Resolución del Consejo Nacional de la Magistratura

Nº 219 -2013-P-CNM

San Isidro, 26 DIC. 2013

VISTOS:

El Informe Nº 114-2013-OPCT-CNM, de la Oficina de Planificación y Cooperación Técnica y el Memorando Nº 249-2013-OTI-CNM de la Oficina de Tecnologías de la Información, sobre la propuesta de aprobación de la Directiva Nº 004-2013-P-CNM "Normas y procedimientos para la administración de cuentas y claves de acceso a los usuarios y el uso de los servicios de correo electrónico e internet en el Consejo Nacional de la Magistratura";

CONSIDERANDO:

Que, mediante la Ley Nº 30096 Ley de Delitos Informáticos, publicada con fecha 22 de octubre de 2013, se previene y sanciona las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia;

Que, con Resolución Ministerial Nº 246-2007-PCM, publicada con fecha 22 de agosto de 2007, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición" en todas las Entidades integrantes del Sistema Nacional de Informática;

Que, a través de la Resolución Ministerial Nº 129-2012-PCM, publicada con fecha 25 de mayo de 2012, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", en todas las entidades integrantes del Sistema Nacional de Informática;

Que, mediante Resolución de Contraloría Nº 320-2006-CG se aprueban las normas técnicas de control interno para el sector público;

Que, la Oficina de Planificación y Cooperación Técnica, en coordinación con la Oficina de Tecnologías de la Información ha elaborado el proyecto de Directiva sobre "Normas y procedimientos para la administración de cuentas y claves de acceso a los usuarios y el uso de los servicios de correo electrónico e internet en el Consejo Nacional de la Magistratura", que norma la correcta administración de dichos servicios a nivel institucional en el marco de la seguridad de la información;

De conformidad con lo establecido en el inciso h) del artículo 11º del Reglamento de Organización y Funciones, aprobado por Resolución Nº 088-2011-P-CNM y modificado por las Resoluciones Nºs 020 y 118-2012-P-CNM, y con la visación de los Jefes de las

Oficinas de Planificación y Cooperación Técnica, de Tecnologías de la Información y Asesoría Jurídica, y del Director General;

SE RESUELVE:

Artículo 1º.- Aprobar la Directiva Nº 004-2013-P-CNM "Normas y procedimientos para la administración de cuentas y claves de acceso a los usuarios y el uso de los servicios de correo electrónico e internet en el Consejo Nacional de la Magistratura" cuyo texto forma parte de la presente resolución.

Artículo 2º.- Publicar la presente Resolución en el portal de transparencia de la página electrónica del Consejo Nacional de la Magistratura (www.cnm.gob.pe).

Regístrese, comuníquese y archívese,

Máximo Herrera Bonilla
Presidente
Consejo Nacional de la Magistratura

El Secretario General del Consejo Nacional de la Magistratura CERTIFICA: Que el presente, documento es copia fiel al original.

MARIO ALVAREZ QUISPE
SECRETARIO GENERAL
Consejo Nacional de la Magistratura

Consejo Nacional de la Magistratura

MARIO ALVAREZ QUISPE
SECRETARIO GENERAL
Consejo Nacional de la Magistratura

DIRECTIVA Nº 004-2013-P-CNM

"NORMAS Y PROCEDIMIENTOS PARA LA ADMINISTRACION DE CUENTAS Y CLAVES DE ACCESO A LOS USUARIOS Y EL USO DE LOS SERVICIOS DE CORREO ELECTRONICO E INTERNET EN EL CONSEJO NACIONAL DE LA MAGISTRATURA"

CAPITULO I
GENERALIDADES

1. Finalidad

Cautelar la seguridad de la información a los usuarios, en la administración de las cuentas de usuario, claves de acceso a las plataformas informáticas y sistemas de Información, así como del uso de los servicios de correo electrónico institucional e Internet del Consejo Nacional de la Magistratura.

2. Objetivo

Establecer normas y procedimientos para la correcta administración de las cuentas de usuarios, claves de acceso a las plataformas informáticas y sistemas de información, así como para el uso de los servicios del correo electrónico institucional e Internet, en el Consejo Nacional de la Magistratura.

3. Base Legal

3.1 Ley N° 30096 "Ley de Delitos Informáticos" promulgada por el Congreso de la Republica y publicada el 22 de octubre de 2013.

3.2 Resolución Ministerial Nº 246-2007-PCM, publicada el 22 de agosto de 2007, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición" en todas las Entidades integrantes del Sistema Nacional de Informática.

3.3 Resolución Ministerial Nº 129-2012-PCM, publicada el 25 de mayo de 2012, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática.

