región 1, jefe de revisión pasiva región 1, jefe de evaluación de agentes de comercio exterior región 2, jefe de revisión pasiva región 2, jefe de evaluación de agentes de comercio exterior región 3, jefe de revisión pasiva región 3 e interventores; y tendrá una cobertura de navegación a Internet en los siguientes servicios: - Internet normal - Redes sociales - Correos electrónicos gratuitos - Consultas de valor - Skype

CAT-I3	**INTERNET_JEFES:** Categoría establecida para todos los Jefes departamentales; y tendrá una cobertura de navegación a Internet en los siguientes servicios: - Internet normal - Correos electrónicos gratuitos - Consultas de valor - Skype
CAT-I4	**INTERNET_PRENSA:** Categoría establecida para todos los cargos de periodistas y Web Master; y tendrá una cobertura de navegación a Internet en los siguientes servicios: - Internet normal - Redes sociales - Prensa en línea (periódicos) - YouTube
CAT-I5	**INTERNET_OPERATIVO:** Categoría establecida para todos los técnicos operadores y técnicos especialistas; y tendrá una cobertura de navegación a Internet en los siguientes servicios: - Internet normal - Consultas de valor
CAT-I6	**INTERNET_NORMAL:** Categoría establecida para todos los abogados, analistas, asistentes, auditores, conductores, conserjes, especialistas, estibador, guardalmacén, inspectores de vigilancia aduanera, inventariadores, oficinistas, operadores de central telefónica, secretarias, técnicos, tesorero general de aduana y vigilantes aduaneros; y tendrá una cobertura de navegación a Internet en los siguientes servicios: - Internet normal

8. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasionará que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

SENAE-PI-3-2-002-V2

POLÍTICAS INSTITUCIONALES PARA EL USO DEL CORREO ELECTRÓNICO

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona las directrices a seguir para el buen uso en el servicio de correo electrónico institucional del Senae.		
Objetivo:		
Establecer normas y procedimientos para el uso adecuado del correo electrónico institucional, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
Firmado electrónicamente por: CARLA MARGARITA ORTUNO DELGADO Ing. Carla Ortuno Analista Informático	Seguridad Informática	Elaboración
Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA Ing. Hugo Robayo Jefe de Infraestructura Tencologica	Jefatura de Infraestructura Tecnológica	Revisión
Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ Lsi. Diego Maldonado Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ Ing. Nelson Rodriguez Director de Tecnologías de la Información	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:			
Versión	**Fecha**	**Razón**	**Responsable**
1	Abril 2015	Versión Inicial	Ing. Mario Barragán J.
2	Mayo 2021	Inclusión sobre normativa vigente	Ing. Carla Ortuño D.

ÍNDICE

1. OBJETIVO

Establecer normas, procedimientos y lineamientos para el uso adecuado del correo electrónico institucional, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información, de manera que se garantice una utilización eficiente del recurso.

2. ALCANCE

Está dirigido a todos los usuarios internos que utilicen el servicio de correo electrónico institucional del Senae.

Es necesario que todos los usuarios estén enterados y conscientes de los compromisos, normas y lineamientos que han adquirido para el uso del correo electrónico, tomando todas las medidas que correspondan para que estas directrices se respeten y se cumplan.

El uso del correo electrónico institucional tiene como finalidad fortalecer el flujo de información interna y externa, y apoyar a las diferentes tareas encomendadas para el mejoramiento de nuestras labores. Todos los usuarios están sujetos a esta política y a los términos de este manual, y a una actuación con altos principios morales y éticos al utilizar los recursos, el uso inapropiado del correo electrónico institucional puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de los usuarios que utilicen el servicio de correo electrónico institucional del Senae.

3.2. La actualización y mejoramiento del presente documento le corresponde al área de Seguridad de la Información perteneciente a la Jefatura de Infraestructura Tecnológica de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

4. NORMA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.
- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.
- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto de que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al servicio de correo electrónico institucional:

5.1.1. Usuario: persona que recibe un producto o servicio de un proceso que pertenece al Senae.

5.1.2. Correo interno: servicio de correo electrónico para comunicación de los usuarios dentro del Senae.

5.1.3. Correo externo: servicio de correo electrónico para comunicación con usuarios fuera del Senae.

5.1.4. Mensaje de datos: es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta

enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.

5.1.5. Archivo PST: es un archivo de mensajes de datos de Microsoft Outlook en el que se almacena información del correo electrónico y otros elementos de Outlook, este archivo que tiene una extensión o formato PST se conserva en el equipo, y no está sujeto a los límites de tamaño del buzón en el servidor de correo. Es recomendable que el tamaño de este archivo pst no exceda los 4 GB a fin de evitar daños en los índices de este.

5.1.6. Spam: conocido como correo basura, son los mensajes no solicitados, no deseados o de remitente no conocido o anónimo, habitualmente de tipo publicitario.

5.1.7. Correo normal: acceso al correo electrónico institucional, con servicio de mensajería interna y externa.

5.1.8. Correo OWA: acceso al correo electrónico institucional, pero de forma remota mediante un navegador web y que permite tener las mismas funcionalidades básicas de la aplicación de escritorio.

5.1.9. Correo móvil: acceso al correo electrónico institucional, pero de forma remota mediante un dispositivo móvil (celulares, tablets, etc) y que permite tener las mismas funcionalidades básicas de la aplicación de escritorio.

5.1.10. Buzón de Correo Electrónico: Es el espacio o depósito virtual donde se almacenan los mensajes de datos de una cuenta de correo electrónico.

5.2. La capacidad de almacenamiento máximo de los buzones de correo electrónico institucional para los usuarios de los directores está establecida en 6 Gigabyte (6 GB)

5.3. La capacidad de almacenamiento máximo de los buzones de correo electrónico institucional para los demás usuarios está establecida en 300 Megabyte (300 MB)

5.4. La capacidad máxima establecida para todas las cuentas de correo electrónico, para el envío y recepción de mensajes de datos, es de 5 Megabyte (5 MB)

6. USO DE CORREO ELECTRÓNICO

La Dirección Nacional de Mejora Continua y Tecnologías de la Información considera indispensable regular el uso del servicio de correo electrónico institucional del Senae, para lo cual emite los siguientes parámetros que son de cumplimiento obligatorio para todos los usuarios que utilicen este servicio.

6.1. USO:

6.1.1. Este servicio es personal, no puede compartir su uso con otras personas, bajo ningún concepto o modalidad.

6.1.2. Este servicio debe utilizarse exclusivamente para las tareas propias, establecidas para el cargo que tiene el usuario en el Senae y no debe utilizarse para ningún otro fin.

6.1.3. Cada usuario deberá evitar el envío de correos masivos, a menos que sea estrictamente necesario para los intereses del Senae.

6.1.4. Abstenerse de enviar información que pueda tener implicaciones contractuales o legales para el Senae, a menos que sea para fines específicos debidamente autorizados.

6.1.5. Cada usuario que utilice este servicio debe hacer uso de la opción "Fuera de oficina" cuando el usuario prevea no poder leer sus correos electrónicos durante un intervalo prolongado de tiempo.

6.1.6. El usuario no deberá entre otras cosas: falsificar las cuentas de correo electrónico, hacerse pasar por alguna otra persona, hacer declaraciones falsas, en cualquier otra forma falsificar la identidad de alguna persona, o falsificar los encabezados de los mensajes.

6.1.7. El usuario no deberá adulterar el contenido del mensaje de datos, en los correos electrónicos que usa.

6.1.8. Este servicio no debe ser utilizado para:

- Proselitismo político.
- Proselitismo religioso.
- Negocios Personales.
- Enviar o recibir deliberadamente material pornográfico o indecente.
- Envío de cadenas, chistes, pasquines y cualquier otra información que no sea de índole laboral.
- Ejercer cualquier tipo de coacción ajena a los intereses laborales, tales como actividades comerciales privadas o publicidad no oficial, alteración del orden público o la paz social.
- Difamar, acosar, amenazar o de otra forma infringir los derechos legales (tales como los derechos a la intimidad y a la integridad) de otros.
- Enviar correo electrónico con insultos.
- Enviar correo electrónico impropio de personas cultas y de buena educación.
- Enviar correo electrónico que incluya discriminación sexual o racial; acoso sexual.

- Enviar información del Senae, sin la debida autorización del dueño de esta, es decir, por el Director General y demás puestos Directivos según sea el caso, irrespetando el aviso de confidencialidad que aparece en el respectivo pie de página del correo, divulgándola a terceros no autorizados.
- Enviar todo tipo de correo electrónico que pueda crear responsabilidad para el Senae (por ejemplo: órdenes de bienes, uso indebido de sus facultades firmantes, divulgación de información confidencial, secretos comerciales y de negocios, protección de datos, etc.
- Abrir y/o enviar deliberadamente correo electrónico con archivos adjuntos que contengan virus informáticos, a pesar de existir advertencia previa del Senae para evitar el contagio y/o daño de su sistema o de terceros.
- Envío de información que puede dañar la reputación del Senae o su relación con terceros.
- Envío de información que pueda infringir derechos de autor y otros derechos de propiedad intelectual.

6.1.9. Cada usuario que utilice este servicio debe tomar en cuenta los siguientes lineamientos al momento de enviar un correo:

- Usar palabras en letras mayúsculas sugiere que está expresando emociones fuertes, para enfatizar un término, escríbalo entre comillas.
- No debe dirigir ni responder correo electrónico basura, acosador o cartas en cadena; si se recibe este tipo de correos, no debe contestar dichos mensajes, debe notificar y enviar una copia al buzón de Mesa de Servicios, para que efectúe el seguimiento y la investigación necesaria y luego proceder con su destrucción.
- Revisar siempre los nombres de los destinatarios del correo electrónico antes de efectuar el envío de este.
- No utilice el correo para discusiones emocionales, acosadoras, o insultantes.
- No digite mensajes enteros o en partes en letras de color rojo, para expresar emociones fuertes.
- No digite mensajes enteros o en partes con palabras entre comillas o con letra cursiva en forma indiscriminada.
- Utilice la casilla "CC" con moderación. Informe sólo a quienes necesitan saberlo. Cada copia creada para cada persona crea un mensaje de datos adicional en la red.
- Evite respuestas triviales o innecesarias. Como receptor no es necesario responder a todo mensaje.
- Todas las leyes que rigen los derechos de autor, difamación, discriminación y otras formas de comunicación escrita, también se aplican al correo electrónico.
- El correo electrónico es un documento de validez legal y prueba de evidencia. Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en la ley de comercio electrónico, firmas electrónicas y mensajes de datos.

- Cuando reenvía un mensaje, incluya el mensaje original, para que la o las personas hacia las que va el mensaje conozcan que se está tratando en un momento dado.
- Utilizar siempre el campo "asunto" a fin de resumir el tema del mensaje.
- Evitar el envío de respuestas con copia a todos los destinatarios de un mensaje recibido y en particular cuando se trata de mensajes que originalmente hayan sido dirigidos a un grupo grande de destinatarios; salvo cuando se trate de una respuesta que por su naturaleza o contenido necesariamente requiera ser conocida por todos ellos.

6.2. RESPONSABILIDAD

6.2.1. El usuario que utilice este servicio es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.

6.2.2. El usuario será responsable del uso, mantenimiento y protección de la información almacenada en el buzón de su cuenta de correo electrónico, así como de la información almacenada en las carpetas personales (archivo PST) que utilice.

6.2.3. El usuario puede tener uno o varios archivos PST para organizar de forma personalizada los mensajes y será responsable de la confidencialidad de su información. Los archivos PST son de carácter personal.

6.2.4. El usuario que utilice este servicio es responsable por la destrucción de los mensajes con origen desconocido, ofensivo o spam, y asume la responsabilidad por las consecuencias que pueda ocasionar con la ejecución de los archivos adjuntos.

6.2.5. El usuario que utilice este servicio es responsable de la cantidad de destinatarios que utilice y el tamaño del mensaje que envíe. Los archivos adjuntos que incluya, dependiendo de su tamaño y formato, deberán ser previamente comprimidos en un archivo ZIP. Para cada correo que elabore debe tener en cuenta el tamaño que utiliza entre el texto del mensaje más los archivos adjuntos que utilice, los cuales no debe sobrepasar el límite establecido para el envío y recepción de mensajes de datos.

6.2.6. El usuario será responsable de mantener depurado su correo electrónico para no llegar al límite establecido a cada cuenta, atendiendo las alertas que al respecto advierte el aplicativo de Microsoft Outlook.

6.2.8. El usuario será responsable de la lectura y atención oportuna de sus correos electrónicos.

6.2.9. El usuario será responsable del envío de sus correos electrónicos y de las acciones a seguir cuando el sistema le informe que el destinatario no existe, su buzón se encuentra lleno o se encuentra fuera de oficina.

7. CATÁLOGO DE CATEGORÍAS DE CORREO ELECTRÓNICO

Para el acceso al correo electrónico institucional, se ha establecido grupos o categorías, que están relacionadas con el cargo de cada usuario.

Cada usuario tendrá asociada una cuenta de correo electrónico, que tendrá privilegios de acceso, de acuerdo con la actividad que realiza.

El usuario que requiera por motivos laborales acceso a uno de los servicios y que por su categoría no los tenga, deberá solicitar autorización de su director inmediato, indicando obligatoriamente la vigencia del acceso. Seguir el instructivo de trabajo (SENAE-IT-03-2-005) para el registro de datos en el formulario de solicitud de accesos a cuentas de usuarios.

Se establecen 3 categorías, con el siguiente detalle:

7.1. CATÁLOGO DE ACCESO PARA CORREO ELECTRÓNICO

CAT-C1	**CORREO_TOTAL:** Categoría establecida para el Director General, Subdirectores Generales, Directores Nacionales, Directores Distritales, Directores de Área, Coordinador general de control disciplinario, Asesores y Jefes Departamentales; y tendrá los siguientes privilegios de acceso: - Correo normal - Correo OWA - Correo móvil
CAT-C2	**CORREO_WEB:** Categoría establecida para vigilantes aduaneros, inspectores de vigilancia aduanera, técnicos operadores y técnicos especialistas que se encuentren prestando servicio en localidades donde no existe enlace de datos con el Senae; y tendrá los siguientes privilegios de acceso: - Correo normal - Correo OWA

CAT-C3	**CORREO_NORMAL:** Categoría establecida para todos los abogados, analistas, asistentes, auditores, conductores, conserjes, especialistas, estibador, guardalmacén, inspectores de vigilancia aduanera, interventores, inventariadores, oficinistas, operadores de central telefónica, periodistas, secretarias, técnicos, tesorero general de aduana y vigilantes aduaneros; y tendrá los siguientes privilegios de acceso: - Correo normal

8. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasionará que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

SENAE-PI-3-2-003-V2

POLÍTICAS INSTITUCIONALES DEL PROCEDIMIENTO FORMAL PARA EL REPORTE, ESCALADA Y RESPUESTA ANTE INCIDENTES DE SEGURIDAD DE LA INFORMACION

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona el manual de procedimiento formal para realizar los reportes, la escalada y respuesta de atención ante la presencia de incidentes que amenacen la Seguridad de la Información.		
Objetivo:		
Establecer procedimientos formales para el reporte, escalamiento y respuesta ante incidentes de Seguridad de la Información, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
Firmado electrónicamente por: CARLA MARGARITA ORTUNO DELGADO X Ing. Carla Ortuno Analista Informático	Seguridad Informática	Elaboración
Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA X Ing. Hugo Robayo Jefe de Infraestructura Tencologica	Jefatura de Infraestructura Tecnológica	Revisión
Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ X Lsi. Diego Maldonado Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ X Ing. Nelson Rodriguez Director de Tecnologías de la Información	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:			
Versión	**Fecha**	**Razón**	**Responsable**
1	Junio 2015	Versión Inicial	Ing. Mario Barragán J.
2	Mayo 2021	Inclusión sobre normativa vigente	Ing. Carla Ortuño D.

ÍNDICE

1. OBJETIVO

Establecer procedimientos formales para el reporte, escalamiento y respuesta ante incidentes de Seguridad de la Información, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

2. ALCANCE

El manual de procedimiento formal para realizar los reportes, la escalada y respuesta de atención ante la presencia de incidentes que amenacen la Seguridad de la Información, está dirigido a todos los usuarios de la Dirección Nacional de Tecnologías de la Información del Senae.

Todos los usuarios están sujetos a este procedimiento, el uso inapropiado puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de los usuarios de la Dirección Nacional de Tecnologías de la Información del Senae, en la adecuada y oportuna canalización de incidentes de seguridad de la información.

3.2. La actualización y mejoramiento del presente documento le corresponde al área de Seguridad de la Información perteneciente a la Jefatura de Infraestructura Tecnológica de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

3.3. El área de centro de cómputo de la Dirección de Tecnologías de la Información es responsable de registrar la solución a los incidentes de seguridad de la información con la finalidad de generar la base de conocimiento de incidentes de seguridad de la información.

3.4. Las Jefaturas de la Dirección de Tecnologías de la Información son responsables de clasificar y asignar usuarios responsables para la solución a los incidentes de seguridad de la información.

3.5. La Jefatura de Infraestructura Tecnológica de la Dirección de Tecnologías de la Información es responsable de brindar la plataforma tecnológica para la adecuada atención de los incidentes de seguridad de la información, así como del monitoreo constante de la oportuna solución de los Incidentes de Seguridad con problemas de cierre.

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.
- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.
- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto de que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al presente manual:

5.1.1 Usuario: persona que recibe un producto o servicio de un proceso que pertenece al Senae.

5.1.2. Incidente de Seguridad de Información: es un evento negativo que materializa una amenaza cuando una vulnerabilidad se explota, afectando uno o más activos de información.

5.1.3. Amenazas: es todo elemento o acción capaz de atentar contra la seguridad de la información y surgen a partir de la existencia de las vulnerabilidades, es decir una amenaza solo puede existir si existe una vulnerabilidad que pueda ser aprovechada e independientemente de que se comprometa o no la seguridad de un sistema de información.

5.1.4. Vulnerabilidad: debilidad de cualquier tipo que compromete la seguridad de la información.

5.1.5. Base de conocimientos del centro de cómputo: grupos de eventos registrados por el área de centro de cómputo, los mismos que poseen con una solución que puede ser aplicada en futuros incidentes.

5.1.6. Activo de información: son las personas, sistemas de información, aplicaciones informáticas, bases de datos, equipos computacionales, dispositivos móviles, archivos físicos, documentos electrónicos o cualquier otro activo que por su naturaleza registre, procese, almacene o transmita información considerada relevante para los procesos institucionales.

6. POLÍTICA

6.1. El reporte de los incidente de seguridad de información permite responder en forma apropiada con la solución y/o corrección de cualquier tipo de ocurrencia con la finalidad de mitigar futuros eventos similares.

6.2. Todos los incidentes de seguridad de la información deben registrarse, asignarse, solucionarse, contabilizarse y mantener su histórico electrónico, para ello el punto de contacto para el reporte de los incidentes de seguridad de información, será a través de las cuentas de correo electrónico: operador@aduana.gob.ec, proporcionando la mayor cantidad de información, quienes estarán capacitados para tomar el requerimiento y canalizarlo adecuadamente.

6.3. Los niveles de severidad de los incidentes en seguridad de la información vienen dados por el impacto a los activos de información y se los clasifica de acuerdo con el tipo de servicio afectado, los servicios establecidos con sus son:

Servicios	Nivel de Severidad
Enlaces de comunicaciones	ALTO
Climatización y Sistema de Alarmas Centro Cómputo a nivel nacional	ALTO
Bases de Datos – Producción	ALTO
Portal Ecuapass Interno/Externo - Servidor	ALTO
Instancias Was	ALTO
PRTG Network Monitor - Servicio de Internet Proveedor	ALTO
BANRED	ALTO

Réplicas de job pendientes (BDINTER / BDECPS)	ALTO
DNS (Domain Name System)	ALTO
AD (Active Directory)	ALTO
IPS (Intrusion Prevention System)	ALTO
Antivirus	ALTO
Despacho Importación	ALTO
Despacho Exportación	ALTO
DAS (Importación, Exportación)	ALTO
Carga importación	ALTO
Carga exportación	ALTO
Regímenes Especiales	ALTO
Garantías	ALTO
Perfiles de Riesgo	ALTO
Ventanilla Única	ALTO
Recaudación Tributos	ALTO
Arancel Nacional	ALTO
Portal Ecuapass Interno/Externo - Desarrollo	ALTO
Alerta temprana	ALTO
Bases de Datos – Desarrollo	MEDIO
Respaldos en el TSM (Tivoli Storage Manager)	MEDIO
Portal aduana.gob.ec - Servidor	MEDIO
Cuarto de Ups y Generador eléctrico Centro Cómputo a nivel nacional	MEDIO
Replicas Netapp	MEDIO
Exchange	MEDIO
ISA (Internet Security & Acceleration Server)	MEDIO
Devolución Condicionada	MEDIO
Notas de Crédito	MEDIO

Control Posterior	MEDIO
Portal aduana.gob.ec - Desarrollo	MEDIO
Sistemas Administrativos	MEDIO
Arq. Software	MEDIO
Mesa de servicio	MEDIO
Bases de Datos – Test	BAJO
Bases de Datos – SICE	BAJO
DataWarehouse	BAJO
Modulo Legal	BAJO
Gestor Conocimiento	BAJO
Auditoría	BAJO

6.4. Debe existir un grupo de usuarios responsables y entrenados para el manejo de incidentes de seguridad de la información, que elaboren y promuevan los procedimientos respectivos de respuesta a incidentes de seguridad. Dicho grupo debe reunirse para evaluar los incidentes y solucionar aquellos que estén pendientes, si algún incidente lleva dos reuniones sin solución, se debe elevar el requerimiento al Comité de Seguridad de la Información.

6.5. El grupo de usuarios responsables y entrenados debe estar compuesto por representantes de distintas áreas de la Dirección Nacional de Tecnologías de la Información que permitan hacer preparativos para respuesta ante incidentes, coordinados por el encargado del área Seguridad de la Información.

6.6. La Jefatura de Infraestructura Tecnológica de la Dirección de Tecnologías de la Información debe mantener una lista de los usuarios internos y terceros (proveedores externos) a contactar en caso de detectar un determinado incidente.

6.7. Las páginas web deben incluir información de contacto (teléfono y correo electrónico) para externos que puedan reportar los incidentes que detectan.

6.8. Dependiendo de la gravedad del incidente, se debe comunicar sus antecedentes y repercusiones a todas las áreas afectadas.

6.9. Para el reporte de incidentes de seguridad de información, se establece un grupo de servicios que podrán verse afectados en uno o más activos de información.

6.10. Una vez registrado el incidente y su impacto probable, debe asignarse al personal indicado y apto para el manejo y solución de los incidentes, que se detalla a continuación:

SERVICIO	USUARIO PARA ATENCION DE INCIDENTES
Enlaces de comunicaciones	Luis Chávez / Erwin Gavilanes
Climatización y Sistema de Alarmas Centro Cómputo a nivel nacional	Ángel Ortega/Operadores Distritales/Operador de centro de computo
Bases de Datos – Producción	Soraya Nowak/Tanya Santos
Bases de Datos – Desarrollo	Soraya Nowak/Tanya Santos
Bases de Datos – Test	Soraya Nowak/Tanya Santos
Bases de Datos – SICE	Soraya Nowak/Tanya Santos
Respaldos en el TSM (Tivoli Storage Manager)	Operador de centro de computo
Portal Ecuapass Interno/Externo - Servidor	Giovanni Orellana
Portal aduana.gob.ec - Servidor	Giovanni Orellana
Instancias Was	Soraya Nowak/Tanya Santos
Cuarto de Ups y Generador eléctrico Centro Cómputo a nivel nacional	Angel Ortega/Operadores Distritales/Operador de centro de computo
PRTG Network Monitor - Servicio de Internet Proveedor	Luis Chávez / Erwin Gavilanes
BANRED	Soraya Nowak/Tanya Santos
Réplicas de job pendientes (BDINTER / BDECPS)	Soraya Nowak/Tanya Santos
Replicas Netapp	Giovanni Orellana
Exchange	Giovanni Orellana
DNS (Domain Name System)	Giovanni Orellana
AD (Active Directory)	Giovanni Orellana
IPS (Intrusion Prevention System)	Luis Chávez / Erwin Gavilanes
ISA (Internet Security & Acceleration Server)	Carla Ortuno
Antivirus	Magdeline Rosero
Despacho Importación	Gloria Suarez / Leonel Bernabé
Despacho Exportación	Leonel Bernabé / Ginger Bajaña
DAS (Importación, Exportación)	Leonel Bernabé / Ginger Bajaña
Carga importación	Martha Aguirre / Jaime Samaniego
Carga exportación	Martha Aguirre / Juan Carlos Carvajal
Devolución Condicionada	Leonel Bernabé / Mayra Banchon
Notas de Crédito	Manuel Pazmiño / Mayra Banchon
Regímenes Especiales	Nataly Cajamarca / Gloria Suarez
Garantías	Manuel Pazmiño / Juan Carlos Carvajal

Perfiles de Riesgo	José Luis Guevara / Norma Manzaba
DataWarehouse	Jorge Suárez/Mónica Alvarado
Ventanilla Única	Diana Bajaña/Erick Ortega/Fabián Cansiong
	Norian Pilco
Recaudación Tributos	Tito Lagos / Luis Quijije/Erick Ortega / Fabian Cansiong
Arancel Nacional	Gloria Suarez / Norma Manzaba
Portal Ecuapass Interno/Externo - Desarrollo	Norma Manzaba / Ginger Bajaña
Legal	Galo Arellano/Mayra Banchon
Control Posterior	Norma Manzaba / Jaime Samaniego
Gestor Conocimiento	Galo Arellano/Mayra Banchon
Alerta temprana	Jonathan Ayuquina / Luis Quijije
Auditoría	Jonathan Ayuquina / Luis Quijije
Portal aduana.gob.ec - Desarrollo	Giovanny Córdova / Galo Arellano
Administrativos	Tito Lagos / Galo Arellano
Arq. Software	Luis Quijije/Jonathan Ayuquina

6.11. Los tiempos de atención, en los que un incidente de seguridad de información debe estar solventado, dependerán del nivel de severidad y no deberá superar la siguiente escala:

Nivel de Severidad	Tiempo de atención (minutos)
ALTO	30
MEDIO	60
BAJO	180

6.12. De acuerdo con el nivel de severidad y el tiempo que tiene el incidente activo desde que se reportó el incidente de seguridad de información, y siguiendo el orden jerárquico respectivo se debe comunicar al respecto, bajo el siguiente esquema:

Nivel de Severidad	Jefatura	Dirección Tecnologías de la Información	Dirección Nacional de	Director General

			MCYTI	
ALTO	Atención inmediata	Inmediatamente	30 minutos	1 hora
MEDIO	Atención inmediata	30 minutos	3 horas	-
BAJO	Atención inmediata	1 hora	-	-

7. PROCEDIMIENTOS

7.1. PROCEDIMIENTOS DE ESCALADA Y RESPUESTA

El esquema para seguir en el tratamiento de un incidente de seguridad de la información es el siguiente:

- Preparación y protección.
- Detección o identificación del Incidente
- Registro del Incidente
- Notificación del Incidente
- Clasificación del Incidente
- Priorización del Incidente
- Diagnóstico inicial
- Escalamiento del Incidente
- Investigación y diagnóstico
- Resolución y restauración del servicio
- Cierre del Incidente

No	Actividad	Producto de Entrada	Descripción de Actividad	Responsable	Producto de Salida
1.	Preparación y protección	Políticas y procedimientos	La Dirección de Tecnologías de la Información debe conocer la política y procedimiento de Escalada de Incidentes de Seguridad de la información	Dirección de Tecnologías de la Información	Conocimiento
2.	Detección del Incidente	Incidente	El operador de centro de cómputo detecta o es notificado de la presencia	Operador de centro de cómputo	Identificación del incidente

No	Actividad	Producto de Entrada	Descripción de Actividad	Responsable	Producto de Salida
			de un incidente		
3.	Registro del Incidente	Identificación del incidente	Registrar el incidente en una bitácora de incidentes	Operador de centro de cómputo	Reporte de incidente de seguridad de información
4.	Notificación del Incidente	Reporte de Incidente de Seguridad de Información	Notificar a la respectiva jefatura de acuerdo con el tipo de servicio afectado y al Oficial de Seguridad de la Información.	Operador de centro de cómputo	Correo electrónico
5.	Clasificación del Incidente	Identificación del incidente	Clasificar el incidente de acuerdo con el tipo de servicio afectado y al nivel de severidad.	Jefatura de DTI	Categorización
6.	Priorización del Incidente	Categorización	Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultánea. La prioridad se dará de acuerdo con el nivel de severidad.	Operador de centro de cómputo	Priorización
7.	Diagnóstico Inicial	Identificación del incidente	Revisar si el incidente de seguridad de información suscitado se encuentra registrado en la Base de conocimientos del centro de cómputo y aplicar la solución. Si el incidente es superado se procede con la actividad número 9	Operador de centro de cómputo	Solución
8.	Escalamiento del Incidente	Identificación del incidente	Escalar el incidente, vía correo electrónico, al líder o responsable del servicio, haciendo copia a la jefatura respectiva de acuerdo con el tipo de servicio afectado, al Oficial de Seguridad de la Información, adjuntar bitácora del incidente e indicar el nivel de severidad y la priorización	Operador de centro de cómputo	Correo de escalamiento

No	Actividad	Producto de Entrada	Descripción de Actividad	Responsable	Producto de Salida
			de ser el caso.		
9.	Cierre del Incidente	Solución	Cerrar el incidente cuando se confirme que el mismo ha sido resuelto, actualizando el estado del registro del incidente en la bitácora de incidentes a "resuelto". Notificar a la jefatura respectiva de acuerdo con el tipo de servicio afectado y al Oficial de Seguridad de la Información, que el incidente ha sido superado, adjuntando la información pertinente. Si en el proceso de escalamiento se indica que la solución puede realizarla el operador de centro de cómputo, se debe registrar este nuevo incidente de seguridad de información y la solución respectiva en la Base de conocimientos del centro de cómputo	Operador de Centro de Cómputo	Finalización

7.1.1. Cuando el responsable del servicio es un agente externo:

No	Actividad	Producto de Entrada	Descripción de Actividad	Responsable	Producto de Salida
1.	Análisis	Correo de escalamiento	Investigar y diagnosticar las causas por las cuales se produje el incidente	Área en la que se presenta el incidente	Diagnóstico
2.	Gestión	Diagnóstico	Resolver y restaurar el servicio afectado por el incidente	Área en la que se presenta el incidente	Solución
3.	Reporte	Solución	Generar informe técnico del proceso de remediación	Área en la que se presenta el	Reporte

No	Actividad	Producto de Entrada	Descripción de Actividad	Responsable	Producto de Salida
			del incidente reportado	incidente	
4.	Informe	Reporte	Comunicar vía correo electrónico a la cuenta del Operador del centro de cómputo que el incidente ha sido superado y se adjunta el respectivo informe técnico.	Área en la que se presenta el incidente	Correo de solución

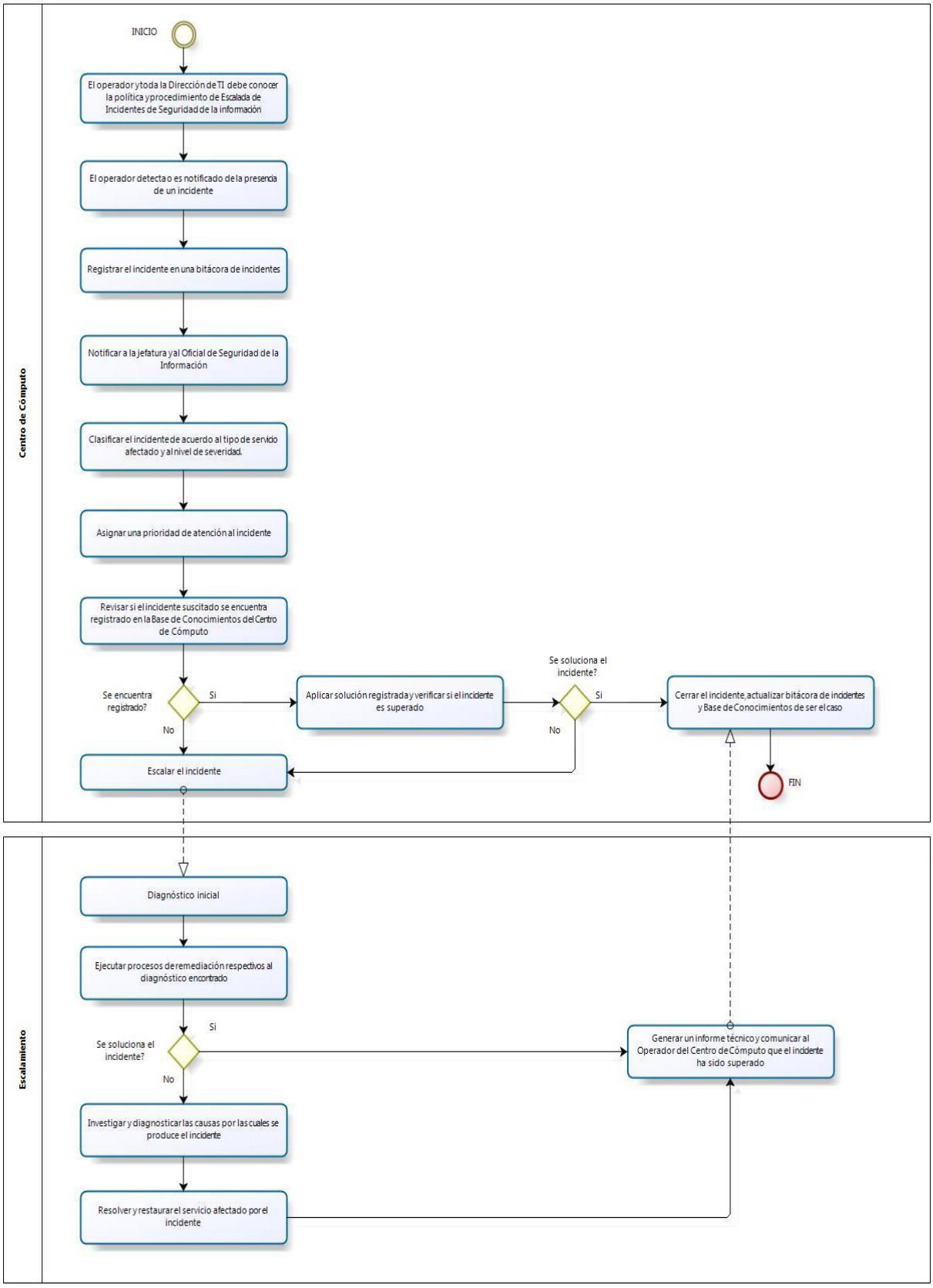
7.1.2. Cuando el responsable del servicio es un usuario interno:

No	Actividad	Producto de Entrada	Descripción de Actividad	Responsable	Producto de Salida
1.	Análisis	Correo de escalamiento	Diagnóstico inicial, determinando mensajes de error producidos y recreando el incidente para identificar sus posibles causas.	Usuario responsable	Diagnóstico
2.	Gestión	Diagnóstico	Ejecutar procesos de remediación respectivos al diagnóstico encontrado. Si el incidente es superado generar un informe técnico y proceder con la actividad número 6	Usuario responsable	Resultado
3.	Análisis	Resultado	Investigar y diagnosticar las causas por las cuales se produce el incidente. El líder puede contactar al proveedor del servicio técnico o al fabricante mismo, de ser el caso.	Usuario responsable	Diagnóstico2
4.	Gestión	Diagnóstico2	Resolver y restaurar el servicio afectado por el incidente	Usuario responsable	Solución
5.	Reporte	Solución	Generar informe técnico del proceso de remediación del incidente reportado	Usuario responsable	Reporte
6.	Informe	Solución	Comunicar vía correo	Usuario	Correo de

No	Actividad	Producto de Entrada	Descripción de Actividad	Responsable	Producto de Salida
			electrónico a la cuenta del operador del centro de cómputo que el incidente ha sido superado y se adjunta el respectivo informe técnico.	responsable	solución

8. FLUJOGRAMA

8.1. PROCESO DE ESCALADA Y RESPUESTA


Centro de Cómputo
INICIO
El operador y toda la Dirección de TI debe conocer la política y procedimiento de Escalada de Incidentes de Seguridad de la información
El operador detecta o es notificado de la presencia de un incidente
Registrar el incidente en una bitácora de incidentes
Notificar a la jefatura y al Oficial de Seguridad de la Información
Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad.
Asignar una prioridad de atención al incidente
Revisar si el incidente suscitado se encuentra registrado en la Base de Conocimientos del Centro de Cómputo
Se encuentra registrado?
Si
No
Aplicar solución registrada y verificar si el incidente es superado
Se soluciona el incidente?
Si
No
Cerrar el incidente, actualizar bitácora de incidentes y Base de Conocimientos de ser el caso
FIN
Escalar el incidente
Escalamiento
Diagnóstico inicial
Ejecutar procesos de remediación respectivos al diagnóstico encontrado
Se soluciona el incidente?
Si
No
Generar un informe técnico y comunicar al Operador del Centro de Cómputo que el incidente ha sido superado
Investigar y diagnosticar las causas por las cuales se produce el incidente
Resolver y restaurar el servicio afectado por el incidente

9. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasionará que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

SENAE-PI-3-2-004-V3

POLÍTICAS INSTITUCIONALES DE LOS REQUERIMIENTOS MÍNIMOS DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona un manual de procedimientos y requerimientos mínimos de control de seguridad para los períodos de adquisición, desarrollo y mantenimiento de los sistemas de información en el Senae.		
Objetivo:		
Establecer requerimientos mínimos o básicos a considerar sobre seguridad, que se deben tomar en consideración en los procesos de adquisición, desarrollo y mantenimiento de los Sistemas de Información en el Senae.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
Firmado electrónicamente por: CARLA MARGARITA ORTUNO DELGADO Ing. Carla Ortuno Analista Informático	Seguridad Informática	Elaboración
X Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA Ing. Hugo Robayo Jefe de Infraestructura Tencologica	Jefatura de Infraestructura Tecnológica	Revisión
X Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ Lsi. Diego Maldonado Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
X Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ Ing. Nelson Rodriguez Director de Tecnologías de la Información	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:			
Versión	**Fecha**	**Razón**	**Responsable**
1	Junio 2015	Versión Inicial	Ing. Mario Barragán J.
2	Marzo 2020	Inclusión sobre derechos de autor	Msig. Nicolás Pulgar S.
3	Abril 2021	Inclusión sobre normativa vigente	Ing. Carla Ortuño D.

ÍNDICE

1. OBJETIVO

Establecer requerimientos mínimos o básicos a considerar sobre seguridad, que se deben tomar en consideración en los procesos de adquisición, desarrollo y mantenimiento de los Sistemas de Información en el Senae.

2. ALCANCE

Está dirigido a todos los usuarios del Senae que intervengan en los procesos para la adquisición, desarrollo y mantenimiento de los Sistemas de Información.

Es necesario que todos los usuarios estén enterados y conscientes de los lineamientos que deben cumplir en los procesos para la adquisición, desarrollo y mantenimiento de los Sistemas de Información del Senae.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de todos los usuarios del Senae.

3.2. La actualización y mejoramiento del presente documento le corresponde al área de Seguridad de la Información perteneciente a la Jefatura de Infraestructura Tecnológica de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.
- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.
- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.

- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto de que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al presente manual:

5.1.1. Usuario: persona que recibe un producto o servicio de un proceso que pertenece al Senae.

5.1.2. Cuenta de usuario: identificación con la que se personaliza el acceso de un usuario a un sistema informático, otorgándole privilegios y niveles de servicios.

5.1.3. Sistema informático: aplicaciones o servicios informáticos disponibles para el usuario, con la finalidad de que sea una herramienta de trabajo para cumplir las funciones otorgadas

5.1.4. Sistema de información: es un conjunto de componentes que interaccionan entre sí para satisfacer necesidades de información. Estos componentes pueden ser personas, datos, sistemas informáticos, actividades o recursos materiales en general, los cuales procesan la información y la distribuyen de manera adecuada, con el fin de cumplir los requerimientos de información.

6. CONTROL DE SESIONES PARA LOS SISTEMAS DE INFORMACIÓN

6.1. Los servidores de aplicación no permitirán más de tres sesiones simultáneas, conectadas remotamente.
6.2. Los sistemas informáticos administrados internamente en el Senae, como el Ecuapass, permitirán un solo inicio de sesión simultáneo.
6.3. Las cuentas de usuarios deberán tener inicio de sesión en un solo equipo, a excepción de usuarios de áreas operativas en las cuales se justifique.

7. REQUERIMIENTOS MÍNIMOS PARA LA ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN

7.1. Los Sistemas de Información que se adquieran deben contar con normas de programación, versionamiento, documentación y pruebas que cumplan la totalidad del requerimiento.

7.2. Los procedimientos de pruebas, en el proceso de adquisición, deben ser funcionales y no funcionales. Las pruebas no funcionales deben incluir las pruebas de seguridad.

7.3. Para sistemas que se adquieran y que interactúen datos, con otros sistemas o bases de datos, deben contar con controles de seguridad en ambos extremos de la comunicación.

7.4. La arquitectura de los sistemas de información que se adquieran debe obedecer a los lineamientos de arquitectura de sistemas adoptado por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

7.5. Para la adquisición de nuevos sistemas de información, se debe especificar los controles de seguridad desde la etapa de elaboración del requerimiento, tales como encriptación de claves, de mensajes, de configuración; auditoria; versionamiento; entre otros. Estos controles deben ser aprobados por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

7.6. Los controles de seguridad, de los sistemas que se adquieran deben ser preferentemente de tipo automático, evitando procesos o intervención manual.

7.7. Los sistemas que se adquieran deben estar bajo procedimientos de control de cambios y de versionamiento.

7.8. Los sistemas de información que sean desarrollados a la medida para el Servicio Nacional de Aduana del Ecuador deben ser registrados ante el registro de derechos de autor en el organismo competente, con el fin de precautelar la integridad, confidencialidad y disponibilidad de los mismos.

8. REQUERIMIENTOS MÍNIMOS PARA EL DESARROLLO DE SISTEMAS DE INFORMACIÓN

8.1. La implementación de un Sistema de Información debe contar con normas de programación, versionamiento, documentación y pruebas para cada etapa del proceso, previo a la autorización de la puesta en producción.

8.2. Los procedimientos de pruebas deben ser funcionales y no funcionales. Las pruebas no funcionales deben incluir las pruebas de seguridad.

8.3. El proceso de desarrollo y pruebas, deben efectuarse en ambientes apropiados.

8.4. Para sistemas que interactúen datos, con otros sistemas o bases de datos, deben contar con controles de seguridad en ambos extremos de la comunicación.

8.5. Se debe considerar controles de seguridad apropiados, deben ser preferentemente de tipo automático, evitando procesos o intervención manual. Estos controles deben ser aprobados por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

8.6. En términos generales, todo sistema que considere transformación de datos de entrada debe ser diseñada y construida considerando controles de integridad de éstos.
8.7. Cuando un sistema tenga previsto el envío de datos que contengan información clasificada como reservada, se debe implementar mecanismos de cifrado de los datos.
8.8. Toda la documentación, archivos ejecutables, códigos fuente y librerías de software de los sistemas en desarrollo, debe estar bajo procedimientos de control de cambios y de versionamiento.
8.9. Todos los Sistemas de Información desarrollados e implementados en el SENAE deben ser registrados ante el registro de derechos de autor en el organismo competente, con el fin de precautelar la integridad, confidencialidad y disponibilidad de los mismos.

9. REQUERIMIENTOS MÍNIMOS PARA EL MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

9.1. Para el proceso de mantenimiento, se debe especificar los controles de seguridad necesarios a considerar. Estos controles deben ser aprobados por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.
9.2. Los controles de seguridad deben ser preferentemente de tipo automático, evitando procesos o intervención manual.
9.3. Los procedimientos de pruebas del proceso de mantenimiento deben ser funcionales y no funcionales. Las pruebas no funcionales deben incluir las pruebas de seguridad
9.4. El proceso de mantenimiento y sus respectivas pruebas deben efectuarse en ambientes apropiados.

10. SEGURIDAD EN PUERTOS DE COMUNICACIÓN

10.1. El acceso a los puertos de diagnóstico y configuración, para los equipos de comunicaciones, debe contar con controles de seguridad físico y lógico, como se describe en el manual de procedimiento emitido por la unidad de Redes y Comunicaciones, de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

10.2. Los puertos de comunicaciones permitidos dentro de los controles de seguridad son los descritos en el manual de procedimiento emitido por la unidad de Redes y Comunicaciones, de la Dirección Nacional de Mejora Continua y Tecnologías de la Información. Para la habilitación de un puerto no permitido, deberá ser analizado y autorizado por la Jefatura de Infraestructura Tecnológica. Los siguientes son un grupo de puerto bloqueados como control de seguridad de Sistemas de Información del Senae:

Puerto	Nombre	Observación
31	Master Paradise	Usado por Troyanos, potencialmente peligroso.

41	DeepThroat y SMTP	Usado por Troyanos, potencialmente peligroso. Simple Mail Transfer Protocol (SMTP) es utilizado para la transferencia simple de correo electrónico.
58	Dmsetup	Usado por Troyanos, potencialmente peligroso.
146	FC Infecto	Usado por Troyanos, potencialmente peligroso.
531	RASmin	Usado por Troyanos, potencialmente peligroso.
555	Stealth Spy	Usado por Troyanos, potencialmente peligroso.
666	Bla, Attack FTP	Usado por Troyanos, potencialmente peligroso.
911	Dark Shadow	Usado por Troyanos, potencialmente peligroso.
999	DeepThroat	Usado por Troyanos, potencialmente peligroso.
1001	Silencer	Usado por Troyanos, potencialmente peligroso.
1010	Doly	Usado por Troyanos, potencialmente peligroso.
1011	Doly	Usado por Troyanos, potencialmente peligroso.
1012	Doly	Usado por Troyanos, potencialmente peligroso.
1015	Doly	Usado por Troyanos, potencialmente peligroso.
1024	Netspy	Usado por Troyanos, potencialmente peligroso.
1025	Unused Windows Services Block	Usado por Troyanos, potencialmente peligroso.
1026	Unused Windows Services Block	Usado por Troyanos, potencialmente peligroso.
1027	Unused Windows Services Block	Usado por Troyanos, potencialmente peligroso.
1028	Unused Windows Services Block	Usado por Troyanos, potencialmente peligroso.
1029	Unused Windows Services Block	Usado por Troyanos, potencialmente peligroso.
1030	Unused Windows Services Block	Usado por Troyanos, potencialmente peligroso.
1042	Bla	Usado por Troyanos, potencialmente peligroso.
1045	RASmin	Usado por Troyanos, potencialmente peligroso.
1090	Extreme	Usado por Troyanos, potencialmente peligroso.
1121	Crimson Skies	Juego on-line de aviones de la segunda guerra mundial.
1234	Ultor's	Usado por Troyanos, potencialmente peligroso.
1243	Backdoor/SubSeven	Usado por Troyanos, potencialmente peligroso.
1492	FTP99CMP	Usado por Troyanos, potencialmente peligroso.
1600	Shiva Burka	Usado por Troyanos, potencialmente peligroso.
1807	Spy Sender	Usado por Troyanos, potencialmente peligroso.
1981	ShockRave y Domain Name System (DNS).	Usado por Troyanos, potencialmente peligroso. Los servidores DNS resuelven la dirección IP de un dominio.
1999	Backdoor/SubSeven, TransScout	Usado por Troyanos, potencialmente peligroso.
2000	TransScout, Remote Explorer	Usado por Troyanos, potencialmente peligroso.

2001	TransScout, Trojan Cow	Usado por Troyanos, potencialmente peligroso.
2002	TransScout	Usado por Troyanos, potencialmente peligroso.
2003	TransScout	Usado por Troyanos, potencialmente peligroso.
2004	TransScout	Usado por Troyanos, potencialmente peligroso.
2005	TransScout	Usado por Troyanos, potencialmente peligroso.
2023	Trojan Ripper	Usado por Troyanos, potencialmente peligroso.
2115	Bugs	Usado por Troyanos, potencialmente peligroso.
2140	DeepThroat	Usado por Troyanos, potencialmente peligroso.
2300	BattleCom	Battlecom es un programa de comunicación de voz pensado para personas que jueguen a través de Internet.
2300	Microsoft Game	Puerto frecuentemente usado para juegos de Microsoft.
2565	Striker	Usado por Troyanos, potencialmente peligroso.
2583	WinCrash	Usado por Troyanos, potencialmente peligroso.
2611	Black and White	Juego on-line de estrategia como protagonistas unos graciosos personajes.
2773	Backdoor/SubSeven	Usado por Troyanos, potencialmente peligroso.
2774	SubSeven 2.1/2.2	Usado por Troyanos, potencialmente peligroso.
2801	Phinneas Phucker	Usado por Troyanos, potencialmente peligroso.
3000	Active Worlds	Juego en 3D que se desarrolla en un mundo y vida virtual.
3024	WinCrash	Usado por Troyanos, potencialmente peligroso.
3040	Crimson Skies	Juego on-line de aviones de la segunda guerra mundial.
3129	Master Paradise	Usado por Troyanos, potencialmente peligroso.
3150	DeepThroat	Usado por Troyanos, potencialmente peligroso.
3453	Bungie	Sistema de multi-juegos on-line.
3700	Portal of Doom	Usado por Troyanos, potencialmente peligroso.
4000	Blizzard Battle.net	Juego on-line.
4092	WinCrash	Usado por Troyanos, potencialmente peligroso.
4267	SubSeven 2.1/2.2	Usado por Troyanos, potencialmente peligroso.
4567	Filenail	Usado por Troyanos, potencialmente peligroso.
5000	Sokets de	Usado por Troyanos, potencialmente peligroso.
5001	Sokets de Trois v1.	Usado por Troyanos, potencialmente peligroso.
5321	FireHotcker	Usado por Troyanos, potencialmente peligroso.
5400	Blade Runner	Usado por Troyanos, potencialmente peligroso.

5401	Blade Runner	Usado por Troyanos, potencialmente peligroso.
5402	Blade Runner	Usado por Troyanos, potencialmente peligroso.
5555	SERV-Me	Usado por Troyanos, potencialmente peligroso.
5556	BO-Facil	Usado por Troyanos, potencialmente peligroso.
5557	BO-Facil	Usado por Troyanos, potencialmente peligroso.
5569	Robo-Hack	Usado por Troyanos, potencialmente peligroso.
5670	Active Worlds	Juego en 3D que se desarrolla en un mundo y vida virtual.
5742	WinCrash	Usado por Troyanos, potencialmente peligroso.
6073	Microsoft Game	Puerto frecuentemente usado para juegos de Microsoft.
6112	Blizzard Battle.net	Juego on-line.
6400	'The Thing'	Usado por Troyanos, potencialmente peligroso.
6500	MRO	Juego de coches ligero, divertido y muy personalizable.
6667	Black and White	Juego on-line de estrategia como protagonistas unos graciosos personajes.
6670	DeepThroat	Usado por Troyanos, potencialmente peligroso.
6771	DeepThroat	Usado por Troyanos, potencialmente peligroso.
6776	Backdoor/SubSeven	Usado por Troyanos, potencialmente peligroso.
6939	Indoctrination	Usado por Troyanos, potencialmente peligroso.
6969	GateCrasher, Priority	Usado por Troyanos, potencialmente peligroso.
6970	GateCrasher	Usado por Troyanos, potencialmente peligroso.
7000	Remote Grab	Usado por Troyanos, potencialmente peligroso.
7000	Active Worlds	Juego en 3D que se desarrolla en un mundo y vida virtual.
7013	Anarchy Online	Juego on-line de lucha futurista.
7215	Backdoor/SubSeven	Usado por Troyanos, potencialmente peligroso.
7300	NetMonitor	Usado por Troyanos, potencialmente peligroso.
7301	NetMonitor	Usado por Troyanos, potencialmente peligroso.
7306	NetMonitor	Usado por Troyanos, potencialmente peligroso.
7307	NetMonitor	Usado por Troyanos, potencialmente peligroso.
7308	NetMonitor	Usado por Troyanos, potencialmente peligroso.
7500	Anarchy Online	Juego on-line de lucha futurista.
7597	QaZ	Usado por Troyanos, potencialmente peligroso.
7777	Active Worlds	Juego en 3D que se desarrolla en un mundo y vida virtual.

7789	'ICKiller'	Usado por Troyanos, potencialmente peligroso.
9872	Portal of Doom	Usado por Troyanos, potencialmente peligroso.
9873	Portal of Doom	Usado por Troyanos, potencialmente peligroso.
9874	Portal of Doom	Usado por Troyanos, potencialmente peligroso.
9875	Portal of Doom	Usado por Troyanos, potencialmente peligroso.
9989	iNi Killer	Usado por Troyanos, potencialmente peligroso.
10067	Portal of Doom	Usado por Troyanos, potencialmente peligroso.
10167	Portal of Doom	Usado por Troyanos, potencialmente peligroso.
10520	Acid Shivers	Usado por Troyanos, potencialmente peligroso.
10607	COMA	Usado por Troyanos, potencialmente peligroso.
11000	Senna Spy	Usado por Troyanos, potencialmente peligroso.
11223	Progenic	Usado por Troyanos, potencialmente peligroso.
12076	GJammer	Usado por Troyanos, potencialmente peligroso.
12223	Keylogger	Usado por Troyanos, potencialmente peligroso.
12345	NetBus	Usado por Troyanos, potencialmente peligroso.
12346	NetBus	Usado por Troyanos, potencialmente peligroso.
12361	Whack-a-Mole	Usado por Troyanos, potencialmente peligroso.
12362	Whack-a-Mole	Usado por Troyanos, potencialmente peligroso.
12363	Whack-a-Mole	Usado por Troyanos, potencialmente peligroso.
12631	WhackJob	Usado por Troyanos, potencialmente peligroso.
13000	Senna Spy	Usado por Troyanos, potencialmente peligroso.
16959	SubSeven DEFCON8 2.1	Usado por Troyanos, potencialmente peligroso.
20034	NetBus	Usado por Troyanos, potencialmente peligroso.
21154	Dark Reign	Juego on-line basado en un cómic.
21554	GirlFriend	Usado por Troyanos, potencialmente peligroso.
22222	Proziack	Usado por Troyanos, potencialmente peligroso.
23456	EvilFTP, UglyFTP	Usado por Troyanos, potencialmente peligroso.
23476	Donald Dick	Usado por Troyanos, potencialmente peligroso.
23477	Donald Dick	Usado por Troyanos, potencialmente peligroso.
26274	Delta Source	Usado por Troyanos, potencialmente peligroso.
27374	SubSeven 2.1/2.2	Usado por Troyanos, potencialmente peligroso.
27900	Black and White	Juego on-line de estrategia como protagonistas unos graciosos personajes.
28801	Crimson Skies	Juego on-line de aviones de la segunda guerra mundial.
28805	Crimson Skies	Juego on-line de aviones de la segunda guerra mundial.

30100	NetSphere	Usado por Troyanos, potencialmente peligroso.
30101	NetSphere	Usado por Troyanos, potencialmente peligroso.
30102	NetSphere	Usado por Troyanos, potencialmente peligroso.
31337	Back Orifice 2000	Usado por Troyanos, potencialmente peligroso.
31785	Hack 'A' Tack	Usado por Troyanos, potencialmente peligroso.
31787	Hack 'A' Tack	Usado por Troyanos, potencialmente peligroso.
31788	Hack 'A' Tack	Usado por Troyanos, potencialmente peligroso.
31789	Hack 'A' Tack	Usado por Troyanos, potencialmente peligroso.
31791	Hack 'A' Tack	Usado por Troyanos, potencialmente peligroso.
31792	Hack 'A' Tack	Usado por Troyanos, potencialmente peligroso.
40421	Master Paradise	Usado por Troyanos, potencialmente peligroso.
40422	Master Paradise	Usado por Troyanos, potencialmente peligroso.
40423	Master Paradise	Usado por Troyanos, potencialmente peligroso.
40425	Master Paradise	Usado por Troyanos, potencialmente peligroso.
40426	Master Paradise	Usado por Troyanos, potencialmente peligroso.
47624	Age of Empires	Juego de estrategia a tiempo real.
47624	Baldur's Gate - BattleCom	Baldur's Gate es un juego de rol on-line. Battlecom es un programa de comunicación de voz pensado para personas que jueguen a través de Internet.
47624	Battlefield Communicator	Un sistema de comunicación por voz pensado especialmente para el conocido juego Battlefield.
47624	Microsoft Game	Puerto frecuentemente usado para juegos de Microsoft.
54283	Backdoor/SubSeven	Usado por Troyanos, potencialmente peligroso.
54320	Back Orifice 2000	Usado por Troyanos, potencialmente peligroso.
54321	Back Orifice 2000	Usado por Troyanos, potencialmente peligroso.
60000	DeepThroat	Usado por Troyanos, potencialmente peligroso.

11. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasionará que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

SENAE-PI-3-2-005-V2

POLÍTICAS INSTITUCIONALES PARA EL ACCESO A SISTEMAS DE INFORMACIÓN

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona el Manual de Políticas de Acceso a Sistemas de Información de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.		
Objetivo:		
Establecer las políticas o lineamientos para los usuarios que tiene acceso a los sistemas de información, con respecto a las responsabilidades y buen uso de su cuenta de usuario y contraseña de acceso.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
Firmado electrónicamente por: CARLA MARGARITA ORTUNO DELGADO Ing. Carla Ortuno Analista Informático	Seguridad Informática	Elaboración
Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA X Ing. Hugo Robayo Jefe de Infraestructura Tencologica	Jefatura de Infraestructura Tecnológica	Aprobación
Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ X Lsi. Diego Maldonado Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ X Ing. Nelson Rodriguez Director de Tecnologías de la Información	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:			
Versión	**Fecha**	**Razón**	**Responsable**
1	Junio 2015	Versión Inicial	Ing. Mario Barragán J.
2	Mayo 2021	Inclusión sobre normativa vigente	Ing. Carla Ortuño D.

ÍNDICE

1. OBJETIVO

Establecer las políticas o lineamientos para los usuarios que tiene acceso a los sistemas de información, con respecto a las responsabilidades y buen uso de su cuenta de usuario y contraseña de acceso.

2. ALCANCE

Está dirigido a todos los usuarios internos y externos que tengan acceso a sistemas de información del Senae.

Es necesario que todos los usuarios estén enterados y conscientes de los compromisos, normas y lineamientos que han adquirido al contar con una cuenta de usuario para el acceso a Sistemas de Información del Senae, tomando todas las medidas que correspondan para que estas directrices se respeten y se cumplan.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de todos los usuarios del Senae.

3.2. Los accesos no autorizados a los sistemas de Información no autorizados pueden conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

3.3. La actualización y mejoramiento del presente documento le corresponde al área de Seguridad de la Información perteneciente a la Jefatura de Infraestructura Tecnológica de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.
- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.

- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto de que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al presente manual:

5.1.1. **Usuario:** persona que recibe un producto o servicio de un proceso que pertenece al Senae.

5.1.2. **Cuenta de usuario:** identificación con la que se personaliza el acceso de un usuario a un sistema informático, otorgándole privilegios y niveles de servicios.

5.1.3. **Sistema informático:** aplicaciones o servicios informáticos disponibles para el usuario, con la finalidad de que sea una herramienta de trabajo para cumplir las funciones otorgadas.

5.2. Si se detecta o sospecha que las actividades de una cuenta de usuario pueden comprometer la integridad y seguridad de la información, el acceso a dicha cuenta será suspendido temporalmente y será reactivada sólo después de haber tomado las medidas necesarias a consideración de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

5.3. Para los efectos de este documento, se entenderá que es responsabilidad personal, sin importar su nivel jerárquico, utilizar en forma responsable la contraseña de usuario que se le asigna.

5.4. Esta política entrará en vigor a partir del siguiente día hábil a su autorización y difusión, y está vigente en tanto no se emita nuevos ordenamientos en la materia.

6. POLÍTICA DE CONTROL DE ACCESO

6.1 Todos los accesos que requieran los usuarios a los sistemas de información deberán ser gestionados utilizando el Formulario de solicitud de accesos a cuentas de usuario (FRM-AS04), para prevenir los accesos no autorizados.

6.2 Los perfiles de acceso de los usuarios a los sistemas de información, se encuentran definidos en el Catálogo de Perfiles de Accesos a Cuentas de Usuario, emitido por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

6.1 La definición de los autorizadores de los permisos de acceso a la información, se encuentran establecidos en el Instructivo de Trabajo para el registro de datos en el formulario de solicitud de accesos a cuentas de usuario (SENAE-IT-03-2-005-V2) emitido por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

7. POLÍTICA DE ASIGNACIÓN Y CAMBIO DE CONTRASEÑA

7.1 Asignación de Contraseña:

7.1.1 El usuario debe realizar el cambio de contraseña al ingresar por primera vez a los sistemas de información.

7.1.2 La contraseña de sesión a la estación de trabajo expira a los 42 días del primer ingreso o después de haber sido cambiada.

7.1.3 Se debe cambiar la contraseña antes de su caducidad o de lo contrario se bloqueará al usuario y será necesario gestionar una contraseña temporal a través de la cuenta de la Mesa de servicios: mesadeservicios@aduana.gob.ec .

7.2 Uso de Contraseña:

7.2.1 Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseña.

7.2.2 La contraseña constituye un medio de validación y autenticación de la identidad de un usuario, consecuentemente un medio para establecer derecho de acceso a los sistemas de información del Senae.

7.2.3 Los usuarios deben mantener las contraseñas en secreto.

7.2.4 Los usuarios deben realizar el respectivo cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

7.2.5 Seleccionar contraseña de calidad, de acuerdo con las prescripciones informadas por la cuenta: seguridadinformatica@aduana.gob.ec.

7.2.6 Los usuarios deben cambiar la contraseña cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

7.2.7 Los usuarios deben notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad a la cuenta de la Mesa de servicios: mesadeservicios@aduana.gob.ec.

8. RESPONSABILIDADES SOBRE USO DE LA CUENTA DE USUARIO Y LA CONTRASEÑA ASIGNADA

8.1. El uso de la cuenta de usuario es responsabilidad de la persona a la que está asignada.

8.2. La cuenta de usuario es de uso personal e intransferible.

8.3. Cada usuario que accede a un sistema informático debe tener una sola cuenta de usuario al sistema.

8.4. No compartir la cuenta de usuario con otras personas.

8.5. Si otra persona demanda hacer uso de la cuenta de usuario hacer referencia a estas políticas.

8.6. La cuenta de usuario se protegerá mediante una contraseña.

8.7. La contraseña asociada a la cuenta de usuario deberá seguir los criterios de complejidad de claves seguras establecidos por el Administrador del servicio del sistema informático.

8.8. Genere contraseñas que pueda recordar fácilmente, una forma de recordarlo con facilidad es crear una contraseña basada en una frase fácilmente recordable.

8.9. Todas las contraseñas deberán ser tratadas con carácter de confidencial.

8.10. Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica instantánea ni vía telefónica.

8.11. Si es necesario el uso de mensajes de correo electrónico para la divulgación de contraseñas, estas deberán transmitirse de forma cifrada.

8.12. Se evitará mencionar y en la medida de lo posible, teclear contraseñas en frente de otros.

8.13. No revele sus contraseñas en ningún cuestionario, reporte o formulario, independientemente de la confianza que le inspire el mismo.

8.14. Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos, bases de datos, correo electrónico y las demás aplicaciones o servicios que utilice.

8.15. Se evitará el activar o hacer uso de la utilidad de "Recordar Contraseña" o "Recordar Password" de las aplicaciones o servicios que utilice.

8.16. No se almacenarán las contraseñas en libretas, agendas, post-it, hojas sueltas, etc. Si se requiere el respaldo de las contraseñas en medio impreso, el documento generado deberá ser único y bajo resguardo y responsabilidad del usuario, implementando algún mecanismo de seguridad.

8.17. No se almacenarán las contraseñas sin encriptación, en sistemas electrónicos personales (asistentes electrónicos personales, memorias USB, teléfonos celulares, agendas electrónicas, etc.)

8.18. Si alguna contraseña es detectada y catalogada como no segura, deberá darse aviso al(los) usuario(s) para efectuar un cambio inmediato en dicha contraseña.

8.19. No revele su contraseña por teléfono a nadie, en ninguna circunstancia.

8.20. No revele la contraseña en mensajes de correo electrónico ni a través de cualquier otro medio de comunicación electrónica.

8.21. No revele su contraseña a sus superiores, ni a sus colaboradores.

8.22. No hable sobre sus contraseñas delante de otras personas.

8.23. No comparta sus contraseñas con familiares ni amistades, por más confianza que tenga en ellos.

8.24. No revele sus contraseñas a compañeros de trabajo cuando se ausente por vacaciones.

8.25. Si sospecha que su contraseña puede haber sido comprometida en su confidencialidad, proceda de inmediato a cambiarla.

8.26. Cambie sus contraseñas con la frecuencia recomendada para cada tipo de cuenta y servicio.

9. REGISTRO DE INICIO SEGURO

Se permite la autentificación de usuario a los sistemas de información, una vez que esté debidamente autorizado y ejecutado lo estipulado en el Instructivo de Trabajo para el registro de datos en el formulario de solicitud de accesos a cuentas de usuarios (SENAE-IT-3-2-005-V2).

10. RESPONSABILIDAD DE BUEN USO DE LA CONTRASEÑA

La contraseña que registre un usuario para el acceso a los sistemas de información deberá estar regida bajo los siguientes lineamientos:

10.1. Debe ser secreta.

10.2. No debe ser compartida con nadie.

10.3. Debe ser robusta usando letras, número y caracteres especiales.

10.4. Debe contener al menos una letra mayúscula.

10.5. Debe poseer una longitud mínima de 7 caracteres.

10.6. No usar el nombre de la cuenta del usuario.

10.7. No usar partes del nombre completo del usuario.

10.8. Se deben aplicar como mínimo tres de las cuatro categorías al momento de crear una nueva contraseña:

- Caracteres en mayúsculas (A hasta la Z)
- Caracteres en minúsculas (a hasta la z)
- Números (0 a 9)
- Caracteres especiales (_, $, #,%, .)

11. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasionará que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

SENAE-PI-3-2-006-V3

POLÍTICAS INSTITUCIONALES DE LOS REQUERIMIENTOS DE SEGURIDAD PARA RESPALDOS DE LA INFORMACIÓN

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:
Este documento proporciona las normas, procedimientos y lineamientos para el respaldo de información que garanticen la continuidad del negocio basados en los Tiempos de Recuperación Objetivo (RTO) y Punto de Recuperación Objetivo (RPO) en el Servicio Nacional de Aduana del Ecuador.
Objetivo:
Establecer el procedimiento de respaldo, retención y restauración de la información, así como el etiquetado de acuerdo a los requisitos del negocio del Servicio Nacional de Aduana del Ecuador.

Elaboración / Revisión / Aprobación:

Nombre / Cargo / Firma / Fecha	Área	Acción
Firmado electrónicamente por: CARLA MARGARITA ORTUNO DELGADO Ing. Carla Ortuno Analista Informático	Seguridad Informática	Elaboración
Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA X Ing. Hugo Robayo Jefe de Infraestructura Tencologica	Jefatura de Infraestructura Tecnológica	Aprobación
Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ X Lsi. Diego Maldonado Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ X Ing. Nelson Rodriguez Director de Tecnologías de la Información	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:

Versión	Fecha	Razón	Responsable
1	Mayo 2015	Versión Inicial	Ing. Gabriela Montesdeoca
2	Abril 2017	Actualización periódica	Ing. Gabriela Montesdeoca
3	Mayo 2021	Inclusión sobre normativa vigente	Ing. Carla Ortuño D.

ÍNDICE

1. OBJETIVO

Establecer normas, procedimientos y lineamientos para el respaldo de información que garanticen la continuidad del negocio basados en los Tiempos de Recuperación Objetivo (RTO) y Punto de Recuperación Objetivo (RPO) en el Servicio Nacional de Aduana del Ecuador.

2. ALCANCE

Está dirigido a todos los usuarios internos que de alguna manera se encuentren involucrados con el respaldo, retención y restauración de la información.

El alcance del presente documento incluye la información que se registra en las tablas auditadas de la base de datos del portal interno del sistema aduanero Ecuapass, así como el etiquetado de acuerdo con la clasificación de la información crítica del negocio del Servicio Nacional de Aduana del Ecuador.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de los usuarios internos y de la Dirección Nacional de Mejora Continua y Tecnologías de la Información, involucrados en el respaldo de la información del Senae.

3.2. La actualización y mejoramiento del presente documento le corresponde al área de Seguridad de la Información perteneciente la Jefatura de Infraestructura Tecnológica de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

3.3. Los servicios tecnológicos detallados en el presente documento corresponden a los servicios que actualmente, el área de centro de computo realiza el respaldo y etiquetado de la información. Es responsabilidad de la Dirección Nacional de Mejora Continua y Tecnologías de la Información mantener el catálogo de servicios tecnológicos actualizados.

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.
- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.
- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.

- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto de que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al respaldo de información:

5..1. Usuario: persona que recibe un producto o servicio de un proceso que pertenece al Senae.

5..2. Respaldo: consiste en una copia de la información a un medio físico en una determinada fecha.

5..3. Información: es un activo que tiene valor y requiere de una protección adecuada.

5..4. RTO (Recovery Time Objective): es el tiempo objetivo para la reanudación de los servicios después de un desastre.

6.1.1.

5..5. RPO (Recovery Point Objective): es el punto mas reciente en el tiempo en el que un sistema puede recuperarse y determina la periodicidad con la que debe respaldarse la información.

6. DESARROLLO

6.1. GESTIÓN DEL RESPALDO DE INFORMACIÓN:

6.1.1. El respaldo de información es una parte fundamental para la continuidad del negocio en caso de algún desastre o incidente de seguridad de la información. Se realiza mediante cintas magnéticas y las tareas de respaldos programadas en la herramienta TSM (Tivoli Storage Manager).

6.1.2. Las tareas que no se encuentran programadas en el TSM (Tivoli Storage Manager), deberán ser realizadas manualmente hasta que sean ingresadas para respaldos automáticos para lo cual debe ser coordinado con el área de centro de cómputo.

6.1.3. El área de centro de cómputo son los custodios de los respaldos de la información y definen 2 tipos de respaldos: total e incremental**.**

- ✓ Respaldo total: es el respaldo completo de toda la información, lo que implica mayor espacio de almacenamiento.
- ✓ Respaldo incremental: es el respaldo de aquellos datos que han sido modificados respecto al ultimo respaldo realizado, es decir, únicamente se respaldan los cambios recientes. El respaldo incremental no sustituye a las copias incrementales anteriores.

6.1.4. La frecuencia de los respaldos es: diaria, mensual, anual y bajo demanda, esto dependerá de la criticidad de la información a respaldar.

6.2. PROCESO DE OPERACIÓN DE LAS COPIAS DE RESPALDO:

6.2.1. Los respaldos de información deben realizarse de acuerdo con un cronograma definido y aprobado por la Jefatura de Infraestructura Tecnológica, Oficial de Seguridad de la Información y propietario de la información para garantizar que los respaldos se realicen de acuerdo con los requerimientos del Senae.

6.2.2. Los propietarios de la información tienen la responsabilidad de solicitar el respaldo de la información que consideren critica. La solicitud debe estar aprobada por el Jefe de Infraestructura Tecnológica y una vez aprobada se debe enviar la solicitud de respaldo de información a la cuenta de correo electrónico del operador de centro de cómputo: operador@aduana.gob.ec (ver anexo 1), quienes analizan el requerimiento y lo canalizarán adecuadamente.

6.2.3. El área de centro de cómputo controlará y monitoreará la realización de los respaldos de información.

6.2.4. El propietario de la información, el operador del área de centro de cómputo y el Oficial de Seguridad de la Información llevaran a cabo pruebas periódicas de restauración para verificar la disponibilidad, confiabilidad e integridad de la información respaldada y asegurar la efectividad de los medios de almacenamiento. Los tiempos son definidos por el Oficial de Seguridad de la Información.

6.2.5. Los respaldos de información deben almacenarse en un sitio seguro con los controles necesarios, en una ubicación diferente a aquella donde se realizan los respaldos y dentro de un área protegida contra cualquier acceso no autorizado.

6.2.6. Todos los requerimientos de restauración de información deben enviarse al Director de cada área quien autorizará el requerimiento y solicitará al Director de Tecnologías de la Información la ejecución de la respectiva tarea de restauración.

6.2.7. El periodo de retención de la información considerada como critica es máximo de 10 años; para la información importante no critica el periodo de retención es mínimo de 1 año hasta un periodo máximo de 10 años.

6.2.8. Las solicitudes de accesos a cuentas de usuarios no son respaldadas, es responsabilidad de cada usuario el resguardo de las solicitudes.

6.3. DESCRIPCIÓN DE LOS SERVICIOS A RESPALDAR

6.3.1. El RPO (Punto Objetivo de Recuperación) determina la posible pérdida máxima de datos para el SENAE desde el último respaldo disponible, los mismos que se indican a continuación:

Tabla 1: Catalogo de servicios con RPO

SERVICIO	DESCRIPCION	RPO (TIEMPO MÁXIMO DE PERDIDA DESDE EL ÚLTIMO RESPALDO)
Bases de datos produccion - Ecuapass	Base de datos	24 horas
Respaldos Tsm (Tivoli Storage Manager)	bdtsmsat02	24 horas
Portal externo / interno produccion (servidor)	/app	24 horas
Portal aduana.gob.ec (servidor)	/app	24 horas
Instancias was	/app	24 horas

SERVICIO	DESCRIPCION	RPO (TIEMPO MÁXIMO DE PERDIDA DESDE EL ÚLTIMO RESPALDO)
Banred	archivos	24 horas
Replicas a Manta	volumenes de datos	1 hora
Exchange	bases y logs	168 horas
Directorio activo	politicas	168 horas
IPS	politicas, logs y configuraciones	360 horas
Filtrado web	logs	24 horas
Filtrado web	politicas	360 horas
Antispam	politicas, logs y configuraciones	168 horas
Antivirus	politicas, logs y configuraciones	168 horas
Datawarehouse	Base de datos	168 horas
Portal externo / interno desarrollo (servidor)	/app /dataresp /oracle /oradata /usr	24 horas
Credimail	/app /archive /attach	24 horas
Ventanilla unica	/data	24 horas
Mineria de datos	/c /d	24 horas
Cognos	Bases de datos modelos paquetes	24 horas
Servidor de impresoras	/c	24 horas
Web services	1 archivo	24 horas
Pases de version	1 archivo	24 horas
Mesa de ayuda	/respaldoOtrs	24 horas

6.4. RESPALDO DE INFORMACIÓN Y TIEMPOS ESTIMADOS DE RPO Y RTO:

6.4.1. La criticidad de la información a respaldar está dada por el nivel de impacto a los activos de la información y se establecen 3 niveles de criticidad: alto, medio y bajo, se proyectan tiempos estimados de RPO y RTO para el respaldo de información de acuerdo a la siguiente tabla:

Tabla 2: Catálogo de servicios con tiempos estimados

SERVICIO	DESCRIPCIÓN	SERVIDOR	RPO	RTO
Bases de datos produccion - Ecuapass	Base de datos		24 horas	4 horas
Respaldos Tsm (Tivoli Storage Manager)	bdtsmsat02		24 horas	6 horas
Portal externo / interno produccion (servidor)	/app	s28prtwb01 s28prtwb02	24 horas	20 minutos x modulo
Portal aduana.gob.ec (servidor)	/app		24 horas	2 horas
Instancias was	/app	s028intws01 s028intws02 s028ptlws01 s028ptlws02	24 horas	5 horas x instancia
Banred	archivos		24 horas	2 horas
Replicas a Manta	volumenes de datos		1 hora	1 hora
Exchange	bases y logs		168 horas	48 horas
Directorio activo	politicas		168 horas	48 horas
IPS	politicas, logs y configuraciones		360 horas	30 minutos
Filtrado web	logs		24 horas	45 minutos
Filtrado web	politicas		360 horas	45 minutos
Antispam	politicas, logs y configuraciones		168 horas	20 minutos

SERVICIO	DESCRIPCIÓN	SERVIDOR	RPO	RTO
Antivirus	politicas, logs y configuraciones		168 horas	4 horas
Datawarehouse	Base de datos		168 horas	48 horas
Portal externo / interno desarrollo (servidor)	/app /dataresp /oracle /oradata /usr	s28devws01 s28testws01 s28intdv01	24 horas	2 horas
Credimail	/app /archive /attach		24 horas	6 horas
Ventanilla unica	/data	s28intbm01 s28intbm02	24 horas	24 horas
Mineria de datos	/c /d		24 horas	48 horas
Cognos	Bases de datos modelos paquetes		24 horas	2 horas
Servidor de impresoras	/c		24 horas	1 hora
Web services	1 archivo		24 horas	2.5 horas
Pases de version	1 archivo		24 horas	24 horas
Mesa de ayuda	/respaldoOtrs		24 horas	24 horas

Nota: el tiempo estimado de RPO y RTO es considerado siempre y cuando el respaldo y la restauración se realice en condiciones óptimas y dependerá de la cantidad de información y tipo de incidente por el que se requiere restaurar la información, disponibilidad de cintas y drives de la librería de respaldos.

6.4.2. Para garantizar que los respaldos se estén realizando de acuerdo con los requerimientos y necesidades del negocio se definen los propietarios de la información de acuerdo con los siguientes servicios tecnológicos:

SERVICIO	DESCRIPCIÓN
Bases de datos produccion - Ecuapass	Base de datos
Respaldos Tsm (Tivoli Storage Manager)	Centro de computo
Portal externo / interno produccion (servidor)	Servidores
Portal aduana.gob.ec (servidor)	Servidores
Instancias was	Base de datos
Banred	Base de datos
Replicas a Manta	Servidores
Exchange	Servidores
Directorio activo	Servidores
IPS	Redes y comunicaciones
Filtrado web	Seguridades
Antispam	Seguridades
Antivirus	Seguridades
Datawarehouse	Desarrollo - SIG
Portal externo / interno desarrollo (servidor)	Desarrollo - SIG
Credimail	Servidores
Ventanilla unica	Desarrollo - VUE
Mineria de datos	Desarrollo - SIG
Cognos	Desarrollo - SIG
Servidor de impresoras	Servidores
Web services	Base de datos
Pases de version	Desarrollo
Mesa de ayuda	Desarrollo

7. ETIQUETADO DE LOS RESPALDOS DE INFORMACIÓN

7.1. Los respaldos de información deben contener una etiqueta con una identificación única para que pueda ser leída por la aplicación de respaldos Tivoli Storage Manager (TSM). Además, debe contener otra etiqueta que permita identificar el contenido, periodicidad y retención del respaldo de la información.

Estructuración de codificación de medios de almacenamiento
SI-XX-NN / DD-MM-AAAA / TT-RR

Donde:

Sigla	Descripción	Ejemplos
SI	Servicio para respaldar	Ecuapass, …
XX	Localidad	DG, GYEM, …
NN	Numero de cinta	01,02,….
DD	Dia del respaldo	01,02,….
MM	Mes del respaldo	01,02,….
AAAA	Año del respaldo	2019, 2020…
TT	Periodicidad	Diaria, quincenal, mensual, anual, bajo demanda
RR	Retención	1,2,…

8. PROCEDIMIENTOS

8.1. Procedimientos de respaldo de información

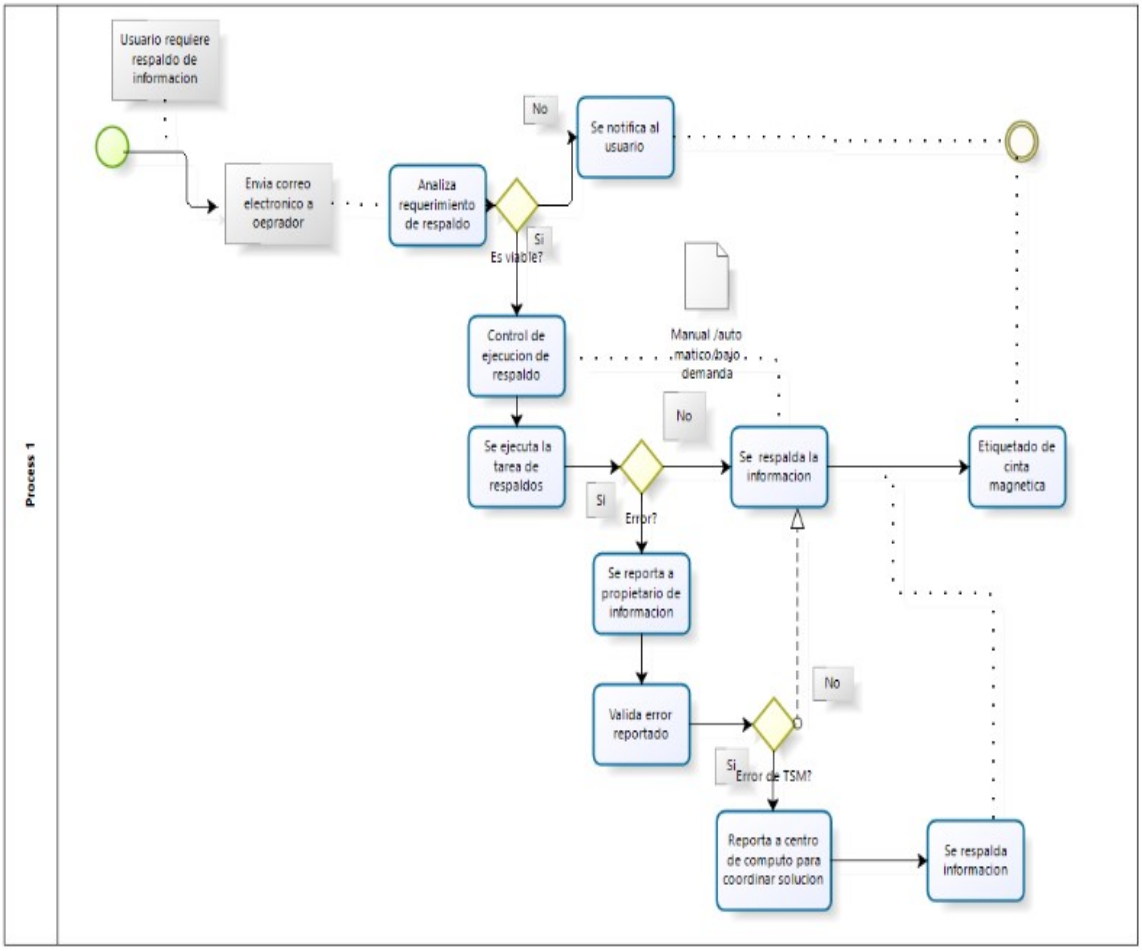
No.	Actividad	Producto de entrada	Descripción de actividad	Responsable	Producto de salida
1	Revisar el cronograma de respaldos	Bitácora de registro	El operador de Centro de Computo revisa la información a respaldar	Operador de centro de cómputo	Información para respaldar
2	Respaldo manual o automático	Información para respaldar	Identifica los respaldos automáticos y manuales. Si el respaldo es manual ejecuta el paso No. 3, caso contrario ejecuta el paso No.4	Operador de centro de cómputo	Decisión de respaldo
3	Respaldo manual	Decisión de respaldo	Respalda la información y la envía a cinta magnética	Operador de centro de cómputo	Validación de errores
4	Respaldo automático	Decisión de respaldo	Monitorear que la ejecución de los respaldos en el TSM se realice de acuerdo con el cronograma de respaldos y se cumplan con el RPO. Si el respaldo se realizó se ejecuta el paso No. 7, caso contrario se	Operador de centro de cómputo	Validación de errores

No.	Actividad	Producto de entrada	Descripción de actividad	Responsable	Producto de salida
			ejecuta el paso No. 5		
5	Monitoreo de respaldo automático	Validación de errores	Si el respaldo automático en TSM no se realizó puede deberse a los siguientes motivos: El proceso de respaldo este encolado y se termina el tiempo de espera, por lo cual no se realiza el respaldo. Se debe ejecutar al siguiente día. Existen varios procesos encolados de información en el TSM, se revisa la criticidad de los respaldos no ejecutados dando prioridad a estos de ser necesario.	Operador de centro de cómputo	Notificación al propietario de la información
6	Respaldo automático	Notificación al propietario de la información	El propietario de la información valida el error, en caso de ser solucionado debe informarse al operador de Centro de cómputo para que ejecute nuevamente el respaldo. En caso de que el inconveniente persista y se deba a un error del TSM se debe indicar al operador de Centro de cómputo para que canalice con el proveedor de servicios. Una vez solucionado el problema debe respaldarse la información.	Operador de centro de cómputo	Cinta magnética
7	Etiquetado de información	Cinta magnética	Se etiqueta el respaldo con el ID que corresponda a la cinta. La etiqueta debe regirse de acuerdo con la Estructura de codificación de los medios del almacenamiento que consta en la política SENAE-PI-3-2-006-V3 numeral 8.	Operador de centro de cómputo	Correo electrónico de notificación

No.	Actividad	Producto de entrada	Descripción de actividad	Responsable	Producto de salida
8	Cierre de respaldo de información	Correo electrónico de notificación	Se notifica a la Jefatura de Infraestructura Tecnológica y propietario de la información de los respaldos realizados. Las cintas magnéticas son retiradas cuando estén llenas.	Operador de centro de cómputo	Finalización

9. FLUJOGRAMA

9.1. Proceso de respaldo de información



10. ANEXO

10.1. Anexo 1: Formato para la solicitud de respaldos

Para: operador@aduana.gob.ec
CC: Jefe de Infraestructura Tecnológica

SOLICITUD DE RESPALDOS DE INFORMACION

Nombre de solicitante: _____

Nombre del archivo: _____

Ruta de acceso: _____

Hora en la que se genera el archivo a respaldar: _____

Tamaño de la información que se va a respaldar: _____

Frecuencia de respaldos
(incremental/mensual/anual): _____

SENAE-PI-3-2-007-V2

POLÍTICAS INSTITUCIONALES DEL CATÁLOGO DE PERFILES DE ACCESO PARA CUENTAS DE USUARIOS

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:
Este documento proporciona una matriz o plantilla que establece los accesos informáticos con sus respectivos privilegios que se deben configurar a cada usuario interno, de acuerdo al cargo y área departamental asignado por la Dirección Nacional de Talento Humano.
Objetivo:
Establecer la normativa para crear y configurar los accesos de los sistemas informáticos utilizados en el Servicio Nacional de Aduana del Ecuador., dependiendo del puesto y área asignada al usuario interno.

Elaboración / Revisión / Aprobación:

Nombre / Cargo / Firma / Fecha	Área	Acción
Firmado electrónicamente por: MAGDELINE ESTEFANIE ROSERO PEREZ X Ing. Magdeline Rosero Analista In	Seguridad Informática	Elaboración
Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA X Mgs. Hugo Robayo Jefe de Infraestructura Tecnológica	Jefatura de Infraestructura Tecnológica	Revisión
Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ X Mgs. Diego Maldonado Director de Tecnologías de la Inform ación	Dirección de Tecnologías de la Información	Aprobación
Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ X Ing. Nelson Rodriguez Director Nacional de Mejora Continua y Tecnologí...	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:

Versión	Fecha	Razón	Responsable
1	Junio 2015	Versión Inicial	Ing. Mario Barragán J.
2	Mayo 2021	Inclusión de normativa vigente	Ing. Magdeline Rosero P.

ÍNDICE

1. OBJETIVO

Establecer la normativa para crear y configurar los accesos de los sistemas informáticos utilizados en el Servicio Nacional de Aduana del Ecuador., dependiendo del puesto y área asignada al usuario interno.

2. ALCANCE

Está dirigido a todos los usuarios internos del Servicio Nacional de Aduana del Ecuador.

Es necesario que todos los usuarios estén enterados y conscientes de los accesos informáticos con los que cuentan, tomando todas las medidas que correspondan para que estas directrices se respeten y se cumplan.

Todos los usuarios están sujetos a este catálogo, el uso inapropiado puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de todos los usuarios internos del Senae.

3.2. La actualización y mejoramiento del presente documento, le corresponde a la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

4. NORMA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.
- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.
- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de

Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.

- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al presente catálogo:

5.1.1. Usuario: Persona que recibe un producto o servicio de un proceso que pertenece al Senae.

5.1.2. Sistemas informáticos: Aplicaciones o servicios informáticos disponibles para el usuario, con la finalidad de que sea una herramienta de trabajo para cumplir las funciones otorgadas.

6. PUESTOS O CARGOS DEL SENAE

Los puestos o cargos que otorga la Dirección Nacional de Talento Humano a nivel nacional son:

NRO.	CARGOS
1	ABOGADO 3
2	ABOGADO ADUANERO
3	ANALISTA DE CONTABILIDAD 1
4	ANALISTA DE CONTABILIDAD 2
5	ANALISTA DE CONTROL DISCIPLINARIO
6	ANALISTA DE MEJORA CONTINUA Y NORMATIVA
7	ANALISTA DE PRESUPUESTO 1
8	ANALISTA DE TALENTO HUMANO 1
9	ANALISTA DE TALENTO HUMANO 2
10	ANALISTA DE TALENTO HUMANO 3
11	ANALISTA INFORMÁTICO 1
12	ANALISTA INFORMÁTICO 2
13	ASESOR 2
14	ASISTENTE DE ABOGACÍA

15	ASISTENTE DE ATENCIÓN AL USUARIO
16	ASISTENTE DE PERIODISMO
17	ASISTENTE DE TALENTO HUMANO
18	CONDUCTOR/CHOFER ADMINISTRATIVO
19	CONSERJE EXTERNO LIMPIEZA Y MANTENIMIENTO
20	CONTADOR GENERAL DE ADUANA
21	COORDINADOR GENERAL DE CONTROL DISCIPLINARIO
22	DIRECTOR ADMINISTRATIVO ADUANERO
23	DIRECTOR ADMINISTRATIVO FINANCIERO
24	DIRECTOR DE ASESORÍA JURÍDICA
25	DIRECTOR DE AUDITORIA E INSPECCIONES
26	DIRECTOR DE AUTORIZACIONES Y EXPEDIENTES OCES
27	DIRECTOR DE COMUNICACIÓN
28	DIRECTOR DE CONTROL ZONA PRIMARIA
29	DIRECTOR DE DESPACHO
30	DIRECTOR DE DESPACHO Y CONTROL ZONA PRIMARIA DISTRITOS
31	DIRECTOR DE ESTUDIOS DE RIEGOS Y VALOR
32	DIRECTOR DE INTELIGENCIA Y PROTECCIÓN
33	DIRECTOR DE MEJORA CONTINUA Y NORMATIVA
34	DIRECTOR DE OPERACIONES MARÍTIMAS
35	DIRECTOR DE PLANIFICACIÓN Y CONTROL DE GESTIÓN INSTITUCIONAL
36	DIRECTOR DE PUERTO
37	DIRECTOR DE RECLAMOS Y RECURSOS
38	DIRECTOR DE RECLAMOS Y TRÁMITES OPERATIVOS
39	DIRECTOR DE RELACIONES ADUANERAS INTERNACIONALES
40	DIRECTOR DE SECRETARÍA GENERAL
41	DIRECTOR DE SEGURIDAD Y SALUD OCUPACIONAL
42	DIRECTOR DE TÉCNICA ADUANERA
43	DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN
44	DIRECTOR DE ZONA
45	DIRECTOR DISTRITAL
46	DIRECTOR FINANCIERO ADUANERO
47	DIRECTOR GENERAL
48	DIRECTOR NACIONAL DE CAPITALES Y SERVICIOS ADMINISTRATIVOS
49	DIRECTOR NACIONAL DE GESTIÓN DE RIESGOS Y TÉCNICA ADUANERA
50	DIRECTOR NACIONAL DE INTERVENCIÓN
51	DIRECTOR NACIONAL DE LA UNIDAD DE VIGILANCIA ADUANERA

52	DIRECTOR NACIONAL DE MEJORA CONTINUA Y TECNOLOGÍAS DE LA INFORMACIÓN
53	DIRECTOR NACIONAL DE TALENTO HUMANO
54	DIRECTOR NACIONAL JURÍDICO ADUANERO
55	DIRECTOR POLÍTICA ADUANERA
56	DIRECTOR PROCESAL
57	DIRECTOR REGIONAL DE INTERVENCIÓN 1
58	DIRECTOR REGIONAL DE INTERVENCIÓN 2
59	DIRECTOR REGIONAL DE INTERVENCIÓN 3
60	ESPECIALISTA EN COOPERACIÓN INTERNACIONAL ADUANERA
61	ESPECIALISTA EN PLANIFICACIÓN ADUANERA
62	ESPECIALISTA EN SEGURIDAD Y SALUD OCUPACIONAL
63	ESPECIALISTA EN TÉCNICA ADUANERA
64	ESPECIALISTA LABORATORISTA 1
65	ESPECIALISTA LABORATORISTA 2
66	ESTIBADOR
67	GUARDALMACÉN ADUANERO
68	GUARDALMACÉN JEFE DE DISTRITO
69	INSPECTOR DE VIGILANCIA ADUANERA 1
70	INSPECTOR DE VIGILANCIA ADUANERA 2
71	INSPECTOR DE VIGILANCIA ADUANERA 3
72	INTERVENTOR
73	INVENTARIADOR
74	JEFE DE ANÁLISIS FUNCIONAL
75	JEFE DE CALIDAD Y MEJORA CONTINUA
76	JEFE DE CLASIFICACIÓN
77	JEFE DE CONTROL DE PROCESOS OPERATIVOS Y PROCESOS DE CAMPO
78	JEFE DE CONTROL POSTERIOR
79	JEFE DE DESARROLLO EN SISTEMAS
80	JEFE DE DOCUMENTACIÓN Y ARCHIVO
81	JEFE DE EVALUACIÓN DE AGENTES DEL COMERCIO EXTERIOR
82	JEFE DE GESTIÓN DE RIESGOS ADUANEROS
83	JEFE DE INFRAESTRUCTURA ADUANERA
84	JEFE DE POLÍTICA Y NORMATIVA ADUANERA
85	JEFE DE PRESUPUESTO ADUANERA
86	JEFE DE PROCESOS ADUANEROS
87	JEFE DE REVISIÓN PASIVA
88	JEFE LEGAL DE CONTRATACIONES
89	OFICINISTA

90	OPERADOR DE CENTRAL TELEFÓNICA
91	OPERADOR DE MONTACARGA
92	SECRETARIA
93	SECRETARIA DE DIRECCIÓN GENERAL, NACIONAL Y DISTRITAL
94	SECRETARIA EJECUTIVA 1
95	SECRETARIA EJECUTIVA 2
96	SUBDIRECTOR DE APOYO REGIONAL
97	SUBDIRECTOR DE ZONA DE CARGA AÉREA
98	SUBDIRECTOR GENERAL DE GESTIÓN INSTITUCIONAL
99	SUBDIRECTOR GENERAL DE NORMATIVA ADUANERA
100	SUBDIRECTOR GENERAL DE OPERACIONES
101	SUPERVISOR DE ATENCIÓN AL USUARIO
102	TÉCNICO DE ANÁLISIS FUNCIONAL
103	TÉCNICO EN ADQUISICIONES 1
104	TÉCNICO EN ADQUISICIONES 3
105	TÉCNICO EN ARCHIVO
106	TÉCNICO EN CONTROL DE BIENES E INVENTARIOS
107	TÉCNICO EN GESTIÓN DE COBRANZAS Y GARANTÍAS 1
108	TÉCNICO EN GESTIÓN DE COBRANZAS Y GARANTÍAS 2
109	TÉCNICO EN INFRAESTRUCTURA
110	TÉCNICO EN SERVICIOS DE MANTENIMIENTO 2
111	TÉCNICO EN SERVICIOS DE MANTENIMIENTO ADUANERO
112	TÉCNICO EN SERVICIOS GENERALES 2
113	TÉCNICO ESPECIALISTA DE RIESGOS ADUANEROS
114	TÉCNICO OPERADOR
115	TESORERO GENERAL DE ADUANA
116	VIGILANTE ADUANERO 1
117	VIGILANTE ADUANERO 2

7. SISTEMAS INFORMATICOS

La Dirección Nacional de Mejora Continua y Tecnologías de la Información administra los siguientes sistemas informáticos, catalogados en dos grupos:

7.1. Infraestructura interna:

- Active Directory
- Base de Datos
- Correo electrónico

- Internet
- Sistema Interno Aduanero (SIA)
- Control de Asistencia (Chronos)
- Cognos
- ECUAPASS

7.2. Infraestructura externa:

- Gestión Documental (Quipux)
- Gobierno por Resultados (GPR)
- Sistema de Administración Financiera (eSigef)

8. CATÁLOGO

Para la asignación de los sistemas informáticos y sus respectivos privilegios, de acuerdo al cargo y área departamental del usuario interno, existen cuatro tipos de catálogos o plantillas, que agrupa los cargos de acuerdo a su jerarquía y funciones.

Los catálogos o plantillas, son archivos en Excel, cuyos nombres son:

- PERFILES - DIRECTORES.xls
- PERFILES - JEFES.xls
- PERFILES - OPERATIVOS.xls
- PERFILES - COMPLEMENTARIO.xls

9. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasionará que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

SENAE-PI-3-2-008-V2

POLITICAS INSTITUCIONALES PARA EL USO DE LOS SISTEMAS DE VIDEOCONFERENCIA

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona el Manual de Uso de los sistemas de videoconferencia de la Dirección Nacional de Mejora Continua y Tecnologías de la Información		
Objetivo:		
Establecer las políticas de las condiciones de uso y/o lineamientos del Sistema de Videoconferencia, con el fin exclusivamente de garantizar la calidad de servicio y la adecuada operación en el Senae, dada la importancia de este sistema para las comunicaciones.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
X Firmado electrónicamente por: MAGDELINE ESTEFANIE ROSERO PEREZ Ing. Magdeline Rosero Analista Informático 2	Seguridad Informática	Elaboración
X Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA Mgs. Hugo Robayo Jefe de Infraestructura Tecnológica	Jefatura de Infraestructura Tecnológica	Revisión
X Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ Mgs. Diego Maldonado Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
X Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ Ing. Nelson Rodriguez Director Nacional de Mejora Continua y Tecnologí...	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:			
Versión	**Fecha**	**Razón**	**Responsable**
1	Noviembre 2016	Versión Inicial	Ing. Mario Barragán J.
2	Mayo 2021	Inclusión de normativa vigente	Ing. Magdeline Rosero P.

ÍNDICE

1. OBJETIVO

Establecer las políticas de las condiciones de uso y/o lineamientos del Sistema de Videoconferencia, con el fin exclusivamente de garantizar la calidad de servicio y la adecuada operación en el Senae, dada la importancia de este sistema para las comunicaciones.

2. ALCANCE

Es necesario que todos los usuarios estén enterados y conscientes de los compromisos, normas y lineamientos que han adquirido en la prestación del servicio, condiciones de uso y las especificaciones para la realización de la videoconferencia.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de todos los usuarios del Senae.

3.2. La actualización y mejoramiento del presente documento, le corresponde a la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

3.3. La administración de videoconferencia, es responsabilidad de la unidad de Soporte Tecnico.

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.
- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.
- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado

en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al presente manual:

5.1.1 **Usuario:** Persona que recibe un producto o servicio de un proceso que pertenece a SENAE.

5.1.2 **Cuenta de usuario:** Identificación con la que se personaliza el acceso de un usuario a un sistema informático, otorgándole privilegios y niveles de servicios.

5.1.3 **Videoconferencia:** Servicio tecnológico que permite la conexión simultánea, en tiempo real de usuarios que se encuentren geográficamente distantes. Esta conexión se realiza mediante audio y video v permite que los usuarios puedan intercambiar información de formar interactiva.

5.2. Esta política entrara en vigor a partir del siguiente día hábil a su autorización y difusión, y está vigente en tanto no se emita nuevos ordenamientos en la materia

6. POLÍTICAS DE USO DE LOS SISTEMAS DE VIDEOCONFERENCIAS

6.1 Condiciones de uso:

6.1.1. La Sala de Videoconferencia es de uso exclusivo para eventos estrictamente laborables.

6.1.2. Todo requerimiento interno o externo para el Uso de la Sala de Videoconferencia deber dirigirse vía correo electrónico a la cuenta: mesadeservicios@aduana.gob.ec, agregando en el campo asunto:" Sala de Videoconferencia", con los datos que se encuentran en el ANEXO 1.

6.1.3. El solicitante deberá proporcionar información completa sobre la(s) institución(es) con la cual se realizara la videoconferencia a fin de establecer contacto. Esta incluye: nombre del responsable técnico, teléfono, dirección de correo electrónico, sitio Web donde se publica la invitación.

6.1.4. Las solicitudes deberán ser realizadas con anticipación a la fecha del evento de acuerdo a los siguientes tiempos:

- Cinco (5) días hábiles de anticipación para solicitar un enlace para presenciar una videoconferencia que vaya a ser transmitida desde alguna otra sede dentro de la Red.
- Diez (10) a quince (15) días hábiles de anticipación para establecer un enlace con una institución que no pertenezca a la Red del Senae.

6.1.5. La asignación de una fecha y hora depende de la disponibilidad de la Sala de Videoconferencia así como de la Sala del sitio remoto del enlace.

6.1.6. La respuesta correspondiente a cada solicitud deberá ser enviada por lo menos dos(2) días hábiles después de su recepción, ofreciendo fechas y horarios alternativos en caso de que los eventos no puedan realizarse en la fecha y hora solicitada.

6.1.7. El horario para la prestación del servicio de videoconferencias es de lunes a viernes de 8:00am a 12:00pm y de 2:00pm a 17:00pm.

6.2 De los Servicios:

6.2.1. Se debe configurar en los Sistemas Polycom dos niveles de acceso a los usuarios que utilizan el sistema en la sala:

- Un usuario inicie sesión para utilizar el sistema.
- Un administrador inicie sesión para ajustar las configuraciones de administrador

6.2.2. Para la configuración de las contraseñas de la sala y acceso remoto se debe definir la contraseña de sala del administrador, la contraseña de acceso remoto del administrador, la contraseña de acceso remoto del usuario y la contraseña de sala del usuario para proporcionar varios niveles de acceso al sistema usando el control remoto o el teclado, o desde un equipo.

6.2.3. Los usuarios deben seguir buenas prácticas de seguridad en la selección y use de contraseña a las cuentas detalladas en el numeral 6.2.1, según lo indicado en el Manual de proceso de asignación y cambio de contraseña.

6.2.4. Se debe habilitar la lista de sesiones para ver información de los que hayan iniciado sesión.

6.2.5. Por temas de seguridad se debe habilitar la opción de bloqueo de cuenta para que no se acepten inicios de sesión tras un numero configurable de intentos fallidos en dichas cuentas. Protegiendo así las cuentas locales del administrador y del usuario del sistema.

7. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasiona que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

8. ANEXO

8.1 ANEXO 1: Solicitud de Uso de Sala de Videoconferencia

De: Pazmiño Manuel – DES GYE
Para: mesadeservicios@aduana.gob.ec
ASUNTO: SALA DE VIDEOCONFERENCIA

DIA	04 DE MAYO DE 2021
HORA DE COMIENZO	8:00AM
HORA DE FINALIZACION	11:00AM
ASUNTO	CHARLA DE MENAJE DE CASA
VIDEOCONFERENCIA: SI/NO	NO
CANTIDAD DE PERSONAS	15
CAPACITACIÓN: INTERNA O EXTERNA	EXTERNA

SENAE-PI-3-2-009-V2

POLÍTICAS INSTITUCIONALES DE LOS REQUERIMIENTOS MÍNIMOS DE SEGURIDAD PARA ESTACIONES DE TRABAJO Y EQUIPOS DE CENTRO DE CÓMPUTO

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona un manual de requerimientos mínimos o directrices de seguridad que se deben cumplir por parte de los usuarios que utilicen estaciones de trabajo y equipos del Centro de Cómputo en el Senae.		
Objetivo:		
Establecer requerimientos mínimos o básicos a considerar sobre seguridad, que se deben tomar para el uso de las estaciones de trabajo y los equipos del Centro de Cómputo en el Senae.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
Firmado electrónicamente por: MAGDELINE ESTEFANIE ROSERO PEREZ X Ing. Magdeline Rosero Analista Informático 2	Seguridad Informática	Elaboración
Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA X Mgs. Hugo Robayo Jefe de Infraestructura Tecnológica	Jefatura de Infraestructura Tecnológica	Aprobación
Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ X Mgs. Die[illegible]o Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ X Ing. Nelson Rodriguez Director Nacional de Mejora Continua y Tecnologí...	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:			
Versión	**Fecha**	**Razón**	**Responsable**
1	Junio 2015	Versión Inicial	Ing. Mario Barragán J.
2	Mayo 2021	Inclusión de normativa vigente	Ing. Magdeline Rosero P.

ÍNDICE

1. OBJETIVO

Establecer requerimientos mínimos o básicos a considerar sobre seguridad, que se deben tomar para el uso de las estaciones de trabajo y los equipos del Centro de Cómputo en el Senae.

2. ALCANCE

Está dirigido a todos los usuarios del Senae que utilicen o tengan a su cargo estaciones de trabajo o equipos en el centro de cómputo.

Es necesario que todos los usuarios estén enterados y conscientes de los lineamientos que deben cumplir y que se detallan en el presente documento..

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de todos los usuarios del Senae.

3.2. Es responsable de verificar el cumplimiento de los presentes lineamientos la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

3.3. La actualización y mejoramiento del presente documento, le corresponde a la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.
- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.
- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las

instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.

- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al presente manual:

5.1.1. Usuario: Persona que recibe un producto o servicio de un proceso que pertenece al Senae.

5.1.2. Estación de trabajo: Es un computador personal con la que se puede trabajar conectado a una red que facilita a los usuarios el acceso a los servidores, aplicaciones y periféricos de la red.

5.1.3. Equipos de centro de cómputo: Todos los dispositivos electrónicos que conforman un centro de cómputo, como son servidores, equipos de comunicación, UPS, etc.

6. SEGURIDAD PARA ESTACIONES DE TRABAJO

6.1. Cada persona es responsable de la estación de trabajo que le ha sido asignado, por tanto, procurará entregarle los cuidados considerados en el correcto uso del mismo.

6.2. El uso de las estaciones de trabajo deberá ser apropiado, legal, ético y laboral.

6.3. El uso de las estaciones de trabajo es personal e intransferible, debiendo ser utilizado para realizar actividades laborales del Senae. Por tanto el usuario asume responsabilidad en forma expresa de su uso personal o por parte de terceros.

6.4. Toda estación de trabajo del Senae deberá usar la configuración definida por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

6.5. No está permitido el traslado, interna o externamente de las instalaciones del Senae, de todo tipo de componentes computacionales, programas, software u otros elementos que conforman la estación de trabajo, sin la correspondiente autorización de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

6.6. Todo medio de almacenamiento removible, debe ser revisado por posible presencia de virus, por medios tecnológicos de forma automática.

6.7. La correcta utilización de las estaciones de trabajo es responsabilidad del usuario custodio del bien, debiendo éste, informar a través de los canales formales cualquier falla, deterioro o evento anormal de los dispositivos, así como la indebida instalación de programas computacionales no autorizados por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

6.8. La incorporación, deshabilitación o modificación de cualquier dispositivo de hardware o software, incluido el intercambio de componentes de un computador con otro debe efectuarse sólo por personal del área de Soporte Técnico.

6.9. Está prohibido deshabilitar los mecanismos de control de acceso, el software antivirus o cualquier otro componente de seguridad de un computador.

6.10. Toda falencia técnica debe ser notificada a la Mesa de servicios.

6.11. Cualquier requerimiento de cambio de configuración debe ser previamente autorizado y justificado por el superior respectivo y efectuado por personal del área de Soporte Técnico.

6.12. Los archivos almacenados en el disco local de las estaciones de trabajo y su respaldo, es responsabilidad directa del usuario, además es responsable de administrar periódicamente sus archivos, haciendo uso de las funcionalidades del área de Soporte Técnico.

6.13. Los equipos informáticos ingresados en forma temporal deben contar con la autorización de la Dirección Nacional de Mejora Continua y Tecnologías de la Información y cumplir con el control de acceso de equipos realizado por la unidad de Soporte Técnico.

6.14. Queda prohibida la instalación o conexión de cualquier dispositivo o herramienta que no sea propiedad del Senae, salvo con la autorizado de la Dirección Nacional de Mejora Continua y Tecnologías de la Información. La instalación o conexión la efectuará personal del área de Soporte Técnico.

6.15. El área de Soporte Técnico deberá instalar únicamente software que cuente con licencia de uso vigente y hardware, que hayan sido adquiridos por el Senae.

6.16. Toda instalación, configuración y mantenimiento, de hardware y software, la debe realizar sólo el personal del área de Soporte Técnico.

6.17. El equipo informático no debe ser abierto, desarmado, golpeado ni trasladado de lugar sin la respectiva autorización.

7. SEGURIDAD PARA EQUIPOS DE CENTRO DE CÓMPUTO

7.1. Todo acceso al Centro de Cómputo deberá ser autorizado por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

7.2. Se prohíbe la manipulación del equipamiento de servidores, equipos de comunicación y todo tipo de equipo ubicado en el Centro de Cómputo, salvo con la autorización de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

7.3. Al finalizar cualquier trabajo en el Centro de Cómputo, deberá asegurarse que los cables estén bien instalados y ordenados, dentro de sus gabinetes, así como las puertas cerradas apropiadamente.

7.4. No se podrá instalar equipos inalámbricos o antenas en las dependencias del Centro de Cómputo.

7.5. No se permiten las conexiones en cadena de varias regletas de tomas eléctricas, en los gabinetes de servidores, del Centro de Cómputo.

7.6. Todo ingreso o salida, de equipos del Centro de Cómputo, deberá contar con la autorización de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

7.7. Toda instalación, desinstalación o configuración, de hardware o software, de los equipos del Centro de Cómputo, deberá contar con la autorización de la Jefatura de Infraestructura Tecnológica y deberá ser realizada o supervisada por personal del área de Servidores o Redes.

7.8. Toda reinicio de equipos de servidores deberá contar con la autorización de la Jefatura de Infraestructura Tecnológica.

7.9. Queda estrictamente prohibido acercarse, manejar, usar o inspeccionar el equipo o gabinetes ajenos a la actividad a realizar

7.10. Se prohíbe el acceso a las instalaciones del Centro de Cómputo de cámaras fotográficas, filmadoras, pendrive, discos portátiles, computadores personales, tablets y cualquier otro artículo similar a los antes mencionados, salvo con la autorización de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

7.11. Se prohíbe el uso de circuitos destinados a la alimentación de Racks para conectar otros equipos ajenos al Centro de Cómputo, como cargadores de celulares, aspiradoras, ventiladores, entre otros.

7.12. Se prohíbe interceptar, modificar, adulterar, desconectar o conectar equipos y entre otras acciones, y que puedan afectar el normal funcionamiento del Centro de Cómputo y sus servicios que presta.

8. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasionará que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

SENAE-PI-3-2-010-V2

POLÍTICAS INSTITUCIONALES DEL PROCEDIMIENTO DE BORRADO SEGURO EN LOS DISPOSITIVOS DE ALMACENAMIENTO Y EN EL PROCESO DE REUTILIZACIÓN DE LAS ESTACIONES DE TRABAJO

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona las políticas y procedimiento a seguir para realizar un borrado seguro en los dispositivos de almacenamiento y garantizar la eliminación de la información.		
Objetivo:		
Establecer la política y el procedimiento formal para realizar un borrado seguro en los dispositivos de almacenamientos y en el proceso de reutilización de las estaciones de trabajo, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
X Firmado electrónicamente por: MAGDELINE ESTEFANIE ROSERO PEREZ Ing. Magdeline Rosero Analista Informático 2	Seguridad Informática	Elaboración
X Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA Mgs. Hugo Robayo Jefe de Infraestructura Tecnológica	Jefatura de Infraestructura Tecnológica	Aprobación
X Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ Mgs. Die[illegible]o Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
X Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ Ing. Nelson Rodriguez Director Nacional de Mejora Continua y Tecnologí...	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación
Actualizaciones / Revisiones / Modificaciones:		
Versión	**Fecha**	**Razón**	**Responsable**
1	Septiembre 2015	Versión Inicial	Ing. Mario Barragán J.
2	Mayo 2021	Inclusión de normativa vigente	Ing. Magdeline Rosero P.

ÍNDICE

1. OBJETIVO

Establecer la política y el procedimiento formal definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información para realizar un borrado seguro en los dispositivos de almacenamientos y en el proceso de reutilización de las estaciones de trabajo.

2. ALCANCE

El manual de política y procedimiento de borrado seguro en los dispositivos de almacenamiento de las estaciones de trabajo, está dirigido a todos los usuarios del Senae.

Todos los usuarios están sujetos a esta política y procedimiento, el uso inapropiado puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de todos los usuarios del Senae.

3.2. La actualización y mejoramiento del presente documento, le corresponde a la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

3.3. La Unidad de Control de Bienes e Inventarios proporcionará oportunamente a la Jefatura de Infraestructura Tecnológica el inventario actualizado de todas las estaciones de trabajo y dispositivos de almacenamiento existentes en el Senae.

3.4. La Jefatura de Infraestructura Tecnológica llevará un inventario actualizado de todos los dispositivos de almacenamientos del Senae, internos y externos, utilizadas en todas las estaciones de trabajo, con información técnica del dispositivo, nombre del respectivo responsable y que se encuentren codificados por la Unidad de Control de Bienes e Inventarios.

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.
- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.

- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al presente manual:

5.1.1 Usuario: Persona que recibe un producto o servicio de un proceso que pertenece al Senae.

5.1.2 Información: Es un activo que tiene valor y requiere de una protección adecuada.

5.1.3 Dispositivos de almacenamiento: Se consideraran todos aquellos dispositivos que almacenen información digital ya sea temporal o permanente entre ellos están: unidad de cinta magnética, unidad de disco rígido o duros, unidades de estado sólido como memorias flash y tarjetas de memoria, etc.

5.1.4 Estación de trabajo: Computador, tabletas y dispositivos móviles asignado al usuario para el desempeño de sus funciones.

5.1.5 Borrado Seguro: Es la acción que se realiza sobre la información contenida en un medio o dispositivo de almacenamiento, obteniendo como resultado que la misma ya no esté disponible.

5.2. Muchos dispositivos de almacenamiento contienen información confidencial tan valiosa que no debe ser vista por alguien sin autorización, así que una vez que termina la vida útil del dispositivo de almacenamiento, se deberá realizar una destrucción controlada del mismo

5.3. Cualquier dispositivo de almacenamiento puede ser sometido a un proceso de borrado seguro, de manera que la información contenida quedará eliminada.

5.4. Para completar el ciclo de vida de la información, es indispensable cubrir un aspecto de suma importancia como es el borrado seguro de la información.

5.5. Para los efectos de este documento, se entenderá que es responsabilidad personal, sin importar su nivel jerárquico, utilizar en forma responsable las políticas y procedimientos establecidos.

5.6. Esta política entrará en vigor a partir del siguiente día hábil a su autorización y difusión, y está vigente en tanto no se emita nuevos ordenamientos en la materia.

6. POLÍTICA DE BORRADO SEGURO Y DESTRUCCIÓN CONTROLADA EN LOS DISPOSITIVOS DE ALMACENAMIENTO

6.1. Todos los usuarios serán responsables de la información que contenga los dispositivos de almacenamiento de su estación de trabajo.

6.2. Todos los usuarios serán responsables de solicitar al Buzón Mesa de Servicios Institucional para que proceda con el borrado seguro.

6.3. La Jefatura de Infraestructura Tecnológica será únicamente la encargada de realizar o supervisar toda operación de instalación, mantenimiento, reparación o sustitución, de todo dispositivo de almacenamiento en las estaciones de trabajo.

6.4. Todo dispositivo de almacenamiento que contenga información y ya no se considere para su reutilización, se deberá proceder con la destrucción controlada del mismo.

6.5. La Jefatura de Infraestructura Tecnológica, a través de su Unidad de Soporte Técnico, será la encargada de realizar los procesos de borrado seguro. De acuerdo al dispositivo de almacenamiento, se aplicará distintas técnicas y procedimientos, entre las cuales está:

- Borrado: Método de borrado mediante el uso de software o hardware, los cuales borran la información contenida.
- Destrucción: Método utilizado para la eliminación de la información y no reutilización del dispositivo de almacenamiento.

Método de borrado adecuado en función al dispositivo de almacenamiento

Dispositivo de almacenamiento	Tipo	Destrucción	Borrado
Discos rígidos o duros	Magnético	✓	✓
Cintas magnéticas	Magnético	✓	✓

Memorias flash/tarjetas de memoria	Electrónico	✓	✓

6.6. La Jefatura de Infraestructura Tecnológica, a través de su Unidad de Soporte Técnico, será la encargada de realizar la destrucción controlada de los dispositivos de almacenamiento, que dependiendo del medio podrá aplicar diferentes tipos de técnicas y procedimientos para la destrucción física de los dispositivos de almacenamiento y será ejecutada en presencia de un delegado de la Unidad de Control de Bienes e Inventarios.

6.7. Posterior a cada procedimiento de borrado seguro o destrucción controlada, el líder de la Unidad de Soporte Técnico validará la efectividad del proceso solicitado y se registrará la atención satisfactoria al servicio solicitado a través de Mesa de Servicio.

7. POLÍTICA DE REUTILIZACIÓN DE LAS ESTACIONES DE TRABAJO

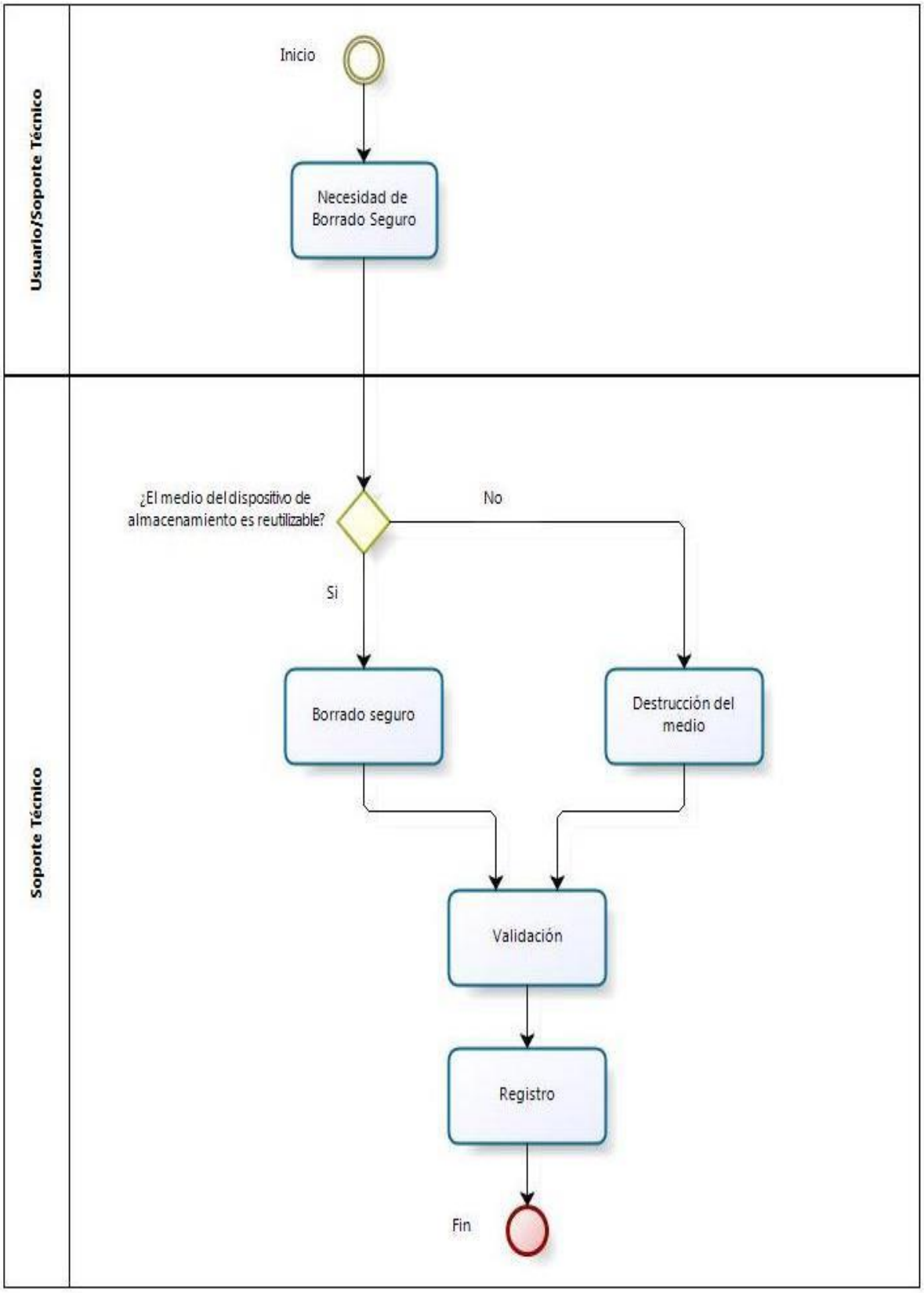
7.1. Toda estación de trabajo que va a ser reutilizada, antes de ser asignada a otro usuario, el Jefe o el Director departamental donde se encuentra la estación de trabajo, serán los responsables de informar a la Unidad de Soporte Técnico, la información que de ser necesario se deberá respaldar.

7.2. Toda estación de trabajo que va a ser reutilizada, antes de ser asignada a otro usuario, la Jefatura de Infraestructura Tecnológica, a través de su Unidad de Soporte Técnico, realizará los procedimientos de borrado seguro a toda la información de usuarios anteriores, existentes en los dispositivos de almacenamiento.

8. PROCEDIMIENTO

No	Actividad	Producto de Entrada	Descripción de Actividad	Responsable	Producto de Salida
1.	Necesidad de Borrado Seguro	Requerimiento a través de Mesa de Servicio	Necesidad de realizar un borrado seguro, por medida de seguridad del responsable de la información o por reutilización del dispositivo de almacenamiento	Usuario/Soporte Técnico	Dispositivo de almacenamiento
2.	Análisis de reutilización	Dispositivo de almacenamiento	Si el medio del dispositivo de almacenamiento ya no va a ser reutilizado se procede con su destrucción, caso contrario se continúa con la actividad 4	Soporte Técnico	Acción a ejecutar para el borrado
3.	Destrucción del medio	Acción a ejecutar para el borrado	Se procede con la destrucción total física del medio y se continúa con la actividad 5	Soporte Técnico	Destrucción física del medio
4.	Borrado seguro	Acción a ejecutar para el borrado	De acuerdo al dispositivo de almacenamiento, se procede con el proceso de Borrado Seguro	Soporte Técnico	Medio del dispositivo de almacenamiento borrado completamente
5.	Validación	Destrucción física del medio/Medio del dispositivo de almacenamiento borrado completamente	Se valida que el proceso haya sido exitoso	Líder de Soporte Técnico	Proceso exitoso
5.	Registro de atención en Mesa de Servicio	Proceso exitoso	Se registra el evento realizado en el requerimiento abierto en Mesa de Servicio	Soporte Técnico	Atención satisfactoria

9. FLUJOGRAMA



10. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasionará que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

SENAE-PI-3-2-011-V2

POLÍTICAS INSTITUCIONALES DE SEGURIDAD PARA LOS EQUIPOS INFORMÁTICOS

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona las políticas de seguridad que se deben cumplir para el uso, preparación, entrega y mantenimiento de los equipos informáticos; también para la instalación, desinstalación, configuración y uso de software informático, de todos los equipos informáticos del Servicio Nacional de Aduana del Ecuador.		
Objetivo:		
Establecer las políticas de seguridad, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información para el uso, preparación, entrega y mantenimiento de los equipos informáticos; también para la instalación, desinstalación, configuración y uso de software informático, de todos los equipos informáticos del Servicio Nacional de Aduana del Ecuador.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
X Firmado electrónicamente por: MAGDELINE ESTEFANIE ROSERO PEREZ Ing. Magdeline Rosero Analista Informático 2	Seguridad Informática	Elaboración
X Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA Mgs. Hugo Robayo Jefe de Infraestructura Tecnológica	Jefatura de Infraestructura Tecnológica	Revisión
X Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ Mgs. Diego Maldonado Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
X Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ Ing. Nelson Rodriguez Director Nacional de Mejora Continua y Tecnologí...	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación
Actualizaciones / Revisiones / Modificaciones:		
Versión	**Fecha**	**Razón**	**Responsable**
1	Noviembre 2016	Versión Inicial	Ing. Mario Barragán J.
2	Mayo 2021	Inclusión de normativa vigente	Ing. Magdeline Rosero P.

ÍNDICE

1. OBJETIVO

Establecer las políticas de seguridad, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información para el uso, preparación, entrega y mantenimiento de los equipos informáticos; también para la instalación, desinstalación, configuración y uso de software informático, de todos los equipos informáticos del Servicio Nacional de Aduana del Ecuador.

2. ALCANCE

El presente manual de política de seguridad para el uso, preparación, entrega y mantenimiento de los equipos informáticos; también para la instalación, desinstalación, configuración y uso de software informático, está dirigido a todos los usuarios del Servicio Nacional de Aduana del Ecuador.

Todos los usuarios están sujetos a esta política, el uso inapropiado puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de todos los usuarios del Servicio Nacional de Aduana del Ecuador.

3.2. La actualización y mejoramiento del presente documento, le corresponde a la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

3.3. La Jefatura de Infraestructura Tecnológica, a través de sus Unidades de Soporte Técnico y Servidores son los encargados de la preparación, entrega y mantenimiento preventivo, de todos los equipos informáticos del Servicio Nacional de Aduana del Ecuador que se encuentren codificados por la Unidad de Control de Bienes e Inventarios.

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.
- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.
- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.

- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al presente manual:

5.1.1 **Base de definiciones:** Conjunto de firmas o algoritmos mediante los cuales una solución antivirus ofrece protección frente a amenazas de virus, hackers y cibercriminales.

5.1.2 **BIOS:** Sistema Básico de Entrada y Salida (BIOS - Basic Input Output System) que, al encender el equipo, busca el sistema operativo para iniciarlo, acorde al medio de almacenamiento configurado con anterioridad.

5.1.3 **Cibercriminales:** Cualquier delito o actividad ilegal cometido con la ayuda de un equipo informáticos y sus respectivos periféricos como una comunicación vía internet, contra una persona, sus bienes, negocios o ente permisible a ser víctima de un delito. También es conocido como delito informático, donde esencialmente es la extensión de los delitos tradicionales con la ayuda de estas técnicas y medios informáticos.

5.1.4 **Desfragmentación:** Es un proceso que consiste en volver a organizar los datos fragmentados de un archivo, para mejorar los accesos al disco duro y que funcione con mayor eficacia. La fragmentación ocurre con el paso del tiempo, a medida que se guardan, cambian o eliminan archivos; estos generalmente se almacenan internamente en el disco duro en un lugar diferente donde originalmente se encontraba el archivo, ocasionado que con el paso del tiempo los datos de un archivo terminen estando fragmentados, y el rendimiento del equipo disminuye porque este tiene que buscar en distintos lugares para abrir un único archivo.

5.1.5 **Directorio Activo:** Es una herramienta para la gestión y organización de los recursos de una red de computadores, donde se almacena toda la información de los objetos que la componen, bajo un esquema jerárquico, permitiendo centralizar su administración.

5.1.6 **Equipo informático:** Servidores, computadores de escritorio, computadores portátiles y tabletas, asignados al usuario para el desempeño de sus funciones.

5.1.7 **Hacker:** Es una persona con un alto conocimiento en el área informática y afines, cuyo propósito principal es descubrir debilidades o vulnerabilidades en los sistemas informáticos; aprovechando estos conocimientos con fines benignos o malignos.

5.1.8 **Hardening:** Es el proceso de asegurar un sistema informático mediante la reducción de vulnerabilidades o agujeros de seguridad en el mismo, donde su objetivo es prevenir incidentes de seguridad de la información y obstaculizar la actividad de un atacante evitando que la misma se concrete en su totalidad.

5.1.9 **Licenciamiento:** Es el derecho a uso de un sistema informático, otorgado por el autor o fabricante, al usuario final; en este caso el Servicio Nacional de Aduana del Ecuador.

5.1.10 **Mantenimiento correctivo:** Actividad que se realiza luego de que ocurre una falla o avería en el funcionamiento de un equipo informático, y consiste en localizar los daños o defectos y corregirlos o repararlos; hasta devolverle la funcionalidad correcta.

5.1.11 **Mantenimiento preventivo:** Actividades de revisión que se realiza a un equipo informático en forma programada, para prevenir, encontrar y corregir fallas en su operatividad, con el fin de optimizar su desempeño y seguridad.

5.1.12 **Mesa de Servicios:** Plataforma informática implementada como canal de atención para prestar soporte a diferentes niveles de usuarios informáticos, con la finalidad de gestionar y solucionar incidentes de manera integral.

5.1.13 **Plantilla de Seguridad:** Conjunto de actividades y controles de seguridad (Hardening) que deben aplicarse en las estaciones de trabajo para reforzar al máximo las vulnerabilidades del mismo y evitar la labor del atacante y las consecuencias de un incidente de seguridad.

5.1.14 **Políticas de Grupo:** Es un conjunto de una o más políticas del sistema, creadas dentro de un Directorio Activo, cada una establece una configuración del objeto al que afecta, por ejemplo ocultar panel de control, establecer fondo de escritorio, protector de pantalla, deshabilitar el uso del comando REGEDIT.EXE para evitar cambios no autorizados en los Registros del Sistema Operativo Windows, etc.

5.1.15 **Políticas de Grupo del Directorio Activo para el Equipo:** Definición de configuraciones específicas (proceder del sistema operativo, apariencia del escritorio, configuración de las aplicaciones, de seguridad, etc.) para un equipo que es parte del Directorio Activo. Se aplican cuando se inicia el sistema operativo.

5.1.16 **Políticas de Grupo del Directorio Activo para el Usuario:** Definición de configuraciones específicas (acceso al panel de control, configuración de red, fondo de escritorio, protector de pantalla, configuración de Internet Explorer, etc.) para un usuario que es parte del Directorio Activo. Se aplica al momento en que el usuario se conecta a una computadora con su cuenta y contraseña.

5.1.17 **Sectores dañados:** Segmentos de un disco duro en donde se presentan problemas de lectura o escritura de información.

5.1.18 **Sistema Operativo:** Es el programa básico o principal de un equipo informático que provee una interfaz entre el resto de programas del equipo, sus dispositivos y el usuario. Sus funciones básicas son administrar los recursos de la máquina, coordinar sus periféricos y organizar archivos y directorios en sus dispositivos de almacenamiento. Los Sistemas Operativos más utilizados son Windows, Linux y OS X.

5.1.19 **Software:** Grupo de programas informáticos con licenciamiento activo, adquiridos a nombre del Servicio Nacional de Aduana del Ecuador y grupo de programas de código abierto, distribución libre.

5.1.20 **Usuario:** Persona que recibe un producto o servicio de un proceso que pertenece al Servicio Nacional de Aduana del Ecuador.

5.1.21 **Virus:** Es un tipo de programa informático o software malicioso, que tiene como objetivo infiltrarse o dañar un equipo informático o sistema de información, ocasionando efectos molestos, destructivos e incluso irreparables sin el consentimiento y/o conocimiento del usuario.

5.2. Estas políticas entran en vigor a partir del siguiente día hábil a su autorización y difusión, y está vigente en tanto no se emitan nuevos ordenamientos en la materia.

6. EQUIPOS INFORMÁTICOS

6.1. Los equipos informáticos propiedad del Servicio Nacional de Aduana del Ecuador, se utilizan únicamente para actividades laborales que permitan alcanzar las metas y objetivos planteados por la Institución.

6.2. Para poder conectar un equipo informático que no sea propiedad del Servicio Nacional de Aduana del Ecuador, se requiere la autorización correspondiente al Director Nacional de Mejora Continua y Tecnologías de la Información o su delegado, a través de Mesa de Servicios; y se debe inspeccionar el equipo informático con el fin de comprobar que dicho dispositivo no constituye un riesgo para la seguridad de los servicios, red y recursos informáticos de la Institución. Análisis que debe ser realizado por la Unidad de Soporte Técnico o Servidores, según corresponda.

6.3. Solo el personal de Soporte Técnico y Servidores, es el encargado de desensamblar los equipos informáticos propiedad del Servicio Nacional de Aduana del Ecuador.

6.4. Todos los equipos informáticos conectados a la red del Servicio Nacional de Aduana del Ecuador cuentan con el software antivirus provisto por la Institución. En caso de un equipo informático que no sea propiedad del Servicio Nacional de Aduana del Ecuador, debe tener instalado el software antivirus definido por el Servicio Nacional de Aduana del Ecuador para este tipo de equipos. Tanto el software antivirus como las bases de definiciones en ambos casos debe estar actualizadas antes que el equipo se conecte a la red.

6.5. Todo equipo informático que presente fallos o inconvenientes en su funcionalidad, el usuario responsable del equipo, debe reportarlo a Mesa de Servicios

6.6. El equipo informático que por motivos técnicos ya no pueda ser reutilizado, debe ser entregado a la Unidad de Control de Bienes e Inventarios, con un informe técnico de la Unidad de Soporte Técnico.

7. ENTREGA DE EQUIPOS INFORMÁTICOS

7.1. Todo equipo informático, antes de ser entregado al usuario, la Unidad de Soporte Técnico, debe verificar lo siguiente:

- Funcionamiento correcto del equipo, en forma general.
- Sistema Básico de Entrada y Salida (BIOS) del equipo actualizado a la última versión disponible por el fabricante.
- Antivirus institucional instalado, funcionando y bases de definiciones actualizadas.
- Firewall habilitado y con reglas de acceso configuradas.
- Sistema operativo actualizado con los últimos parches de seguridad y rendimiento.
- Controladores de los componentes del equipo actualizados
- Eliminación segura de todos los documentos, imágenes, archivos Outlook de emails (.pst), etc de usuarios que hayan utilizado previamente el equipo.
- Software instalado en el equipo debe contar con licenciamiento vigente y a nombre del Servicio Nacional de Aduana del Ecuador.
- Software instalado en el equipo actualizado con las últimas versiones, parches de seguridad y rendimiento.

- Ningún usuario configurado como Administrador del equipo.
- Sistema Básico de Entrada y Salida (BIOS) configurado para evitar el arranque del sistema operativo desde un dispositivo externo.
- Aplicación de Plantilla de Seguridad en el equipo.
- Aplicación de las Políticas de Grupo del Directorio Activo para el Equipo.
- Aplicación de las Políticas de Grupo del Directorio Activo para el Usuarios.

8. EXCEPCIONES

8.1. Todo usuario que requiera por motivos estrictamente necesarios tener privilegios como Administrador del equipo que utiliza, debe solicitar vía correo electrónico la autorización al área de Seguridad Informática indicando los motivos y el tiempo de vigencia del privilegio solicitado. Una vez aprobada la solicitud por parte del Director de Tecnologías de la Información, la aplicación está a cargo de la Unidad de Soporte Técnico.

9. INSTALACIÓN, CONFIGURACIÓN, DESINSTALACIÓN Y USO DE SOFTWARE INFORMÁTICO AUTORIZADO

9.1. La instalación, mantenimiento o desinstalación de software en los equipos informáticos del Servicio Nacional del Aduana del Ecuador, es una actividad exclusivamente del personal de la Jefatura de Infraestructura Tecnológica, para su ejecución o supervisión. Ningún usuario sea interno o externo al Servicio Nacional de Aduana del Ecuador puede realizar instalación, mantenimiento o desinstalación de software en los equipos informáticos del Servicio Nacional de Aduana del Ecuador, independientemente de la procedencia o tipo de licenciamiento.

9.2. Cuando un usuario requiera, por motivos laborales, instalar, actualizar, modificar o desinstalar un software, en el equipo informático a su cargo, debe solicitarlo vía correo electrónico a Mesa de Servicios, con la respectiva autorización del Director de área o su delegado, para que la Jefatura de Infraestructura Tecnológica analice su factibilidad.

9.3. Se prohíbe el uso de software no autorizado por la Dirección Nacional de Mejora Continua y Tecnologías de la Información en equipos de la red del Servicio Nacional de Aduana del Ecuador.

9.4. No se realiza entrega de software con licenciamiento a los usuarios a través de medios físicos o números de serie.

9.5. Todo software informático termina su ciclo de vida, cuando:

- Su licencia de uso expira.
- Sus características ya no se adaptan a las necesidades del Servicio Nacional de Aduana del Ecuador.

- Tecnológicamente se imposibilite su instalación o uso.
- El fabricante deje de dar soporte de actualizaciones de seguridad y rendimiento al software.

10. MANTENIMIENTO PREVENTIVO O CORRECTIVO DE LOS EQUIPOS INFORMÁTICOS.

10.1. Se realizan mantenimientos preventivos de acuerdo al calendario anual establecido por la Jefatura de Infraestructura Tecnológica, y mantenimientos correctivos en caso de alguna anomalía con los equipos. Éstos están a cargo de la unidad de Soporte Técnico, Servidores, Seguridades y Comunicaciones; según corresponda.

10.2. Para el buen funcionamiento de los equipos informáticos, se ejecutan tareas programadas semanalmente en los equipos de la Institución. Dentro de las mismas están:

- Revisión rápida del Antivirus
- Desfragmentación de información almacenada en discos.
- Eliminación de Archivos Temporales.

10.3. La Jefatura de Infraestructura Tecnológica, a través de sus Unidades de Soporte Técnico, Servidores, Seguridades y Comunicaciones, son únicamente las encargadas de realizar o supervisar toda operación de mantenimiento o servicio técnico, en todos los equipos informáticos del Servicio Nacional de Aduana del Ecuador.

10.4. Los mantenimientos preventivos, incluyen al menos las siguientes actividades:

- Limpieza de los componentes internos del equipo informático.
- Limpieza externa del equipo informático.
- Revisión de los discos duros, ejecutando procesos de comprobación de sectores dañados y desfragmentación de la información.
- Eliminación de archivos temporales.
- Revisión de las alertas de aplicaciones del sistema operativo
- Revisión de las alertas de seguridad del sistema operativo
- Revisión del estado de la memoria
- Revisión del estado del procesador
- Revisión de operatividad y alertas en el antivirus
- Actualizaciones disponibles para el software instalado.
- Revisión del software instalado, que cumpla con las políticas del presente manual
- Revisión del consumo de recursos de las aplicaciones y realizar los correctivos necesarios para su optimización
- Eliminación de archivos de la papelera de reciclaje
- Realizar las respectivas correcciones para el normal funcionamiento del equipo.

11. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasiona que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

SENAE-PI-3-2-012-V2

POLÍTICAS INSTITUCIONALES PARA EL PROCEDIMIENTO DE GESTIÓN DE PARCHES DE SOFTWARE

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona las políticas, responsabilidades y procedimiento para la gestión de parches de software.		
Objetivo:		
Establecer las políticas, responsabilidades y el procedimiento formal para la gestión de parches de software, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
X Firmado electrónicamente por: MAGDELINE ESTEFANIE ROSERO PEREZ Ing. Magdeline Rosero Analista Informático 2	Seguridad Informática	Elaboración
X Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA Mgs. Hugo Robayo Jefe de Infraestructura Tecnológica	Jefatura de Infraestructura Tecnológica	Revisión
X Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ Mgs. Diego Maldonado Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
X Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ Ing. Nelson Rodriguez Director Nacional de Mejora Continua y Tecnologí...	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:			
Versión	**Fecha**	**Razón**	**Responsable**
1	Noviembre 2016	Versión Inicial	Ing. Mario Barragán J.
2	Mayo 2021	Inclusión de normativa vigente	Ing. Magdeline Rosero P.

ÍNDICE

1. OBJETIVO

Establecer las políticas, responsabilidades y el procedimiento formal para la gestión de parches de software, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

2. ALCANCE

El presente manual de política y procedimiento para la gestión de parches de software, está dirigido a todos los usuarios del Servicio Nacional de Aduana del Ecuador.

Todos los usuarios están sujetos a esta política y procedimiento, el uso inapropiado puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

3. RESPONSABILIDAD

3.1. La actualización y mejoramiento del presente documento, le corresponde a la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

3.2. El área de Servidores, de la Jefatura de Infraestructura Tecnológica, es la responsable de realizar las actualizaciones en el software de los Servidores; rigiéndose bajo los lineamientos del presente documento y los indicados en el documento SENAE-PI-3-2-013-V2 "POLÍTICAS INSTITUCIONALES PARA EL CONTROL DE CAMBIOS A LOS PROCESOS OPERATIVOS DE LA JEFATURA DE INFRAESTRUCTURA TECNOLÓGICA"

3.3. El área de Soporte Técnico, de la Jefatura de Infraestructura Tecnológica, es la responsable de realizar las actualizaciones en el software de los computadores de escritorio, portátiles y tabletas; rigiéndose bajo los lineamientos del presente documento y los indicados en el documento SENAE-PI-3-2-013-V2 "POLÍTICAS INSTITUCIONALES PARA EL CONTROL DE CAMBIOS A LOS PROCESOS OPERATIVOS DE LA JEFATURA DE INFRAESTRUCTURA TECNOLÓGICA"

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.
- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.

- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al presente manual:

5.1.1 **Equipo informático:** Servidores, computador de escritorio, portátiles y tabletas.

5.1.2 **Parche:** Es un código de programa que puede corregir un problema o ampliar las funciones de un software.

5.1.3 **Software:** Grupo de programas informáticos con licenciamiento activo, adquiridos a nombre del Servicio Nacional de Aduana del Ecuador y grupo de programas de código abierto, distribución libre o sin licenciamiento.

5.1.4 **Usuario:** Persona que recibe un producto o servicio de un proceso que pertenece al Servicio Nacional de Aduana del Ecuador.

5.2. Los parches para la actualización de software tendrán tres categorías:

- **Actualización:** Los parches de Actualización modifican un programa con el objetivo de incorporar metodologías más nuevas, utilizar algoritmos mejorados, añadir funcionalidades, eliminar secciones obsoletas del software, etc.
- **Críticos:** Los parches Críticos solucionan un problema concreto que resuelve un error de software (bug) crítico y no relacionado con la seguridad del software.
- **Seguridad:** Los parches de seguridad solucionan agujeros o vulnerabilidades de seguridad, no modifican la funcionalidad del software.

5.3. Estas políticas entran en vigor a partir del siguiente día hábil a su autorización y difusión, y está vigente en tanto no se emitan nuevos ordenamientos en la materia.

POLÍTICAS A CUMPLIR

6.1. La aplicación de parches, se realiza de manera periódica y consiste en la instalación de parches de software para solucionar agujeros, vulnerabilidades o fallas de seguridad; para reparar errores, optimizar y añadir funcionalidades.

6.2. La Jefatura de Infraestructura Tecnológica, a través de sus Áreas de Seguridad Informática, Servidores y Soporte Técnico, son únicamente las encargadas de analizar la aplicabilidad de parches en los equipos informáticos en el Servicio Nacional de Aduana del Ecuador.

6.3. Una vez analizados los parches que se van a aplicar en los equipos informáticos, deben ser instalados y monitoreados durante un tiempo máximo de 72 horas.

6.4. Los servidores que cuenten con ambientes de prueba, se debe primero instalar los parches en los equipos de prueba, monitorearlos durante un tiempo máximo de 72 horas y si no se presenta ningún inconveniente en los servicios que presta, se procede con la aplicación de los parches en sus respectivos equipos en producción. Los servidores en Producción también son monitoreados durante un tiempo máximo de 72 horas.

6.5. El área de Servidores, es la encargada de la instalación y monitoreo de los parches en el software de los Servidores; su análisis y aplicación será mensual.

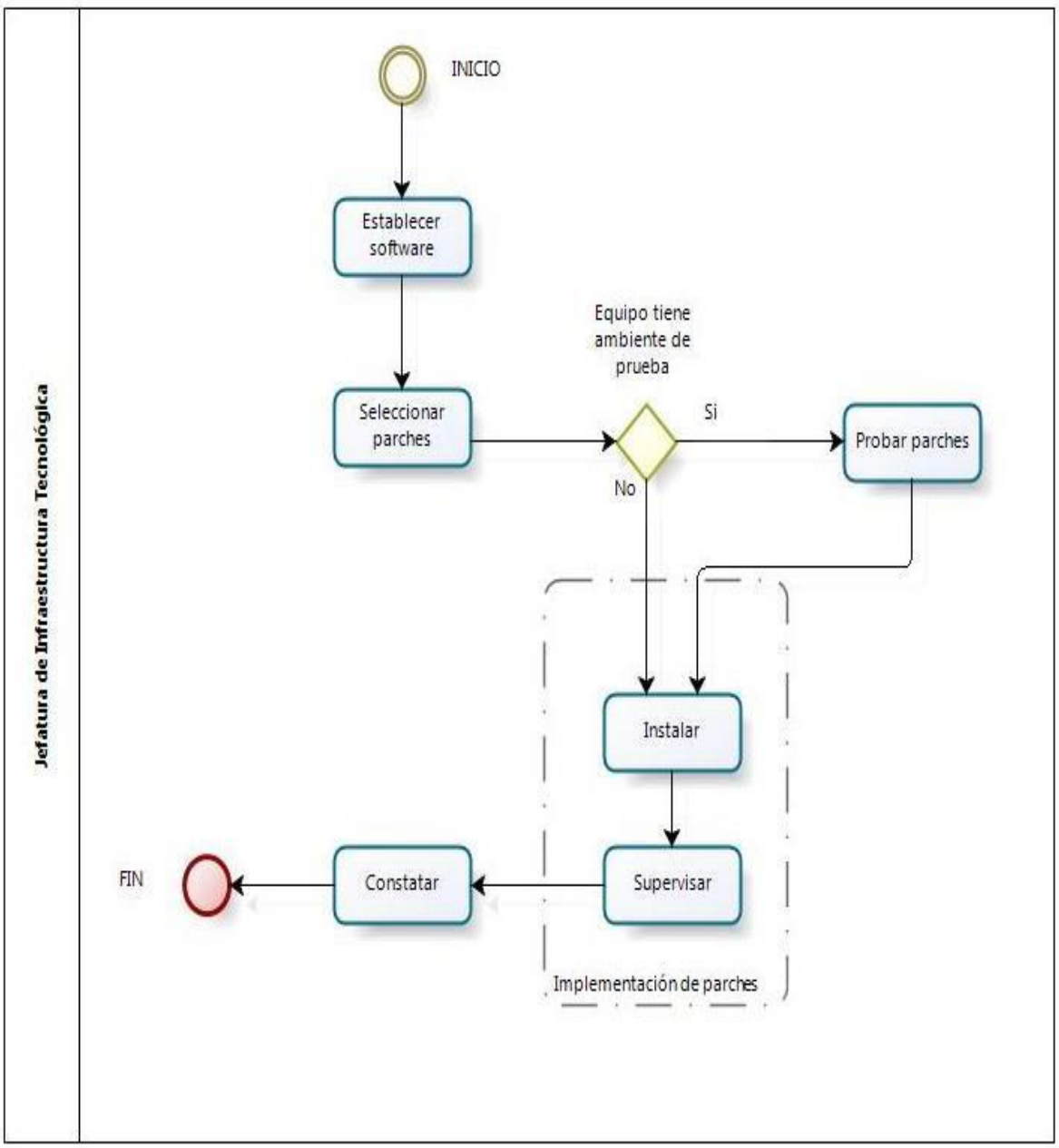
6.6. El área de Soporte Técnico, es la encargada de la instalación y monitoreo de los parches en el software de los computadores de escritorio, portátiles y tabletas; su análisis y aplicación será trimestral.

6.7. El área de Seguridad Informática, es la encargada de la supervisión y constatación de la implementación de los parches en los equipos informáticos en el Servicio Nacional de Aduana del Ecuador.

7. PROCEDIMIENTO

No	Actividad	Producto de Entrada	Descripción de Actividad	Responsable	Producto de Salida
1.	Establecer software y configuración de entorno	Ejecución del proceso de parches de software	Establecer los software a los que se requiere instalar parches y agruparlos por categoría	Seguridad Informática/Servidores/Soporte Técnico	Listado de software
2.	Seleccionar parches	Listado de software	Seleccionar los parches que son lanzados por el proveedor, necesarios de acuerdo al software	Seguridad Informática/Servidores/Soporte Técnico	Listado de parches seleccionados
3.	Verificación de ambiente de prueba	Listado de parches seleccionados	Para servidores que tiene ambiente de prueba se procede con la actividad 4, caso contrario se continúa con la actividad 5	Servidores/Soporte Técnico	Aplicación de parches
4.	Probar parches	Aplicación de parches	Instalación de los parches seleccionados, en los servidores que se encuentran en ambiente de prueba	Servidores	Aplicación de parches en ambiente de prueba
5.	Instalar y supervisar implementación de parches	Aplicación de parches/ Aplicación de parches en ambiente de prueba	Instalación y supervisión de los parches seleccionados, en los equipos informáticos. Para servidores se aplicaran los parches que no presentaron inconvenientes en el ambiente de prueba	Seguridad Informática /Servidores/Soporte Técnico	Parches instalados
6.	Constatación de parches	Parches instalados	Se constata aplicación de parche en los equipos informáticos	Seguridad Informática	Constatación de parches instalados

8. FLUJOGRAMA



9. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasiona que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

SENAE-PI-3-2-013-V2

POLÍTICAS INSTITUCIONALES PARA EL CONTROL DE CAMBIOS A LOS PROCESOS OPERATIVOS DE LA JEFATURA DE INFRAESTRUCTURA TECNOLÓGICA

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona las políticas y responsabilidades para el control de cambios a los procesos operativos de la Jefatura de Infraestructura Tecnológica.		
Objetivo:		
Establecer las políticas de seguridad y responsabilidades, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información para el control de cambios a los procesos operativos de la Jefatura de Infraestructura Tecnológica.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
Firmado electrónicamente por: CARLA MARGARITA ORTUNO DELGADO Ing. Carla Ortuno Analista Informático	Seguridad Informática	Elaboración
X Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA Ing. Hugo Robayo Jefe de Infraestructura Tencologica	Jefatura de Infraestructura Tecnológica	Revisión
Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ X Lsi. Diego Maldonado Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ X Ing. Nelson Rodriguez Director de Tecnologías de la Información	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:			
Versión	**Fecha**	**Razón**	**Responsable**
1	Noviembre 2016	Versión Inicial	Ing. Mario Barragán J.
2	Mayo 2021	Inclusión sobre normativa vigente	Ing. Carla Ortuño D.

ÍNDICE

1. OBJETIVO

Establecer las políticas de seguridad y responsabilidades, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información para el control de cambios a los procesos operativos de la Jefatura de Infraestructura Tecnológica.

2. ALCANCE

El presente manual de política de seguridad para el control de cambios a los procesos operativos de la Jefatura de Infraestructura Tecnológica, está dirigido a todos los usuarios de la Jefatura de Infraestructura Tecnológica, del Servicio Nacional de Aduana del Ecuador.

Todos los usuarios de la Jefatura de Infraestructura Tecnológica están sujetos a esta política, el uso inapropiado puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de todos los usuarios de la Jefatura de Infraestructura Tecnológica, del Servicio Nacional de Aduana del Ecuador.

3.2. La actualización y mejoramiento del presente documento le corresponde al área de Seguridad de la Información perteneciente a la Jefatura de Infraestructura Tecnológica de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

3.3. La Jefatura de Infraestructura Tecnológica, a través de sus Unidades de Soporte Técnico, Servidores, Comunicaciones, Seguridades y Base de Datos, son las encargadas de:

- Planificar, coordinar y ejecutar los cambios en la infraestructura tecnológica y aplicaciones.
- Planificar e instalar los nuevos sistemas aplicativos o actualizaciones en los ya existentes.
- Realizar control de las aprobaciones y atender las solicitudes y requerimientos de usuarios.

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.

- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.
- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al presente manual:

5.1.1 Antispam: Dispositivo para prevenir el correo basura o no deseado a través de distintas técnicas. Se utilizan múltiples metodologías para detectar el correo no deseado, como utilizar un diccionario especial para detectar palabras que suelen aparecer en estos correos o analizar cada uno de los emails para identificar si son o no spam utilizando bases de datos con información (direcciones IP, nombres, textos, etc.) para identificar el correo no deseado.

5.1.2 BIOS: Sistema Básico de Entrada y Salida (BIOS - Basic Input Output System) que, al encender el equipo, busca el sistema operativo para iniciarlo, acorde al medio de almacenamiento configurado con anterioridad.

5.1.3 Cambios Emergentes: Son implementaciones o actualizaciones a nivel de programación, de proyectos realizados por la Jefatura de Desarrollo para mejoras en el sistema Ecuapass, que deben ser atendidos inmediatamente.

5.1.4 Firewall: Es un dispositivo (hardware, software o combinación de ambos) que analiza la información procedente de Internet o de otra red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.

5.1.5 Hojas de Cambio: Son formularios que se utilizan para gestionar procesos de actualización o inserción de información sobre tablas específicas en las Base de Datos del Ecuapass. Se los ejecuta en horarios previamente establecidos.

5.1.6 Informe de Operación: Son formularios que se utilizan para gestionar procesos de actualización o inserción de información sobre tablas específicas en las Base de Datos del Ecuapass, que deben ser atendidos inmediatamente.

5.1.7 LTM (Local Traffic Manager): Dispositivo para una gestión inteligente del tráfico de la red, permitiendo un equilibrio o balanceo de carga sofisticado, optimizando la velocidad y fiabilidad de los datos.

5.1.8 OpenLDAP: Es un servidor de datos optimizado para la realización rápida de consultas de lectura y orientado al almacenamiento de datos a modo de directorio. En el Servicio Nacional de Aduana del Ecuador se lo utiliza para almacenar las réplicas de las Listas de Revocación de Certificados (CRL) del Banco Central del Ecuador y Security Data S.A.

5.1.9 Pases de Versión: Son implementaciones o actualizaciones a nivel de programación, de proyectos realizados por la Jefatura de Desarrollo para mejoras en el sistema Ecuapass. Se los realiza en horarios previamente establecidos.

5.1.10 Servidor proxy: Es un dispositivo que actúa como intermediario entre los equipos de una red de área local e Internet. Proporcionan seguridad, ya que pueden filtrar cierto contenido web y programas maliciosos; permitiendo bloquear sitios considerados maliciosos o sitios considerados improductivos en relación a la actividad de la empresa.

5.1.11 Sistemas de prevención de intrusiones (IPS): Son dispositivos que detectan y bloquean cualquier intento de intrusión, transmisión de código malicioso o amenazas a través de la red. Los IPS toman decisiones de control de acceso basado en los contenidos del tráfico, al reconocer una determinada cadena de bytes en cierto contexto de ataque.

5.1.12 Usuario: Persona que recibe un producto o servicio de un proceso que pertenece al Servicio Nacional de Aduana del Ecuador.

5.1.13 VPN: Es una tecnología de red que permite crear una extensión de una red privada de área local (LAN) sobre una red pública o no controlada como Internet. Se realiza estableciendo una conexión virtual privada y segura punto a punto mediante el uso de conexiones dedicadas. Es de mucha utilidad cuando se utiliza redes inalámbricas WiFi pública, debido a que el tráfico que se genera viaja cifrado y se dificulta que un tercero pueda robar información.

5.1.14 WAF (Web Application Firewall): Protección Firewall especializado para aplicaciones Web que protege contra múltiples amenazas y vulnerabilidades.

5.1.15 WiFi: Es una tecnología de comunicación inalámbrica que permite conectar inalámbricamente equipos electrónicos, como computadoras, tablets, smartphones o celulares, etc., a una red de computadoras, mediante el uso de radiofrecuencias para la trasmisión de la información; con privilegios de acceso y servicios, que son configurables de acuerdo a las necesidades de su implementación.

5.2. Estas políticas entran en vigor a partir del siguiente día hábil a su autorización y difusión, y está vigente en tanto no se emitan nuevos ordenamientos en la materia.

6. PROCESOS A CONTROLAR

6.1. Comunicaciones

6.1.1 Actualizaciones y configuraciones en los Firewall y LTM (Local Traffic Manager)

6.1.2 Atención a requerimientos de acceso a telefonía IP, redes WiFi, VPN y navegación por Firewall

6.2. Base de Datos

6.2.1 Atención de requerimiento de Pases de versión

6.2.2 Atención de requerimiento de Hojas de cambio

6.2.3 Atención de requerimiento de Cambios emergentes

6.2.4 Atención de requerimiento de Informes de operación

6.2.5 Atención de requerimiento de Formulario de Solicitud de Accesos a Cuentas de Usuarios

6.2.6 Actualización y configuración de Base de Datos

6.3. Servidores

6.3.1. Actualización y configuración de Sistemas Operativos para Servidores

6.3.2. Actualización del Firmware en los Servidores

6.4. Seguridades

6.4.1. Actualización y configuración del Sistema de Prevención de Intrusos

6.4.2. Actualización y configuración del Sistema WAF (Web Application Firewall)

6.4.3. Actualización y configuración del servidor Proxy

6.4.4. Actualización y configuración del producto OpenLDAP

6.4.5. Actualización y configuración de la Solución Antivirus

6.4.6. Actualización y configuración de la Solución AntiSpam

6.4.7. Atención de requerimiento de Formulario de Solicitud de Accesos a Cuentas de Usuarios

6.5. Soporte

6.5.1. Actualización del BIOS de los computadores de escritorio

6.5.2. Actualización del firmware de los computadores de escritorio

6.5.3. Actualización de los controladores de los computadores de escritorio

6.5.4. Atención de requerimiento de Formulario de Solicitud de Accesos a Cuentas de Usuarios

7. ANTES DEL PROCESO DE CAMBIO

7.1. Para actualizaciones y configuraciones, desarrollar una planificación detallada de cada una de las etapas:

7.1.1 Objetivo del cambio

7.1.2 Alcance:

- Grupo de usuarios que son afectados
- Aplicaciones que son afectadas
- Hardware/Software que son intervenido

7.1.3 Descripción de la operación:

- Recursos necesarios para el proceso de cambio
- Cronograma de actividades a realizar
- Respaldos previos
- Conjunto de pruebas pre y post instalación
- Plan de vuelta atrás
- Riesgos involucrados

7.1.4 Para las actualizaciones, llevar un control de las versiones

7.1.5 Coordinar el cambio con las áreas involucradas o propietarios de los sistemas afectados, para que se efectúe durante periodos de menor impacto.

7.1.6 Solicitar la correspondiente autorización del Jefe de Infraestructura Tecnológica

7.2. Para la Atención a requerimientos:

7.2.1. Recepción del requerimiento a través del medio de comunicación establecido

7.2.2. Verificación de las autorizaciones requeridas, acorde al requerimiento

7.2.3. Registro del estado actual, para histórico o posible reverso de lo atendido.

8. DURANTE EL PROCESO DE CAMBIO

8.1. Para actualizaciones y configuraciones, contar siempre con el contacto de las empresas de soporte externo relacionadas al proceso de cambio.

