



Buenos Aires, 11 de junio de 2015

RES. CM N° 61 /2015

VISTO:

Las Resoluciones CM Nros. 872/2004 y 239/2013, y la Actuación N° 29987/2013, y

CONSIDERANDO:

Que por Res. CM N° 239/2013 se aprobó la reglamentación en materia informática en concordancia con lo dictaminado por la Dirección General de Asuntos Jurídicos mediante Dictamen N° 5445/2013.

Que en atención a ello se instruyó a la Secretaría de Legal y Técnica para que, a través del Departamento de Análisis Normativo, proceda a la redacción de la reglamentación sobre las políticas de uso de los sistemas, con el propósito de establecer procedimientos que mejoren los parámetros de seguridad.

Que el Departamento de Análisis Normativo presentó un documento denominado "texto actualizado, ordenado y corregido de la Res. CM N° 872/2004 "Política de uso Aceptable de los Servicios de Red y de Internet" a efectos de corregir errores e incongruencias.

Que por Dictamen CAGyMJ N° 7/2014 la Comisión de Administración, Gestión y Modernización Judicial aprobó, proponiendo al Plenario el mismo trato, el referido texto ordenado, actualizado corregido.

Que en una nueva intervención, la ahora Dirección General de Informática y Tecnología propone, ante la necesidad de resguardar la información sensible a la que tienen acceso los agentes que se desempeñan en esa Dirección General, la incorporación de normas de seguridad y confidencialidad las que deberán ser suscriptas, a modo de convenio de confidencialidad, por la totalidad de los agentes que se desempeñan en dicha dependencia.

Que asimismo propone establecer parámetros sobre la titularidad de la propiedad intelectual de posibles desarrollos informáticos efectuados por sus agentes o personal contratado.



Que los textos propuestos fueron analizados y acordados conjuntamente con el personal designado por la Dirección General de Informática y Tecnología y el Departamento de Análisis Normativo.

Que de conformidad con los fundamentos expuestos, corresponde aprobar la Política de Uso Aceptable de los Recursos Informáticos, Servicios de la Red y de Internet; y las Políticas de Seguridad y Normas de Confidencialidad.

Por ello, en ejercicio de las atribuciones otorgadas por Art. 116 de la Constitución de la Ciudad Autónoma de Buenos Aires y la Ley N° 31,

**EL CONSEJO DE LA MAGISTRATURA
DE LA CIUDAD AUTONOMA DE BUENOS AIRES
RESUELVE:**


Artículo 1º: Aprobar la Política de Uso Aceptable de los Recursos Informáticos, Servicios de la Red y de Internet, que como Anexo I forma parte de la presente resolución.

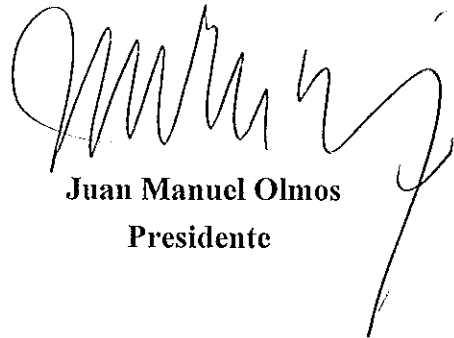
Artículo 2º: Aprobar las Políticas de Seguridad y Normas de Confidencialidad, que como Anexo II forma parte de la presente resolución.

Artículo 3º: Derogar las Resoluciones CM Nros. 872/2004 y 239/2013.

Art. 4º: Regístrese, publíquese en la página de internet del Poder Judicial, comuníquese a la Secretaría Legal y Técnica y, oportunamente, archívese.

RESOLUCION CM N° 61 /2015


Marcela Basterra
Secretaria


Juan Manuel Olmos
Presidente



Res. CM N° 61 /2015

ANEXO I

Política de Uso Aceptable de los Recursos Informáticos, Servicios de la Red y de Internet

Art. 1 Introducción.

El Consejo de la Magistratura promueve el uso de Internet para que los empleados, funcionario y magistrados realicen trabajos específicos a su función y alienta a todos sus agentes y personal contratado a desarrollar habilidades y conocimiento en su uso.

Este reglamento establece las políticas para la utilización de los recursos informáticos y las normas de conducta razonable que deben observar los agentes y funcionarios, cuando utilicen equipamiento, software, direcciones de Internet o nombres de dominio de éstos últimos o cualquier otro recurso informático, teniendo por finalidad la minimización de todos aquellos riesgos que hagan incurrir en responsabilidad a este Consejo de la Magistratura.

Art. 2 Objeto.

Esta política se aplica a la totalidad de los recursos informáticos, los servicios de la red y de Internet y, más específicamente, al acceso a dicha red y al uso del correo electrónico, proporcionados por el Consejo de la Magistratura, cualquiera sea el horario en que se efectúe y la obligación de confidencialidad de los agentes en relación a la totalidad de la información a la que pudieran tener acceso con motivo u ocasión del cumplimiento de sus tareas en el mismo.

No cubre los requerimientos, estándares y procedimientos para el desarrollo e implementación de sitios de información en Internet pertenecientes al Organismo.

Art. 3 Recursos Informáticos.

Se entiende por Recursos Informáticos los equipos informáticos de escritorio o portátiles, teléfonos fijos y móviles, servidores, routers, switches, firewalls, servicios de mensajería de texto, por radio o por cualquier otro medio, el acceso a Internet o a cualquier red interna de computadoras, Intranets, Extranets, o redes de tipo LAN o WAN, servicio de fotocopiadora, fax, impresoras, software de base, software de aplicación, sistemas de copiado de información por medios magnéticos, ópticos y de cualquier otra naturaleza, casillas de correo electrónico (e-mail) y cualquier otro sistema de mensajería a través de Internet o de redes internas provistas o administrados por el Consejo de la Magistratura

Art. 4 Sujetos Comprendidos.



