

**DISPOSICIONES PARA EL ACCESO Y USO DE LOS ACTIVOS DE
TECNOLOGÍAS DE INFORMACIÓN DEL SERVICIO NACIONAL DE
CERTIFICACIÓN AMBIENTAL PARA LAS INVERSIONES SOSTENIBLES
– SENACE**

1. OBJETO

Establecer las disposiciones para el acceso y uso de los activos de tecnologías de la información, contribuyendo con la gestión de la seguridad de la información hacia los usuarios de los órganos y unidades orgánicas del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles - SENACE.

2. ALCANCE

La presente Directiva es de obligatorio cumplimiento para todos los órganos y unidades orgánicas del SENACE.

3. BASE NORMATIVA

- 3.1. Ley N° 29968, Ley de creación del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles - Senace y sus modificatorias.
- 3.2. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y sus modificatorias.
- 3.3. Decreto Legislativo, N° 1412, que aprueba la Ley de Gobierno Digital.
- 3.4. Decreto Supremo N° 031-2005-MTC, que aprueba el Reglamento de la Ley N° 28493 que regula el envío del correo electrónico comercial no solicitado (SPAM).
- 3.5. Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales.
- 3.6. Decreto Supremo N° 009-2017-MINAM, que aprueba el Reglamento de Organización y Funciones (ROF) del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles (SENACE).
- 3.7. Resolución Jefatural N° 207-2002-INEI, que aprueba la Directiva N°010-2002-INEI/DTNP, “Normas Técnicas para la asignación de nombres de Dominio de las entidades de la Administración Pública” y sus modificatorias.
- 3.8. Resolución Jefatural N° 088-2003-INEI, que aprueba la Directiva sobre “Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública”.
- 3.9. Resolución Ministerial N° 073-2004-PCM, que aprueba la Guía para la Administración Eficiente del Software Legal en la Administración Pública.

Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: “<https://www.senace.gob.pe/verificacion>” ingresando el código de verificación que aparece en la parte superior izquierda de este documento.

- 3.10. Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a Edición”, en todas las entidades integrantes del Sistema Nacional de Informática y sus modificatorias.

4. RESPONSABILIDAD

- 4.1. La Oficina de Tecnologías de la Información es la encargada de velar por el cumplimiento de la presente Directiva.
- 4.2. Los órganos y unidades orgánicas del SENACE son responsables del fiel cumplimiento de la presente Directiva.

5. DEFINICIONES

- 5.1. **Activo:** comprende cualquier recurso o competencia. Los activos pueden ser de alguno de los siguientes tipos: gestión, organización, procesos, conocimientos, personas, información, aplicaciones, infraestructura o el capital financiero. Entendiendo por activo todo aquello que tiene valor para la organización, cualquier componente (Información, software, físico, servicios, personal e intangibles) que soporta uno o más procesos y, en consecuencia, debe ser protegido.
- 5.2. **Ancho de banda:** cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado.
- 5.3. **Área usuaria:** es el órgano o unidad orgánica que requiere un servicio, acceso o uso de los activos de tecnologías de la información.
- 5.4. **Ataque informático:** intento organizado e intencionado causado por una o más personas para infringir daños o problemas a un sistema informático o red.
- 5.5. **Código malicioso:** código informático que crea brechas de seguridad para dañar un sistema informático.
- 5.6. **Credencial de acceso:** conformada por la combinación de usuario y contraseña.
- 5.7. **Cuenta de dominio:** representa la identificación digital, única e intransferible, a través de la cual el usuario hace uso de los demás activos de tecnologías de la información del SENACE.
- 5.8. **Data Center:** centro de procesamiento de datos, conformado por el Centro de Cómputo, fuentes de alimentación eléctrica y Centro de Control.
- 5.9. **Datos sensibles:** aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad.
- 5.10. **Host:** computadora u otro dispositivo conectado a una red que provee y utiliza servicios de ella.

- 5.11. **Oficial de Seguridad de la Información:** es la persona que tiene la responsabilidad de gestionar las acciones para salvaguardar la confidencialidad, integridad y disponibilidad de la información del SENACE.
- 5.12. **Red informática:** conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos.
- 5.13. **Sistema HelpDesk:** conjunto de recursos técnicos y humanos que permiten dar soporte a diferentes niveles de usuarios informáticos del SENACE.
- 5.14. **Software:** conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.
- 5.15. **Usuario:** se refiere a los servidores bajo la modalidad de contratación administrativa de servicios, practicantes, nómina de especialistas y locadores de servicios según corresponda, que requieren acceso y uso de los activos de tecnologías de la información, y bajo las disposiciones de la presente directiva.

