

INEI

Aprueban Directiva sobre “Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública

RESOLUCION JEFATURAL N° 088-2003 INEI

CONCORDANCIAS: R. N° 324-2003-SUNARP-SN

Lima, 31 de marzo de 2003

CONSIDERANDO:

Que, conforme a lo dispuesto por el Decreto Legislativo N° 604, que aprueba la Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática, concordante con su Reglamento aprobado por el Decreto Supremo N° 043-2001-PCM, el INEI es el organismo central y rector de los Sistemas Nacionales de Estadística e Informática, responsable de promover el desarrollo de sistemas y aplicaciones informáticas de uso común para el sector estatal a nivel nacional;

Que, los referidos dispositivos legales precisan que el INEI norma, supervisa y evalúa los métodos, procedimientos y técnicas estadísticas e informáticas utilizados por los Organos de los Sistemas y establece las normas y estándares nacionales para la regulación y compatibilización de los sistemas de tratamiento de la información;

Que, de acuerdo a los resultados de la IV Encuesta de Recursos Informáticos y Tecnológicos, el 80,2% de las 531 entidades públicas del país que cuentan con redes, disponen del servicio de correo electrónico;

Que, el Correo Electrónico institucional es una herramienta importante de comunicación e intercambio de información entre personas y entidades de la Administración Pública, por lo que resulta necesario promover su correcta aplicación, como recurso de comunicación intra e inter-institucional y regular su uso racional para optimizar su aprovechamiento, estableciendo procedimientos para el uso del servicio de correo electrónico en las entidades de la Administración Pública;

Estando a lo propuesto por la Dirección Técnica de Normatividad y Promoción, con la opinión favorable de la Subjefatura de Informática y visación de la Oficina Técnica de Asesoría Jurídica;

En uso de las atribuciones conferidas por el artículo 8 del Decreto Legislativo N° 604 Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática;

SE RESUELVE:

Artículo Único.- Aprobar la Directiva N° 005-2003-INEI/DTNP sobre "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública", que forma parte integrante de la presente Resolución.

Regístrese y comuníquese.

EMILIO FARID MATUK CASTRO
Jefe

DIRECTIVA N° 005-2003-INEI/DTNP

NORMAS PARA EL USO DEL SERVICIO DE CORREO ELECTRÓNICO EN LAS ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA

I. FINALIDAD

Normar los procedimientos de gestión de los servicios de correo electrónico en las entidades públicas del país.

II. OBJETIVO

Dar lineamientos para el uso correcto del servicio de correo electrónico oficial.

III. ALCANCE

La presente Directiva es de cumplimiento obligatorio por las entidades del Poder Ejecutivo, Legislativo y Judicial, Organismos Autónomos, Organismos Públicos Descentralizados, Gobiernos Regionales, Locales y Empresas Públicas a nivel nacional.

IV. BASE LEGAL

- Decreto Legislativo N° 604 - Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática.

- Decreto Supremo N° 043-2001-PCM - Reglamento de Organización y Funciones del Instituto Nacional de Estadística e Informática.

- Ley N° 27444 - Ley del Procedimiento Administrativo General.

- Ley N° 27269 - Ley de Firmas y Certificados Digitales.

- Decreto Supremo N° 019-2002-JUS - Reglamento de la Ley de Firmas y Certificados Digitales.

V. DISPOSICIONES GENERALES

5.1 El correo electrónico institucional es una herramienta de comunicación e intercambio de información oficial entre personas, no es una herramienta de difusión indiscriminada de información, con la excepción de las listas de interés establecidas por las instituciones para fines institucionales.

5.2 Cada institución establecerá, de acuerdo a su política institucional, la asignación de cuentas de correo electrónico institucional a parte de, o a todos sus trabajadores.

5.3 La Oficina de Informática (o la que haga sus veces) de cada institución será la responsable de capacitar al personal en el uso del correo electrónico institucional, sobre cómo asignar contraseñas a su correo y sobre las diferencias entre el correo electrónico institucional y el correo electrónico privado.

5.4 El tener una cuenta de correo institucional compromete y obliga a cada usuario a aceptar las normas establecidas por la institución y a someterse a ellas.

5.5 Los usuarios de las cuentas de correo electrónico son responsables de todas las actividades que realizan con sus cuentas de correo electrónico proporcionado por la institución donde laboran. Cualquier usuario que deje su cuenta de correo abierta en un lugar público es responsable de todo aquello que se realice desde dicha cuenta.

5.6 Las cuentas de correo para empleados de las instituciones públicas deben usarse para actividades que estén relacionadas con el cumplimiento de su función en la institución.

5.7 La institución debe garantizar la privacidad de las cuentas de correo electrónico institucional de todos los usuarios. Sólo en el caso de que se detecte que un usuario está cometiendo una falta grave contra lo establecido por la institución por medio de su cuenta de correo, la Oficina de Informática (o quien haga sus veces) podrá tomar las medidas que más le convenga respecto de dicha cuenta de correo. La Oficina de Informática (o quien haga sus veces) establecerá los procedimientos para la detección de faltas graves cometidos por los usuarios mediante correo electrónico.