3.4 Resolución de Contraloría N° 320-2006-CG donde "Aprueban normas técnicas de control interno para el sector público".

3.5 Resolución de la Presidencia Nº 091-2006-P-CNM, que aprueba la Directiva N° 006-2006-P-CNM, "Normas para Seguridad de la Información en el Consejo Nacional de la Magistratura" del 04 de julio del 2006.

4. Alcance

La presente Directiva es de aplicación en las unidades orgánicas del Consejo Nacional de la Magistratura.

CONSEJO NACIONAL DE LA MAGISTRATURA
OFICINA DE PLANIFICACIÓN Y COOPERACIÓN TÉCNICA

5. Definición de Términos

5.1 **Usuario**: Persona que realiza determinada labor dentro de una unidad orgánica del CNM, y a quién se le ha asignado una identificación digital, para acceder a ciertos recursos informáticos y de telecomunicaciones disponibles en la red.

5.2 **Información confidencial:** Toda aquella información restringida que debe ser accesada por personas expresamente autorizadas, en base al concepto de "necesidad-de-conocer" (need-to-know). Su divulgación requiere del consentimiento formal del responsable de la misma.

5.3 **Información interna:** Toda aquella información de uso interno del CNM y cuyo acceso puede ser permitido a cualquier empleado de la institución; sin embargo, no puede ser transmitida fuera del CNM sin autorización escrita de quien generó la información.

5.4 **Información pública:** Toda aquella información cuya divulgación fuera del CNM no representa riesgo alguno para la institución.

5.5 **Cuenta de usuario:** Identificación proporcionada a un usuario, que le permite tener acceso a un sistema informático, estación de trabajo, punto de red, entre otros. La cuenta se encuentra relacionada a un nombre de usuario y una clave de acceso.

5.6 **Clave de acceso:** Combinación de números, letras y signos que deben de teclearse para tener acceso a un sistema informático, estación de trabajo, punto de red, entre otros.

5.7 **Administrador de Red:** Persona designada por el Jefe de la Oficina de Tecnologías de la Información para establecer los accesos y configuración de la plataforma tecnológica que permita acceder o no a los servicios informáticos del Consejo Nacional de la Magistratura; además, se encarga de proteger la información de la distribución, acceso, modificación, destrucción y/o uso no autorizado.

5.8 **Controlador de Dominio:** Servidor de red donde los usuarios se autentican, guarda las políticas de acceso, seguridad, y sirve como mecanismo de control.

5.9 **Mesa de ayuda (Help Desk):** Servicio de ayuda y soporte en línea informático que se brinda a todos los usuarios de la Institución. Cuenta con herramientas de hardware y software para resolver cualquier tipo de problema.

5.10 **Virus**: Pequeño programa escrito intencionalmente para auto instalarse en la computadora de un usuario sin el conocimiento o el permiso de éste. Normalmente se comporta como un programa parásito, pues infecta y ataca a los archivos del sistema y del usuario. Para propagarse se replica a sí mismo ilimitadas veces, llegando a producir serios daños que pueden afectar a los sistemas y archivos en general, pudiendo estos últimos daños ocasionar que se borren o destruyan los archivos.

5.11 **Correo electrónico**: Es un servicio de red para permitir a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónicos.

5.12 **Internet**: Conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, funcionando como una red lógica única.

5.13 **Firewall**: Normalmente conocido como barrera cortafuegos. Es un filtro de software y/o hardware que controla todas las comunicaciones entrantes y

salientes de una red a otra red, cuya función principal es denegar o permitir el acceso a comunicación. Así para denegar o autorizar una comunicación el firewall, primero analiza el perfil del usuario si tiene o no acceso a un determinado servicio: (acceso a Internet, correo, transferencia FTP, etc.) y luego denegará o permitirá el acceso a la comunicación.

5.14 **Navegación Web**: También denominada navegación por la red, es la actividad que consiste en explorar en Internet en búsqueda de información útil.

6. Disposiciones Generales

6.1 El Jefe de la Oficina de Tecnologías de la Información tiene a su cargo:

- Controlar el proceso de otorgamiento de accesos, validando las solicitudes recibidas y atendiendo aquellas debidamente autorizadas.
- Administrar el servicio de correo electrónico, internet, entrega de claves de acceso a los usuarios para los sistemas informáticos, así como el velar por el cumplimiento de la presente directiva.
- Administrar adecuadamente el acceso al servicio de Internet a los usuarios autorizados del CNM. La Oficina de Tecnologías de la Información (OTI) es la unidad orgánica encargada de la administración del servicio de internet tomando las acciones que sean necesarias para asegurar la confiabilidad del mismo, en función a los recursos y capacidades disponibles.
- Autorizar requerimientos de manera excepcional, establecidos en el presente documento.

6.2 El Administrador de red es responsable de:

- Velar por la adecuada configuración de las políticas de seguridad definidas (usuarios y contraseñas) en los servicios de Internet del CNM.
- Apoyar al personal a cargo de los sistemas de información (propietarios de la información, gestión y de su utilización en el proceso de definición y mantenimiento de los perfiles asignados en las aplicaciones).
- Controlar que el proceso de otorgamiento de cuentas de correo a los usuarios se realice de acuerdo a lo estipulado por la Norma para la Administración de Cuentas y Claves de Acceso de Usuarios.
- Controlar el proceso de otorgamiento de cuentas de usuario con acceso a Internet, en cada uno de sus niveles.

6.3 Los usuarios son responsables de:

- Hacer uso de la identificación asignada de forma personal para acceder a la red y a los sistemas informáticos del CNM (cuenta de usuario y contraseña), según las normas que se establecen en la presente directiva.
- Hacer buen uso del correo electrónico según las normas establecidas en la presente directiva.
- Hacer buen uso de los permisos de navegación a internet, según los normas establecidas en la presente directiva.

7. Responsabilidad

Los funcionarios, servidores públicos, contratados y locadores de servicios de las diversas unidades orgánicas del Consejo Nacional de la Magistratura, son responsables de la aplicación y cumplimiento de la presente Directiva en el ámbito de su competencia.

8. Abreviatura

CNM: Consejo Nacional de la Magistratura.

CAPITULO II
ADMINISTRACIÓN DE CUENTAS Y CLAVES DE ACCESO DE USUARIOS

9. Administración de Perfiles y Cuentas de Usuario

9.1 Toda cuenta de usuario debe tener un perfil asociado a cada sistema y/o equipo al que le corresponda acceder en base a sus funciones.

9.2 Toda cuenta de usuario debe tener asociada obligatoriamente una contraseña. Dicha contraseña debe ser exigida en el proceso de autenticación, debe tener como mínimo 8 caracteres alfanuméricos, incluyendo mayúsculas, minúsculas y números.

9.3 Se prohíbe compartir la cuenta de usuario con otras personas, independientemente de la jerarquía del solicitante.

9.4 Las cuentas de usuarios deben ser otorgadas únicamente a personal del CNM. El propietario de la información es el encargado de autorizar los accesos requeridos. La cuenta del usuario debe estar conformada por el primer nombre más el primer apellido del trabajador. De existir duplicidad del nombre de la cuenta por homonimia se deberá añadir al final de la cadena de caracteres el número 01 y así sucesivamente.

9.5 Para el caso de locadores de servicios, la cuenta de usuario se crearán sólo a solicitud expresa de las áreas usuarias y con la autorización adicional del Jefe de la Oficina de Tecnologías de la Información. Estas cuentas deberán hacer referencia sólo a la abreviación del servicio que se ofrece. En estas cuentas no deberá utilizarse el nombre del prestatario.

9.6 Se prohíbe el uso de cuentas genéricas, que permitan el acceso de varios usuarios haciendo uso de una misma identificación. En aquellos casos en que sea absolutamente necesario y justificado el uso de dichas cuentas genéricas, su creación deberá contar con una aprobación explícita del Jefe de la Oficina de Tecnologías de la Información. Se deberá asignar un

responsable único por cada cuenta genérica y registrar dicha asignación y responsabilidad por escrito.

10. Políticas de Contraseña

10.1 Las contraseñas, son de carácter reservado y de uso estrictamente personal.

10.2 Los usuarios no deben habilitar en los sistemas de información que lo permitan la opción de guardar la contraseña. Dicha opción permite al usuario a futuro, ingresar al sistema sin indicar su contraseña.

10.3 No se debe anotar las contraseñas de acceso en lugares públicos, tales como: bajo del teclado, en agendas, bajo el teléfono, detrás de una foto, etc. Cualquier contraseña encontrada en estos medios será informada al Administrador de red para que proceda al bloqueo de la cuenta y emita el informe respectivo.

10.4 No se debe transmitir las contraseñas verbalmente a través de líneas telefónicas, ni en texto mediante redes. Se debe utilizar un medio confiable para la comunicación de las mismas.

10.5 Las contraseñas deben ser conformadas por caracteres alfanuméricos y con un largo mínimo de 8 caracteres alfanuméricos que incluya una letra mayúscula y un número como mínimo. Es recomendable que el usuario, al registrarlas, considere que esta debe ser fácil de recordar, pronunciable y que cumpla con las siguientes características:

10.5.1 No basarse en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, aquellas palabras comunes como lugares geográficos, entre otros.

10.5.2 Obligatoriamente debe contener al menos un dígito numérico y al menos un carácter en mayúscula y otro en minúscula.

10.5.3 En el proceso de cambio de contraseñas, esta no se debe ser igual a las últimas 3 contraseñas utilizadas.

10.5.4 La contraseña no debe estar en blanco.

Alguna de las características antes mencionadas podrá ser validada por el sistema, de modo tal que su aplicación sea obligatoria.