6. ABREVIATURAS

GG	: Gerencia General
LOG	: Unidad de Logística
OA	: Oficina de Administración.
OTI	: Oficina de Tecnologías de la Información.
SENACE	: Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles.

7. DISPOSICIONES GENERALES

7.1. De las responsabilidades y obligaciones:

7.1.1. De la Oficina de Tecnologías de la Información:

- Administrar los activos de tecnologías de la información, así como brindar el soporte técnico necesario que garantice su operatividad.
- Establecer las restricciones y capacidad máxima para el acceso y uso de los activos de tecnologías de la información, previa aprobación de la Gerencia General.
- Gestionar los accesos y brindar la continuidad de los activos de tecnologías de la información del SENACE, lo que incluye las reasignaciones, modificaciones y acciones en caso de cese o terminación del servicio.
- Garantizar la seguridad de la información de los activos de tecnologías de la información del SENACE, con el apoyo del Oficial de Seguridad de la Información.
- Elaborar y mantener actualizada la documentación de administración y uso de los activos de tecnologías de la información.

- f) Realizar el mantenimiento preventivo y correctivo de los activos de tecnologías de la información.
- g) Mantener actualizado el registro de los activos de tecnologías de la información, con la finalidad de identificar sus usuarios, conocer su estado y ubicación, para complementar esta información con la que cuenta LOG.
- h) Emitir un informe técnico dirigido a LOG, para gestionar la baja de los equipos informáticos que se encuentren tecnológicamente obsoletos, en desuso o malogrados; en concordancia, con la normativa interna respecto a la gestión del patrimonio del Senace.
- i) Realizar el respaldo de la información contenida en los equipos informáticos del personal saliente o cesante, dentro de las 24 horas en que se produzca el cese, para que estos equipos sean retirados y entregados en calidad de custodia a cargo de LOG.
- j) Cuando un usuario culmine su relación contractual con el SENACE, la OTI en plazo no mayor de veinticuatro (24) horas procederá a retirar o trasladar los activos de tecnologías de la información, y procederá con el respaldo y borrado de información de los activos, a fin de entregar a LOG el bien informático, en calidad de custodia.

7.1.2. De los responsables de las áreas usuarias:

- a) Los requerimientos de contratación de personal bajo el régimen de contratación administrativa de servicios, practicantes y nómina de especialistas, cuya prestación se realice dentro de las instalaciones del Senace, deberán contar con el documento adjunto denominado “Solicitud de Acceso y Uso de los Activos de TI” (Anexo), el cual debe estar autorizado por el Director/a o Jefe/a del área usuaria, aprobación de la OTI respecto a la disponibilidad del equipamiento tecnológico, y con la autorización de LOG respecto a la disponibilidad de mobiliario, puntos eléctricos y otros requerimientos para el desarrollo de sus labores, según corresponda.
- b) Coordinar con LOG en caso de requerir trasladar, reubicar, de un sitio a otro, o reasignar patrimonialmente equipos informáticos. La OTI no realizará ningún traslado de equipos en tanto no se cuente con la autorización de LOG.
- c) Coordinar con la OTI, la proyección de crecimiento del área a su cargo, a fin de identificar la demanda de activos de tecnologías de la información, adquisición de hardware y provisión de asistencia técnica. Las áreas usuarias no deben tener bajo custodia activos de tecnologías de la información que no estén usando.

7.1.3. De la Oficina de Administración:

- a) En un plazo no mayor de veinticuatro (24) horas de efectuada la contratación, remitir a la OTI a través del Sistema EVA la “Solicitud de Acceso y Uso de los Activos de TI” (Anexo) de la presente directiva, suscrito por el/la directora/a o jefe del área usuaria.
- b) Comunicar a la OTI a través del Sistema EVA, las acciones de desplazamiento y cese de usuarios, en un plazo no mayor de veinticuatro (24) horas de haber tomado conocimiento.
- c) Mantener actualizado, a través de LOG (Control Patrimonial), el inventario de activos de tecnologías de la información.

