

**"USO CORRECTO DE LOS EQUIPOS DE CÓMPUTO Y SERVICIOS DE RED,
INTERNET Y CORREO ELECTRÓNICO INSTITUCIONAL EN
EL MINISTERIO DEL INTERIOR"**

I. OBJETO

Establecer las obligaciones y responsabilidades para el uso correcto de los equipos de cómputo y Servicios de Red, Internet y Correo electrónico institucional en el Ministerio del Interior (MININTER).

II. FINALIDAD

La presente norma tiene por finalidad optimizar el uso de los equipos de cómputo y los Servicios de Red, Internet y Correo Electrónico institucional garantizando la integridad de la red y equipos del Ministerio del Interior, así como su uso eficiente.

III. ALCANCE:

La presente Directiva es de cumplimiento obligatorio, bajo responsabilidad, para los funcionarios, servidores y personal en general de los Órganos Policiales y no Policiales del Ministerio del Interior a nivel nacional.

IV. BASE LEGAL:

1. Decreto Legislativo N° 276, "Ley de Bases de la Carrera. Administrativa y de Remuneraciones del Sector Público".
2. Ley N° 29334, "Ley de Organización y Funciones del Ministerio del Interior."
3. Ley N° 27444 y sus modificatorias, "Ley del Procedimiento Administrativo General."
4. Ley N° 27309, "Ley que incorpora los Delitos Informáticos al Código Penal".
5. Ley N° 27269, "Ley de Firmas y Certificados Digitales".
6. Decreto Supremo N° 052-2008-PCM, "Reglamento de la Ley de Firmas y Certificados Digitales."
7. Decreto Supremo 004-2005-IN y sus modificatorias, que aprueba el "Reglamento de Organización y Funciones del Ministerio del Interior".
8. Decreto Supremo N° 066-2001-PCM, que aprueba los "Lineamientos de Políticas Generales para promover la masificación del acceso a Internet en el Perú."
9. Decreto Supremo N° 005-90-PCM, "Reglamento de la Ley de Bases de la Carrera Administrativa y de Remuneraciones."
10. Directiva N° 005-2003-INEI/DTNP, "Normas para el uso del correo electrónico en las entidades de la Administración Pública."
11. Resolución Ministerial N° 1646-2004-IN-0301 que aprueba la Directiva N° 009-2004-IN-0305 sobre "Lineamientos para la formulación, aprobación y modificación de Directivas en el Ministerio del Interior".



V. DISPOSICIONES GENERALES

1. Los equipos de cómputo y los servicios de red, Internet y correo electrónico institucional deben emplearse para las actividades directamente relacionadas con el cumplimiento de las funciones en la institución.

En cumplimiento de lo señalado en el párrafo precedente, ningún usuario podrá descargar música, vídeos, juegos o cualquier otro programa procedente de Internet, ni instalarlos, actualizarlos o copiarlos de cualquier fuente, ni almacenar fotos que superen 5GB, ni acceder a lugares que incluyan material pornográfico o material en perjuicio de terceros.

No está permitido el envío de mensajes a foros de discusión (listas de distribución y/o newsgroups), por ponerse en riesgo la información de la institución.

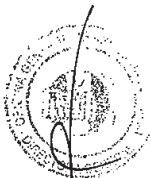
2. La Oficina General de Informática y Telecomunicaciones - OFITEL- es la encargada de la administración de los servicios de red, Internet y correo electrónico y otorga el acceso a dichos servicios, conforme a las necesidades específicas de cada usuario de los Órganos No Policiales. Así mismo supervisa a DIRTEL PNP en la administración de los servicios de red, Internet y correo electrónico y acceso a dichos servicios en los Órganos Policiales.
3. El usuario deberá utilizar la cuenta que le ha sido asignada para tener acceso a los servicios de red, Internet y correo electrónico. Es responsable de proteger y no olvidar su contraseña. En caso de olvido el computador no permitiera su acceso, solicitará la asesoría de OFITEL O DIRTEL PNP SEGÚN CORRESPONDA.
4. La Oficina de Personal y la Dirección de Recursos Humanos PNP, o quien haga sus veces, comunicará a OFITEL y/o la DIRTEL PNP la relación de trabajadores que hayan dejado de laborar en la entidad para la desactivación de la cuenta correspondiente.

Asimismo, el Jefe ó Director General de la respectiva Unidad u Oficina podrá solicitar a OFITEL O DIRTEL PNP según corresponda, el procedimiento de Backup de la información contenida en el equipo asignado al usuario, en forma física y digital, en medio magnética (CD, DVD) según sus necesidades.

