Resolución de Subsecretaría General

N° 048 -2017-DP/SSG

Lima, 29 DIC. 2017

VISTO: el Memorando N° 1668-2017-DP-SSG/OGPM e Informe Nº 032-2017-DP-SSG/OGPM-GICM de la Oficina General de Planeamiento, Presupuesto y Modernización, sobre proyecto de Directiva denominada: "Directiva de Seguridad Informática en el Despacho Presidencial";

CONSIDERANDO:

Que, mediante Resolución del Subsecretario General de la Presidencia de la República N° 007-2007-DP/SSGPR de fecha 18 de abril de 2007 se aprueba la Directiva N°001-2007-DP/ SSGPR "Política de Seguridad Informática en el Despacho Presidencial";

Que, el artículo 22° A del Reglamento de Organización y Funciones del Despacho Presidencial, aprobado por Decreto Supremo N° 077-2016-PCM, y modificado por el Decreto Supremo N° 037-2017-PCM, establece que la Oficina de Tecnologías de la Información tiene, entre otras, la función de formular, proponer y evaluar los lineamientos y planes de gestión en materia de tecnologías de la información en el Despacho Presidencial, en concordancia con las políticas nacionales y los principios de buen gobierno sobre la materia; de administrar el funcionamiento de los medios informáticos, tanto al interior del país como en los enlaces con el extranjero; así como los sistemas de software personalizados o adquisición de sistemas de acuerdo a las necesidades del Despacho Presidencial; y de administrar las redes locales y remotas, así como las diferentes bases de datos del Despacho Presidencial;

Que, el artículo 28° del mencionado Reglamento dispone que la Oficina General de Planeamiento, Presupuesto y Modernización es la responsable de brindar asesoramiento a la Alta Dirección y a los demás órganos del Despacho Presidencial en asuntos relacionados a la conducción de procesos de planeamiento, presupuesto, inversión pública y modernización de la gestión pública;

Que, el artículo 5° de la Directiva N° 001-2016-DP/SSG "Lineamientos para la elaboración, aprobación y modificación de directivas del Despacho Presidencial", aprobada por la Resolución de Subsecretaría General N° 041-2016-DP/SSG del 02 de diciembre de 2016, señala que la Oficina General de Planeamiento, Presupuesto y Modernización es la encargada de la conducción y revisión de directivas del Despacho Presidencial;

Que, dentro de este contexto, la Oficina General de Planeamiento, Presupuesto y Modernización, a través de los documentos del visto, opina favorablemente por la aprobación de la Directiva propuesta por la Oficina de Tecnologías de la Información;

Que, efectuada la evaluación correspondiente y contando con las respectivas conformidades respecto a la aprobación del citado documento, esta Subsecretaría General

estima procedente que sea aprobado, a fin de coadyuvar el mejor cumplimiento de los fines institucionales;

Que, en virtud de la delegación de facultades dispuesta mediante la Resolución de Secretaria General N° 084-2017-DP/SG, corresponde a la Subsecretaria General aprobar directivas, manuales de procedimientos y todo tipo de disposiciones internas vinculadas a la conducción de la institución;

De conformidad con el Reglamento de Organización y Funciones del Despacho Presidencial, aprobado mediante Decreto Supremo N° 077-2016-PCM, modificado por Decreto Supremo N° 037-2017-PCM y la Directiva N° 001-2016-DP/SSG "Lineamientos para la elaboración, aprobación y modificación de directivas del Despacho Presidencial", aprobada por la Resolución de Subsecretaría General N° 041-2016-DP/SSG, y;

Contando con los vistos de la Oficina General de Planeamiento, Presupuesto y Modernización; la Oficina General de Asesoría Jurídica; y, la Oficina de Tecnologías de la Información;

SE RESUELVE:

Artículo 1°.- Aprobación de la Directiva
Aprobar la Directiva denominada "Directiva de Seguridad Informática en el Despacho Presidencial", la misma que consta de cuatro (04) Capítulos, dieciséis (16) Artículos, una (01) Disposición Complementaria y dos (02) anexos que obran adjuntos como parte integrante de la presente Resolución.

Artículo 2°.- Derogación
Déjese sin efecto la Resolución del Subsecretario General de la Presidencia de la República N° 007-2007-DP/SSGPR de fecha 18 de abril de 2007 que aprueba la Directiva N°001-2007-DP/ SSGPR "Política de Seguridad Informática en el Despacho Presidencial".

Artículo 3°.- Vigencia
La Directiva aprobada por la presente Resolución entrará en vigencia a partir del día siguiente de su publicación en el Portal Institucional.

Artículo 4°.- Difusión
Disponer la publicación de la presente Resolución y de la Directiva que forma parte de la misma en el Portal del Estado Peruano, en la página web de la Entidad (www.presidencia.gob.pe) y en la intranet institucional.

Regístrese y Comuníquese.

EMMA LEON VELARDE AMÉZAGA
Subsecretaria General de la
Presidencia de la República

Despacho Presidencial

DIRECTIVA DE SEGURIDAD INFORMÁTICA EN EL DESPACHO PRESIDENCIAL

Directiva N°011-2017-DP/SSG

ROL	ORGANO	SELLO Y FIRMA
ELABORADA POR	Subsecretaría General - Oficina de Tecnologías de la Información	Ing. KATHERINE PATRICIA PALOMINO REYNA Directora de la Oficina de Tecnologías de la Información Despacho Presidencial
REVISADA	Oficina General de Planeamiento, Presupuesto y Modernización	RAYDA RUTH JERÓNIMO ZACARÍAS Directora General Oficina General de Planeamiento, Presupuesto y Modernización Despacho Presidencial
	Oficina de Recursos Humanos	ITALO ALBERTO LACA RAMOS Director de la Oficina de Recursos Humanos DESPACHO PRESIDENCIAL
	Oficina General de Administración	ANALI YSABEL VÁSQUEZ MOTTA Directora General de Administración Despacho Presidencial
	Oficina General de Asesoría Jurídica	ERICKSON GUTIERREZ BOBADILLA DIRECTOR GENERAL OFICINA GENERAL DE ASESORÍA JURÍDICA DESPACHO PRESIDENCIAL
APROBADA POR	Subsecretaría General	EMMA LEON VELARDE AMÉZAGA Subsecretaria General de la Presidencia de la República

ÍNDICE

CAPÍTULO I

DISPOSICIONES PRELIMINARES

Artículo 1º Objetivo

Establecer lineamientos que garanticen la seguridad de todos los recursos informáticos del Despacho Presidencial, así como el uso adecuado de los mismos, estableciendo mecanismos de gestión para administrarlos adecuadamente.