7.1.4. De los usuarios:

- a) Usar los activos de tecnologías de la información para el cumplimiento de las funciones institucionales.
- b) Mantener sus credenciales de acceso en reserva, por ser de uso personal y confidencial.
- c) Apagar los equipos informáticos al concluir las labores del día, así como bloquear o cerrar la sesión de trabajo al dejar de usar la computadora o laptop, conforme a las medidas de ecoeficiencia establecidas para el sector público.
- d) Informar sobre alguna anomalía o problema que identifique en los activos de tecnologías de la información asignados, a través del Sistema HelpDesk, en caso no cuente con acceso a este sistema, puede pedir al usuario más cercano informar la anomalía o problema.
- e) Mantener el estado en el que le fueron asignados los activos de tecnologías de la información.
- f) Tener instalado en sus equipos de cómputo, sólo software autorizado e instalado por la OTI.
- g) Se encuentra prohibido toda manipulación o traslado, sin coordinación previa con LOG y la OTI, los cuales deben ser solicitados según formatos establecidos por la Superintendencia Nacional de Bienes Estatales o Directiva interna vigente.
- h) Observar las prohibiciones establecidas en las disposiciones de la presente Directiva.

7.2. Todo requerimiento que implique el uso de la “Solicitud de Acceso y Uso de los Activos de TI” (Anexo) de la presente directiva, se realiza de forma oportuna, el cual es remitido a la OTI a través del Módulo de Gestión Documental del

Sistema EVA. El formato debe estar firmado digitalmente por el responsable del área usuaria.

- 7.3. Toda acción relacionada a incidentes en los activos de tecnologías de la información se realiza a través del Sistema HelpDesk (<http://helpdesk.senace.gob.pe>). Esta disposición permite tener la trazabilidad y seguimiento del requerimiento, así mismo permite estimar los recursos para una eficiente atención.
- 7.4. En el marco de la ecoeficiencia y en la medida de lo posible, optimizar el uso adecuado del papel y materiales conexos, energía, agua, cartuchos de tinta, tóner de impresión, logrando prevenir la contaminación ambiental y obtener un ahorro económico para la entidad.

8. DISPOSICIONES ESPECÍFICAS

8.1. Niveles por tipo de usuario

Los responsables de las áreas usuarias autorizan los niveles de usuario para el acceso y uso de los activos de tecnologías de la información, correspondientes a los requerimientos de contratación administrativa de servicios, practicantes y nómina de especialistas, según sea el caso.

Para efectos de la presente Directiva, los usuarios de activos de tecnologías de la información se encuentran agrupados de acuerdo a los siguientes niveles de acceso:

Nivel	Usuarios	Acceso a internet	Email	Acceso a USB CD/DVD	Acceso telefónico	Acceso a unidades de red
Nivel 0	Practicante	Acceso básico a internet	Si	No	Sin anexo	Escritura en carpeta propia
Nivel 1	Auxiliar Asistente Administrativo I – II Técnico I – II	Acceso básico a internet	Si	No	Anexo interno + fijo local	Lectura en carpetas públicas + escritura en carpeta propia + escritura en carpetas compartidas
Nivel 2	Asistente Especialistas Profesional I – II – III Coordinador de TI Especialista de la Nómina Gestor de Proyecto Líder de Proyecto Subdirector Jefe de Unidad	Acceso básico a internet + *(multimedia + redes sociales)	Si	No	Anexo interno + fijo local + fijo nacional	Lectura en carpetas públicas + escritura en carpeta propia + escritura en carpetas compartidas
Nivel 3	Jefe de Órgano de Control Institucional Jefe de Oficina Director Asesor I – II Gerente/a General	Acceso básico a internet + multimedia + redes sociales	Si	Si **	Anexo interno + fijo local + fijo nacional + móvil +	Lectura en carpetas públicas. Escritura en carpeta propia + escritura en carpetas compartidas + lectura en unidad

Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: "<https://www.senace.gob.pe/verificacion>" ingresando el código de verificación que aparece en la parte superior izquierda de este documento.

Nivel	Usuarios	Acceso a internet	Email	Acceso a USB CD/DVD	Acceso telefónico	Acceso a unidades de red
	Presidente/a Ejecutivo				internacional	de red del área usuaria

* El acceso es a solicitud del Jefe/a inmediato por un periodo de tiempo específico.

**Incluye equipos de microformas de la Línea Certificada del SENACE.

8.2. Cuenta de dominio

8.2.1. La OTI crea las cuentas de dominio, según las siguientes nomenclaturas de acuerdo al tipo de vínculo laboral de los usuarios:

- a) Para el caso de usuarios con régimen CAS o practicantes: letra inicial del primer nombre del usuario, seguido del apellido paterno. El sistema automáticamente unirá el nombre de la cuenta de dominio creada, con el nombre de dominio de la institución (senace.gob.pe), ejemplo:

Nombre de usuario: Carlos Augusto Pérez Becerra

Cuenta de dominio: cperez@senace.gob.pe

Si al crear una cuenta de dominio ésta ya existe, se adiciona la letra inicial del segundo apellido del usuario al final del nombre de la cuenta, ejemplo:

Nombre de usuario: César Enrique Pérez Becerra

Cuenta de dominio: cperezb@senace.gob.pe

Solo de presentarse coincidencias a este nivel, la OTI realiza las coordinaciones para la creación de la cuenta. No se contempla en ningún caso requerimientos personalizados para la creación de cuenta.