Esta política alcanza a los siguientes usuarios de Internet:

- a) Agentes de planta del Organismo.
- b) Personal contratado que esté autorizado a usar equipos y/o software del Organismo.
- c) Las personas ajenas al Organismo que tengan expresa autorización de un funcionario, agente o personal contratado por la institución, siendo responsabilidad del autorizante toda consecuencia legal, de naturaleza administrativa o judicial emanada de dicha autorización.

Art. 5 Reglas Generales.

- a) Los sistemas de computación del Organismo sólo pueden ser utilizados para propósitos de uso oficial.
- b) Los agentes deberán utilizar Internet para mejorar su conocimiento del trabajo; para acceder a información científica, técnica, o toda otra relativa a temas que tengan relevancia para el Organismo, comunicándose para ello con otras Organizaciones Públicas, Instituciones Académicas y con el Sector Privado en general.
- c) Los usuarios deben tomar conocimiento que las direcciones de correo electrónico, direcciones IP(1) y nombres de dominio y demás recursos pertenecientes al Concejo de la Magistratura, incluyendo la información almacenada, constituyen bienes intangibles de valor económico de propiedad del mismo, por lo que su utilización será considerada como realizada en su representación, salvo que expresamente se dejase aclarado que la misma y sus consecuencias no constituyen la posición oficial del Organismo.
- d) Es indispensable que no se utilice Internet para propósitos que puedan influir negativamente en la imagen del Organismo o de sus autoridades y agentes.
- e) Ante cualquier desperfecto o mal funcionamiento de los equipos computadoras, los usuarios deberán reportar en forma inmediata dicho evento a la MESA DE AYUDA, de la Dirección General de Informática y Tecnología, quedando prohibido a los agentes, intentar solucionar el desperfecto o mal funcionamiento por sí, atento que ello podría generar daños a los sistemas informáticos o invalidar garantías.

Art. 6 Derechos de los Usuarios.

Los agentes podrán realizar las siguientes actividades:

- a) Acceder a información relacionada con su función.
- b) Utilizar el correo electrónico, listas de discusión y otros servicios, siempre que tengan relación directa con su función en el Organismo. Si se expresan opiniones personales, deberá aclararse que las mismas no son necesariamente la posición oficial del Organismo.

Art. 7 Normas Generales sobre el Acceso y Uso de los Recursos Informáticos.

- a) Todo agente solo tiene acceso a los recursos informáticos que explícitamente se le autoricen.



- b) Ante una licencia prolongada de un agente, su cuenta de usuario será desactivada para proteger el acceso indebido a sus documentos e información personal. La misma será restablecida el día en que el agente se reincorpore.
- c) Los cambios de contraseña de todo servicio informático deberá ser solicitado por nota a la Dirección General de Informática y Tecnología, completando el "Formulario de Cambio de Contraseñas".
- d) Los nombres de usuario están sujetos a la disponibilidad, estando compuestos por la primera letra del nombre y el apellido completo. En el caso de ser un usuario que utilice el sistema de gestión judicial Iurix existe una limitación de ocho (8) caracteres.
- e) Las altas de usuario se realizan completando el "Formulario de Alta de Usuarios", siendo uno de los requisitos para que en la Dirección General de Factor Humano se le pueda dar de alta al legajo personal y deberá ser remitido a la Dirección General de Informática y Tecnología para su procesamiento.
- f) Las bajas de usuario deberán ser notificadas a la Dirección General de Informática y Tecnología por el responsable de la dependencia en la cual prestaba servicios el agente. En caso de ser notificada la resolución a la Dirección General de Informática y Tecnología previamente a la notificación del área correspondiente, se tomará la misma como válida para proceder a la baja del usuario.
- g) Los pases o traslados de personal a otra dependencia y/o edificio se realizan completando y enviando el "Formulario de Traslado de Usuarios" que deberá ser remitido a la Dirección General de Informática y Tecnología.

Art. 8 Prohibiciones o Usos Inaceptables.

Se encuentra prohibido el acceso a la red, a Internet o al correo electrónico del Poder Judicial de la Ciudad Autónoma de Buenos Aires a toda persona ajena al Organismo.

Art. 8.1. Prohibiciones Generales.

Se prohíbe a los agentes, en ejercicio u ocasión de sus funciones, dentro o fuera del horario laboral, el uso de los equipos y/o internet provistos por el Organismo para:

- a) Acceder sin autorización a sistemas de cómputo, a la red del Organismo o transgredir la autorización que como usuario restringido se hubiere otorgado.
- b) Violar los derechos de privacidad de terceras personas.
- c) Transmitir amenazas, material obsceno o de hostigamiento.
- d) Transmitir publicidad no deseada.
- e) Corromper o destruir datos o realizar cualquier otra acción que pueda impedir el acceso legítimo a los datos, incluyendo la carga de un virus, de gusanos o de cualquier software dañino en cualquier sistema de cómputo conectado a la red.
- f) Cualquier uso condenado por las políticas de uso aceptable de la red conectada.



- g) Realizar cualquier conducta considerada ilegal, por ser contraria a la legislación aplicable de cualquier país al que se pueda tener acceso por la red.
- h) Utilizar la red para juegos recreativos.
- i) Distribuir material por Internet que cause daños, tal como la piratería, el sabotaje y más específicamente la distribución de software dañino.

Art. 8.2. Prohibiciones Particulares.