5.8 El nombre de la cuenta de correo electrónico institucional para cada usuario debe estar formado por la letra inicial del nombre de pila

del usuario seguido inmediatamente del apellido paterno, ligado con el símbolo @ al nombre de dominio de la institución (establecido por la Directiva N° 010-2002-INEI/DTNP "Normas Técnicas para la Asignación de Nombres de Dominio de las entidades de la Administración Pública"). En caso de existir dos construcciones similares, el Administrador de Correo Electrónico en coordinación con las personas involucradas, acordarán el nombre de la cuenta tratando de seguir la regla aquí definida.

VI. DISPOSICIONES ESPECÍFICAS

6.1 DEL BUEN USO DEL CORREO ELECTRÓNICO

6.1.1 Uso de Contraseñas

- Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben establecer una contraseña para poder utilizar su cuenta de correo, y esta contraseña la deben mantener en secreto para que su cuenta de correo no pueda ser utilizada por otra persona.
- Cuando el usuario deje de usar su estación de trabajo deberá de cerrar el software de correo electrónico, para evitar que otra persona use su cuenta de correo.

6.1.2 Lectura de Correo

- Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben mantener en línea el software de correo electrónico (si lo tiene disponible todo el día), 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.
- Se debe eliminar permanentemente los mensajes innecesarios.
- Se debe mantener los mensajes que se desea conservar, agrupándolos por temas en carpetas personales.
- Al recibir un mensaje que se considere ofensivo, se debe reenviar el mensaje hacia el Administrador de Correo Electrónico de la institución, con el fin de que se pueda tomar las acciones respectivas.

6.1.3 Envío de Correo

- Utilizar siempre el campo "asunto" a fin de resumir el tema del mensaje.
- Expresar las ideas completas, con las palabras y signos de puntuación adecuados en el cuerpo del mensaje.

- Enviar mensajes bien formateados y evitar el uso generalizado de letras mayúsculas.
- No utilizar tabuladores, ya que existen softwares administradores de correo que no reconocen este tipo de caracteres, lo que puede introducir caracteres no válidos en el mensaje a recibirse.
- Evite usar las opciones de confirmación de entrega y lectura, a menos que sea un mensaje muy importante, ya que la mayoría de las veces esto provoca demasiado tráfico en la red.
- Evite enviar mensajes a personas que no conoce, a menos que sea por un asunto oficial que los involucre.
- Evite enviar mensajes a listas globales, a menos que sea un asunto oficial que involucre a toda la institución.
- Antes de enviar el mensaje revisar el texto que lo compone y los destinatarios, con el fin de corregir posibles errores de ortografía, forma o fondo.

6.1.4 Reenvío de Mensajes

- Para el reenvío de un mensaje, incluir el mensaje original, para que el destinatario conozca el contexto en que se está dando el mensaje que recibe. No incluir ningún archivo adjunto que se pueda haber recibido originalmente, a no ser que se haya realizado modificaciones al(los) archivo(s).

6.1.5 Autofirmas

- La firma debe ser breve e informativa, no debiendo ocupar más de tres líneas.
- No incluir la dirección de correo en la firma, porque ésta ya fue incluida de manera automática en la parte superior del mensaje.

6.1.6 Tamaño de los mensajes

- La Oficina de Informática (o la que haga sus veces) de cada institución determinará el tamaño máximo que deben tener los mensajes del correo electrónico institucional.

6.1.7 Vigencia de los mensajes

- Los mensajes tendrán una vigencia no mayor de 30 días desde la fecha de entrega o recepción de los mismos, o de acuerdo a la política

establecida por la Oficina de Informática (o la que haga sus veces) de cada institución. Superada la fecha de vigencia, los mensajes deberán ser eliminados del servidor de correo.

- Si se desea mantener un mensaje en forma permanente, éste debe almacenarse en carpetas personales.

6.1.8 Listas de Correos

- Al enviar un mensaje a una lista o grupo de usuarios, revisar que el mensaje sea enviado a los usuarios correctos.

- Evitar en lo posible enviar mensajes con archivos adjuntos a grupos de usuarios.

- Evitar suscribirse por Internet a listas ajenas a la función institucional, para evitar saturación en la recepción de mensajes.

6.1.9 Uso del Correo Institucional desde fuera del local de la Institución

- La Oficina de Informática (o la que haga sus veces) de cada institución mediante una directiva establecerá las políticas de uso del correo institucional desde fuera del local de la institución, de acuerdo a los métodos de trabajo establecidos por la institución.

6.2 DEL MAL USO DEL CORREO ELECTRÓNICO

6.2.1 Se considera falta grave facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas. Los usuarios deben conocer la diferencia de utilizar cuentas de correo electrónico institucionales y cuentas privadas ofrecidas por otros proveedores de servicios en Internet.

6.2.2 Se considera como mal uso del correo electrónico institucional las siguientes actividades:

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

- Participar en la propagación de mensajes encadenados o participar en esquemas piramidales o similares.

- Distribuir mensajes con contenidos impropios y/o lesivos a la moral.

- Falsificar las cuentas de correo electrónico.

- Utilizar el correo electrónico institucional para recoger los mensajes de correos de otro proveedor de Internet.

6.2.3 Se penalizará con la cancelación de la cuenta de correo, el envío de mensajes a foros de discusión (listas de distribución y/o newsgroups) que comprometan la información de la institución o violen las leyes del Estado Peruano, sin perjuicio de poder ser sujeto de otras sanciones y/o penalidades derivadas de tal actividad.

6.2.4 Se considera, adicionalmente, malas prácticas en el uso de correo electrónico:

6.2.4.1 Difusión de contenido inadecuado.

- Son considerados contenidos inadecuados todo lo que constituya complicidad con hechos delictivos, por ejemplo: apología del terrorismo, uso y/o distribución de programas piratas, todo tipo de pornografía, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general.

- Contenido fuera de contexto en un foro temático.

6.2.4.2 Difusión a través de canales no autorizados.

- Uso no autorizado del servidor de correo institucional para enviar correo personal. Aunque el mensaje en sí sea legítimo, se están utilizando los recursos de la institución sin consentimiento de directiva interna que la autorice.

6.2.4.3 Difusión masiva no autorizada

- Enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado, "spam".

6.2.4.4 Ataques con objeto de imposibilitar o dificultar el servicio, "mail bombing".

- Dirigir a un usuario o al propio sistema de correo electrónico, mensajes que tengan el objetivo de paralizar el servicio por saturación de las líneas, de la capacidad del servidor de correo, o del espacio en disco del usuario.

- Suscripción indiscriminada a listas de correo. Es una versión de "mail bombing", en que los ataques no vienen de una sola dirección, sino de varias, los cuales son mucho más difíciles de controlar.

6.3 DE LA SEGURIDAD DEL CORREO ELECTRÓNICO

6.3.1 Las instituciones públicas deben contar con políticas de seguridad para el uso de correo electrónico, las que serán establecidas por la Oficina de Informática (o la que haga sus veces) de cada institución.

6.3.2 Uso del Antivirus

- Los antivirus de la institución, para servidores y estaciones de trabajo, deben activarse de tal forma que se verifiquen todos los archivos, aún los que se encuentren compactados, y la acción por defecto a seguir será la de eliminar el virus automáticamente.

- Los servidores de correo deben contar con antivirus para correo. Si el mensaje que detecta contiene un virus o "troyano" - "caballo de troya" que no puede ser removido, debe eliminarse el mensaje inmediatamente. Así mismo se deberá informar, al destinatario de correo, el nombre del remitente y que su mensaje fue borrado por contener virus.

- Revisar en forma constante la computadora para evitar remitir virus al momento de enviar documentos adjuntos. En tal sentido, se responsabilizará a los usuarios por los archivos adjuntos que envíen.

- La Oficina de Informática (o la que haga sus veces) de cada institución se encargará de verificar la presencia de virus en el servidor de correo.

6.4 DE LA VALIDEZ OFICIAL DEL CORREO ELECTRÓNICO

6.4.1 La institución podrá establecer, mediante una directiva interna, la validez oficial de los mensajes que se transmitan entre sus trabajadores, así como la validez en el intercambio de información entre otras instituciones públicas y los ciudadanos.

6.4.2 Para el intercambio de información entre instituciones públicas, se deberá propender a la utilización del correo electrónico seguro, para lo que se podrá utilizar la firma y certificados digitales u otro medio de seguridad y verificación

6.4.3 Los mensajes de correo electrónico y sus archivos adjuntos, tendrán validez legal si están firmados digitalmente, bajo el marco de la Ley N° 27269, "Ley de Firmas y Certificados Digitales" y de su Reglamento aprobado mediante Decreto Supremo N° 019-2002-JUS.

VII. DISPOSICIONES COMPLEMENTARIAS

7.1 Las notificaciones institucionales pueden efectuarse mediante correo electrónico conforme el numeral 20.1.2 de la Ley N° 27444, Ley del Procedimiento Administrativo General.

7.2 Los correos electrónicos que adjunten documentos que no son propios del remitente, deberán citar siempre la fuente de origen y/o los autores, a fin de respetar los derechos de propiedad intelectual.

7.3 Si se recibe algo cuestionable o ilegal, comunicar a la Oficina de Informática (o la que haga sus veces) de la institución para que se tome las acciones del caso.

7.4 Toda institución pública que disponga de correo electrónico deberá asignar la función de administración del correo electrónico a su Oficina de Informática (o la que haga sus veces).

7.5 La Oficina de Recursos Humanos de cada institución debe comunicar a la Oficina de Informática (o la que haga sus veces) la relación de trabajadores que hayan ingresado a laborar y de los que han dejado de hacerlo, para la activación o desactivación de las cuentas de correo respectivas.

7.6 La Oficina de Informática (o la que haga sus veces) de cada institución es la responsable de que el personal de la institución cumpla con lo dispuesto en la presente directiva y podrá elaborar un código de ética adicional a esta directiva.