Artículo 2º Finalidad

Brindar criterios que permitan resguardar adecuadamente la información generada, almacenada y/o gestionada a través de los recursos informáticos del Despacho Presidencial.

Artículo 3º Base Legal

3.1. Decreto Supremo N° 077-2016-PCM, que aprueba el Reglamento de Organización y Funciones del Despacho Presidencial, modificado por Decreto Supremo N°037-2017-PCM.

3.2. Ley N° 27588. Que establece prohibiciones e incompatibilidades de funcionarios y servidores públicos, así como de personas que presten servicios al Estado bajo cualquier modalidad contractual y su reglamento aprobado mediante y Decreto Supremo N°019-2002-PCM.

3.3. Resolución de Subsecretaría General N°041-2016-DP/SSG, que aprueba la Directiva N°001-2016-DP/SSG "Lineamientos para la Elaboración, Aprobación y Modificación de Directivas del Despacho Presidencial".

3.4. Decreto Supremo N° 013-2003-PCM, por el cual se dictan medidas para garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del Sector Público.

3.5. Decreto Supremo N°076-2010-PCM, que modifica el Decreto Supremo N°013-2003-PCM; estableciendo disposiciones referidas a las adquisiciones de computadoras personales que convoquen las entidades públicas.

3.6. Directiva N° 004-2009-DP/SSGPR - "Administración de los Bienes Muebles del Despacho Presidencial", aprobada por Resolución de la Subsecretaria General N° 026-2009-DP/SSGPR.

3.7. Resolución de Secretaría General N° 093-2017-DP/SG, que aprueba la Política de Seguridad de la Información del Despacho Presidencial

3.8. Resolución Directoral N° 088-2003-INEI, que aprueba la Directiva N° 005-2003-INEI/DTNP - Normas para el uso del Servicio de Correo Electrónico en las Entidades de la Administración Pública.

3.9. Resolución Jefatural N°386-2002-INEI, que aprueba la Directiva N°016-2002-INEI/DTNP - Normas Técnicas para el almacenamiento y respaldo de la información procesada por las entidades de la Administración Pública.

3.10. Resolución de Contraloría N° 320-2006-CG, que aprueba Normas de Control Interno.

Artículo 4º Ámbito de Aplicación

La presente Directiva es de cumplimiento obligatorio para todos los órganos y unidades orgánicas que conforman el Despacho Presidencial que utilicen recursos informáticos para el almacenamiento y procesamiento de la información, sin distinción del régimen laboral o contractual o de nivel jerárquico.

Artículo 5º Responsabilidad

5.1. A cargo de los usuarios de los recursos informáticos:

a) Cumplir estrictamente con lo señalado en la presente directiva.

b) Cambiar y custodiar adecuadamente sus claves de acceso a la red institucional evitando compartirla, escribirla en un papel o agenda procurando memorizarla.

c) No hacer uso indebido de los recursos informáticos a los que tenga acceso el usuario, siendo responsabilidad de éste, las consecuencias que se puedan generar de dichas acciones.

d) Comunicar mediante los Jefes de los Órganos y Unidades Orgánicas, cualquier movimiento o traslado de equipos de cómputo al Área de Control Patrimonial de la Oficina de Abastecimiento.

e) El incumplimiento de las disposiciones contenidas en la presente Directiva, generará responsabilidad administrativa, civil o penal, según corresponda, la misma que será determinada conforme a la normatividad vigente.

5.2. A cargo de los Jefes de Órganos y Unidades Orgánicas:

a) Supervisar el cumplimiento de la Directiva de Seguridad Informática dentro de cada órgano o unidad orgánica, según corresponda.

b) Poner en conocimiento a la Oficina de Tecnologías de la Información cualquier situación de incumplimiento de la presente Directiva, a fin de que inicie las acciones que correspondan.

c) En caso requieran designar a otra persona para la firma de autorizaciones y solicitudes relacionados con la presente Directiva, deberán comunicar formalmente a la Oficina de Tecnologías de la Información a fin de considerar válidas dichas autorizaciones y solicitudes.

5.3. A cargo de la Oficina de Abastecimiento:

a) Emitir oportunamente, mediante el Área de Control Patrimonial, las "Actas de Asignación" de equipos informáticos, para el visado por un especialista de la Oficina de Tecnologías de la Información.

b) Supervisar permanentemente que la información del inventario de bienes informáticos corresponda a su ubicación física y al personal que utiliza dicho bien, lo cual debe constar en las "Actas de Asignación".

5.4. A cargo de la Oficina de Tecnologías de la Información:

a) Supervisar que los usuarios de equipos y servicios informáticos den el estricto cumplimiento de la presente Directiva.

b) Poner de conocimiento de la Oficina de Recursos Humanos cualquier situación de incumplimiento de la presente Directiva, a fin de que inicie las acciones que correspondan.

c) Tener el inventario técnico actualizado de los usuarios por cada equipo informático en uso.

5.5. A cargo de la Oficina de Recursos Humanos:

a) Poner de conocimiento a la Oficina de Tecnologías de la Información sobre el goce de vacaciones, licencias, cese o cualquier otra circunstancia que determine la ausencia de un usuario.