En particular y a los fines relacionados con el cumplimiento de la función desempeñada en el Organismo queda prohibido:

- a) Efectuar el downloading (2) de archivos, salvo que esta posibilidad no implique vulnerar o infringir los derechos de terceros titulares de derechos de autor. Entiéndase por “downloading”, el proceso consistente en “bajar” a través de internet u otras redes, archivos de programas, etc. desde una computadora cualquiera a la propia
- b) Realizar cualquier actividad contraria a los intereses del Organismo, tal como publicar información reservada, acceder sin autorización a recursos o archivos o impedir el acceso a otros usuarios mediante el mal uso deliberado de recursos comunes.
- c) Utilizar la red para propósitos no relacionados con las actividades del Organismo, prohibiéndose su utilización para el desarrollo de cualquier actividad comercial personal en Internet, ya sea la compra, venta u oferta de bienes o servicios o bien utilizar la red para la transmisión de publicidad comercial relacionada con dicha actividad.
- d) Utilizar la red para conducir al personal a la realización de actividades lucrativas.
- e) Iniciar cualquier actividad que pueda comprometer la seguridad de los servidores del Organismo.
- f) Dar autorización o permiso a una persona no conectada a la red del Organismo para que la utilice ilegalmente.
- g) Revelar a terceros contraseñas de acceso (3) o compartirlas con otros usuarios.
- h) Realizar cualquier actividad de recaudación de fondos.
- i) Realizar cualquier actividad de recreación personal o de promoción de intereses personales (tales como creencias religiosas, hobbies, etc.).
- j) Iniciar sesiones de Internet (4) usando recursos del Organismo desde ubicaciones remotas, salvo que estén especialmente autorizados para ello.

Art. 9 Responsabilidades de los Superiores.

Los superiores de los agentes y del personal contratado tendrán las siguientes responsabilidades:

- a) Evaluar la necesidad de los agentes de acceder a Internet para cumplir con sus funciones, contemplando aquellas situaciones donde el requerimiento se encontrare



dirigido a obtener información técnica sobre determinado producto o bien a obtener ayuda en línea.

- b) Obtener acceso a Internet para los agentes que lo necesiten en razón de sus funciones debiendo cumplirse, en cuyo caso, con las normas de procedimiento que habilitan el acceso a Internet publicadas por la Oficina Nacional de Tecnologías de Información.
- c) Autorizar excepcionalmente el acceso a Internet en días no laborables para propósitos relacionados con la función que el agente cumple dentro del Organismo, estableciéndose como regla general la imposibilidad de acceso en las referidas circunstancias.
- d) Comunicar a los agentes las restricciones en el empleo de recurso del Organismo para acceder a los servicios de internet para uso personal, guardando copia de las respectivas notificaciones.
- e) Asegurar que los agentes conozcan esta "Política de Uso Aceptable" y llamar su atención cuando se tome conocimiento de su falta de cumplimiento.
- f) Poner en conocimiento del personal las sanciones que les podrían corresponder, -(desde llamado de atención, prohibición de acceso a Internet hasta el inicio de las correspondientes acciones administrativas y/o judiciales)-, como consecuencia de su incumplimiento.
- g) Notificar al administrador de la red cuando un agente deja de prestar servicio en el Organismo para que sus cuentas sean deshabilitadas.

Art. 10 Responsabilidades de los Usuarios.

Los usuarios de la red y de internet, a fin de evitar inconvenientes por falta de recursos y garantizar la seguridad física y lógica de los mismos, tendrán las siguientes responsabilidades:

- a) Conocer y aplicar lo establecido en la Política de Uso Aceptable.
- b) Seguir las políticas y procedimientos de seguridad existentes para el uso de los servicios de la red y de Internet (5) y evitar toda práctica que pueda dañar los sistemas de computación y archivos de datos del Organismo, como por ejemplo, aquellos que puedan dar lugar a ataques de virus cuando se recuperen archivos de Internet.
- c) Limitar sus comunicaciones con terceros a los temas respecto de los cuales tienen conocimiento y responsabilidad profesional.
- d) Identificarse adecuadamente en toda comunicación con terceros, indicando su nombre, dirección electrónica y dependencia a la que pertenecen.
- e) Conducirse de forma que refleje positivamente la imagen del Organismo, ya que se encuentran identificados como empleados del mismo.
- f) Cumplir las indicaciones y pautas establecidas por el Organismo para reducir los problemas de seguridad así como el impacto de virus en la red.



Art. 11 Correo Electrónico.

El Consejo de la Magistratura proporciona a sus agentes una dirección de correo electrónico que se conformará con el nombre del mismo, el símbolo @ y el dominio "jusbaire.gov.ar" u otro dominio de titularidad del Consejo de la Magistratura; pudiendo por razones de mejor administración, modificar la dirección de correo electrónico del agente sin que éste tenga derecho a reclamo alguno.

La utilización del correo electrónico como medio de transmisión de información por parte de los agentes del Poder Judicial de la Ciudad Autónoma de Buenos Aires debe favorecerse, teniendo en cuenta sus notorias ventajas sobre los medios tradicionales (economía, rapidez, eficiencia y confiabilidad).

Sin embargo, sus características también exigen un comportamiento responsable por parte de los usuarios, con el fin de convertirlo en un sistema ágil y seguro.

El uso del correo electrónico resulta el más apropiado cuando el usuario:

- a) No tiene urgencias en recibir una respuesta y/o en ubicar al receptor.
- b) Desea enviar el mensaje a más de un receptor.
- c) Necesita información específica sobre determinados temas.
- d) Necesita dejar evidencia escrita respecto de los mensajes transmitidos.

Art. 11.1 Normas básicas para el uso del Correo Electrónico.