- b) Para el caso de usuarios locadores de servicio, en los casos que corresponda: siglas del área responsable de la contratación, seguida de un guion inferior, seguido de un número correlativo, ejemplo:
oac_05@senace.gob.pe

- c) Para el caso de usuarios de la nómina de especialistas: siglas del área responsable de la contratación, seguido de un guion inferior, seguido de la palabra nómina, seguido de un guion inferior, seguido de un número correlativo, ejemplo:
dein_nomina_02@senace.gob.pe

8.2.2. El usuario debe cambiar obligatoriamente la contraseña asignada por defecto en el primer inicio de sesión con su cuenta de dominio. La OTI ha configurado como periodo máximo de tres (03) meses, para la solicitud automática de cambio de contraseñas de acceso por parte del usuario, la cual debe contener mínimo 10

caracteres entre letras mayúsculas y minúsculas, números y caracteres especiales.

- 8.2.3. Respecto a las cuentas de dominio, se encuentra prohibido:
- Intentar obtener o utilizar una cuenta de dominio y contraseña que no le ha sido asignada.
 - Burlar o intentar burlar las restricciones establecidas para una cuenta de dominio.
 - Ceder su cuenta a un usuario distinto, bajo responsabilidad solidaria.

8.3. Correo electrónico institucional

8.3.1. La cuenta de correo electrónico institucional asignada a los usuarios del SENACE, constituye un servicio que debe ser utilizado sólo para la comunicación e intercambio de información de índole institucional, acorde a las funciones o actividades a desarrollar.

8.3.2. Las cuentas de correo electrónico institucional siguen las mismas reglas de nomenclatura que las cuentas de dominio, señalada en el numeral 8.2. de la presente Directiva.

8.3.3. El envío y recepción de mensajes provenientes de cuentas de correo electrónico de dominios gratuitos (Hotmail, Gmail y similares) está restringido para todo el personal. En adición, el personal de la Nómina de Especialistas sólo puede enviar y recibir mensajes del dominio @senace.gob.pe. Los responsables de las áreas usuarias pueden solicitar la habilitación de envío y/o recepción de mensajes para los usuarios a su cargo, lo que debe constar en la "Solicitud de Acceso y Uso de los Activos de TI" (Anexo) de la presente directiva, especificando cómo este aspecto contribuye directamente al desempeño y cumplimiento de sus funciones.

Se encuentran exceptuados de esta disposición los usuarios del Nivel 3, a través de las cuentas de correo electrónico institucionales publicadas en el Portal Institucional. (www.senace.gob.pe).

Ejemplo:

Cuenta de correo: oti@senace.gob.pe

Adicionalmente, se encuentran exceptuadas las cuentas de correo electrónico de contacto con la ciudadanía (ej. solicitudes de acceso a la información), lo que debe ser señalado en el Anexo de la presente Directiva.

8.3.4. El modo de acceso al correo electrónico institucional se realiza mediante un cliente de correo electrónico (por ejemplo, Microsoft Outlook) o a través de internet, ingresando a la siguiente dirección web: <https://mail.senace.gob.pe>.

- 8.3.5. La capacidad máxima para el envío de documentos adjuntos es de 20MB¹. La OTI recomienda no exceder la capacidad de 5MB para evitar incrementar el tráfico en la red informática.
- 8.3.6. La OTI puede crear grupos de distribución para el envío de mensajes masivos que respondan al interés institucional, lo que debe ser solicitado por el área usuaria correspondiente, a través del Sistema HelpDesk.
- 8.3.7. La GG, a través de la Unidad de Comunicaciones e Imagen Institucional, es responsable del envío de correos masivos al personal del SENACE.
- 8.3.8. Los usuarios deben utilizar el formato estándar de firmas para el correo electrónico, configuradas por la OTI de acuerdo a las normas de identidad institucional del SENACE y de acuerdo a su modalidad de contratación.
- 8.3.9. Los usuarios deben informar a la OTI y al Oficial de Seguridad de la Información, ante cualquier comportamiento inusual que se presente en su cuenta de correo electrónico (por ejemplo, recepción o envío masivo de correos electrónicos) o ante cualquier mensaje de correo electrónico que considere ofensivo, cuestionable o de dudosa procedencia.
- 8.3.10. Durante el periodo vacacional, licencias u otros motivos de ausencia prolongada, los usuarios deben habilitar la opción de respuesta automática, consignando los datos de contacto de la persona reemplazante y la fecha de retorno prevista.
- 8.3.11. Respecto al correo electrónico institucional, se encuentra prohibido:
- Prestar o dar acceso a la cuenta del correo electrónico a terceras personas.
 - Difundir contenido inadecuado. Se considera contenido inadecuado todo aquello que constituya complicidad con hechos delictivos como apología del terrorismo, distribución de software no licenciado, todo tipo de pornografía, amenazas, información que pueda derivar en fraudes y/o esquemas de enriquecimiento piramidal, así como el envío de código malicioso en general.
 - Intentar o lograr apoderarse de la contraseña de acceso de otros usuarios mediante cualquier mecanismo, así como acceder, enviar y/o modificar mensajes de otros usuarios.
 - Enviar correos electrónicos para la difusión de mensajes de autores anónimos.

