Consejo Ejecutivo del Poder Judicial

RESOLUCIÓN ADMINISTRATIVA N° 027-2010-CE-PJ

Lima, 25 de enero de 2010

VISTO:

El Oficio N° 001-2010-PERS-COM-SEG-PJ, cursado por el Presidente de la Comisión de Seguridad del Poder Judicial, remitiendo propuesta de Directiva denominada "Normas de Seguridad de la Información Almacenada en los Equipos del Poder Judicial" y

CONSIDERANDO:

Primero: Que, mediante Resolución Administrativa de la Gerencia General del Poder Judicial N° 419-2006-GG-PJ, de fecha 06 de setiembre del 2006; se aprobó la Directiva N° 005-2006-GG-PJ, "Normas de Seguridad de la Información Almacenada en los Equipos del Poder Judicial";

Segundo: Que, debido al continuo avance tecnológico en esta campo, es necesario actualizar la directiva mencionada, la cual requiere normas y disposiciones específicas para garantizar la confidencialidad, integridad y disponibilidad de la información institucional;

Tercero: Que, de acuerdo a la Resolución de Contraloría N° 320-2006-CG, que aprueba las Normas de Control Interno aplicables a las Entidades del Estado, corresponde a la Institución desarrollar las actividades de control de las tecnologías de información y comunicación que garanticen el procesamiento de la información para el cumplimiento misional y de los objetivos de la organización;

Cuarto: Que, el Comité de Seguridad del Poder Judicial ha elaborado el proyecto de actualización de la referida directiva, documento normativo que es conveniente aprobar;

El Consejo Ejecutivo del Poder Judicial, en uso de sus atribuciones, en sesión ordinaria de la fecha, por unanimidad,

RESUELVE:

Artículo Primero.- Aprobar la Directiva N° 002-2010-CE-PJ, "Normas de Seguridad de la Información Almacenada en los Equipos del Poder Judicial", que en anexo adjunto forma parte de la presente resolución.

Artículo Segundo.- Dejar sin efecto la Directiva N° 005-2006-GG-PJ, de fecha 06 de setiembre de 2006.

Artículo Tercero.- Autorizar a la Gerencia General para que a través de la Gerencia de Informática, proceda a la difusión del contenido y alcance de la directiva materia de aprobación.

Regístrese, publíquese, comuníquese y cúmplase.

SS.

CONSEJO EJECUTIVO DEL PODER JUDICIAL

JAVIER VILLA STEIN

ROBINSON O. GONZALES CAMPOS

JORGE ALFREDO SOLÍS ESPINOZA

FLAMINIO VIGO SALDAÑA

DARÍO PALACIOS DEXTRE

HUGO SALAS ORTIZ

DIRECTIVA N°002-2010-CE-PJ

NORMAS DE SEGURIDAD DE LA INFORMACION ALMACENADA EN LOS EQUIPOS DEL PODER JUDICIAL

I. OBJETIVO

Establecer normas para la seguridad de la información institucional administrada en los equipos de cómputo y equipos de comunicación que almacene información del Poder Judicial.

II. FINALIDAD

2.1 Proteger la información administrada en los equipos del Poder Judicial.

2.2 Garantizar la continuidad del servicio informático a las dependencias del Poder Judicial.

2.3 Establecer las responsabilidades de los usuarios, en relación con la información por ellos manejada.

III. ALCANCE

Esta directiva es de alcance a todo usuario de las dependencias del Poder Judicial, a nivel nacional, que tenga acceso al servicio de equipos de cómputo y equipos de comunicación que almacenen información institucional.

IV. BASE LEGAL

4.1 Texto Único Ordenado de la Ley Orgánica del Poder Judicial aprobado por Decreto Supremo N° 017-93-JUS, y demás leyes modificatorias.

4.2 Ley N° 29277, Ley de la Carrera Judicial.

4.3 Ley Nº 27444 - Ley del Procedimiento Administrativo General.

4.4 Decreto Legislativo No. 276, Ley de Bases de la Carrera Administrativa y su reglamento aprobado mediante Decreto Supremo N.005-90-PCM.

4.5 Reglamento de Organización y Funciones de la Oficina de Control de Magistratura del Pode Judicial, aprobado por Resolución Administrativa No. 129-2009-CE-PJ.

4.6 Reglamento Interno de Trabajo aprobado mediante Resolución Administrativa N° 010-2001-CE-PJ.

4.7 Reglamento de Régimen disciplinario de los auxiliares judiciales del Poder Judicial, aprobado mediante Resolución Administrativa No. 227-2009-CE-PJ.

4.8 Resolución Administrativa N° 245-2007-P-PJ que conforma el Comité de Seguridad del Poder Judicial.

4.9 Directiva Nº 005-2003-INEI/DTNP, aprobada por Resolución Jefatural Nº 088-2003-INEI.

V. VIGENCIA

Entrará en vigencia a los 30 días de publicada en el Diario Oficial El Peruano, la Resolución Administrativa que aprueba la presente Directiva.

VI. NORMAS GENERALES

6.1 Los usuarios de los equipos de cómputo y servicios de red del Poder Judicial deberán observar una conducta o actuación prudente y responsable que evite poner en riesgo la seguridad, integridad y confiabilidad de los equipos, las redes, la información, los programas y los sistemas del Poder Judicial y que puedan ocasionar daño físico, mental, moral, problemas interpersonales o un menoscabo de la reputación de los usuarios, de personas ajenas al Poder Judicial o de la misma institución.

6.2 Los servicios asociados, tanto internos como externos, el sistema de correspondencia electrónica (e-mail), el acceso a la Internet y los documentos y programas que existen en los equipos informáticos del Poder Judicial, son de su propiedad y sólo podrán utilizarse para propósitos lícitos, prudentes, responsables y en cumplimiento de las funciones asignadas a los usuarios.

6.3 Los usuarios del Poder Judicial cuidarán que las contraseñas o claves de acceso se mantengan en estricta confidencialidad. Las claves de acceso son la principal protección contra ingresos no autorizados a los Servicios de Red, Sistemas, Internet y Correo Electrónico del Poder Judicial, por cuanto a través de ellas se verifica inequívocamente la identidad de los usuarios.

6.4 Los usuarios al acceder a los Servicios de Red, Sistemas, Acceso a Internet y Correo Electrónico de la Institución, deberán cumplir las normas que se aprueban mediante la presente Directiva.

6.5 Los usuarios deberán comunicar a la Gerencia de Informática o al personal de informática de las dependencias del Poder Judicial a nivel nacional, cualquier situación, incidente o problema de

seguridad, acceso indebido o violación voluntaria o involuntaria de las presentes normas, que surjan en el uso de los equipos del Poder Judicial.

6.6 La Gerencia de Informática emitirá de manera mensual un reporte de las incidencias de seguridad y las propuestas de solución al Comité de Seguridad del Poder Judicial.

6.7 La Gerencia de Informática, se reserva el derecho de revisar y vigilar el cumplimiento de la presente directiva en los equipos de cómputo, garantizando que se utilicen para los propósitos y gestiones relacionadas con el trabajo a desarrollar. En caso de revisión de equipos de cómputo de magistrados, se realizará a solicitud de los órganos de control del Poder Judicial.

6.8 Los antivirus de la institución, para equipos servidores y estaciones de trabajo, deben activarse por la Gerencia de Informática, 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.

6.9 La Gerencia de Informática a través de la Subgerencia de Soporte Técnico o el personal de informática de las dependencias del Poder Judicial a nivel nacional, son los únicos autorizados para la instalación de software en los equipos de cómputo del Poder Judicial, en cumplimiento de la Directiva 001-2004-CE-PJ.

VII. NORMAS ESPECÍFICAS

7.1 Seguridad en el Uso de Claves de Acceso a los servicios de Red y de Sistemas

7.1.1 Las claves de acceso tienen carácter secreto y son de uso exclusivo del usuario a quién se le asignó, no debiendo ser compartidas con otros usuarios.

7.1.2 Todo usuario autorizado, poseedor de una clave de acceso, es responsable directo y absoluto del uso que se haga de ella.

7.1.3 Las claves de acceso serán asignadas a los usuarios que cuenten con autorización expresa del Gerente, Jefe de Oficina, funcionario de similar nivel o Jefe de la Oficina de Administración de la Sede donde labora el usuario, a través de una comunicación oficial a los órganos competentes, según sea el caso.

7.1.4 Es responsabilidad de la autoridad que solicita una clave de acceso, comunicar oficialmente a la Gerencia de Informática o al personal informático de las dependencias

del Poder Judicial, cuando deba darse de baja a una clave de acceso, o a un usuario de red.

7.1.5 Al momento de seleccionar una clave de acceso, se debe tener en cuenta lo siguiente:

- Debe tener una longitud mínima de 6 caracteres, y tener al menos un carácter numérico y uno alfabético, dentro de su conformación.
- No debe empezar o terminar con un número, o tener más de tres caracteres consecutivos idénticos, en cualquier posición, a los de una clave de acceso utilizada anteriormente.
- No debe tener más de dos caracteres iguales consecutivos.

  Debe ser cambiada, por lo menos, cada 60 días, para usuarios generales, y cada 30 días, para usuarios con ciertos tipos de privilegio.
- No debe contener el identificador del usuario (login name o nombre de usuario), como parte de la clave de acceso.

7.1.6 En el caso que algún usuario olvide su clave de acceso, ésta sólo podrá ser reemplazada mediante una solicitud escrita del Gerente, Jefe de Oficina, funcionario de similar nivel o Jefe de la Oficina de Administración de la Sede donde labora el usuario, como si fuera la primera vez que solicita una clave de acceso.

7.1.7 Si debido a las funciones que cumple el usuario, utilizara sistemas de otras Instituciones (RENIEC, SUNARP, SUNAT, etc.), por ningún motivo deberá utilizar claves de acceso similares a las que utiliza para acceder a los sistemas del Poder Judicial, en razón de que podría ser detectada y utilizada por terceros para accesos no autorizados.

7.2 Seguridad en el uso del Servicio de Red del Poder Judicial

7.2.1 Toda información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho que surja, se cree o modifique mediante el uso de una de las computadoras del Poder Judicial, será propiedad de la Institución, aunque la información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho haya surgido mediante el

esfuerzo personal del usuario.

7.2.2 Los programas informáticos o recursos del Poder Judicial, deben contar una licencia o autorización de uso válida a nombre del Poder Judicial.

7.2.3 Para copiar programas del Poder Judicial e instalarlos en otras computadoras, se requiere la autorización por escrito de la Gerencia de Informática y deberá será realizada por personal de dicha Gerencia o por el personal de informática de las dependencias del Poder Judicial.

7.2.4 Se encuentra prohibido la conexión y acceso a la red local del Poder Judicial desde computadoras o equipos portátiles que no pertenecen a la institución, salvo bajo autorización de la Gerencia de Informática o por el personal de informática de las dependencias del Poder Judicial.

7.2.5 El usuario evitará utilizar los recursos electrónicos del Poder Judicial para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro servicio ajeno a las funciones de la Institución.

7.2.6 Por razones de seguridad, se podrá permitir codificar, asignar contraseñas o modificar alguna información a fin de evitar que otras personas puedan leerla; estando facultado el Poder Judicial para decodificar la misma o restituirla a su condición original, siendo responsable el usuario de proveer todos los datos para lograr el acceso a la información o archivo.

7.2.7 El usuario no debe realizar modificación de los parámetros o configuración de las computadoras del Poder Judicial para darle la capacidad de recibir llamadas telefónicas o cualquier otro tipo de acceso o conexión remota que permita intrusiones no autorizadas a la red de la institución.

7.2.8 Los archivos que se creen en las computadoras o equipos portátiles conectados en red, deben almacenarse en el directorio asignado a cada usuario u oficina, con el propósito de que puedan protegerse mediante los mecanismos de resguardo (backup) existentes.

7.2.9 Son considerados como archivos, todo aquel documento, video, audio y cualquier ejecutable necesarios para el uso laboral.

7.2.10 Está prohibido el almacenamiento de música, videos, audio, ejecutables y otros archivos que no sean requeridos

para la realización de labores netamente institucionales en los directorios asignados a cada usuario.

7.2.11 Está prohibido el manejo o transmisión de material obsceno, profano u ofensivo a través del sistema de computadoras o de cualquier sistema de comunicación electrónica del Poder Judicial. Esto incluye a modo de ejemplo, acceso a materiales eróticos, bromas de cualquier forma o cualquier comentario o chiste que pueda ser considerado como discriminatorio o como hostigamiento sexual.

7.2.12 Se prohíbe que se utilicen protectores de monitores (screen savers) con fotos de personas, artistas, modelos, deportistas, fotos de calendario o cualquier otra imagen que pueda resultar poco seria u ofensiva. Frente a ello, la Gerencia de Informática, a través de la red, aplicará un protector de pantalla estándar del Poder Judicial a todas las estaciones de trabajo.

7.2.13 Se prohíbe la divulgación por cualquier medio de opiniones personales específicas con relación a raza, origen nacional, sexo, orientación sexual, edad, ideas o creencias religiosas o políticas, así como opiniones sobre personas con impedimento físico o mental.

7.2.14 El usuario está prohibido de usar programas de charlas (Chats de comunicación externa) a menos que sean autorizados expresamente por la Gerencia de Informática, quien atenderá las solicitudes en un plazo máximo de 24 horas, bajo responsabilidad.

Para ello, deberá existir una evaluación de las ventajas que podría traer consigo la utilización de estos programas, en el cumplimiento de las funciones encomendadas

7.3 Seguridad en el uso de los dispositivos de almacenamiento externo de los equipos de computo

7.3.1 El uso de dispositivos de almacenamiento como memory card, lectoras ópticas (CD, DVD), diskettes, discos externos debe ser autorizado por la Gerencia de Informática, brindando las medidas de seguridad necesarias.

7.3.2 La Gerencia de Informática a través de un software autorizado administrará el uso de los dispositivos de almacenamiento en los equipos de cómputo. Este software permitirá auditar las acciones realizadas sobre estos dispositivos, con el objetivo de minimizar la fuga de la información institucional.

7.4 Seguridad en el uso de equipos portátiles

7.4.1 Los equipos portátiles asignados por la institución son de uso exclusivo del usuario para el cumplimiento de las funciones propias del Poder Judicial.

7.4.2 Todo usuario que tenga asignado un equipo portátil es responsable directo y absoluto del uso que se haga del mismo.

7.4.3 La seguridad en los equipos portátiles contempla lo indicado en el *punto 7.3*

7.4.4 El usuario de un equipo portátil deberá considerar los siguientes aspectos de seguridad, según las funcionalidades que contemple:

7.4.4.1 El antivirus debe encontrarse en estado activo

7.4.4.2 El firewall del sistema operativo debe estar habilitado.

7.4.4.3 Si fuera necesario compartir carpetas del disco duro a través de la red, el usuario deberá ejecutar dicha acción con cautela y responsabilidad, velando por la confidencialidad de la información almacenada.

7.4.4.4 Los correos electrónicos o toda aquella información que involucre datos confidenciales de la institución no deberá encontrarse almacenada en estos equipos. El usuario deberá regirse a lo mencionado en el punto 7.2.8 de la presente directiva.

7.4.4.5 Se debe configurar una clave de seguridad para el inicio de actividades en el equipo portátil.

7.4.4.6 En caso de pérdida de algún equipo portátil o computadoras y similares, se debe comunicar a la Gerencia de Administración y Finanzas, Oficinas de Administración de las Cortes Superiores o quien haga sus veces en las demás dependencias, previa denuncia policial dentro de las 24 horas, la que a su vez informará a la Subgerencia de Logística para que efectúe el trámite que corresponda.

VIII. NORMAS COMPLEMENTARIAS

8.1 La Gerencia General, a través de sus dependencias correspondientes, pondrá en conocimiento, todo mal uso de los equipos de cómputo a los órganos competentes contemplados en

las normas vigentes, a fin de que adopten las medidas que consideren pertinentes.

8.2 Los aspectos no contemplados en la presente Directiva, serán resueltos por el Comité de Seguridad del Poder Judicial.

8.3 La Gerencia General, a través de los órganos competentes administrativos y jurisdiccionales, realizará la capacitación y difusión para la aplicación de la presente directiva a los usuarios del Poder Judicial. Esta capacitación y difusión deberá llevarse a cabo a partir de la aprobación de la Resolución Administrativa.