Los usuarios del sistema de correo electrónico deben:

- a) Tomar conciencia que el correo electrónico y la cuenta de e-mail proporcionados por el Organismo para el cumplimiento de sus tareas, son de titularidad del mismo independientemente del nombre y clave de acceso que fueren necesarias para su utilización.
- b) Asumir una absoluta responsabilidad respecto al contenido de todo mensaje que envíen utilizando los recursos o medios proporcionados por el Organismo. Estos deben ser explícitos y concisos, escritos en un tono amable y utilizando un lenguaje adecuado, que no exceda los límites del buen gusto ajustándose a las normas convencionales de ética, conducta y cortesía.
- c) Transmitir y almacenar información considerada confidencial solo en caso de encontrarse debidamente autorizados.
- d) Evitar en todos los casos la divulgación de sus claves o contraseñas de acceso personales.
- e) Verificar diariamente sus casillas electrónicas, evitando la acumulación de mensajes en ellas. En este sentido se advierte que debido a políticas internas relativas a la administración de los recursos informáticos, al exceder determinado volumen dichos mensajes serán eliminados automáticamente.



f) Queda prohibido falsear, confundir, ofuscar, sustituir o suplantar la identidad de un usuario de comunicación electrónica. El nombre de usuario, la dirección de correo electrónico y los datos relacionados incluidos en los mensajes deben ser certeros e indicar el verdadero origen de los mismos. No se deben enviar comunicaciones anónimas o que puedan generar error sobre la persona del emisor.

g) Respecto al correo electrónico rige la misma política de monitoreo establecida para Internet y la red. Sólo se procederá a la comprobación o interceptación de los contenidos de los e-mails de los agentes por orden judicial o cuando existan razones de amenaza para el funcionamiento y/o seguridad del Organismo al cual representan.

Art. 11.2 Reglas de Estilo para la Utilización del Correo Electrónico.

a) Los agentes deberán respetar las siguientes reglas de estilo.

- Firma debe contener la siguiente información:
- Nombre y apellido del agente
- Dependencia en la que desarrolla sus tareas
- Teléfono e interno
- Teléfono celular si fuese provisto por el Consejo de la Magistratura.

b) Tener en cuenta que al utilizar las direcciones de correo electrónico del Organismo están actuando en su representación. Si las opiniones que expresan son a título personal, deben aclarar que esa no es la posición oficial del Consejo de la Magistratura. A tal fin deberá incluirse al pie de los mensajes de correo electrónico la siguiente leyenda:

“Cuidemos el Medio ambiente imprimiendo solo lo necesario.

El contenido del presente mensaje y sus adjuntos es privado, estrictamente confidencial y exclusivo para su destinatario, pudiendo contener información protegida por normas legales y de secreto profesional. Bajo ninguna circunstancia su contenido puede ser transmitido o relevado a terceros ni divulgado en forma alguna. En consecuencia de haberlo recibido por error, solicitamos contactar al remitente y eliminarlo del sistema.

Todas las opiniones contenidas en este mail son propias del autor del mensaje y no necesariamente coinciden con las del Consejo de la Magistratura.

El Consejo de la Magistratura no asume responsabilidad ni obligación legal alguna por cualquier información incorrecta o alterada contenida en este mensaje”.

Art. 12. Uso de Claves de Acceso.

Las Claves de Acceso constituyen un elemento fundamental de la seguridad.

Los agentes son los únicos responsables de la confidencialidad de sus claves de acceso a las computadoras, a las casillas de correo electrónico provisto, como a todo otro medio informático cuya utilización requiera una clave de acceso.



Son la primera protección de las cuentas de usuario. Una Clave de Acceso inapropiada puede comprometer a toda la red institucional del Poder Judicial de la Ciudad. Por lo tanto, todos los usuarios de los sistemas del Organismo (incluyendo a terceros con acceso a estos sistemas) son responsables de adoptar las medidas que aseguran un correcto empleo de sus Claves de Acceso.

Dichas claves de acceso serán, en todos los casos, definidas por los agentes, quienes en caso de considerar que las mismas pudieran estar en conocimiento de terceros, deberán dar aviso a su superior jerárquico a fin de que se tomen las medidas de seguridad pertinentes.

Art. 12.1. Procedimientos.

- a) Todas las Claves de Acceso a nivel de sistema (por ejemplo: root, Administradores NT /W2003, Linux y cualquier otra forma de administración) deben ser cambiadas periódicamente.
- b) Todas las Claves de Acceso de los sistemas en producción deben ser administradas en forma global.
- c) Todas las Claves de Acceso a nivel de usuarios (por ejemplo: Correo electrónico, acceso a la red o a los puestos de trabajo) deben ser cambiadas como mínimo cada seis meses. El intervalo recomendado es cada cuatro meses.
- d) Las Claves de Acceso no deben ser transmitidas vía correo electrónico u otras formas de comunicación electrónica.
- e) Todas las Claves de Acceso tanto a nivel de usuario como de sistema deben conformarse según las instrucciones que se destacan a continuación.

Para la construcción de Claves de Acceso se debe utilizar Claves de Acceso apropiadas (fuertes) para toda identificación que sea permanente y para toda cuenta de usuario asignada por el Organismo.

Art. 12.2. Claves de Acceso Apropiadas.

Las Claves de Acceso apropiadas (fuertes) se caracterizan por.

- a) Contener caracteres en Mayúsculas y Minúsculas (i.e.: a-z, A-Z)
- b) Contener dígitos y signos de puntuación además de letras (i.e.: , 0-9, !@#\$\$%^&*()_+|~- =\`{}[]:;'\<>?,./)
- c) Tener un mínimo de ocho caracteres.
- d) No ser palabras que pertenecen a ningún idioma o dialecto.
- e) No estar basadas en información personal.
- f) Las Claves de Acceso nunca deben ser escritas o almacenadas en línea. Trate de crear Claves de acceso que sean fáciles de recordar. Una manera es usar cierta frase conocida como referencia, por ejemplo la frase "Yo te saludo mañana" puede generar la clave YtSalu2mña.



Art. 12.3. Claves de Acceso Débil o Inapropiada.