5. OFITEL y DIRTEL PNP garantizan la privacidad de las cuentas de correo electrónico institucional de todos los usuarios, conforme a los códigos de ética profesional pertinentes en el manejo de la información contenida en los equipos de cómputo y obtenida a través de los servicios de red, Internet y correo electrónico.
6. La información contenida en las computadoras y los mensajes de correo electrónico no podrán reproducirse o utilizarse para fines ajenos a las funciones del usuario en la institución.
7. Los usuarios son responsables exclusivos de la información obtenida de Internet, del contenido de los mensajes enviados a través de Internet, así como de los enviados a través de su cuenta de correo electrónico institucional. Para dichos efectos, deberán extremar medidas



J. Suárez N.



M. E. JUSCAMA

de seguridad a fin de que otras personas no hagan uso o se adueñen de su usuario y/o password.

8. Los usuarios deben abstenerse de utilizar el acceso de otra persona, intentar apoderarse de las contraseñas de sus compañeros o intentar burlar los sistemas de seguridad.
9. A efectos de que se tomen las medidas correctivas y administrativas pertinentes, OFITEL ó DIRTEL PNP según corresponda informará al Jefe Inmediato del usuario infractor, cualquier contravención a la presente Directiva que detecte.

VI DISPOSICIONES ESPECÍFICAS

1. Acceso a los Servicios de Red, Internet y Correo Electrónico Institucional

- 1.1 El acceso a los servicios es solicitado por el titular del órgano correspondiente, mediante documento escrito, dirigido a OFITEL ó a DIRTEL PNP, de ser el caso, de conformidad al ANEXO 1 de la presente norma.
- 1.2 Para la creación del usuario (login) se utiliza la primera letra del primer nombre y el apellido paterno. En caso de coincidir con el de otro usuario, se considerará la letra inicial del segundo apellido materno y a su vez la segunda letra del apellido materno, si fuese necesario.
- 1.3 El usuario será ingresado a la cuenta Ministerio (para el Órgano no Policial), así como a la cuenta de grupo de oficina al que pertenece. Para los usuarios del Órgano Policial se le ingresará al grupo de cuenta donde pertenecen.
- 1.4 La comunicación de la contraseña se realizará de forma personal o vía teléfono, la misma que deberá ser cambiada inmediatamente por el usuario.
- 1.5 Para elegir una contraseña, se recomienda lo siguiente:
 - 1.5.1 Difícil de adivinar: Elegida aleatoriamente de un conjunto suficientemente grande como para evitar la identificación como consecuencia de una búsqueda exhaustiva.
 - 1.5.2 Secreta: Conocida solo por su dueño.
 - 1.5.3 Tener al menos seis caracteres.
 - 1.5.4 Tener una mezcla de letras, dígitos y/o signos de puntuación.
 - 1.5.5 No consistir en: el número de cuenta o login, número de DNI, placa del automóvil o palabras escritas al revés.
 - 1.5.6 Usar combinaciones de palabras cortas no relacionadas con uno o más signos de puntuación (rosa\$vela, city%%vidrio), palabras con dígitos insertados (avEN213ida, in80util), acrónimos, (EuDIImdCnnQa (en un lugar de la mancha de cuyo nombre no quiero acordarme), errores ortográficos (=olgasan), consonantes y vocales alternados en forma pronunciable pero sin sentido (bedugale, tuponsiga).
 - 1.5.7 Evitar usar el mismo password para dos sistemas distintos.



J. Suárez N.



- 1.5.8 Mantener siempre deshabilitada la opción de los navegadores Web que ofrecen recordar su password para su próxima visita a una página.

2. Uso de los Equipos de Cómputo

- 2.1 La Oficina de Control Patrimonial o quien haga sus veces, remitirán periódicamente (mensualmente), el registro de todos los equipos de cómputo de propiedad del Ministerio del Interior a la OFITEL o DIRTEL PNP de ser el caso.
- 2.2 Los usuarios deben brindar un uso adecuado a las computadoras que se les asigne, con el objeto de evitar su deterioro. El usuario es responsable del cuidado físico de los equipos que se le asigna.
- 2.3 En virtud de lo señalado en el numeral precedente, los usuarios se encuentran prohibidos de:
- Pegar stickers en las computadoras.
 - Ingerir alimentos sobre las computadoras, así como colocar y/o manipular líquidos en su cercanía.
 - Rociar sobre las computadoras líquidos ambientadores.
 - Fumar cerca de las computadoras.
 - Colocar y/o apilar documentos u otros objetos sobre las computadoras y en ubicaciones que obstruyan o impidan su adecuada ventilación y uso.
 - Ubicar el CPU en una posición distinta a su diseño original (horizontal o vertical).
 - Dejar los equipos portátiles (laptop) y sus accesorios, en lugares inseguros.
 - Conectar artefactos eléctricos sobre la línea eléctrica estabilizada de uso exclusivo para las computadoras o sobre los estabilizadores de corriente.
 - Instalar programas informáticos en las computadoras.
 - Utilizar protectores de pantalla para los monitores que atente contra la moral o las buenas costumbres o que pueda resultar ofensivo.
 - Modificar los parámetros o configuración de las computadoras, así como el software y/o sistema informático instalado.
 - Abrir las computadoras, así como extraer o cambiar componentes.
 - Cualquier otro uso no autorizado y que ponga en riesgo la integridad y/o funcionalidad de los equipos.
- 2.4 La instalación, reubicación, reasignación y cualquier movimiento de equipos de cómputo en la entidad deberá ser realizado en coordinación con OFITEL o DIRTEL PNP, de ser el caso.