¹ Dicha capacidad podrá ser ampliado de manera temporal previa autorización.

- e) Usar el correo electrónico institucional para propósitos personales, fraudulentos, comerciales, publicitarios, difamatorios, racistas, obscenos y/o distintos a fines laborales.
- f) Modificar el formato de firma de correo electrónico configurada por la OTI.
- g) Utilizar mecanismos y/o sistemas que intenten ocultar o suplantar la identidad del emisor del correo.
- h) Enviar archivos adjuntos con extensiones utilizadas para propagación de código malicioso. La OTI debe garantizar el bloqueo del envío o recepción de correos electrónicos conteniendo esta clase de archivos.
- i) Utilizar el correo electrónico para enviar información considerada como datos personales o sensibles, de conformidad con la Ley N° 29733, Ley de protección de datos personales.

8.3.12. Respecto al tiempo de retención y disposición de las cuentas de correo electrónico:

- a) Toda cuenta de correo electrónico institucional de los usuarios que culmina su relación contractual es dada de baja.
- b) A solicitud del usuario cesante, la OTI podrá realizar la copia del contenido de su cuenta de correo electrónico institucional, con un plazo de retención de la copia de treinta (30) días, contados a partir de la baja de la cuenta de usuario. Durante este periodo el usuario cesante puede solicitar a la OTI una copia del contenido de su cuenta de correo electrónico.
- c) La disposición, posterior al vencimiento del tiempo de retención, es la eliminación de la copia.

8.3.13. La OTI, con la autorización de la GG, está facultada para cancelar una cuenta de correo electrónico institucional, si detecta incumplimiento a lo dispuesto en la presente Directiva.

8.4. Acceso a internet

8.4.1. El uso autorizado del internet es un recurso que brinda el SENACE exclusivamente para las actividades institucionales, guardando relación con las responsabilidades asignadas.

8.4.2. Es función de la OTI bloquear el acceso a los usuarios a páginas web que impliquen riesgo informático, de acuerdo con las políticas de seguridad de la información.

8.4.3. La OTI es responsable de gestionar adecuadamente el ancho de banda del servicio de Internet, a través de la asignación de perfiles de navegación web, según el siguiente detalle:

Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: "<https://www.senace.gob.pe/verificacion>" ingresando el código de verificación que aparece en la parte superior izquierda de este documento.

Usuarios del Nivel 0 y 1:

Acceso básico a internet, que comprende principalmente, páginas de gobierno, educación, investigación, acceso a servicios web de correo gratuitos, y descarga de archivos de páginas consideradas seguras.

Usuarios del Nivel 2:

Acceso básico a internet.

Pudiendo solicitar acceso a páginas web con contenido multimedia y redes sociales, de acuerdo a las labores a desarrollar.

Usuarios del Nivel 3:

Acceso a toda página web, con excepción de lo expresamente prohibido.

Los responsables de las áreas usuarias del SENACE pueden solicitar la restricción o ampliación de los perfiles antes señalados, lo que debe constar en "Solicitud de Acceso y Uso de los Activos de TI" (Anexo) de la presente directiva, especificando cómo este aspecto contribuye directamente al desempeño y cumplimiento de sus funciones.

8.4.4. Respecto al acceso a internet, se encuentra prohibido:

- a) El acceso a páginas web de contenido pornográfico.
- b) El acceso a páginas web relacionadas con actividades ilegales o delictivas.
- c) El acceso a páginas web de actividades lúdicas u otros sitios de entretenimiento.
- d) Utilizar el servicio de internet para realizar ataques informáticos a sitios o hosts de internet.
- e) La descarga o publicación de material protegido por la normativa de propiedad intelectual, sin autorización de su propietario.
- f) Realizar publicaciones en medios digitales sobre asuntos relacionados al SENACE que no hayan sido previamente difundidos a través de las cuentas oficiales del SENACE, y efectuar declaraciones en medios digitales sobre asuntos relacionados al SENACE, sin autorización.

8.5. Telefonía IP

8.5.1. El acceso al servicio de telefonía IP es habilitado a través de un código de acceso personal e intransferible, otorgado por la OTI, en virtud al requerimiento del responsable de área usuaria del SENACE (Anexo) de la presente directiva. Los usuarios del Nivel 0 (practicantes) no cuentan con telefonía IP.

8.5.2. Los perfiles de consumo de telefonía IP son los siguientes:

Usuarios del Nivel 1:

Anexo interno + fijo local

Usuarios del Nivel 2:

Anexo interno + fijo local + fijo nacional

Usuarios del Nivel 3:

Anexo interno + fijo local + fijo nacional + móvil + internacional

Los responsables de las áreas usuarias del SENACE pueden solicitar la restricción o ampliación de los perfiles antes señalados, lo que debe constar en la "Solicitud de Acceso y Uso de los Activos de TI" (Anexo) de la presente directiva, especificando cómo este aspecto contribuye directamente al desempeño y cumplimiento de sus funciones.

8.5.3. El traslado del teléfono IP del lugar en donde fue instalado por la OTI debe ser coordinado primeramente con LOG y solicitado a través del Sistema HelpDesk.

8.5.4. Respecto a la telefonía IP, se encuentra prohibido:

- a) Intentar obtener o utilizar un código de acceso que no le ha sido asignado.
- b) Burlar o intentar burlar las restricciones establecidas para su código de acceso.
- c) Dañar el equipo asignado o exponerlo a deterioro.
- d) Ceder su código a un usuario distinto, bajo responsabilidad solidaria.

8.6. Puertos USB y Lector CD/DVD

8.6.1. Como medida de seguridad de la información, se encuentra inhabilitado el uso de los puertos USB y lector CD/DVD de los equipos informáticos del SENACE. Se encuentran exceptuados de esta disposición los usuarios del Nivel 3 y los equipos destinados para la grabación de microformas de la Línea Certificada del Senace.

8.6.2. Los responsables de las áreas usuarias pueden solicitar la habilitación de los puertos USB y lector CD/DVD para los equipos de cómputo de los usuarios a su cargo, lo que debe constar en la "Solicitud de Acceso y Uso de los Activos de TI" (Anexo) de la presente directiva, especificando cómo este aspecto contribuye directamente al desempeño y cumplimiento de sus funciones.

8.6.3. La OTI implementa mecanismos alternativos al uso de puertos USB y lector CD/DVD, tal como el uso de unidades de red para compartir información de manera segura. Además, se realiza el escaneo automático a dispositivos externos, con la finalidad de prevenir el acceso de software malicioso.

8.7. Unidades de Red/Impresión y escaneo en red

8.7.1. Todo usuario tiene acceso a las carpetas públicas (carpeta pública y carpeta temporal) y a su propia carpeta que se encuentra dentro del contenedor de la unidad de red asignado a su respectiva área. Si el usuario requiere acceso a otros contenedores debe constar en la "Solicitud de Acceso y Uso de los Activos de TI" (Anexo) de la presente directiva.

- 8.7.2. La carpeta pública debe ser utilizada para guardar información de interés de todo el personal del SENACE, la cual no debe ser eliminada, salvo se requiera su actualización o eliminación por considerarse obsoleta.
- 8.7.3. La carpeta temporal P: (unidad pública) debe ser utilizada para cubrir la necesidad de compartir información entre las áreas usuarias del SENACE. Su contenido será eliminado automáticamente todos los fines de semana (sábado) por la OTI.
- 8.7.4. Los perfiles de acceso a la unidad de red del área son los siguientes:
- Usuarios del Nivel 0:
Escritura en carpeta propia.
- Usuarios del Nivel 1 y 2:
Lectura en carpetas públicas.
Escritura en carpeta propia + escritura en carpetas compartidas.
- Usuarios del Nivel 3:
Lectura en carpetas públicas.
Escritura en carpeta propia + escritura en carpetas compartidas + lectura en unidad de red del área usuaria.
- 8.7.5. La OTI, en coordinación con los responsables de las áreas usuarias definen:
- La estructura de la unidad de red correspondiente a su área.
 - La información contenida en las carpetas públicas y su actualización, además se define el personal autorizado para cargar información a estas carpetas.
- 8.7.6. Los usuarios deben guardar sus archivos de trabajo en su carpeta de red asignada. Los archivos almacenados en cualquier otra ubicación no son respaldados por la OTI.
- 8.7.7. La OTI configura las impresoras y escáner de red teniendo en cuenta lo siguiente:
- Todas las impresiones son automáticamente en doble cara y en escala de grises.
 - Todos los escaneos son almacenados en la unidad de red del área usuaria correspondiente.
- 8.8. **Dispositivos móviles**
- 8.8.1. Se consideran dispositivos móviles a las computadoras portátiles, teléfonos celulares, tabletas o similares.