Una Clave de Acceso débil o inapropiada se caracteriza por:

- a) Contener menos de ocho caracteres.
- b) Puede ser encontrada en un Diccionario.
- c) Es un nombre propio, por ejemplo:
 - Nombres de familiares, mascotas, amigos, compañeros de trabajo, personajes públicos y otros de este tipo.
 - Términos y nombres de computadoras, sitios, empresas, sistemas y/o equipamiento,
 - Fechas de cumpleaños y cualquier otra información personal, tales como direcciones y números telefónicos.
 - Combinaciones con letras repetidas o secuenciales del tipo aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Todas las anteriores escritas en orden inverso.
 - Todas las anteriores precedidas o seguidas por un número (por ejemplo, secret1, 1secret).

Art. 12.4. Protección de Claves de Acceso.

Todas las claves deben ser tratadas como información sensible y secreta del Organismo, en razón de ello, los usuarios deben, respetar las siguientes pautas.

- a) No se debe utilizar la misma clave empleada en el ámbito del Organismo en otros ambientes, si necesitase utilizar más de una clave en el CMCABA, las mismas deberán ser diferentes.
- b) No debe revelar su clave vía telefónica a nadie.
- c) No debe revelar su clave en un mensaje de correo.
- d) No debe proporcionar su clave a sus superiores.
- e) No debe hablar sobre sus claves con otros.
- f) No debe revelar su clave en cuestionarios o formularios de ningún tipo.
- g) No debe compartir su clave con familiares.
- h) No debe revelar su clave a sus compañeros de trabajo al irse de vacaciones.
- i) Si alguien le pide su clave refiérale estos procedimientos.
- j) No debe compartir con nadie su clave de acceso, incluyendo al personal administrativo, asistentes o secretarías.
- k) No debe utilizar las facilidades de "Recuerde la Clave" encontradas en ciertas aplicaciones.
- l) Las claves no deben ser escritas ni guardadas en ninguna computadora o medio magnético sin antes ser encriptadas.



m) En caso de que la clave pudiera estar en conocimiento de terceros, se deberá dar aviso a su superior jerárquico a fin de que se tomen las medidas de seguridad pertinentes.

En forma aleatoria este Organismo puede analizar la factibilidad de “romper” (buscar hasta encontrar) su clave. Si esto ocurre Usted será notificado y deberá proceder al cambio de la misma en forma inmediata.

Art. 12.5. Estándares para el Desarrollo de Aplicaciones.

Los desarrolladores de aplicaciones deben asegurar que las aplicaciones desarrolladas / implementadas contemplen los criterios de seguridad siguientes:

- a) La autenticación debe ser realizada a nivel de usuarios y no grupos.
- b) Las Claves de Acceso no deben ser almacenadas sin previa encriptación.
- c) Deben permitir el uso de roles que eviten recurrir al uso de la clave de un usuario en particular para completar tareas rutinarias.
- d) Deberán soportar autenticación vía TACACS+ , RADIUS y/o X.509 con LDAP, siempre que sea posible.

Art. 12.6. Uso de Claves de Acceso y Frases para Acceso Remoto de Usuarios.

El acceso a la red del Organismo vía remota deberá ser controlado sea mediante claves válidas para un único uso o utilizando sistemas de Claves Públicas provisto de frases claves fuertes.

Art. 12.7. Frases Claves.

Las Frases Claves son generalmente utilizadas en los procesos de autenticación de claves pública / privada. Un sistema de claves pública / privada define una relación matemática entre la clave pública (conocida) y la privada (conocida solo por el usuario). Las Frases Claves se utilizan para acceder a la clave privada.

Las Frases Claves no son lo mismo que las Claves de Acceso. La Frase Clave es una versión más larga que una clave común y por lo tanto más segura. La Frase Clave está compuesta por múltiples palabras.

Todas las reglas enumeradas para la evaluación y construcción de Claves de Acceso son válidas a la hora de definir Frases Claves.

Art. 13 Titularidad de Propiedad Intelectual de Desarrollos Informáticos. Conforme art. 4 inc. d) de la Ley 11.723 modificada Ley N° 25.036 B.O. 11/11/1998) Ley de Propiedad Intelectual.

El agente o personal contratado que desarrolle o reformule un sistema informático deberá realizar las pruebas y ajustes necesarios para el correcto funcionamiento del programa, debiendo entregar la totalidad de los archivos ejecutables, las indicaciones técnicas, los



manuales de uso, el código fuente y realizar la capacitación que sobre el mismo se le requiera.

Queda expresamente estipulado que el agente o personal contratado a que se hace referencia en el párrafo anterior **no será**, en ningún caso, titular de los derechos de propiedad intelectual sobre el sistema propiamente dicho, que hubiese desarrollado o reformulado, renunciando expresamente, a favor del Consejo de la Magistratura, a todos los derechos y acciones que pudieran corresponderle reconociendo al Consejo de la Magistratura de la Ciudad de Buenos Aires, como único titular de la totalidad de los derechos sobre el mismo.

Art. 14 Responsabilidad del Administrador de Correo Electrónico.

El Administrador de correo electrónico del Organismo no podrá, bajo ninguna circunstancia, retener, desviar, divulgar o alterar mensajes que no estén dirigidos específicamente a su dirección.

Deberá proveer los medios para que sea devuelto a su emisor todo mensaje recibido que no pueda ser transferido a su destinatario (por ejemplo, un mensaje con dirección errónea).

Además, deberá arbitrar medidas para borrar el cuerpo principal de todo mensaje fallido (es decir, que no pueda ser entregado, cualquiera sea la causa) para luego devolverlo al emisor.

Art. 15 Breve Glosario de Términos.

(1) **Direcciones IP:** Número que identifica un host (máquina) unívocamente en una red, representado usualmente por cuatro números entre 0 y 255 separados por puntos.

(2) **Downloading:** Es el proceso para "bajar" (traer) a través de Internet u otras redes, archivos de programas, etc. desde una computadora cualquiera a la propia.