CAPÍTULO II

DISPOSICIONES GENERALES

Artículo 6º Siglas y Definiciones

Para los efectos de la presente directiva se establecen las siguientes siglas:

Sigla	Descripción
OGA	Oficina General de Administración
OTI	Oficina de Tecnologías de la Información
ORH	Oficina de Recursos Humanos
OA	Oficina de Abastecimiento

Asimismo, se establecen las siguientes definiciones:

Tema	Definición
Recurso Informático	Se utilizará este término para referirse a la generalidad de equipos informáticos (hardware), programas de computadora (software, aplicaciones y sistemas de información) y cuentas de acceso a la red institucional, correo institucional, internet e intranet.
Administración de los recursos informáticos	Son todos los actos de gestión y decisión destinados a cautelar, organizar, controlar o supervisar los recursos informáticos, de acuerdo a lo señalado en la "Directiva para la Administración de los Bienes Muebles del Despacho Presidencial" vigente.
Área, Órgano y Unidad Orgánica	a) Área, Subdivisión de una Unidad Orgánica para el mejor cumplimiento de sus funciones, no forman parte de la estructura orgánica. b) Órgano, término genérico con que se identifica a los órganos de la Alta Dirección, de Línea, de Apoyo, de Asesoría y de Control Institucional, que integran la estructura orgánica del Despacho Presidencial y que están expresamente señalados en el Reglamento de Organización y Funciones (ROF). c) Unidad Orgánica, Subdivisión de un órgano para el mejor cumplimiento de sus funciones, forman parte de la estructura orgánica y se encuentran descritas en el ROF.
Asignación de recursos informáticos	Es el acto por el cual, se entrega a un determinado empleado público, recursos informáticos (ver la definición de "Recurso informático") específicos, de acuerdo al pedido formulado ante la Oficina de Abastecimiento. Los únicos autorizados a formular dicha solicitud son los empleados responsables del órgano respectivo, sea éste de la Alta Dirección, de Línea, de Apoyo, de Asesoría o de Control Institucional.
Backup	Copia de seguridad de la información gestionada por la Oficina de Tecnologías de la Información, en adicción a la información establecida en el artículo 12° como respaldo frente a eventualidades.
Computadora personal	Computador u ordenador asignado al personal del Despacho Presidencial, conforme a los procedimientos previstos en esta Directiva. Comprende el CPU (incluye teclado y mouse) y el Monitor.
Correo electrónico oficial	Toda referencia al "correo electrónico" se entiende referida al correo electrónico institucional que asigna el Despacho Presidencial a los empleados, para fines propios del ejercicio de sus funciones. Dichos correos electrónicos utilizan el dominio "presidencia.gob.pe".
Confidencialidad	Es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento del Despacho Presidencial. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a ésta información.
Empleado	Término utilizado para referirse a todas las personas naturales que prestan servicios en el Despacho Presidencial, sea que cuenten con vínculo laboral o que se trate de personal destacado, conforme ROF.
Red Institucional	Se refiere a la Red de Datos, consistente en la interconexión entre las computadoras con que cuenta el Despacho Presidencial. La Red de Datos incluye tanto el hardware como el software necesarios para la interconexión de los distintos dispositivos y el tratamiento de la información.

Seguridad Física de los Recursos Informáticos	Se refiere a las medidas de seguridad externa o física, destinada a proteger la integridad física de los equipos informáticos con que cuenta el Despacho Presidencial para el almacenamiento y procesamiento de la información.
Seguridad lógica de los Recursos Informáticos	Se refiere a las herramientas informáticas destinadas a proteger la información almacenada en los equipos informáticos del Despacho Presidencial.
Soporte Técnico	Es el servicio de asesoría, capacitación, mantenimiento y reparación que brinda la OTI a los usuarios del Despacho Presidencial (ver definición de "usuario"), en forma presencial o remota, mediante comunicaciones telefónicas, por correo electrónico o por cualquier otro medio de comunicación institucional.
Inventario Técnico	Se refiere al registro descriptivo permanente de las principales características de los recursos informáticos, según corresponda, sobre el cual se basará la planificación, programación, adquisición y control de los mismos.
Usuario	Es la persona a quien se le ha asignado un recurso informático, asumiendo con ello la responsabilidad del mismo, debiendo dar cuenta ante la OTI y la Oficina de Abastecimiento, sobre cualquier circunstancia que amerite actividades de soporte técnico o el desplazamiento del equipo para su reparación, mantenimiento u otro que corresponda. Los usuarios son todos los empleados y adicionalmente todas aquellas personas que por la naturaleza de su función requieren usar temporalmente recursos informáticos. Previamente son identificados por la Oficina de Recursos Humanos, y la asignación es autorizada por la Unidad Orgánica en donde desarrollará sus actividades.

Artículo 7º Uso de los recursos informáticos para fines institucionales

7.1. Los recursos informáticos asignados a los usuarios, serán utilizados para la realización de actividades referidas a los fines institucionales, conforme a la presente Directiva y en concordancia con la directiva vigente para la Administración de los Bienes Muebles del Despacho Presidencial.

7.2. Los usuarios se encuentran prohibidos de utilizar o permitir que un tercero utilice los recursos informáticos que se les ha asignado, para fines distintos a los institucionales.

CAPÍTULO III

DISPOSICIONES ESPECÍFICAS

Artículo 8º Solicitud de Recursos Informáticos

8.1. La asignación de recursos informáticos será solicitada utilizando el Formulario de Solicitud de Recursos Informáticos **Anexo N°01**, el cual debe ser entregado a la OTI debidamente llenado por el Órgano o Unidad Orgánica solicitante.

8.2. El Formato de Solicitud debe estar firmado por el solicitante y autorizado por el Jefe del Órgano y/o Unidad Orgánica, con su respectiva firma y sello.

8.3. El Jefe del Órgano o Unidad Orgánica, puede solicitar se le asigne algún recurso informático temporalmente en el marco del cumplimiento de sus funciones en el Despacho Presidencial. En este caso deberá remitirse el Anexo N°01 consignando los datos del empleado que asumirá la responsabilidad del recurso informático así como el período de vigencia del usuario temporal solicitado.