11. Sistema de Control de Acceso

11.1 En las plataformas y/o sistemas de información donde se procese y/o almacene información confidencial, interna o pública debe implementarse un sistema de control de accesos automático o adoptar los controles pertinentes que permitan mitigar los riesgos inherentes al acceso no autorizado.

11.2 Se debe implementar en la medida que las plataformas o sistemas de información lo permitan un sistema de control de accesos que registre los eventos relacionados con la seguridad.

11.3 Se debe adoptar medidas de seguridad apropiadas para asegurar que los registros de eventos relacionados con la seguridad no sean consultados, alterados o eliminados sin previa autorización.

11.4 La Oficina de Administración y Finanzas en coordinación con la Oficina de Tecnologías de la Información serán las encargadas de la implementación del sistema de control de accesos.

12. Administración de Accesos

12.1 Se debe autenticar a todos los usuarios antes de que éstos accedan a los recursos asignados.

12.2 Debe restringirse totalmente el acceso a información del sistema al que el usuario se está conectando, hasta que este haya sido debidamente autenticado y el proceso de conexión a los recursos haya terminado satisfactoriamente.

12.3 La conexión sólo permitirá al usuario acceder a la información a la cual está autorizado de conformidad con los requerimientos de su trabajo.

12.4 En la medida que los sistemas lo permitan, los intentos infructuosos de conexión deberán contabilizarse, estableciéndose hasta un máximo de 3 para proceder al bloqueo del usuario inutilizando su conexión; estos intentos infructuosos deberán ser registrados como eventos de seguridad.

12.5 El usuario debe desconectarse al terminar su sesión. Siempre que la tecnología lo permita, el sistema deberá controlar los terminales inactivos de forma que proceda a su desconexión automática luego de 30 minutos de permanecer sin actividad.

12.6 El acceso a las funciones de administración de las plataformas y/o sistemas de información deberán estar restringidos a personal autorizado. En estos casos, en la medida que las herramientas disponibles lo permitan, se debe tener un control más detallado del acceso a los sistemas de información mediante dichas cuentas.

CONSEJO NACIONAL DE LA MAGISTRATURA Vº Bº Oficina de Tecnologías de la Información

CONSEJO NACIONAL DE LA MAGISTRATURA OFICINA DE PLANIFICACIÓN Y COOPERACIÓN TÉCNICA

MARIO ALVAREZ QUISPE
SECRETARIO GENERAL
Consejo Nacional de la Magistratura

13. Asignación de cuentas de usuario

13.1 Las solicitudes de creación, modificación y/o eliminación de cuentas de usuario deben ser enviadas al Jefe de la Oficia de Tecnologías de la Información por parte de la unidad orgánica a la cual pertenece el usuario.

13.2 De no mediar problema el Jefe de la Oficina de Tecnologías de la Información reenviará la solicitud de acceso al Administrador de Red para que otorgue los accesos solicitados.

13.3 En el caso del personal nombrado o contratado, el Jefe del Área de Recursos Humanos, deberá comunicar al Jefe de la Oficina de Tecnologías de la Información, la solicitud de cancelación de las cuentas de acceso respectivas, de igual forma para el caso de locadores de servicios, la persona encargada del Área de Logística, responsable de las contrataciones de personal, enviará la solicitud de cancelación de las cuentas de acceso correspondientes. El Jefe de la Oficina de Tecnologías de la Información reenviará dichas solicitudes al Administrador de Red para que cancele los accesos solicitados.

14. Auditoria y revisión de las solicitudes de acceso a usuarios

14.1 El Jefe de la Oficina de Tecnologías de la Información debe verificar lo adecuado de cada solicitud de acceso antes de que la misma sea enviada al Administrador de red.

14.2 El Administrador de Red y personal de Soporte técnico estarán facultados para monitorear los accesos y las actividades realizadas por los usuarios con el objetivo de identificar actividades sospechosas que pudieran evidenciar un uso inadecuado de los privilegios asignados y que ponga en riesgo la estabilidad de la información del CNM.

15. Otras consideraciones

15.1 El usuario debe efectuar el cambio de sus contraseñas cada vez que considere que éstas están comprometidas o hayan sido divulgadas a terceros, independientemente del cambio periódico solicitado automáticamente por el sistema.

15.2 Bajo ningún motivo el usuario podrá compartir su identificación de usuario y contraseña.

15.3 El usuario no anotará en lugar visible o de fácil localización sus contraseñas, debiendo ser estrictamente reservados en su manejo.

15.4 Cada persona es totalmente responsable de las acciones efectuadas con la identificación de usuario asignado. Por tal motivo, las acciones que se

CONSEJO NACIONAL DE LA MAGISTRATURA Vº Bº Oficina de Tecnologías de la Información

CONSEJO NACIONAL DE LA MAGISTRATURA OFICINA DE PLANIFICACIÓN Y COOPERACIÓN TÉCNICA

realicen durante su ausencia son de su total responsabilidad, sin importar si puede demostrar que no estaba frente a su computadora personal.

CAPITULO III
USO DEL CORREO ELECTRÓNICO

16. Asignación de correo y acceso

16.1 La dirección de correo electrónico asignada a los servidores es propiedad del CNM y es suministrada únicamente con el propósito de enviar y recibir comunicación del CNM, proveedores y terceros relacionados a los fines institucionales.

16.2 La dirección de correo electrónico debe estar conformada por el primer nombre más el primer apellido del trabajador. De existir duplicidad del nombre de la cuenta por homonimia se deberá añadir al final de la cadena de caracteres el número 01 y así sucesivamente.

16.3 El correo electrónico es un medio de comunicación cuya confidencialidad está en función de una contraseña de acceso personal e intransferible. En el caso de que se envíe y/o reciba a través de Internet documentos altamente confidenciales, éstos deberán estar protegidos con una contraseña adicional, para lo cual podrán solicitar apoyo al soporte técnico de la Institución.

16.4 El CNM mediante la Oficina de Tecnologías de la Información (OTI) tendrá el derecho o facultad para verificar el uso adecuado que se está dando a la cuenta de correo asignada, por lo que podrá acceder a la información contenida en los mismos para realizar investigaciones por sospecha y abuso; y solo pondrá realizarlo cuando exista una razón de interés institucional que afecte o ponga en riesgo la continuidad de las operaciones del CNM.

16.5 El uso de cuentas grupales de correo por Dirección General, Secretaria General, Oficinas y a todo el personal, es exclusivamente para envío de comunicaciones con fines institucionales; quedando estrictamente prohibido su uso para envío de comunicaciones personales, cadenas o mensajes que no involucren directamente a los destinatarios.

16.6 Se encuentra prohibida la transmisión vía correo electrónico de los siguientes elementos: usuarios, identificadores de entrada al sistema (Login, IDs), contraseñas, configuraciones de redes internas, direcciones y nombres de sistemas.

CONSEJO NACIONAL DE LA MAGISTRATURA Vº Bº Oficina de Tecnologías de la Información

CONSEJO NACIONAL DE LA MAGISTRATURA OFICINA DE PLANIFICACIÓN Y COOPERACIÓN TÉCNICA

MARIO ALVAREZ QUISPE
SECRETARIO GENERAL
Consejo Nacional de la Magistratura

17. Buen uso del correo electrónico

17.1 El servicio de correo es provisto por CNM a los usuarios con el objeto de apoyar el desarrollo de sus funciones, por lo tanto toda información transferida por este medio es de propiedad del CNM.

17.2 El CNM definirá el estándar de una plataforma de correo institucional única; asimismo queda estrictamente prohibido la utilización de otro sistema de correo como medio oficial.

17.3 El uso aceptable del correo se basará fundamentalmente en la comunicación entre trabajadores internos y usuarios externos para fines institucionales.

17.4 Los correos electrónicos enviados desde las cuentas provistas por CNM deben tener las mismas consideraciones tomadas en cuenta al enviar una carta formal con el membrete del CNM.

17.5 En la comunicación por correo se deberá mantener las mismas reglas de cortesía y formalidades de la información escrita, aplicando también todas las reglas semánticas y ortográficas.

17.6 Los mensajes de correo electrónico enviados después del horario de trabajo normal del usuario, se considerarán enviados el día laboral siguiente.

17.7 Cuando se incluya el mensaje original en una respuesta, se sugiere eliminar toda información accesoria que no esté relacionada con el contenido de la respuesta. En estos casos queda estrictamente prohibido introducir modificaciones a los mensajes anteriores sin advertir por escrito esa circunstancia.

17.8 Cada usuario es responsable de mantener el espacio asignado en su cuenta o límites de correo para permitir la correcta recepción de mensajes, para lo cual deberá realizar labores de mantenimiento y limpieza de su correo.

17.9 El Administrador de red tendrá la facultad de borrar correos, condicionado a eventos de seguridad que ponga en juego la disponibilidad del servicio. Si llegase a hacer uso de esta facultad, y fuese posible, deberá respaldar estos correos.

17.10 El CNM no es responsable por el efecto que pueda causar un mensaje enviado por un trabajador a otro trabajador o a un grupo de trabajadores. Los mensajes enviados desde cualquier cuenta de correo son responsabilidad únicamente de la persona a la que se le confió dicha cuenta.

17.11 Los usuarios deben estar informados que el texto de los correos electrónicos no es tomado como información confidencial, que las comunicaciones electrónicas pueden, dependiendo de la tecnología, ser re-enviadas,

CONSEJO NACIONAL DE LA MAGISTRATURA Vº Bº Centro de Tecnologías de la Información

CONSEJO NACIONAL DE LA MAGISTRATURA OFICINA DE PLANIFICACIÓN Y CONSERVACIÓN TÉCNICA

interceptadas, impresas y almacenadas por otros, por lo tanto dicha información es susceptible de fraudes y alteraciones.

17.12 El CNM deberá agregar en el pie de cada correo enviado, una nota que indique la confidencialidad de esta información.

17.13 Al pie de cada mensaje los usuarios deberán insertar una autofirma, a fin que permita al receptor de datos identificar formalmente a su autor, de manera que esté vinculada únicamente a él y a los datos a que se refiere el mensaje, permitiendo detectar cualquier modificación posterior al contenido del mismo, garantizando así la identidad del titular y que éste no pueda desconocer la autoría del documento.

18. Cuentas genéricas de correo electrónico

18.1 El Jefe de la Oficina de Tecnologías de la Información deberá aprobar el uso de las cuentas genéricas de correo electrónico, éstas deberán ser asignadas a una persona, la cual será la responsable de la cuenta y aparecerá como tal.

18.2 Todas las cuentas genéricas deberán tener contraseñas robustas, deben ser conformadas por caracteres alfanuméricos y con un largo mínimo de 8 caracteres alfanuméricos que incluya una letra mayúscula y un número como mínimo.

19. Prohibiciones del servicio de correo electrónico

19.1 Se prohíbe el uso del correo electrónico para fines ajenos a la institución, tales como recibir o transmitir música, videos, humor, gráficos e imágenes inapropiadas. El contenido de los mensajes no debe ser injurioso, ofensivo o irrespetuoso. Los correos electrónicos deben ser de contenido de temas propios y de interés de la Institución.

19.2 En el caso que la información particular sea canalizada a través de una persona que se ausente del CNM, ésta deberá delegar esta función a otra persona de la misma dependencia durante su ausencia y anunciar a sus corresponsales el motivo del cambio.

19.3 Se prohíbe difundir por correo electrónico al interior de la organización, noticias que provengan de Internet o de otros medios, o tomar información de dicha red dándola por cierta.

19.4 Cualquier documento que se adjunte a un mensaje, deberá estar libre de virus. Será responsabilidad del usuario emisor del mensaje la revisión mediante antivirus. Las áreas receptoras de mensajes infectados con virus

CONSEJO NACIONAL DE LA MAGISTRATURA Vº Bº Oficina de Tecnologías de la Información

CONSEJO NACIONAL DE LA MAGISTRATURA OFICINA DE PLANIFICACIÓN Y COOPERACIÓN TÉCNICA

deberán abstenerse de abrirlos y deberán informar al Administrador de Red sobre su presencia.

19.5 Sólo el Administrador de Red puede utilizar el correo electrónico para advertir sobre virus o su posible existencia en las PC, habiendo verificado la autenticidad de la fuente de información.

19.6 Se prohíbe difundir por correo electrónico, dentro o fuera del CNM información clasificada como confidencial. Sin embargo si este fuera el caso el correo electrónico deberá tener en el campo asunto la palabra CONFIDENCIAL, y de ser posible se deberá utilizar técnicas de encriptación, para lo cual deberá coordinar con la Oficina de Tecnologías de la Información para realizar un envío seguro.

19.7 Los empleados del CNM no deben utilizar el correo electrónico como base de datos. Es exclusiva responsabilidad de los usuarios copiar al disco duro de su computadora los archivos recibidos como anexos o adjuntos y los mensajes de correo que estime importantes. El resto de mensajes debe eliminarse periódicamente.

20. Bloqueo de correos electrónicos

20.1 Se bloquearán los mensajes provenientes de servidores de correo gratuito (Hotmail, Yahoo, Gmail, etc.), siempre que se detecte que de cuentas creadas en estos servidores se envíe información mal intencionado a los usuarios del CNM, tales como correos SPAM (correos basura de publicidad), correos PHISHING (correos suplantando identidades).

20.2 Se bloquearán los mensajes provenientes de servidores gratuitos que tengan adjuntos de archivos de los siguientes tipos: ejecutables (*.exe, *.msi, etc.), comprimidos (*.zip, *.rar, etc.), de música y video en todos sus formatos (*.mp3, *.wav, etc.), entre otros; pues podrían contener virus, spyware, gusanos, etc.

20.3 Se evita la usurpación de identidad, impidiendo el ingreso de mensajes provenientes de Internet de supuestos remitentes que pertenecen al dominio "CNM.gob.pe", pues los remitentes permitidos enviarán siempre mensajes desde dentro de la red del CNM y no de fuera de ella.

20.4 La Oficina de Tecnologías de la Información (OTI) será la encargada de los bloqueos indicados en los puntos 1, 2 y 3 del título "bloqueo de correos electrónicos".

CONSEJO NACIONAL DE LA MAGISTRATURA Vº Bº Oficina de Tecnologías de la Información

CONSEJO NACIONAL DE LA MAGISTRATURA OFICINA DE PLANIFICACIÓN Y COOPERACIÓN TÉCNICA

CAPITULO IV
USO DEL SERVICIO DE INTERNET

21. Acceso y uso de Internet

21.1 Los usuarios a utilizar los servicios de Internet provisto por el CNM deben tener precaución con las páginas que ofrecen servicios gratuitos a cambio de una inscripción donde se solicita un conjunto de datos. Se debe tener precaución con la información que se suministra. No debe suministrarse información del CNM ni de su infraestructura tecnológica ni de comunicaciones.

21.2 La Oficina de Tecnologías de la Información implementará mecanismos de seguridad, como filtros de contenido, Proxy y Firewall que disminuyan la posibilidad de acceder a las redes del CNM a personas no autorizadas. Como principio general se debe utilizar "*todos los servicios que se encuentran deshabilitados a excepción de los que se encuentran explícitamente aprobados*".

21.3 Sólo se podrá hacer uso de los servicios de Internet (navegación, correo y otros) a través del canal de comunicación provisto por CNM. No se podrá efectuar conexiones a Internet vía modem o medios alternativos a no ser que se cuente con la autorización formal por parte del Administrador de Red de la Información (o quien haga sus veces).

21.4 Se prohíbe el uso de Internet para fines que no sean netamente laborales, así como participar en actividades políticas, religiosas o comerciales que puedan comprometer la información del CNM, estar involucrado en actividades fraudulentas o distribuir intencionalmente información falsa o difamatoria que podría deteriorar la imagen del CNM.

21.5 Se prohíbe el uso de Internet para acceder a música, pornografía u otros tópicos que no concuerden con las funciones o actividades asignadas por CNM.

21.6 Cuando por propósitos justificados para el desarrollo de las responsabilidades de un servidor público del CNM sea necesario obtener software desde Internet, éste será canalizado a través del encargado de Soporte Técnico (Help Desk). Las faltas al respecto serán monitoreadas e informadas al Administrador de Red.

21.7 Se debe controlar la introducción de virus en forma intencional o accidental a través de archivos obtenidos de Internet.

21.8 En caso que algún usuario requiera tener acceso a un servicio no autorizado, por las tareas que tiene asignada, el Administrador de Red deberá evaluar la

CONSEJO NACIONAL DE LA MAGISTRATURA Vº Bº Oficina de Tecnologías de la Información

CONSEJO NACIONAL DE LA MAGISTRATURA OFICINA DE PLANIFICACIÓN Y COOPERACIÓN TÉCNICA

MARIO ALVAREZ QUISPE
SECRETARIO GENERAL
Consejo Nacional de la Magistratura

posibilidad de incorporar mecanismos que permitan asegurar la confidencialidad e integridad de la información transferida por ese medio y activar el servicio de darse el caso, previa autorización del Jefe de la Oficina de Tecnologías de la Información.

21.9 Está prohibido acceder o intentar acceder al Internet utilizando otras configuraciones de Proxy, DNS, Puertas de enlace y otras sin autorización del Administrador de Red.

21.10 El uso de las herramientas de navegación y el acceso a Internet debe orientarse a cubrir las necesidades específicas del CNM.

21.11 El CNM se reservará el derecho de monitorear o hacer el seguimiento de la navegación web que realicen los usuarios del servicio de Internet, pudiendo tomar medidas correctivas en caso de incumplimiento de la presente norma.

22. Buen uso del servicio de navegación

22.1 Comunicación entre trabajadores internos y usuarios externos para cubrir las necesidades específicas del CNM.

22.2 Soporte técnico para temas de tecnología de información.

22.3 Revisión de sitios Web de proveedores y empresas allegadas al sector para obtener información de los productos, obtener referencia sobre marcos legales, información técnica y recursos.

22.4 Obtener información financiera, técnica, de actualidad, etc. relevante a las necesidades específicas del CNM.

22.5 Comunicación con otras empresas, socios estratégicos, etc.

22.6 El uso de Internet con fines de investigación y desarrollo personal, tales como capacitaciones, desarrollo de tesis, elaboración de monografías, entre otros, relativos a estudios de capacitación y/o especialización, estará permitido únicamente fuera de horarios de oficina y bajo conocimiento del Jefe inmediato superior; a excepción de aquellas en donde el Consejo Nacional de la Magistratura sea el organizador, patrocinador o se cuente con la aprobación de la Alta Dirección.

23. Prohibiciones del servicio de navegación

23.1 Todos los usuarios del CNM sin excepción estarán prohibidos de navegar a sitios no alineados con las buenas conductas como son los de contenido pornográfico, actividades ilegales (drogas, terrorismo, actividades criminales, etc.), juegos en línea, aplicaciones de escritorio remoto, compras en línea, entre otros.

CONSEJO NACIONAL DE LA MAGISTRATURA V°B° Oficina de Tecnologías de la Información

CONSEJO NACIONAL DE LA MAGISTRATURA OFICINA DE PLANIFICACIÓN Y COOPERACIÓN TÉCNICA

23.2 Los usuarios tendrán prohibido el uso de herramientas de Chat, redes sociales, videos en línea y correos electrónicos gratuitos, compras en línea, aplicaciones de escritorio remoto, salvo exista la justificación de accesos mediante solicitud formal del Jefe inmediato superior dirigido al Jefe de la Oficina de Tecnologías de la Información (OTI).

23.3 La habitualidad de visita a estos sitios no aceptables, constituye una infracción ética por parte de los empleados públicos del CNM.

23.4 Navegar o acceder a servicio de Internet desde los servidores, para bajar un parche, actualización de firmware o conectarse a servicio técnico remoto, salvo que sea estrictamente necesario.

24. Asignación de accesos a los servicios de Internet

24.1 El acceso a los servicios de Internet deberá ser solicitado por el Jefe inmediato superior de la dependencia a la que pertenece el usuario, mediante un Memorando dirigido al Jefe de la Oficina de Tecnologías de la Información (OTI), donde deberá indicar el nivel de acceso que requiere para el usuario, así como la justificación de dicha necesidad.

24.2 Los niveles de acceso para la navegación a Internet son:

24.2.1 Nivel I: Acceso sin restricciones, en este nivel el usuario podrá hacer uso sin ningún tipo de limitaciones a la navegación hacia Internet, con excepción de lo señalado en el punto 1 del título "Prohibiciones del Servicio de Navegación".

24.2.2 Nivel II: Acceso con restricciones, en este nivel se restringirá el acceso a páginas de video en línea, chat en línea, redes sociales, juegos, transmisiones de radio o tv por internet y lo señalado en el punto 1 del título "Prohibiciones del Servicio de Navegación".

24.2.3 Nivel III: Acceso Limitado, en este nivel solo se podrá acceder a las páginas de gobierno (.gob), paginas educativas (.edu), paginas militares (.mil), páginas de organismos no gubernamentales (.org), páginas de diarios e información. Todas las demás páginas quedaran restringidas, considerando lo señalado en el punto 1 del título "Prohibiciones del Servicio de Navegación".

24.2.4 Nivel IV: Sin acceso, en este nivel solo se podrá acceder a las En caso existan facilidades técnicas y/o las capacidades del servicio de Internet lo permitan, la Oficina de Tecnologías de la Información (OTI) aprobará la solicitud realizada, y dispondrá a habilitar el servicio respectivo para el usuario.

CONSEJO NACIONAL DE LA MAGISTRATURA V° B° Oficina de Tecnologías de la Información

CONSEJO NACIONAL DE LA MAGISTRATURA OFICINA DE PLANIFICACIÓN Y COOPERACIÓN TÉCNICA

24.3 Cuando un usuario con acceso al servicio de Internet es dado de baja, la Unidad Orgánica responsable deberá solicitar la desactivación del servicio a la Oficina de Tecnologías de la Información a través de un Memorando, en lo posible el mismo día del cese de funciones del usuario.

24.4 Los servicios de Internet deberán ser provistos a los usuarios de acuerdo a las necesidades específicas del CNM.

25. Auditoria y revisión del uso correcto de los servicios de Internet

25.1 El encargado de Soporte Técnico (Help Desk), se reserva el derecho de realizar revisiones de los registros de auditoria de conexiones a Internet, directorios de archivos personales y cualquier otra información almacenada sobre las estaciones de trabajo del CNM, en cualquier momento y sin previo aviso, con el objetivo de asegurar el cumplimiento de las políticas internas.

25.2 El Administrador de red preparará mensualmente un informe en base a la revisión, análisis y reacción ante incidentes reportados por el filtro de contenido, Firewall, Proxy Server u otras herramientas de seguridad de Internet cuando se vislumbre un accionar u navegación irregular a fin de comunicarse a la Jefatura de la Oficina de Tecnologías de la Información.

25.3 El Administrador de Red deberá incorporar en sus actividades la revisión selectiva de los reportes de incidentes de acceso o uso inadecuado de Internet.

CONSEJO NACIONAL DE LA MAGISTRATURA
Vº Bº
Oficina de Tecnologías de la Información

CONSEJO NACIONAL DE LA MAGISTRATURA
OFICINA DE PLANIFICACIÓN Y COOPERACIÓN TÉCNICA