Política Específica de Uso Aceptable de los Recursos Informáticos

Elaborado por: **Jonathan Jair Ortiz Muñoz** Cargo: **Oficial de Seguridad de la Información**	Fecha: 15/04/2021 Firma: 
Revisado por: **Orlando Vásquez Rubio** Cargo: **jefe de la Unidad de Sistemas e Informática**	Fecha: 15/04/2021 Firma: 

ÍNDICE

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir reglas claras para el uso de los sistemas y de otros activos de información en la Agencia Peruana de Cooperación Internacional (APCI).

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los trabajadores de la Agencia Peruana de Cooperación Internacional (APCI).

2. DOCUMENTOS DE REFERENCIA

- Norma Técnica Peruana ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos, capítulos A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3 y A.18.1.2.
- Política General de Seguridad de la Información de la APCI, aprobada con RDE N° 080-2020/APCI-DE.

3. POLÍTICA ESPECÍFICA

Todo trabajador de APCI o tercero para el desempeño de sus funciones como organismo, se compromete a lo siguiente:

- Los activos de información solamente pueden ser utilizados a fines de satisfacer necesidades del APCI con el objetivo de ejecutar tareas vinculadas con el mismo.
- Está prohibido utilizar los activos de información de manera tal que ocupen innecesariamente capacidad, que disminuya el rendimiento del sistema de información o que presente una amenaza de seguridad.
- Está prohibido descargar y almacenar música, videos, audio, ejecutables y de otra índole que no sean de carácter institucional en las unidades de red asignadas a cada usuario u oficina según corresponda.
- Está prohibido utilizar dispositivos informáticos móviles para copiar y almacenar información institucional, sin conocimiento y/o autorización de la máxima autoridad de la oficina donde labora.
- Está prohibido cualquier acceso o intento de acceso a la información digital en mención de una aplicación, sea cual sea su repositorio o archivo, que no sea a través de una cuenta y clave.
- No mover los equipos y/o periféricos de un lugar a otro, sin autorización correspondiente.
- No está permitido colocar los equipos en el piso, lugares inestables y/o expuestos a ser golpeados involuntariamente o frente a la luz solar o expuesta al polvo.
- Está prohibido ingerir y dejar alimentos y/o bebidas cerca y/o encima de los equipos informáticos.
- Está prohibido acceder a la red con computadoras o equipos portátiles que no pertenecen a la institución, sin autorización de la Unidad de Sistemas e Informática.
- No está permitido instalar o utilizar herramientas en la red para evitar los controles de seguridad implementados.
- Los servicios y recursos de la red serán usados únicamente con fines laborales. No está permitido utilizar los recursos de los equipos de cómputo para beneficios personales.
- Los equipos, la información o software, independientemente de su formato o soporte de almacenamiento, no pueden ser retirados de las instalaciones sin el permiso escrito del jefe inmediato. Mientras los activos en cuestión permanecen fuera de la organización, deben ser controlados por la persona a la que se le concedió el permiso para retirarlo.
- Al finalizar un contrato de empleo, o de otro tipo, a raíz del cual se utilizan diversos equipos, software o información en formato electrónico o papel, el usuario debe devolver todo ese activo de

información al jefe inmediato y seguir los lineamientos establecidos en las disposiciones y procedimientos para la entrega – recepción de cargo establecido para los colaboradores de APCI.
- En cada equipo de computador debe estar instalado un antivirus con actualización automática activada.
- Los usuarios de los sistemas de información solamente pueden acceder a los activos de sistemas de información para los cuales han sido explícitamente autorizados por el propietario del activo.
- Los usuarios pueden utilizar los sistemas de información únicamente para las actividades para las cuales han sido autorizados; es decir, para las cuales les han sido otorgados derechos de acceso.
- Los usuarios no deben participar en actividades que puedan ser utilizadas para eludir controles de seguridad de los sistemas de información.
- El usuario no debe, directa ni indirectamente, permitir que otra persona utilice sus derechos de acceso; es decir, su nombre de usuario; y no debe utilizar el nombre de usuario y/o clave de otra persona. El uso de nombres de usuario grupales está prohibido.
- El propietario de la cuenta de usuario es responsable de su uso y de todas las transacciones realizadas con dicha cuenta de usuario.
- Cada empleado, proveedor o tercero que esté en contacto con datos y/o sistemas de APCI debe reportar toda debilidad del sistema incidente o evento que pudiera derivar en un posible incidente

En caso de no cumplir con la presente Política Específica de Uso Aceptable de los Recursos Informáticos, los lineamientos de seguridad de la información u otros directivas o procedimientos de seguridad de la información, se reportará el evento al Oficial de Seguridad de la Información para que tome conocimiento y disponga las acciones correspondientes, de considerarlo necesario. De esta forma, la autoridad competente de APCI, tomará las medidas disciplinarias necesarias, las cuales están sujetas a la normativa vigente de APCI.

3.1. DEL SOFTWARE

Respecto al software, está prohibido:

- Instalar cualquier tipo de software ya sean los de programa de libre uso u otros descargados de Internet, o aquellos que son adquiridos de manera personal, aun si contaran con licencia propia.
- Desinstalar los softwares base (aplicaciones pre instaladas por la USI) de la computadora.
- La comercialización del software adquirido, instalado o asignado en las computadoras de la institución.
- Utilizar aplicaciones Java Script, controles Active X y otros códigos móviles, excepto cuando esté autorizado por la Unidad de Sistemas e Informática.
- Utilizar herramientas criptográficas (encriptado) sobre los equipos de cómputo.
- Los usuarios no deben realizar copias no autorizadas del software que pertenece a la APCI, excepto en los casos permitidos por ley o por el mismo APCI, si el usuario requiere hacer una copia debe solicitarlo a la APCI por medio de un informe dirigido a la jefatura de la Unidad de Sistemas e Informática.
- Los usuarios no deben copiar software ni otros materiales originales de otras fuentes, y son responsables por todas las consecuencias que pudieran surgir bajo la ley de propiedad intelectual.

3.2. DEL CORREO ELECTRÓNICO

Respecto al uso del correo electrónico:

- El correo electrónico institucional es una herramienta de comunicación e intercambio de información oficial entre usuarios, de uso exclusivo para las actividades que estén relacionadas con la APCI, no constituye un medio de difusión indiscriminada de información. Los usuarios solamente pueden enviar mensajes que contengan información veraz.
- Los usuarios no deben enviar mensajes “spam”. Si un usuario recibe un correo electrónico “spam”, debe informar al soporte técnico de la Unidad de Sistemas e informática.
- Si se envía un mensaje con una etiqueta de confidencialidad, el usuario debe protegerlo.

- Si se desea mantener un mensaje de forma permanente, este debe almacenarse en carpetas personales en la PC asignada. La Unidad de Sistemas e informática se encargará de brindar el apoyo necesario. Por fines de seguridad en la información, hará copias de respaldo de los correos electrónicos de ser necesarios, pero no son obligatorios.
- Cuando se presenten incidentes se deberá recurrir a la Mesa de Ayuda para informar sobre ellos o escribir un correo a soporte@apci.gob.pe.
- Está prohibido utilizar el correo electrónico institucional para cualquier propósito comercial, financiero o ajeno de la APCI y a los fines del sector.
- No está permitido enviar correos a destinatarios internos o externos en forma masiva, no siendo ellos parte de sus funciones.
- No distribuir mensajes, signos, figuras, fotografías, videos y demás, con contenidos impropios y/o lesivos a la moral o relacionados con la delincuencia o terrorismo.
- Está prohibido facilitar u ofrecer la cuenta y/o buzón de correo electrónico a terceras personas.
- Los usuarios no deben utilizar la cuenta de correo electrónico institucional para registrarse en empresas u organizaciones con fines personales (foros de estudio, medios de publicación, comercio, etc.).
- No se deberá enviar correos locales o externos solicitando información sobre accesos a sistemas de red de otros usuarios, sistemas y servicios informáticos para beneficio personal. Si en caso de recibir algo cuestionable o ilegal, se deberá comunicar a la Unidad de Sistemas e Informática para que se tomen las acciones del caso.

3.3. DEL INTERNET

Respecto al uso del Internet:

- Solo se puede acceder a Internet a través de la red local de la organización, con la infraestructura y protección de firewall adecuadas. El acceso directo a Internet mediante módems, Internet móvil, red inalámbrica u otros dispositivos de acceso directo a Internet, está bajo la autorización y supervisión de la Unidad de Sistemas e Informática.
- El administrador de la infraestructura tecnológica puede bloquear el acceso a determinadas páginas de Internet para usuarios individuales, grupos de usuarios o para todos los trabajadores de la APCI. Si el acceso a algunas páginas web está bloqueado, el usuario puede elevar una petición escrita a su jefe inmediato y este a su vez solicita acceso a la Unidad de Sistemas e Informática solicitando autorización para acceder a dichas páginas. El usuario no debe intentar eludir por su cuenta esa restricción.
- El usuario no debe considerar como confiable la información recibida a través de sitios web no verificados. Este tipo de información puede ser utilizada con fines institucionales solamente después de haber verificado su autenticidad y veracidad.
- El usuario es responsable por todas las posibles consecuencias que surjan por el uso no autorizado o inadecuado de servicios o contenidos de Internet.
- Está prohibido acceder a páginas que contengan signos, figuras, dibujos, fotografías, videos u otros con contenidos impropios y/o lesivos a la moral o relacionados a la delincuencia o terrorismo.
- No está permitido ingresar y utilizar páginas web dedicadas a la mensajería instantánea y salas de chats recreativas.
- El usuario no debe acceder a páginas que vayan en perjuicio o pongan en riesgo la seguridad de las redes y sistemas de la APCI.
- Está prohibido transferir información de la APCI que contravengan las normas legales.
- El usuario no debe realizar descargas de software que perjudiquen los recursos informáticos.
- No está permitido utilizar herramientas y/o software que evadan los controles del servicio de Internet.
- No está permitido la suscripción a páginas dedicadas a la publicidad vía correo electrónico cuyo contenido no se encuentre acorde a las funciones laborales del usuario.
- No está permitido ingresar y utilizar páginas web que permitan obtener contraseñas de software o sistemas informáticos; no adquiridos formalmente.

- No se permite el acceso y uso de sitios web de descarga de contenidos, ni el uso de aplicaciones que permitan las descargas de contenido tipo torrent, ares, eDonkey y similares.

3.4. COMPUTACIÓN MÓVIL

Entre los equipos de computación móvil se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos.

Se debe tener especial cuidado cuando los equipos de computación móvil se encuentran en vehículos u otros medios de transporte, espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencia y demás áreas no protegidas exteriores a las instalaciones de la APCI. La persona que se lleva equipos de computación móvil fuera de las instalaciones debe cumplir las siguientes reglas:

- El equipamiento de computación móvil que contiene información importante, sensible o crítica no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave o se deben utilizar bloqueos especiales para asegurarlo.
- Cuando se utiliza equipamiento de computación móvil en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- La protección contra códigos maliciosos se instala y actualiza mediante la consola de administración del antivirus instalado.
- La persona que utiliza equipamiento de computación móvil fuera de las instalaciones es responsable de realizar periódicamente copias de seguridad de datos siguiendo los lineamientos establecidos en la Política Específica de Copia de Seguridad.
- La conexión a redes de comunicación y el intercambio de datos debe reflejar la sensibilidad de los datos y se realiza mediante herramientas de colaboración con que se cuentan (Drive, correo) y/o medios extraíbles previa autorización de la jefatura del área de usuarios.
- La información que se encuentra en los ordenadores portátiles debe estar encriptada en coordinación con la USI.
- En el caso que el equipamiento de computación móvil sea desatendido, se deben aplicar las reglas para equipamiento de usuario desatendido de acuerdo a la Política Específica de Pantalla y Escritorio Limpio.
- El Oficial de Seguridad de la Información es el responsable de la capacitación y concienciación de las personas que utilizan equipamiento de computación móvil fuera de las instalaciones de la organización.

3.5. SUPERVISIÓN DEL USO DE SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN

- Todos los datos creados, almacenados, enviados o recibidos a través del sistema de información, o de otro sistema de comunicación de la APCI, incluyendo diversas aplicaciones, correo electrónico, Internet, fax, etc., independientemente de si es personal o no, se consideran propiedad de la APCI.
- A solicitud del jefe inmediato del área es posible realizar copias de respaldo de la información de los usuarios que dejen de laborar en la APCI.
- APCI puede utilizar herramientas especializadas para identificar y bloquear métodos prohibidos de comunicación y para filtrar contenidos prohibidos.

4. REGISTROS

Código	Nombre de Registro	Responsable del Control	Tiempo de Conservación
N/A	N/A	N/A	N/A

5. CONTROL DE CAMBIOS

Versión	Acción	Fecha de Acción	Tipo de Cambio	Descripción del Cambio	Responsable de la Acción	Distribuido a	Aprobado por
1.0	C	09/07/2019	Creación	Creación del documento	Oficial de Seguridad de la Información	Todo el personal de la APCI	Comité del SGSI
1.1	M	15/04/2021	Modificación	Modificación del documento	Oficial de Seguridad de la Información	Todo el personal de la APCI	Comité del SGSI
C=Creación, M=Modificación, D=Distribución, A=Aprobación							