(3) **Contraseñas de acceso:** Sucesión de letras y números que permiten a un usuario acceder a un servicio de la red.

(4) **Sesiones de Internet:** Conexiones a Internet realizados por los usuarios

(5) **Servicios de Internet:** Facilidad que presta el organismo para que los usuarios puedan consultar páginas por Internet, acceder al Correo Electrónico, etc.

Art. 16 Son Obligaciones sobre el Software.

a) El personal dependiente de la Dirección General de Informática y Tecnología es el único autorizado a instalar, desinstalar y administrar el software, aplicaciones y sistemas instalados en todas las computadoras del Poder Judicial de la Ciudad Autónoma de Buenos Aires.

b) Ante la necesidad de incorporar o instalar un software, el mismo tiene que ser solicitado por nota a la Dirección General de Informática y Tecnología fundamentando el



requerimiento sin especificar una versión o producto específico. La Dirección le dará prioridad a aplicaciones para las que el Consejo de la Magistratura (CABA) ya es propietario o aplicaciones con licencia GNU/GPL.

c) Las aplicaciones P2P (peer-to-peer) fomentan la propagación de virus, malware, spyware, troyanos, y aplicaciones maliciosas para las cuales el Consejo de la Magistratura (CABA) no tiene licencia y por tal motivo quedan explícitamente prohibidas. Algunos ejemplos de estas aplicaciones son Edonkey y Kazaa, entre muchas otras.

d) El correcto funcionamiento de aplicaciones de mensajería instantánea queda sujeto a la prestación del servicio por parte del proveedor. La Dirección General de Informática y Tecnología va a garantizar la disponibilidad del servicio en función de los recursos informáticos, tales como ancho de banda de red y recursos en los servidores.

Art. 17 Son Obligaciones sobre el Correo Electrónico.

a) El recupero de emails eliminados deberá ser solicitado completando el “Formulario de Recupero de Información” que deberá ser remitido a la Dirección de Informática y Tecnología.

b) La capacidad (“cuota”) inicial de una cuenta de correo electrónico es de 512 MB debiendo el usuario liberar en forma periódica espacio en la casilla de correo provista, siendo responsable por las comunicaciones que no pudieran serle entregadas por encontrarse llena la casilla.

c) Para evitar la propagación de virus queda limitado el envío y recepción de archivos ejecutables, siendo bloqueados en tiempo de envío en el servidor de correo electrónico. Los archivos ejecutables son aquellos que en su mayoría son virus o contienen código malicioso.

d) Todos los agentes que tengan usuario de red poseen cuenta de correo electrónico oficial.

Art. 18 Son Obligaciones sobre las Listas de Correo.

a) Las listas de correo deberán ser solicitadas por nota a la Dirección General de Informática y Tecnología con las direcciones de correo electrónico que componen la misma, con la limitación que tienen que ser cuentas de correo oficiales (@jusbaire.gov.ar).

b) Las listas de correo pueden tener una demora en la moderación y en la entrega de correos. No siendo las listas de correo el método preferido ante la necesidad de notificar algo en lo inmediato.

Art. 19 Son Obligaciones sobre el Uso de las Impresoras.



- a) El personal autorizado a realizar el cambio de toners y mantenimiento general de las impresoras es el personal perteneciente a la Dirección de Informática y Tecnología, y el personal contratado a tal fin.
- b) El movimiento físico de las impresoras dentro y entre dependencias es realizado por personal autorizado, caso contrario no podrán ser utilizadas existiendo demora en la puesta en funcionamiento de las impresoras luego del traslado.
- c) En lo referente al máximo de hojas que se pueden imprimir en un solo "trabajo de impresión", queda limitado a cien (100) hojas y/o 20Mb. Un "trabajo de impresión" corresponde a una solicitud de impresión por una cantidad de hojas o copias concreta. Superando el límite establecido pueden presentarse demoras, inconvenientes con la impresión y la imposibilidad total o parcial de imprimir el "trabajo de impresión".

Art. 20 Son Obligaciones sobre los Equipos Informáticos.

- a) El ingreso a las dependencias con equipos informáticos no provistos por la Dirección de Informática y Tecnología queda supeditado a la Resolución CM N° 766/2005 sobre el Procedimiento para el Inventario y Registro de Bienes Muebles del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires.
- b) Todo equipo incautado para el cual haga falta hacer un relevamiento y/o diagnóstico deberá ser solicitado por nota a la Dirección de Informática y Tecnología. La demora para la realización de las tareas que se requieran queda sujeta a la disponibilidad y a los recursos con los que cuente el servicio técnico asignado a la dependencia.
- c) Queda prohibido conectar a la red eléctrica y de voz/datos cualquier equipo informático, telefonía o afín, siendo el responsable de cualquier daño producido a personas, bienes y/o instalaciones del Poder Judicial de la Ciudad Autónoma de Buenos Aires aquella persona que haya realizado la conexión sin previa autorización y asistencia del personal técnico correspondiente.

Art. 21 Son Obligaciones sobre la Conexión a Internet.

- a) El tráfico a Internet es autenticado con usuario y contraseña. El mismo que se requiere para utilizar un equipo de la red informática.
- b) La conexión a Internet es uno de los recursos informáticos limitados a autorización expresa.
- c) Todo agente que no posea autorización para acceder a Internet, tiene acceso a las páginas locales, para así poder acceder a la Intranet del Poder Judicial de la Ciudad Autónoma de Buenos Aires, al sistema de gestión judicial JusCABA, al sistema administrativo GesCABA y otros sitios desarrollados por la Dirección General de Informática y Tecnología.



Art. 22 Son Obligaciones sobre las Unidades de Red y los Documentos.