3. Uso del Servicio de Correo Electrónico

- 3.1 El uso del correo electrónico institucional queda establecido como medio oficial de envío y recepción de información y documentación de la institución, una vez que se hayan cumplido con los procedimientos establecidos por las normas legales pertinentes para dicho fin.

- 3.2 Los usuarios que tienen asignada una cuenta de correo electrónico institucional deben mantener en línea el software de correo electrónico y activada la opción de avisar cuando llegue un nuevo mensaje; o conectarse al correo electrónico con la mayor frecuencia posible para leer sus mensajes.
- 3.3 Los mensajes innecesarios deben ser permanentemente eliminados, debiendo mantenerse los mensajes en carpetas personales.
- 3.4 En caso de recibir un mensaje que se considere ofensivo, se debe reenviar al Administrador de correo electrónico, con el fin que se puedan tomar las medidas pertinentes.
- 3.5 Utilizar siempre el campo "asunto" con el fin de resumir el tema del mensaje.
- 3.6 Enviar mensajes formateados, de ser posible y evitar el uso de letras mayúsculas.
- 3.7 Para el reenvío de un mensaje, incluir el mensaje original, para que el destinatario conozca el contexto en el que está dado el mensaje que recibe.
- 3.8 Niveles aplicables para la recepción y envío de archivos:

NIVEL A: Alta Dirección, Directores Generales y funcionarios de nivel equivalente. Envío y recepción de mensajes hasta 10.0 Mb o su equivalente de 10240 Kb.

NIVEL B: Directores, Sub Directores, Jefes de Unidad y funcionarios de nivel equivalente. Envío y recepción de mensajes hasta 5.0 Mb o su equivalente de 5120 Kb.

NIVEL C: Profesionales, Técnicos, Secretarias, Auxiliares y Practicantes. Envío y Recepción de Mensajes hasta 2.0 Mb o su equivalente de 2048 Kb.

NIVEL D: Acceso específico, este nivel contará para el Envío y Recepción de Mensajes, el tamaño de acuerdo a la necesidad de casos especiales sustentados.



VI. DISPOSICIONES COMPLEMENTARIAS

1. RESPONSABILIDAD DE OFITEL Y DIRTEL PNP.

OFITEL y DIRTEL PNP, conforme a sus competencias funcionales, adopta, propone y/o coordina las medidas pertinentes, a fin de garantizar la integridad y el correcto funcionamiento de los equipos y de los servicios de red, Internet y correo electrónico del Ministerio del Interior. Dichas medidas comprenden, pero no se limitan a:

- 1.1 Efectuar el mantenimiento preventivo y correctivo de los equipos de cómputo, la conservación de su instalación, la verificación de la seguridad física, así como su acondicionamiento. El personal técnico de las diferentes Direcciones Generales, harán esa función

coordinando permanentemente e informando semestralmente sobre el estado general de los servicios de red, Internet y correo electrónico a la Oficina General de Informática y Telecomunicaciones del MININTER o DIRTEL PNP, según corresponda.

- 1.2 Realizar la actualización de los equipos de cómputo, a fin de conservar e incrementar la calidad del servicio que se prestan.
- 1.3 Proveer de la infraestructura de seguridad adecuada en atención a los requerimientos específicos de cada área.
- 1.4 Establecer las disposiciones pertinentes para el acceso a áreas críticas (centros de cómputo) y uso de equipos cuya misión es crítica (información clasificada), así como para el registro del tráfico de personal en dichas áreas, teniendo en cuenta las situaciones de emergencia o de urgencia manifiesta.
- 1.5 Acceder a cualquier equipo de cómputo conectado a la red, que no sea de propiedad de la institución, a fin de garantizar la seguridad de los sistemas operativos.
- 1.6 Proporcionar el servicio de acceso remoto (fuera del centro laboral) a personal autorizado y establecer las disposiciones complementarias pertinentes para salvaguardar la integridad de la red.
- 1.7 Efectuar el monitoreo constante de las tecnologías de Internet e intranet, así como de los sistemas considerados críticos.
- 1.8 Controlar el acceso a la red e Internet, restringiendo el acceso al usuario que contravenga las normas contenidas en la presente Directiva.
- 1.9 Implementar herramientas que filtren y limiten aquellos contenidos y servicios que se ofrecen en Internet, que puedan atentar contra el buen desempeño de los usuarios, la moral, entre otros.
- 1.10 Mantener instalados software antivirus licenciados en todos los equipos de cómputo y en especial en aquellos donde se han instalado cuentas de Internet, correo electrónico y sistemas informáticos.
- 1.11 Coordinar, evaluar y proponer las medidas pertinentes para solucionar los problemas informáticos correspondientes.

2. El personal técnico responsable de cada Dirección: DIGEMIN, DIGIMIN, DICSCAMEC y DGGI coordinaran permanentemente e informarán semestralmente sobre el estado general de los servicios de red, Internet y correo electrónico a la Oficina General de Informática y Telecomunicaciones del MININTER ó DIRTEL PNP, según corresponda.

3. GLOSARIO INFORMATICO

Para efectos de la presente Directiva, se entenderá por:

- i. **ANTIVIRUS:** Programa cuya finalidad es prevenir los virus informáticos así como curar los ya existentes en un sistema. Estos programas deben actualizarse periódicamente.



M. E. JORDANAGA



J. Suárez N.

- ii. **CORREO ELECTRÓNICO:** El correo electrónico o e-mail, es el medio por el cual se pueden intercambiar mensajes utilizando un dispositivo electrónico.
- iii. **INTERNET:** Es una gran comunidad de computadoras conectadas entre sí por medio de líneas de comunicaciones especiales.
- iv. **INTRANET:** Es una red privada que utiliza tecnología de Internet pero cuyo contenido sólo está disponible al interior de una entidad.
- v. **LOGIN:** Clave de acceso que se le asigna a un usuario con el propósito de que pueda utilizar los recursos de una computadora. El login define al usuario y lo identifica dentro de Internet junto con la dirección electrónica de la computadora que utiliza.
- vi. **NAVEGADOR:** Es un programa que provee una interface para acceder y ver archivos en Internet.
- vii. **RED:** Network en inglés. Sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en lugares más o menos próximos. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.
RED DE ACCESO: Conjunto de elementos que permiten conectar a cada usuario con la red central de la que depende.
- viii. **SOFTWARE:** Conjunto de programas, documentos, procesamientos y rutinas asociadas con la operación de un sistema de computadoras, es decir, la parte intangible o lógica de una computadora.



ANEXO 1

FORMATO DE OFICIO PARA LA CREACION O CANCELACION DE CUENTAS DE USUARIO PARA LOS ACCESOS A LOS SERVICIOS DE RED, INTERNET Y CORREO ELECTRONICO EN EL MININTER

Lima,

OFICIO N° 2009-IN-XXXX

Señor.
Director General de OFITEL (o a quien haga sus veces)
Ministerio del Interior

Asunto: Solicita (Creación ó cancelación) de Usuario que se indica.

Es grato dirigirme a usted para saludarlo cordialmente, y a la vez solicitarle lo siguiente:

DEPENDENCIA: _____
FECHA: ____/____/____

1. DATOS PERSONALES

APELLIDOS Y NOMBRES: _____
DNI /CIP: _____
OFICINA: _____
CARGO: _____

2. SERVICIOS A SOLICITAR

RED () INTERNET () CORREO INSTIUCIONAL ()

3. NIVEL DE ACCESO

DIRECTOR GENERAL / ASESOR ()
DIRECTOR DE OFICINA ()
USUARIO ()
USUARIO SIAF ()

4. SUSTENTO DE LA SOLICITUD

DIRECTOR GENERAL SOLICITANTE



ANEXO 2

FORMATO CON LOS NIVELES DE ACCESOS PARA EL USO DE INTERNET EN EL MININTER

NIVEL DE PERMISO	CATEGORÍA DEL ACCESO O PERMISO	OBSERVACIÓN
A	<p>ACCESO ALTO CON PRIVILEGIOS Tienen acceso para la navegación en el uso del radio de noticias en línea, correo externo, mensajería, accesos ftp y tiene acceso total. DIRECTORES GENERALES Y ASESORES</p>	
B	<p>ACCESO ALTO Tienen acceso para la navegación y el correo externo. Excepto mensajería, ftp y radio. DIRECTORES Y PERSONAL AUTORIZADOS</p>	
C	<p>ACCESO MEDIO Tienen acceso para la navegación media, no tiene acceso al correo externo, ni mensajería, ni comunicación en línea (radio, videos, etc.). SOLO PÁGINAS PERMITIDAS Y AUTORIZADAS POR EL DIRECTOR DE LA UNIDAD ORGÁNICA.</p>	
D	<p>ACCESO ESPECIFICO Este nivel se le da a las cuentas con fines específicos sustentados de acuerdo a necesidades especiales.</p>	