8.4. Toda entrega de un recurso informático al usuario debe constar en el "Acta de Entrega" emitida por el Área de Control Patrimonial de la Oficina de Abastecimiento. Para ello, cuando la OTI asigne un equipo informático, comunicará al Área de Control Patrimonial los datos a considerar en la citada Acta, la que debe ser suscrita por un representante del área de control patrimonial, el usuario y contar con el visto bueno de un representante de la OTI.

El usuario a quien se le haya asignado un recurso informático, sea de hardware o software, se hace automáticamente responsable del correcto uso del mismo, a fin de garantizar el adecuado funcionamiento de los recursos asignados.

8.5. El Jefe del Órgano o Unidad Orgánica, no puede delegar la facultad para solicitar la asignación de recursos informáticos, a que se refieren los numerales 8.1, y 8.2 y 8.3 que anteceden, con excepción de la Secretaría General, cuyos requerimientos podrán ser efectuados por la Subsecretaría General, y de las Vicepresidencias por quien designe formalmente.

Artículo 9º Entrega e Instalación de Equipos Informáticos

9.1. Tratándose de equipos informáticos, su entrega incluye también la respectiva instalación a cargo del personal de la OTI. El usuario a quien se asigne el equipo está prohibido de participar en dicha instalación, salvo cuando tenga que ingresar algún dato confidencial durante la instalación.

9.2. La instalación de software o modificación de configuraciones de recursos informáticos, no realizadas y/o autorizadas por la OTI quedan bajo responsabilidad del usuario a quien se le asignó el recurso informático, quien asumirá las consecuencias que se deriven de dicha acción.

9.3. Las computadoras, laptops, tablets, impresoras y scanner se entregarán completamente operativas, incluyendo únicamente el software y hardware permitido y autorizado por la OTI y los sistemas de información solicitados en Anexo N° 01.

Artículo 10º Uso de los Equipos Informáticos

10.1. El usuario y clave gestionado con el Anexo N°01 es personal e intransferible y sólo deberá ser utilizada por el usuario del equipo, quien será el único responsable de su confidencialidad.

10.2. Para acceder a un equipo informático ante necesidad justificada y ausencia del usuario del equipo, es necesario que el Jefe del Órgano o Unidad Orgánica, envíe una solicitud formal dirigida al Director de la OTI, para que autorice el acceso con la cuenta y clave del usuario administrador que posee el área de soporte técnico para el acceso respectivo.

Artículo 11º Uso de los accesos a la Red Institucional

11.1. La OTI proporcionará acceso a la red institucional únicamente a los usuarios que lo hayan solicitado mediante el Formulario de Solicitud de Recursos Informáticos **Anexo N°01**, firmado por el Jefe del Órgano o Unidad Orgánica. Para dicho acceso, se le asignará un "nombre de cuenta de usuario", el mismo que se forma con la primera letra de su primer nombre, seguido del primer apellido del usuario o del segundo apellido en caso de existir una cuenta previamente creada.

11.2. Para la creación de usuarios de red, correo electrónico, base de datos y demás servicios informáticos, la OTI, deberá validar previamente los datos personales y el código del empleado solicitante a través del sistema de personal de Recursos Humano.

11.3. El acceso a la red institucional y/o servicios informáticos (tales como sistemas institucionales, correo electrónico, internet, intranet, etc.), será dado de baja, a pedido del Jefe del Órgano o Unidad Orgánica, mediante el formato de entrega de cargo, o cuando la Oficina de Recursos Humanos comunique el cese de un determinado usuario.

11.4. La Oficina de Recursos Humanos deberá comunicar a la Oficina de Tecnologías de la Información, por documento y/o correo electrónico, sobre el goce de vacaciones, licencias, cese o cualquier otra circunstancia que determine la ausencia de un usuario, detallando como mínimo los datos completos del personal y el período de ausencia (según aplique), en un plazo de 48 horas previos a la suspensión de labores, a fin de que se desactive el acceso a red y demás servicios informáticos.

11.5. El acceso a la red institucional a través de las computadoras y laptops tiene como mecanismo de seguridad lógica el uso de una clave con una longitud mínima de 8 caracteres alfanuméricos y de 14 como máximo, se deberá utilizar mayúsculas, minúsculas y números. No está permitido el uso de claves en blanco para usuarios.

Al quinto intento fallido utilizando una contraseña incorrecta, quedará bloqueado el acceso a la Red institucional para el usuario a quien pertenece dicha contraseña. El bloqueo podrá levantarse previa solicitud formal del responsable de la cuenta.

11.6. La Clave de acceso a la Red institucional deberá ser cambiada por los mismos usuarios cada 60 días. Esta medida de seguridad ha sido programada para que dicho cambio sea solicitado a cada usuario en forma automática.

Además, cuando transcurra más de 15 minutos de inactividad del usuario en el computador, se activará un protector de pantalla para evitar el acceso no autorizado, la misma que será desactivada ingresando su clave de acceso a la red institucional.

Artículo 12°.- Uso de Directorios compartidos de la Red Institucional

12.1. En la red existen 3 tipos de Carpetas: Personales, Grupales y de Aplicativos, teniendo cada una de ellas funciones diferentes. La información de estas carpetas será respaldada y resguardada semanalmente en el proceso de Backup ejecutado por la OTI.

a) **Las carpetas Personales:** Unidad "H" (unidad de red generada de manera automática a todos el personal del DP con acceso a perfil de usuario) su función es almacenar los archivos de los usuarios, cuyo tipo de información son considerados alta o medianamente crítica, esta información sólo podrá ser accedida por el propio usuario y en la cuota que establezca la OTI en base a la disponibilidad de recursos de almacenamiento.

b) **Las carpetas Grupales:** Unidad "G" (unidad de red generada para uso del personal del DP) su función es almacenar archivos de interés del área de trabajo del Usuario, esta información podrá ser accedida por el propio usuario y por todos los colaboradores los cuales indique el Jefe del Órgano o Unidad Orgánica, y en la cuota que establezca la OTI en base a la disponibilidad de recursos de almacenamiento.

c) **Las carpetas Aplicativos:** Unidades "F", "I", "J", "M", "N", "O", "P", "Q", "R", "S", "T", "U", "W", "X" y "Z", estas unidades son de uso exclusivo para el almacenamiento de los archivos ejecutables de los Sistemas Informáticos Institucionales del Despacho Presidencial, por lo que está prohibido la copia de archivos de tipo Personales y Grupales en estas unidades, cualquier archivo que fuese ingresado en estas unidades, será eliminado automáticamente.

12.2. En el caso de archivos cuyo contenido sea reservado, los usuarios deberán almacenarlos en la propia computadora personal (Generar un carpeta en la partición del disco de la PC, comúnmente es la unidad "D"), debiendo abstenerse de copiarlos en los Directorios Grupales.

12.3. Está prohibido copiar a la Red institucional archivos de entretenimiento, como videos, música, etc., que no guarden relación con las funciones del Despacho Presidencial, estos tipos de archivos serán restringidos automáticamente, salvo autorización expresa del Jefe del Órgano o Unidad Orgánica, a donde pertenezca el usuario.

Artículo 13° Uso de Correo Electrónico Institucional

13.1. La OTI proporcionará acceso al correo electrónico institucional únicamente a los usuarios que lo hayan solicitado mediante **Anexo N°01** suscrito por el Jefe del Órgano o Unidad Orgánica. Para ello, se le asignará un "nombre de cuenta de usuario", el mismo que se forma con la primera letra de su primer nombre, seguido del primer apellido del usuario o del segundo apellido en caso de existir una cuenta previamente creada.

13.2. Los usuarios a quienes se ha asignado una cuenta de correo electrónico institucional, son responsables de todas las actividades que se realizan con dichas cuentas. La contraseña de correo electrónico es confidencial, personal e intransferible, bajo responsabilidad del usuario.

13.3. El nombre de la cuenta de correo electrónico institucional es el mismo del usuario de red (11.1) y está ligado con el símbolo "@" al nombre del dominio "presidencia.gob.pe".

13.4. Los usuarios deben mantener activo permanentemente el correo electrónico y conectarse, como mínimo, una vez al día, para leer los mensajes, comunicados o cualquier tipo de notificación institucional, debiéndose presumir su lectura y conocimiento por el titular del correo a partir de las 24 horas del día hábil siguiente de la recepción del mensaje correspondiente, salvo excepciones debidamente justificadas.

13.5. El uso de las opciones de confirmación de entrega y lectura, deberá restringirse a mensajes de alta importancia, a fin de evitar excesos de tráfico en la red institucional. El correo electrónico sólo debe ser utilizado como una herramienta de comunicación e intercambio de información oficial. Los usuarios deben evitar que los archivos adjuntos superen los 10 Mb, por motivos de mantener un adecuado desempeño de la red institucional y disponibilidad de espacio de almacenamiento institucional.

13.6. La capacidad de almacenamiento para cada casilla de correo electrónico o cuota de espacio, está definida por tipos de usuarios: General (512 Mb), Director General/Director/Asesor Director (3 Gb), Alta Dirección / Asesores Alta Dirección (9 Gb); para evitar su saturación, el usuario debe de eliminar permanentemente los mensajes de correo innecesarios y/o generar copias locales de los correos de mayor antigüedad en cuyo caso puede solicitar por documento y/o correo electrónico el soporte técnico de la OTI.

13.7. Las copias locales de correo electrónico, se encontrarán siempre a disposición del usuario en tanto su almacenamiento se realiza en el disco duro de su computadora (Unidad "D").

13.8. El uso del correo electrónico es solo para fines laborales, está totalmente prohibido su utilización para envío de cadenas de correo electrónico, spams, archivos de entretenimiento, música, videos, imágenes, entre otros, salvo que las necesidades y naturaleza del servicio justifique su uso.

13.9. El correo electrónico es otro de los medios utilizados en el DP para intercambiar o comunicar alguna indicación, recomendación, instrucción o disposición, sobre aspectos técnicos, administrativos u operativos, de competencia del emisor.

13.10. Los usuarios deberán ser cautelosos en la recepción de cualquier correo electrónico con remitentes y archivos adjuntos desconocidos, llámese archivos con extensión .exe, .com, .pif, .tif, entre otros, o correos electrónicos con títulos sugerentes, como "I love you", "Publicidad", "Solicitud de datos personales", entre otros. Estos tipos de correos deberán ser inmediatamente notificados por documento y/o correo electrónico a la OTI, para proceder con el bloqueo correspondiente.

13.11. El número máximo de destinatarios permitidos por cada correo electrónico enviado es de 20 cuentas por vez; un número superior al indicado generaría un alto congestionamiento de la red institucional y podría ser considerado externamente como correo no deseado.

13.12. Ante la necesidad oficial del envío de mensajes masivos que superen el número de destinatarios indicados, corresponde que el Jefe del Órgano o Unidad Orgánica, que lo requiera, lo solicite mediante **Anexo N°1** siendo responsable de su supervisión y en coordinación con la Oficina de Tecnologías de la Información.

13.13. La autofirma en el correo electrónico se encuentra establecida en la Directiva "Lineamientos para la Generación de Documentos Oficiales del Despacho Presidencial" vigente.

PERÚ | Despacho Presidencial

Nombre y Apellidos (Calibri 10)
Cargo que desempeña (Calibri 10)
Órgano, unidad orgánica y/o área funcional (Calibri 10)
Telf.: (511) 311-3900 - Anexo xxx (Calibri 10)

13.14. El usuario debe aceptar que será responsable por los daños y perjuicios que pudieran ocasionarse al Despacho Presidencial como consecuencia de cualquier infracción de confidencialidad del usuario.

13.15. Los usuarios que por fines laborales tengan acceso a los buzones de correo electrónico, se comprometen a cumplir con la obligación de secreto y confidencialidad respecto del contenido de éstos, para lo cual firmarán, por intermedio de ORH, una declaración jurada de compromiso explícito respecto a los asuntos o información de carácter reservado. Asimismo, el envío de información institucional a cuentas de correo no pertenecientes a entidades del Estado, deberán ser autorizadas y/o sustentadas previamente ante el Jefe del Órgano o Unidad Orgánica en que se desempeña.

13.16. Constituye infracción administrativa funcional, pasible de sanción administrativa, las siguientes acciones en el uso del correo electrónico oficial:

a) Facilitar u ofrecer la cuenta y/o buzón del correo electrónico a terceras personas.

b) Suscribirse por Internet a listas de envío de correos electrónicos globales ajenas a la función institucional

c) Utilizar el correo electrónico institucional para cualquier propósito comercial o financiero ajeno a la institución.

d) El envío y recepción de mensajes que comprometan la información del Despacho Presidencial, y/o violen las leyes del Estado Peruano, sin perjuicio de la responsabilidad penal, civil o administrativa a que hubiere lugar.

13.17. El acceso web al correo y/o configuración en dispositivo móvil será atendido previa solicitud conforme lo precisado en el numeral 13.1, y genera las mismas responsabilidades que el correo en versión local para el usuario.

Artículo 14° Uso de Internet

14.1. La Subsecretaría General, a través de la Oficina de Tecnologías de la Información, es la encargada de administrar el servicio de acceso a internet de acuerdo a las normas y políticas que se encuentren vigentes.

14.2. El Despacho Presidencial destina el servicio de acceso a internet para consultar información e interactuar con sitios web que ayuden a realizar las actividades laborales en forma más eficiente y eficaz. Promoviendo la investigación en temas que estén relacionados con las actividades institucionales.

14.3. La asignación de cuentas para el acceso a internet inalámbrica (WIFI) deberán contar con la autorización del Jefe del Órgano o Unidad Orgánica, a la que pertenezca el usuario, el cual se hace responsable del uso adecuado del mismo, accediendo a información relacionada con las funciones que cumple en la Entidad. El usuario se hace responsable de la confidencialidad de la clave que se le brinde para acceder al WIFI institucional.

14.4. Se encuentra bloqueado el acceso a ciertas categorías de páginas web como las de contenido obsceno o de sexo explícito, música, video, redes sociales, juegos, apuestas, glamour y otros de tipo de entretenimiento que establezca la Subsecretaría General a propuesta de la OTI.

14.5. Debido a la saturación que ocasiona el ejecutar los programas de radio por Internet, tanto musical como noticioso y conexiones remotas, el uso de estas funcionalidades se encuentra restringido y sólo se podrá acceder a ellos por temas relacionados a la naturaleza de su función solicitado formalmente por el Jefe del Órgano o Unidad Orgánica, donde se encuentra el usuario que requiere el acceso.

14.6. Todos los usuarios que cuenten con el servicio de acceso a Internet o WIFI, al margen del régimen de contratación están obligados a cumplir la presente directiva bajo responsabilidad de uso.

Artículo 15º Uso de Software Licenciado

15.1. En caso de que el usuario necesite un software y/o utilitario adicional, el Jefe del Órgano o Unidad Orgánica que corresponda deberá solicitarlo formalmente a la OTI, mediante el envío del Formulario de Solicitud de Instalación de Software **Anexo N°02**, la misma que evaluará el pedido, y de ser necesario procederá a la elaboración de las especificaciones técnicas y/o términos de referencia, para lo cual, debe comunicar como mínimo los siguientes datos: Nombres, apellidos, código de fotocheck del usuario a quien se asignará el software así como la respectiva justificación de uso del software solicitado.

15.2. Está terminantemente prohibido la instalación de software sin autorización de la OTI, quien deberá verificar la Licencia de software a instalar.

Artículo 16º Medidas de Seguridad Informática

16.1. Los usuarios están prohibidos de instalar directamente, en los equipos informáticos que le han sido asignados, cualquier tipo de software o dispositivo de hardware adicional (ejemplo: Llave USB, Parlantes, Cámara Digital, etc.), en los casos que ello sea necesario deberá solicitarse su instalación por documento y/o correo electrónico a la OTI.

16.2. Se encuentra prohibida la copia de archivos de música, fotografías de terceros y/o ejecutables en la computadora del usuario que no guarden relación con sus actividades, ya que el computador es un recurso facilitado por el Despacho Presidencial y debe ser usado con fines netamente laborales.

16.3. Al finalizar la jornada de labores o al retirarse del mismo, el usuario deberá apagar la computadora personal que se le ha asignado, salvo excepciones previamente coordinadas con el Jefe del Órgano o Unidad Orgánica, a la que pertenezca, conjuntamente con la OTI.

16.4. La institución cuenta con un sistema de energía eléctrica estabilizada, el cual alimenta a las tomas de corriente de color rojo de las oficinas y/o áreas de la sede principal, las que son para uso exclusivo de los equipos de cómputo, por lo que queda terminantemente prohibido conectar otro tipo de aparatos eléctricos y/o electrónicos a las mencionadas tomas.

16.5. Está prohibido conectar cualquier aparato electrónico ajeno a los equipos de cómputo en el estabilizador de voltaje (en caso se cuente con uno), el cual ha sido instalado exclusivamente para protegerlos, en las oficinas y/o áreas donde no se cuenta con energía estabilizada. Tampoco deben conectarse impresoras en el mismo estabilizador de voltaje de una PC, ya que podría rebasar la capacidad eléctrica del estabilizador.

16.6. Está prohibido pegar calcomanías o cualquier tipo de adornos en la computadora personal; salvo etiquetas de inventario o de identificación para efectos del control patrimonial.

16.7. Los usuarios están prohibidos de fumar o ingerir alimentos o bebidas, cuando se encuentren frente al teclado o cerca a orificios o rejillas de ventilación de los equipos. Cualquier desperfecto imputable a estas conductas serán de responsabilidad única del usuario y dará lugar a que se le cargue a éste el costo de reparación correspondiente, sin perjuicio de la respectiva sanción administrativa, conforme a la normatividad vigente.

16.8. Los usuarios deberán colocar correctamente y con sumo cuidado, los discos extraíbles USB, memorias externas y discos compactos en las lectoras internas de la computadora personal asignada. Estarán prohibidos de hacerlo cuando tengan conocimiento que pueden poner en riesgo el equipo o sea notorio este riesgo.

16.9. Los usuarios no deben distribuir información referida a las vulnerabilidades del sistema y deben reportar inmediatamente las alertas emitidas por el equipo de cómputo (como por ejemplo: alertas del sistema operativo Windows, como la actualización de algún componente, alertas del sistema antivirus, alertas del programa office y otros) , además de riesgos y fallas sospechosas las cuales deben ser notificadas de forma inmediata por documento y/o correo electrónico a la OTI.

16.10. No deberá moverse o reubicarse ningún equipo informático, ya sea en forma parcial o en su totalidad, sin la previa coordinación y aprobación del Jefe del Órgano o Unidad Orgánica, en coordinación con la OTI. Es de responsabilidad comunicar mediante su coordinador patrimonial del movimiento de los bienes, al área de control patrimonial de la Oficina de Abastecimiento.

16.11. En caso el traslado de equipos informáticos se realice entre locales o sedes (Palacio, Edificio y Loreto), se deberá realizar un Acta de Desplazamiento Interno, la misma que deberá ser generada por el Órgano o Unidad Orgánica usuaria en el sistema con la autorización y firma del Jefe responsable del traslado.

16.12. El personal está prohibido de abrir dispositivos y/o equipos informáticos debiendo considerar para ello única y exclusivamente al personal especializado de la OTI.

16.13. Los usuarios que tienen asignada una computadora personal son responsables de realizar el respaldo de su información local almacenada en el disco duro de su computadora, siendo responsables también de la custodia de dicho respaldo y de las consecuencias derivadas de su uso. El disco duro de las computadoras personales, será depurado cuando los usuarios hayan cesado en sus labores previa confirmación de la ORH.

16.14. Los usuarios deberán tener en cuenta los siguientes criterios a fin de elegir adecuadamente las claves:

a) Evitar utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres y apellidos (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades).

b) Evitar usar contraseñas completamente numéricas con algún significado (teléfono, DNI, etc.).

c) Las claves más seguras, en cuanto a su confidencialidad, son aquellas que combinan caracteres alfabéticos (mayúsculas y minúsculas) y números.

d) El usuario debe cambiar las claves inmediatamente luego de su primera apertura de cuenta, asignada por la OTI en el caso de los sistemas institucionales o correo electrónico.

e) Otros criterios que adicionalmente pueda recomendar la OTI.

16.15. En caso que un usuario se encuentre de vacaciones, licencia o cualquier circunstancia similar y desee acceder remotamente a los servicios informáticos, el Jefe del Órgano o Unidad Orgánica, deberá solicitarlo por documento y/o correo electrónico a la OTI a fin de que se suspenda la desactivación y se habilite el acceso remoto.

16.16. En caso que un Jefe del Órgano o Unidad Orgánica, requiera acceder a la computadora de un usuario ausente, deberá solicitarlo por documento y/o correo electrónico a la OTI, quienes accederán con el usuario "Administrador" a fin de recabar la información indicada por el solicitante, siendo este responsable por las consecuencias derivadas de su uso.

16.17. Está prohibido el retiro y/o eliminación parcial o total de la información, aplicativo o utilidad, almacenado, procesado o desarrollado mediante los recursos informáticos del Despacho Presidencial, ésta le pertenece a la entidad de manera exclusiva y excluyente.

16.18. Está prohibido permitir, a personas ajenas a la institución, que no son usuarios, que accedan a la información contenida en las computadoras de la institución.

16.19. Queda exceptuada de lo señalado en el numeral anterior la información pública, que sea solicitada por un administrador mediante un proceso administrativo de Acceso a la Información Pública, o cuando exista un mandato judicial u otra autoridad competente.

CAPÍTULO IV

DISPOSICIONES COMPLEMENTARIAS

Única. La Oficina de Tecnologías de la Información deberá difundir la presente directiva entre todos los titulares de los Órganos y Unidades Orgánicas del Despacho Presidencial, los que deberán hacerla de conocimiento del personal a su cargo.

ANEXOS.

Anexo N° 01: Formulario de Solicitud de Recursos Informáticos

Anexo N°02: Formulario de Solicitud de Instalación de Software

ANEXO N° 1: Formulario de Solicitud de Recursos Informáticos

Fecha Recepción: ___/___/___ Hora: ___:___ Ticket Nro.: _____ - _____

DESPACHO PRESIDENCIAL

Formulario de Solicitud de Recursos Informáticos

Se recibirán las fichas que cuenten con los DATOS DEL SOLICITANTE y FIRMAS DE AUTORIZACIÓN llenados completa y correctamente.

DATOS DEL SOLICITANTE:

☐ Empleado(276,728,CAS) | Destacado: ☐ Civil ☐ Policía ☐ Militar | ☐ PAC/FAG | ☐ PRACT. | ☐ OTRO _____

Nombres : _____ Apellidos : _____

*Oficina : _____ Correo Electrónico: _____@presidencia.gob.pe *(en caso de que ya cuente con uno)*

*Cargo / Función: _____ Anexo: _____ * Código Fotocheck: ☐☐☐☐☐☐☐☐

** De requerir mayor precisión, gestionarlo con Recursos Humanos.*

CREACION DE USUARIO: ( ) Si ( )No

En caso de nuevo usuario : ¿Existe Físicamente un punto de Red Identificado? ( ) Si ( ) No

En caso de que ya cuente con usuario : Nombre del Equipo: _____

SERVICIOS / SISTEMAS QUE SOLICITA: *(Marcar con una "X" lo requerido)*

ACCESO A SERVICIOS					
( ) Internet	( ) Cuenta de correo	( ) Usuario WIFI	( ) SIAF	( ) SIGA MEF	( ) SPIJ

( ) Creación de unidad de Red	Nombre de la Unidad de Red: ..... *(si conoce la ruta, indíquela)* Letra de Unidad: ..... *(si conoce la letra, indíquela)*
( ) Acceso a unidad de red	Indique el tipo de acceso : [ ] Lectura [ ] Escritura

Tipo de Perfil	Accesos
( ) Jefe	*Perfil que puede registrar, aprobar y enviar en todos los sistemas masivos (trámite documentario, movilidades, viáticos, SIAD, etc.).*
( ) Accesos delegado de Jefe	*Perfil que puede registrar en todos los sistemas masivos y aprobar en nombre del Jefe en los sistemas que seleccione a continuación:* ( ) Tramite Documentario ( ) Papeletas de Personal FUT ( ) Orden de Trabajo ( ) Solicitud de Movilidad ( ) Autorización de Ingreso de Visitas ( ) Notas de Alimentos ( ) Viáticos ( ) Bienes Asignados
( ) Registrador de Oficina	*Perfil que puede registrar en todos los sistemas masivos que seleccione a continuación:* ( ) Tramite Documentario ( ) Papeletas de Personal FUT ( ) Orden de Trabajo ( ) Solicitud de Movilidad ( ) Autorización de Ingreso de Visitas ( ) Notas de Alimentos ( ) Viáticos ( ) Bienes Asignados
Otros Sistemas:	....

Reconozco que, como USUARIO de los servicios y recursos informáticos del Despacho Presidencial, tendré acceso a datos e información privilegiada, los cuales, mantendré protegidos. Reconozco mi responsabilidad en el uso de mis accesos a la información de la Institución, incluyendo el uso de software legal o autorizado y del equipamiento para procesar o generar información, para fines propios de mis funciones o autorizados por la Institución. Mantendré y protegeré mi "password", dándole un uso exclusivamente propio. Seré responsable de dar cumplimiento a los puntos indicados en la Directiva de Política de Seguridad Informática vigente. Asimismo declaro conocer que la violación de la Ley N°27588, implicará la transgresión del principio de la buena fe y será sancionada con mi inhabilitación para prestar servicios al estado, sin perjuicio de las acciones administrativas civiles y penales con los que proceda la Institución.

FIRMAS DE AUTORIZACIÓN:

Firma del Solicitante

Jefe de Orgánico o Unidad Orgánica
Nombre completo, Firma, Sello

/ / Fecha

PARA SER LLENADO POR LA OFICINA QUE ATIENDE EL REQUERIMIENTO:

N°	Acción	Detalle / Observación[1]	Fecha y Hora de Atención	Atendido Por[2]
1	Creación de cuenta de red		/ / ___:___	
2	Creación de cuenta de correo		/ / ___:___	
3	Configuración de Sistemas		/ / ___:___	
4	Instalación en Equipo		/ / ___:___	

(1) Incluye Datos de la Cuenta, Sistema y Equipo (2) Incluye Datos del Personal

Form001_DP_OTI_V1

ANEXO N° 2: Formulario de Solicitud de Instalación de Software

Fecha Recepción: ____/____/____ Hora: ____:____ Ticket Nro.: ____ - _____

DESPACHO PRESIDENCIAL

Formulario de Solicitud de Instalación de Software

Se recibirán las fichas que cuenten con los DATOS DEL SOLICITANTE y FIRMAS DE AUTORIZACIÓN llenados completa y correctamente.

DATOS DEL SOLICITANTE:

* ☐ Empleado(276,728,CAS) | Destacado: ☐ Civil ☐ Policía ☐ Militar | ☐ PAC/FAG ☐ PRACT. ☐ OTRO _____

Nombres: _____ Apellidos: _____

* Oficina: _____ Correo Electrónico: _____@presidencia.gob.pe *(en caso de que ya cuente con uno)*

* Cargo / Función: _____ Anexo: _____ * Cod. Fotocheck: ☐☐☐☐☐☐☐☐

** De requerir mayor precisión, gestionarlo con Recursos Humanos.*

Tipo de Instalación Requerida:

☐ Por Evaluación ☐ Para uso Oficial ☐ Por Adquisición ☐ Software Libre ☐ Software Propietario

EL USUARIO SOLICITANTE MANIFIESTA TENER CONOCIMIENTO:

Que, en cumplimiento del Decreto Supremo N° 013-2003-PCM, la Directiva de Política de Seguridad Informática, vigente indica que en caso de que el usuario necesite un software y/o utilitario adicional, el Jefe de Órgano o Unidad Orgánica que corresponda deberá solicitar formalmente a la OTI, mediante el envío del presente formulario. También reconozco que, como USUARIO de los servicios y recursos informáticos del Despacho Presidencial tendré acceso a muchos datos e información, la cual debe ser protegida. Por consiguiente, reconozco, mi responsabilidad en el uso de software ilegalmente instalado.

FIRMAS DE AUTORIZACIÓN:

Firma del Solicitante	Jefe de Órgano o Unidad Orgánica Nombre completo, Firma, Sello	/ / Fecha

CODIGO PATRIMONIAL DE LA PC: ☐☐☐☐☐☐☐☐☐☐☐☐

SOFTWARE REQUERIDO A INSTALAR

Descripción	Periodo de Uso	Funcionalidad	VoBo

PARA SER LLENADO POR EL AREA DE SOPORTE TECNICO

Usuario: _____ Fecha Instalación: ____/____/____ Atendido por: _____

Form002_DP_OTI V1