- a) Toda la información eliminada, de la que la Dirección General de Informática y Tecnología posee resguardos y sea autorizada, puede ser recuperada en el curso del día siempre y cuando haya sido eliminada durante el mismo día. El recupero de información previa al día de la fecha es solicitada por nota y remitida a la Dirección de Informática y Tecnología, completando el "Formulario de Recupero de Información".
- b) Los documentos considerados valiosos, para los que se les da prioridad para realizar el resguardo, son aquellos que son almacenados en las unidades remotas H: (Personal de cada usuario) y G: (Recurso Compartido). Siendo estos las unidades de almacenamiento correctas para almacenar información crítica. No se realizan backups de unidades de almacenamiento locales, como discos rígidos, unidades de zip, disketteras, llaveros USB y documentos almacenados en los escritorios.
- c) La unidad pública conocida con la letra P: es de acceso total por todos los agentes. No hay control en cuanto a la modificación, eliminación y lectura de ninguno de los documentos. Asimismo tampoco se realizan resguardos.
- d) De la unidad de almacenamiento pública conocida con la letra P: se realizan limpiezas semestrales de todos los archivos que no fueron modificados por más de seis (6) meses.
- e) La utilización de unidades removibles como un diskette o un zip queda a criterio de los usuarios. No es recomendado almacenar información en los mismos siendo un medio obsoleto y con una alta probabilidad de pérdida total o parcial de información; menos aún para información valiosa o crítica. Se recomienda utilizar como medio de transporte de datos el correo electrónico, las unidades de red privadas o los llaveros USB.

Art 23 Administradores de los Sistemas.

- a) Las responsabilidades y facultades sobre la administración de sistema deben ser justificada y documentada.
- b) Los administradores de los sistemas deben tener usuarios individualizados con acceso restringido que permitan únicamente realizar las tareas de administración de los sistemas que se les fue asignadas.
- c) La asignación o denegación de responsabilidades las realizará el área y deben quedar documentadas.
- d) No se debe administrar los sistemas con usuarios genéricos o que imposibiliten delimitar las responsabilidades sobre las acciones tomadas
- e) Los administradores de los sistemas deben registrar el acceso, motivo y resolución tomada cada vez que ingresen a los sistemas.
- f) Los administradores deben implementarse medidas que garanticen la imposibilidad de robo de claves y contraseñas y el impacto que esto conlleve.



- g) Los usuarios y contraseñas de administración total no deben ser utilizadas salvo extrema necesidad y deben existir un procedimiento que garantice su resguardo seguro y su disponibilidad ante una emergencia.
- h) Deben promoverse herramientas que permitan una administración centralizada y segura que permita auditorías sobre la administración.
- i) Los usuarios, contraseñas y/o privilegios asignados a los administradores deben ser bloqueados o eliminados en el momento de no requerirse más.

Art. 24 Transferencia de Conocimiento y Supervisión.

- a) El área debe instrumentar los medios necesarios para que los administradores estén capacitados para realizar sus tareas.
- b) La tarea de administración debe estar supervisada por el área.
- c) Todos los procedimientos de administración de sistemas deben estar documentados y deben ser conocidos por los administradores.

Art. 25 Instalación y Configuración de Sistemas.

- a) Los procedimientos de puesta en producción de los sistemas deben estar documentados.
- b) Los sistemas deben que instalarse por defecto con todas las configuraciones de seguridad y auditoría que posean activadas.
- c) Todos los sistemas que se instalen deben ser auditados antes de su puesta en producción.
- d) Deben realizarse auditorías de seguridad periódicamente en todos los sistemas.
- e) Debe evaluarse constantemente las incorporaciones de nuevas herramientas, procedimientos o técnicas que mejoren la seguridad de los sistemas y reduzcan los costos de administración.

Art. 26 Registro de Eventos.

- a) Todos los eventos, sucesos o alertas de todos los sistemas deben registrarse y almacenarse por XXX de manera centralizada.
- b) Se deberá crear un procedimiento de seguridad para restringir el acceso al servidor que almacena los eventos permitiendo su acceso controlado y documentado solo para auditorías o de ser necesario mantenimiento.
- c) Todos los usuarios que tengan los permisos para ver, borrar o modificar los registros deben autorizar su ingreso con herramientas de autenticación de múltiples factores y éstas estar resguardadas por el presidente de la Comisión de Administración, Gestión y Modernización Judicial.
- d) Los registros almacenados deben protegerse de su alteración o eliminación y estar disponibles para su análisis.
- e) Debe existir una réplica del servidor a más de doscientos (200) metros del principal.



f) Deben implementarse herramientas que permitan una auditoría completa de la administración de los sistemas.

Art. 27 Respaldo seguro de la Información.

- a) Toda la información que se genere y/o se almacene en los sistemas deben estar clasificada y deben ser respalda según su clasificación.
- b) Debe documentarse la manera que se respalda la información y los procedimientos para su verificación y recuperación.
- c) Debe limitarse el acceso a la información respaldada al personal de administración de sistemas que explícitamente tenga acceso.
- d) Debe registrarse todo acceso a la información respaldada y su motivo.

Art. 28 Reciclado o Destrucción de Medios de Almacenamiento de Información.

- a) Antes del reciclado para su sobreutilización de los medios de almacenamiento el área debe garantizar que la información que éste contenga sea completamente eliminada.
- b) Se debe garantizar la integridad y vida útil de todos los dispositivos de almacenamiento de información que se reutilicen.
- c) Todos los dispositivos de almacenamiento de información que no se utilicen más deben ser destruidos físicamente garantizando la inaccesibilidad de la información antes contenida previamente a su baja patrimonial.



Res. CM N° 61 /2015

ANEXO II

Políticas de Seguridad y Normas de Confidencialidad

1. Alcance: Todo agente dependiente de la Dirección General de Informática y Tecnología deberá suscribir a modo de notificación un ejemplar de las Políticas de Seguridad y Normas de Confidencialidad que se detallan a continuación el que será agregado a su legajo.