9. POSTERIOR AL PROCESO DE CAMBIO

9.1. Registrar los cambios realizados

9.2. Para actualizaciones y configuraciones, de ser necesario reversar el cambio, aplicar el proceso de vuelta atrás.

10. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasiona que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

SENAE-PI-3-2-014-V2

POLÍTICAS INSTITUCIONALES PARA LA PROTECCIÓN CONTRA SOFTWARE MALICIOSO

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona las políticas de seguridad que se deben cumplir para la protección contra software malicioso, de todos los equipos informáticos del Servicio Nacional de Aduana del Ecuador.		
Objetivo:		
Establecer las políticas de seguridad, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información para la protección contra software malicioso, de todos los equipos informáticos del Servicio Nacional de Aduana del Ecuador.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
Firmado electrónicamente por: CARLA MARGARITA ORTUNO DELGADO Ing. Carla Ortuno Analista Informático	Seguridad Informática	Elaboración
X Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA Ing. Hugo Robayo Jefe de Infraestructura Tencologica	Jefatura de Infraestructura Tecnológica	Revisión
X Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ Lsi. Diego Maldonado Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
X Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ Ing. Nelson Rodriguez Director de Tecnologías de la Información	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:			
Versión	**Fecha**	**Razón**	**Responsable**
1	Noviembre 2016	Versión Inicial	Ing. Mario Barragán J.
2	Abril 2021	Inclusión sobre normativa vigente	Ing. Carla Ortuño D.

ÍNDICE

1. OBJETIVO

Establecer las políticas de seguridad, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información para la protección contra software malicioso, de todos los equipos informáticos del Servicio Nacional de Aduana del Ecuador.

2. ALCANCE

El presente manual de política de seguridad para la protección contra software malicioso, está dirigido a todos los usuarios del Servicio Nacional de Aduana del Ecuador.

Todos los usuarios están sujetos a esta política, el uso inapropiado puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de todos los usuarios del Servicio Nacional de Aduana del Ecuador.

3.2. La actualización y mejoramiento del presente documento le corresponde al área de Seguridad de la Información perteneciente a la Jefatura de Infraestructura Tecnológica de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

3.3. La Jefatura de Infraestructura Tecnológica es la encargada de implementar soluciones tecnológicas para la protección contra software malicioso, de todos los equipos informáticos del Servicio Nacional de Aduana del Ecuador.

3.4. La Jefatura de Infraestructura Tecnológica, a través de la Unidad de Seguridad Informática es la encargada de generar y publicar campañas para concienciar al usuario, en materia de Seguridad de la Información.

3.5. La Dirección Nacional de Talento Humano es la encargada de suministrar copia de las Políticas Institucionales vigentes, emitidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información, al nuevo personal que ingresa al Servicio Nacional de Aduana del Ecuador.

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.

- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.
- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al presente manual:

5.1.1 Equipo informático: Servidores, computadores de escritorio, portátiles y tabletas, asignados al usuario para el desempeño de sus funciones.

5.1.2 Software malicioso: Es un tipo de programa informático que tiene como objetivo infiltrarse o dañar un equipo informático o sistema de información, ocasionando efectos molestos, destructivos e incluso irreparables sin el consentimiento y/o conocimiento del usuario. Puede incluso tomar control del equipo remotamente (backdoor o puerta trasera), ocasionar el robo de información (como claves, números de cuenta, etc.), secuestro de información a través de la encriptación de los datos haciendo imposible tener acceso a los mismos a menos que se pague un rescate.

5.1.3 Usuario: Persona que recibe un producto o servicio de un proceso que pertenece al Servicio Nacional de Aduana del Ecuador.

5.2. La herramienta de Antivirus implementada en el Servicio Nacional de Aduana del Ecuador, tiene carácter obligatorio su instalación y uso en todo el equipamiento computacional sean estos servidores, estaciones de trabajo y otros dispositivos tanto móviles como fijos. Cualesquiera equipos que no cuenten con esta protección de antivirus, no podrá ser conectado a la red local de la Institución.

5.3. Estas políticas entran en vigor a partir del siguiente día hábil a su autorización y difusión, y está vigente en tanto no se emitan nuevos ordenamientos en la materia.

6. CONTROL CONTRA SOFTWARE MALICIOSO

6.1. El usuario debe evitar abrir vínculos de sitios web desconocidos, no seguros o sospechosos, a pesar que éstos parecen tener un origen legítimo.

6.2. El usuario antes de ejecutar cualquier archivo que le resulte sospechoso, debe analizarlo con el programa antivirus.

6.3. Los dispositivos de almacenamiento externo conectados a los equipos informáticos del Servicio Nacional de Aduana del Ecuador son analizados completamente por el programa antivirus, antes de ser utilizado.

6.4. El usuario no podrá interrumpir los análisis automáticos que realiza la solución antivirus en el equipo informático y dispositivos conectados.

7. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasiona que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

SENAE-PI-3-2-015-V2

POLÍTICAS INSTITUCIONALES PARA LA CLASIFICACIÓN Y ENTREGA DE INFORMACIÓN

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona las políticas a seguir para la clasificación y entrega de la información.		
Objetivo:		
Establecer la política a seguir para la clasificación y entrega de la información, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
Firmado electrónicamente por: CARLA MARGARITA ORTUNO DELGADO X Ing. Carla Ortuno Analista Informático	Seguridad Informática	Elaboración
X Ing. Hugo R Jefe de Infra Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA encologica	Jefatura de Infraestructura Tecnológica	Revisión
Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ X Lsi. Diego Maldonado Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ X Ing. Nelson Rodriguez Director de Tecnologías de la Información	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:			
Versión	**Fecha**	**Razón**	**Responsable**
1	Noviembre 2016	Versión Inicial	Ing. Mario Barragán J.
2	Abril 2021	Inclusión sobre normativa vigente	Ing. Carla Ortuño D.

ÍNDICE

1. OBJETIVO

Establecer la política a seguir para la clasificación y entrega de la información, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

2. ALCANCE

El presente manual de política para la clasificación y entrega de la información, está dirigido a todos los usuarios del Servicio Nacional de Aduana del Ecuador.

Todos los usuarios están sujetos a esta política, el uso inapropiado puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

Esta política no incluye la destrucción de la información almacenada en medio tecnológico ni etiquetado por lo cual deberá referirse a las políticas SENAE-PI-3-2-006 - Políticas Institucionales de los Requerimientos de Seguridad para Respaldos de la Información y SENAE-PI-3-2-010 - Políticas Institucionales del Procedimiento de Borrado Seguro en los Dispositivos de Almacenamiento y en el Proceso de Reutilización de las Estaciones de Trabajo.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de todos los usuarios del Servicio Nacional de Aduana del Ecuador.

3.2. La actualización y mejoramiento del presente documento corresponde al área de Seguridad de la Información perteneciente a la Jefatura de Infraestructura Tecnológica de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

3.3. Todos los usuarios están comprometidos con el buen uso de la información, y acceso de acuerdo a su clasificación.

3.4. Propietario de la información:

- Clasificar la información de acuerdo al grado de sensibilidad y criticidad de la misma.
- Documentar y mantener actualizada la clasificación de la información.
- Definir qué usuarios deberán tener permisos de acceso a la información.
- Definir en conjunto con la Jefatura de infraestructura tecnológica de la Dirección de Tecnologías de la Información, las estrategias para la generación, retención y rotación de las copias de respaldo de la información.

- Autorizar la divulgación de la información.

3.5. Comité de Seguridad de la Información del Servicio Nacional de Aduana del Ecuador: designa a los propietarios de la información de las diferentes áreas del Servicio Nacional de Aduana del Ecuador.

3.6. El usuario debe acatar los lineamientos de clasificación de la información para el acceso, divulgación, almacenamiento, copia, transmisión y eliminación de la información.

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.
- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.
- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al presente manual:

5.1.1 Activos de Información: Son todos los datos con valor para el Servicio Nacional de Aduana del Ecuador y que requieren de una protección adecuada, cualquier sea el soporte que la contiene, así como los documentos, los equipos y sistemas que los almacenes o procesen y las personas que los administren o utilicen

5.1.2 Acuerdo sobre confidencialidad y uso de la información: Documento en el que se suscribe de manera libre y voluntaria, un convenio entre el representante legal del Servicio Nacional de Aduana del Ecuador y el destinatario, donde el receptor de la Información Confidencial se obliga a mantener estricta confidencialidad sobre la documentación e información que conozca, reciba o intercambie con ocasión de la relación laboral, contractual y/o legal.

5.1.3 Cifrado: El cifrado es un mecanismo que se utiliza para ocultar el contenido de archivos informáticos, donde sólo el propietario del archivo cifrado o conocedor de la clave de seguridad, pueda leerlo.

5.1.4 Confidencialidad: Es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados; es decir que la información es accesible solo para aquellos autorizados a tener acceso, previniendo que se divulgue la información a personas o sistemas no autorizados.

5.1.5 Criticidad de la información: Una información es considerada crítica cuando su pérdida o ausencia de disponibilidad puede afectar a la continuidad operacional de algún proceso, proyecto o actividad. Este atributo está relacionado con la integridad y disponibilidad de la información.

5.1.6 Descifrado: Es el mecanismo inverso al cifrado, es decir los datos retornan a su formato original a través de la clave de seguridad con la que fue cifrado el archivo.

5.1.7 Disponibilidad: Es el aseguramiento de que la información se encuentre siempre a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones; es decir tener el recurso autorizado para este acceso, en el momento que así lo requiera.

5.1.8 Integridad: Es la garantía de mantener los datos libres de modificaciones no autorizadas; es decir mantener con exactitud y completitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

5.1.9 Propietario de la información: Son los responsables de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma.

5.1.10 Sensibilidad de la Información: Una información es considerada sensible cuando su uso no autorizado causaría perjuicios a los intereses económicos, comerciales y éticos de una entidad. Este atributo está relacionado con la confidencialidad de la información.

5.1.11 Usuario: Persona que recibe un producto o servicio de un proceso que pertenece al Servicio Nacional de Aduana del Ecuador.

5.2. Toda información adquirida, almacenada, procesada y transmitida por la infraestructura tecnológica del Servicio Nacional de Aduana del Ecuador y aquella utilizada para la operación y gestión de esta infraestructura son de propiedad del Servicio Nacional de Aduana del Ecuador.

5.3. Estas políticas entran en vigor a partir del siguiente día hábil a su autorización y difusión, y está vigente en tanto no se emitan nuevos ordenamientos en la materia.

6. CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

6.1. Toda información del Servicio Nacional de Aduana del Ecuador debe ser identificada, clasificada y documentada de acuerdo a la Clasificación establecida en el presente documento.

6.2. La información que colecciona y mantiene el Servicio Nacional de Aduana del Ecuador es clasificada de acuerdo al grado de sensibilidad y criticidad de la misma,

La información es clasificada, por su grado de sensibilidad, en:

- **Pública**: Es la información cuya difusión ha sido aprobada. Dicha autorización deberá ser otorgada por el Propietario de la información.
- **Confidencial:** Será de uso restringido basado en el concepto de necesidad de conocer. Por su sensibilidad, esta información debe ser resguardada, limitando su acceso solo a aquellos usuarios previamente autorizadas por el Propietario de la información, protegiéndola en su almacenamiento de origen, envío o transmisión y en el almacenamiento destino (incluyendo respaldos), asegurando el acceso a los usuarios autorizados.

Y de acuerdo a su grado de criticidad, en:

- **Criticidad alta:** Si la información es Confidencial y adicionalmente se cumple al menos una de las siguientes condiciones:
  - Si debido a modificaciones no autorizadas en la información, es difícil o imposible su reparación y puede dejar pérdidas significativas.
  - La no disponibilidad de la información, a corto plazo, podría causar pérdidas significativas.
- **Criticidad media:** Si la información es Pública o Confidencial, y adicionalmente se cumple al menos una de las siguientes condiciones:
  - Si debido a modificaciones no autorizadas en la información, se puede reparar y puede dejar pérdidas significativas.
  - La no disponibilidad de la información, a largo plazo, podría causar pérdidas significativas.

- **Criticidad baja:** Si la información es Pública o Confidencial, y adicionalmente se cumple al menos una de las siguientes condiciones:
  - Si debido a modificaciones no autorizadas en la información, se puede reparar fácilmente y sin pérdidas significativas.
  - La no disponibilidad de la información, no afecta.

6.3. Toda información impresa, escaneada o fotocopiada, debe de ser recogida inmediatamente para evitar su divulgación no autorizada.

6.4. Los escritorios deberán encontrarse libres de documentos y medios de almacenamientos, que no son utilizados para el desempeño de sus labores. Así mismo, éstos deberán estar almacenados ante una ausencia del puesto de trabajo.

6.5. La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

6.6. El usuario que, en el cumplimiento de sus funciones, tenga que acceder a Información clasificada como Confidencial debe contar con la autorización expresa del Propietario de la Información.

7. ENTREGA DE LA INFORMACIÓN

7.1. El Propietario de la Información debe asegurar la protección de la información en el momento de ser transferida o intercambiada con otras entidades y debe establecer los procedimientos y controles necesarios para el intercambio de información; así mismo, debe establecer un "Acuerdo sobre Confidencialidad y uso de la información" con las terceras partes con quienes se realice dicho intercambio.

7.2. El propietario de la información debe velar porque la información del Servicio Nacional de Aduana del Ecuador sea protegida de divulgación no autorizada por parte de terceros y verificar las cláusulas relacionadas con el "Acuerdo sobre Confidencialidad y uso de la información".

7.3. El propietario de la información debe verificar que el intercambio de información con terceros deje registros del tipo de información intercambiada, el emisor, el receptor de la misma y la fecha de entrega/recepción.

7.4. El usuario no debe utilizar el correo electrónico como medio para enviar o recibir información clasificada como confidencial, mientras que la misma no se encuentre cifrada y con clave (Ver numeral 8).

7.5. El usuario debe evitar revelar ningún tipo de información Confidencial al momento de tener una conversación telefónica o mantener conversaciones sin tomar los controles necesarios, precautelando el principio de confidencialidad.

8. CIFRADO

8.1. El usuario debe utilizar métodos de cifrado, para la protección de la información Confidencial transportada o almacenada en cualquier medio de almacenamiento.

8.2. El programa de distribución libre actualmente establecido en el Servicio Nacional de Aduana del Ecuador para cumplir esta política es el 7-Zip File Manager. De requerir esta herramienta el usuario debe solicitarlo al Buzón Mesa de Servicios Institucional.

8.3. La clave con la que fue cifrado un archivo será única y exclusivamente de responsabilidad del usuario quién la generó y de las consecuencias generadas por olvido o perdida de la misma.

8.4. La clave utilizada para cifrar el archivo, debe regirse a lo estipulado en la política SENAE-PI-3-2-005 "Políticas Institucionales para el acceso a Sistemas de Información", numeral 10.

9. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasiona que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

SENAE-PI-3-2-016-V2

POLÍTICAS INSTITUCIONALES PARA LA ADMINISTRACIÓN DE LAS CLAVES DE LAS CUENTAS DE USUARIOS PRIVILEGIADOS DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

MAYO 2021

HOJA DE RESUMEN

Descripción del documento:		
Este documento proporciona las políticas y responsabilidades para la administración de las claves de las cuentas de usuarios privilegiados de la Dirección de Tecnologías de la Información.		
Objetivo:		
Establecer las políticas de seguridad y responsabilidades, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información para la administración de las claves de las cuentas de usuarios privilegiados de la Dirección de Tecnologías de la Información.		
Elaboración / Revisión / Aprobación:		
Nombre / Cargo / Firma / Fecha	**Área**	**Acción**
Firmado electrónicamente por: CARLA MARGARITA ORTUNO DELGADO Ing. Carla Ortuno Analista Informático	Seguridad Informática	Elaboración
Firmado electrónicamente por: HUGO CAMILO ROBAYO AYALA X Ing. Hugo Robayo Jefe de Infraestructura Tencologica	Jefatura de Infraestructura Tecnológica	Revisión
Firmado electrónicamente por: DIEGO RAUL MALDONADO SANCHEZ X Lsi. Diego Maldonado Director de Tecnologías de la Información	Dirección de Tecnologías de la Información	Aprobación
Firmado electrónicamente por: NELSON GABRIEL RODRIGUEZ MARTINEZ X Ing. Nelson Rodriguez Director de Tecnologías de la Información	Dirección Nacional de Mejora Continua y Tecnologías de la Información	Aprobación

Actualizaciones / Revisiones / Modificaciones:			
Versión	**Fecha**	**Razón**	**Responsable**
1	Julio 2016	Versión Inicial	Ing. Mario Barragán J.
2	Abril 2021	Inclusión sobre normativa vigente	Ing. Carla Ortuño D.

ÍNDICE

1. OBJETIVO

Establecer las políticas de seguridad y responsabilidades, definidos por la Dirección Nacional de Mejora Continua y Tecnologías de la Información para la administración de las claves de las cuentas de usuarios privilegiados de la Dirección de Tecnologías de la Información.

2. ALCANCE

El manual de política de seguridad para la para la administración de las claves de las cuentas de usuarios privilegiados de la Dirección de Tecnologías de la Información, está dirigido a todos los usuarios del Senae que hacen uso de las cuentas de usuarios privilegiados.

Todos los usuarios que hacen uso de las cuentas de usuarios privilegiados están sujetos a esta política, el uso inapropiado puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

3. RESPONSABILIDAD

3.1. La aplicación, cumplimiento y realización de lo descrito en el presente documento, es responsabilidad de los usuarios que administran cuentas privilegiadas del Senae.

3.2. La actualización y mejoramiento del presente documento le corresponde al área de Seguridad de la Información perteneciente a la Jefatura de Infraestructura Tecnológica de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

3.3. La Jefatura de Infraestructura Tecnológica, a través del área de Centro de Cómputo es la encargada de la administración de las cuentas de usuarios privilegiados de los equipos de producción de la infraestructura tecnológica del Senae.

3.4. Los administradores de servicios serán los responsables de otorgar las facilidades respectivas al Administrador de cuentas de usuarios privilegiados, para que realice los cambios o actualizaciones de claves.

3.5. El área Seguridad informática, como administradores de seguridad, deben realizar pruebas sobre la calidad de las claves asignadas a las cuentas de usuarios privilegiados.

4. NORMATIVA VIGENTE

- Constitución de la República del Ecuador.
- Código Orgánico Integral Penal, Registro Oficial Suplemento Nro. 180 del 10 de febrero de 2014, última modificación 05 de febrero de 2021 y sus posteriores reformatorias.
- Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Nacional de Aduana del Ecuador.
- Ley Orgánica del Servicio Público, publicada en el Segundo Suplemento del Registro Oficial No.294, de fecha 6 de octubre 2010 y sus posteriores reformatorias.
- Ley de comercio electrónico, firmas y mensajes de datos, Ley 67, Registro Oficial Suplemento 557 de 17 de abril de 2002, última modificación 08 de diciembre de 2020 y sus posteriores reformatorias.
- Acuerdo Ministerial No. 025-2019 (Art. 3), emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, publicado en el Registro Oficial - Edición Especial No.228, 10 de enero 2020, mediante el cual se expide el "Esquema Gubernamental de Seguridad de la Información – EGSI-, el cual es de implementación obligatoria en las instituciones de la administración pública central, institucional y que dependa de la función ejecutiva.
- Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, (Acuerdo 039 CG), publicado en el Registro Oficial No. 78, 01 de diciembre 2009, y sus posteriores reformas. (NCI: 401-03, 405-04, 406-02, 406-03, 406-13, 410–03, 410-06, 410-07, 410-08, 410-09, 600-01)

5. CONSIDERACIONES GENERALES

5.1. Con el objeto que se apliquen los términos de manera correcta a continuación se presentan algunas definiciones inherentes al presente manual:

5.1.1 Usuario: Persona que recibe un producto o servicio de un proceso que pertenece al Senae.

5.1.2 Cuenta de usuario privilegiado: Es una cuenta de un producto de TI que es utilizada para la instalación y configuración de los servicios del mismo y que cuenta con acceso irrestricto (Ejemplos: administrador, administrator, admin, root, etc).

5.1.3 Administrador de Cuenta: Son los usuarios responsables de la custodia, actualización y gestión de uso de las claves de las cuentas de usuarios privilegiados de la Dirección de Tecnologías de la Información.

5.1.4 Administrador de Servicio: Son los usuarios responsables de la aplicación que presta el servicio, su funcionamiento, mantenimiento y optimización.

5.1.5 Administrador de Seguridad: Son los usuarios encargados de evaluar la calidad de las claves que son empleadas por los usuarios con acceso privilegiado.

5.1.6 Cuenta de usuario personalizado: Toda cuenta creada en un sistema informático y que tiene asignado los privilegios necesarios acorde a las actividades que tiene que realizar en dicho sistema.

5.2. Esta política entrará en vigor a partir del siguiente día hábil a su autorización y difusión, y está vigente en tanto no se emita nuevos ordenamientos en la materia.

6. SALVAGUARDA

6.1. Las claves de las cuentas de usuario privilegiados deberán ser guardadas en sobres debidamente sellados, con una etiqueta que identifique claramente el nombre del servidor, su dirección IP y la cuenta de usuario de la clave que contiene, los cuales quedarán bajo la custodia del área de Centro de Cómputo, como contingencia de respaldo de las claves.

6.2. Las claves deben ser cambiadas con una periodicidad semestral por el administrador de la cuenta.

6.3. El usuario administrador de servicio no debe tener conocimiento de ninguna clave de cuenta de usuario privilegiado.

7. USO

7.1. Las cuentas de usuarios privilegiados no deben ser utilizadas para la gestión diaria de servicios, para este escenario se debe utilizar la cuenta de usuario personalizado.

7.2. En caso de hacer uso de la cuenta de usuario privilegiado, el área requirente debe solicitar autorización al Jefe de Infraestructura Tecnológica para que el administrador de la cuenta facilite las credenciales respectivas de la cuenta.

8. VERIFICACIÓN DE SEGURIDAD

8.1. El área de Seguridad informática, como Administrador de Seguridad, realizará verificaciones trimestrales en conjunto con el Administrador de Cuenta, sobre la complejidad de las claves asignadas a las cuentas de usuario privilegiado.

8.2. El Administrador de Seguridad seleccionará al azar un grupo de cuentas de usuario privilegiado, que el Administrador de Cuenta deberá proporcionar las claves registradas en cada una de las cuentas.

8.3. El Administrador de Seguridad verificará el respectivo acceso a la cuenta y que la clave cumpla con los lineamientos del documento SENAE-PI-3-2-005-V2 "POLÍTICAS INSTITUCIONALES PARA EL ACCESO A SISTEMAS DE INFORMACIÓN", numeral 10.

8.4. Las claves que no pasen la verificación del punto 8.3 del presente documento, el Administrador de Cuenta procederá de inmediato con los correctivos respectivos y notificará al Administrador de Seguridad cuando el inconveniente esté solventado para su correspondiente verificación.

9. SANCIONES

Cualquier contravención a las políticas dadas en este documento, ocasionará que el usuario sea sujeto de sanciones administrativas, a través de la Coordinación de Control Disciplinario en lo que respecta a sus atribuciones y responsabilidades, proceda a imponer la sanción correspondiente.

Ing. Hugo Del Pozo Barrezueta
DIRECTOR

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Telf.: 3941-800
Exts.: 3131 - 3134

www.registroficial.gob.ec

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

"Al servicio del país desde el 1º de julio de 1895"