- 8.8.2. El SENACE sólo permite la conexión a la red inalámbrica y demás activos de tecnologías de la información a los dispositivos móviles de propiedad de la institución.
- 8.8.3. Por motivos de seguridad de la información, el SENACE establece áreas seguras, en las que se encuentra prohibido el acceso a dispositivos móviles, con excepción de aquellos que se requieran como soporte técnico, tales como:
- a) Oficinas de la Alta Dirección del SENACE, que comprenden la oficina de la Presidencia Ejecutiva, la oficina de la GG y las salas de reuniones del SENACE ubicadas en el segundo piso de la sede.
 - b) Data Center, donde se encuentra el Centro de Cómputo, que alberga y procesa toda la información de los diferentes sistemas informáticos, asimismo, desde esta área se realiza la administración, monitoreo y control de toda la infraestructura tecnológica.
 - c) Las demás que identifique el SENACE, previo informe del Oficial de Seguridad de la Información.

8.9. **Sistemas de información**

- 8.9.1. Los responsables de las áreas usuarias pueden solicitar la habilitación de acceso a los sistemas de información administrados por la OTI, con el nivel de acceso requerido, para los equipos de cómputo de los usuarios a su cargo, lo que debe constar en la "Solicitud de Acceso y Uso de los Activos de TI" (Anexo) de la presente directiva, especificando cómo este aspecto contribuye al desempeño y cumplimiento de sus funciones.

8.10. **Cámaras de video vigilancia**

- 8.10.1. El resguardo de la información generada por las cámaras de video vigilancia, estarán a cargo de la OTI, para lo cual esta oficina dispondrá los mecanismos necesarios para garantizar la disponibilidad e integridad de los equipos como de la información producida por estas. Los videos generados por las cámaras tendrán una permanencia máxima de 2 meses.
- 8.10.2. Las solicitudes de revisión de las grabaciones de las cámaras de video vigilancia serán canalizadas por la OA, para lo cual el responsable de esta área debe solicitar al Jefe/a de la OTI mediante correo electrónico, el detalle del rango de fechas, horas y ubicación de la cámara por la cual se realizó la grabación requerida.
- 8.10.3. La OTI dispondrá de una cuenta de acceso de solo lectura, mediante el cual OA podrá acceder a los videos en tiempo real.

9. DISPOSICIONES COMPLEMENTARIAS FINALES

- 9.1. La OTI difunde los alcances de la presente Directiva a todo el personal y debe, en coordinación con el Oficial de Seguridad de la Información, realizar capacitaciones y/o talleres de sensibilización para garantizar su adecuado cumplimiento.
- 9.2. Toda modificación respecto al uso y acceso a los activos de tecnologías de la información debe gestionarse utilizando la “Solicitud de Acceso y Uso de los Activos de TI” (Anexo) a través del sistema EVA, contando con la autorización del responsable del área correspondiente y expresando los motivos de la modificación solicitada.
- 9.3. Por razones de necesidad del servicio, la OTI puede requerir cambiar, retirar o reasignar algún activo de tecnología de la información, previa coordinación con el responsable del área usuarias del SENACE.
- 9.4. La OTI queda facultada para definir aspectos, en el marco de su competencia, no contemplados en la presente Directiva.

10. ANEXO

ANEXO : Solicitud de Acceso y Uso de los Activos de TI

Nota:

- Cuando solo se cuente con los datos del puesto, realizar la solicitud completando todas las secciones excepto la N°2.
- Cuando ya se cuente con los datos personales del usuario, completar solo la sección la N°2, sobre la misma información registrada en la solicitud en el punto anterior.
- Para la modificación de accesos y/o uso de activos de TI, completar las secciones N° 1 y 2, así como los campos que se modificarán y la sección N° 5 para justificación de la modificación.

 ANEXO - SOLICITUD DE ACCESO Y USO DE LOS ACTIVOS DE TI-				
1. DATOS DEL PUESTO				
Denominación del puesto / objeto contratación:	<input type="text"/> Nivel Usuario: <input type="text"/>			
Área usuaria:	<input type="text"/>			
Condición:	CAS: <input type="checkbox"/> Nómina: <input type="checkbox"/> Practicante: <input type="checkbox"/> Locador: <input type="checkbox"/> Otro: <input type="checkbox"/>			
Fecha Inicio/ Ingreso:/...../.....	Fecha Fin/Cese (en caso corresponda)/...../.....			
2. DATOS PERSONALES DEL USUARIO				
Nombres y Apellidos:	<input type="text"/>			
Nº de contrato/convenio /otro:	<input type="text"/>			
Documento de Identidad:	<input type="text"/> Correo electrónico personal: <input type="text"/>			
3. DATOS DE ACTIVOS DE TI Y ACCESOS				
3.1 PCs:	3.2 Impresoras:	3.3 Internet y correo institucional	3.4 Acceso a Unidades de Red	3.5 Telefonía
Pc Escritorio <input type="checkbox"/>	Laser <input type="checkbox"/>	Usuario/Id de Red: <input type="checkbox"/>	Carpeta Del Área <input type="checkbox"/>	EqTeléfónico IP <input type="checkbox"/>
Pc Portátil <input type="checkbox"/>	Matricial <input type="checkbox"/>	Correo Institucional: <input type="checkbox"/>	Carpeta Pública <input type="checkbox"/>	Acceso a Llamadas <input type="checkbox"/>
Workstation <input type="checkbox"/>	Etiquetas <input type="checkbox"/>	Internet: <input type="checkbox"/>		Punto de Red <input type="checkbox"/>
Tablet <input type="checkbox"/>				
3.6 Sistemas de Información				
Sistema de Gestión Documental y Evaluación – EVA:		Sistema Integrado de Transparencia y Atención al Ciudadano – SITAC:		
Tramite documentario <input type="checkbox"/>	Evaluador <input type="checkbox"/>	Registro De Visitas: <input type="checkbox"/>		
Punto de Control <input type="checkbox"/>	Líder <input type="checkbox"/>	Reclamaciones <input type="checkbox"/>		
Colaborador: <input type="checkbox"/>	Gestor <input type="checkbox"/>	Acceso A La Información <input type="checkbox"/>		
Jefe / Responsable <input type="checkbox"/>		Agenda Institucional <input type="checkbox"/>		
		Consultas <input type="checkbox"/>		
Sistema Integrado de Gestión Administrativa – SIGA				
Modificación Presupuestal <input type="checkbox"/>	OA-Logística <input type="checkbox"/>	OA – Planillas <input type="checkbox"/>		
Cuadro de Necesidades <input type="checkbox"/>	OA-Contabilidad <input type="checkbox"/>	OA – Convocatorias CAS <input type="checkbox"/>		
Requerimientos B/S <input type="checkbox"/>	OA-Tesorería <input type="checkbox"/>	OPP - Planeamiento <input type="checkbox"/>		
Pedido Almacén <input type="checkbox"/>	OA-Almacén <input type="checkbox"/>	OPP - Presupuesto <input type="checkbox"/>		
Permisos y Licencias <input type="checkbox"/>	OA-Control Patrimonial <input type="checkbox"/>	Jefe Unidad OPP <input type="checkbox"/>		
Jefe / Director <input type="checkbox"/>	Jefe Unidad OA <input type="checkbox"/>	Jefe OPP <input type="checkbox"/>		
	Jefe OA <input type="checkbox"/>			
Sistema Peruano de Información Jurídica – SPIJ <input type="checkbox"/>	Sistema Integrado de Administración Financiera – SIAF <input type="checkbox"/>	Otro: <input type="checkbox"/>		
4. OTROS SERVICIOS A CARGO DE LOG				
<ul style="list-style-type: none"> • Equipo Teléfono Celular: • Escritorio y Silla; • Puntos Eléctricos Estabilizados: 				
5. OBSERVACIONES - JUSTIFICACIONES				
<ul style="list-style-type: none"> • [Opinión Técnica de la LOG] / [Opinión Técnica de la OTI] • [Justificación. motivo de solicitud de modificación de accesos y/o uso de activos de TI registrada por el responsable del Área Usuaria] • [Información Adicional registrada por el responsable del Área Usuaria] 				

Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: "<https://www.senace.gob.pe/verificacion>" ingresando el código de verificación que aparece en la parte superior izquierda de este documento.