2. Objeto: Las Políticas sobre Recursos Informáticos y confidencialidad son el conjunto de las principales normas que regulan la utilización de la totalidad de los recursos informáticos proporcionados por el Consejo de la Magistratura y la obligación de confidencialidad de los agentes dependientes de la Dirección General de Informática y Tecnología en relación a la totalidad de la información a la que pudieran tener acceso con motivo o en ocasión del cumplimiento de sus tareas, así como la información de sus proveedores y la de cualquier otra dependencia u organismo público o entidad privada con la que el Consejo de la Magistratura establezca relaciones institucionales.

3. Compromiso de uso: Los agentes se comprometen a utilizar los Recursos Informáticos únicamente en los términos y con las limitaciones descriptas en las normas generales y en la Resolución de la que este Anexo forma parte y con la exclusiva finalidad de prestar más eficientemente las tareas encomendadas quedando prohibida cualquier otra utilización de los mismos con fines comerciales, políticos, en interés particular o cualquier otro que no sea el fin laboral que motivó su provisión por parte de Consejo de la Magistratura.

4. Utilización de los equipos y software: Los agentes deberán utilizar los equipos provistos conforme las indicaciones de sus fabricantes, las que de ser necesario, serán puestas a su disposición.

Solo podrá utilizarse el software que se encuentra debidamente licenciado, provisto o autorizado por Consejo de la Magistratura, debiendo cumplir, en todos los casos con los términos de las licencias de uso. No se podrán, en ningún caso, instalar ni modificar, mediante cualquier operación -ingeniería inversa, alteración del código fuente, o cualquier otra- el software instalado en los equipos provistos, ni realizar copias del software ni de la información almacenada en los referidos equipos, salvo que dichas copias hayan sido expresamente encomendadas en el marco de las políticas de almacenamiento de resguardo (*back up*) del Consejo de la Magistratura.



5. Claves de acceso. Los agentes son los únicos responsables por la confidencialidad de sus claves de acceso a las computadoras, a las casillas de correo electrónico provisto, como a todo otro Medio Informático cuya utilización requiera de una clave de acceso.

6. Titularidad de propiedad intelectual de desarrollos informáticos. Conforme art. 4 inc. d) de la Ley 11.723 modificada Ley N° 25.036 B.O. 11/11/1998) Ley de Propiedad Intelectual.

El agente o personal contratado que desarrolle o reformule un sistema informático deberá realizar las pruebas y ajustes necesarios para el correcto funcionamiento del programa, debiendo entregar la totalidad los archivos ejecutables, las indicaciones técnicas, los manuales de uso, el código fuente, quedando obligado a realizar la capacitación que sobre el mismo se le requiera.

6.1. Reconocimiento Expreso: El agente -o personal contratado- que desarrolle o reformule un sistema informático durante su relación laboral con el Consejo de la Magistratura, reconoce y acepta que **no será**, en ningún caso, titular de los derechos de propiedad intelectual del sistema que hubiese desarrollado o reformulado, reconociendo expresamente al Consejo de la Magistratura de la Ciudad de Buenos Aires, como único titular de todos los derechos sobre el referido sistema y renunciando a su favor la totalidad de las acciones que pudieran corresponderle.

7. Confidencialidad de la información en general. El agente reconoce y acepta que toda información que reciba, y documentos a los cuales tenga acceso en función o como consecuencia de las tareas desarrolladas para Consejo de la Magistratura, no clasificada previamente conforme a la Norma de Tratamiento de Información, tienen el carácter de confidencial respecto de terceros y por ende, deberá abstenerse de revelarla sin consentimiento previo.

Sin perjuicio de otra información que sea expresamente identificada como "Confidencial", a los efectos de estas Políticas se considerará como tal a toda la información de naturaleza técnica, como métodos, procesos, "*know how*", fórmulas, software, tecnología, etc.

La información será considerada confidencial cualquiera sea el soporte o medio en el que se almacene (papeles, libros, registros físicos, magnéticos, electrónicos, informáticos, etc.). Se deberá mantener la confidencialidad de la información aludida mientras dure su vínculo laboral con Consejo de la Magistratura, luego de finalizado éste por cualquier causa, por el término de 2 (dos) años.



En aquellos casos en que se considere necesario, se podrán establecer normas de uso específicas para determinada categoría de medio informático, las que serán complementarias a estas Políticas.

8. Confidencialidad de la información en particular. El agente usuario de la información y de los sistemas utilizados para su procesamiento, solo podrá acceder a aquellos datos y recursos para los que se le concedió autorización.

Tales recursos serán utilizados conforme las funciones asignadas y con los fines para los que fuera autorizado debiendo mantener la confidencialidad y privacidad de la información.

Además de las normas de confidencialidad dispuestas, cumplirá los procedimientos y controles implementados para la utilización de los sistemas y demás recursos de la tecnología de la información, debiendo cumplir y hacer cumplir las medidas de seguridad orientadas a la protección física y lógica de los recursos del Consejo de la Magistratura notificando inmediata y fehacientemente a la Dirección General de Informática y Tecnología las violaciones y riesgos que detecten relacionados con la seguridad.

Cualquier información y/o documentación enviada o recibida a través de las casillas de correo electrónico en violación a las Leyes de Propiedad Intelectual (11.723), de Confidencialidad de la Información (24.766), de Protección de Datos Personales (25.326), o cualquier otra norma, será responsabilidad del agente y dará lugar a las sanciones que corresponda.

9. Notificación:

En el día de la fecha me notifico de las presentes Políticas, las que comprendo y me comprometo a cumplir en todos sus términos.

Nombre y Apellido:

Dependencia donde Realiza las Tareas:

Teléfono e Interno:

Dirección de Mail:

DNI:

Firma:

