ANEXO I

Términos y condiciones

Los/as usuarios/as que ingresen a los Sistemas internos y externos, se obligan a utilizarlo en forma lícita, de acuerdo a los presentes términos y condiciones y respetando la normativa vigente (Plan Integral de Modernización del ANMAC Resolución N°013/2016, GDE -Decreto N° 733/2018 y modificatorias-, Política de Seguridad de la Información de la ANMaC).

1. Los/as usuarios/as autorizados/as a utilizar los aplicativos son los siguientes:
a) Personal interno perteneciente a la Agencia Nacional de Materiales Controlados, ya sean contratados o de planta.
b) Personal Externo perteneciente a instituciones u organismos que se encuentren debida y explícitamente autorizados.
2. El/la usuario/a y clave de otorgados por la ANMaC, habilitará a los/as usuarios/as a operar los módulos necesarios para realizar las tareas asignadas.
3. El código y clave de usuario/a otorgados, serán de exclusiva responsabilidad del/la usuario/a.
4. Al inicio del proceso de registro, el/la usuario/a deberá modificar la clave suministrada en su primer inicio de sesión, siendo responsable de su resguardo.
5. Los/as usuarios/as del Sistema no pueden transferir o divulgar sus claves, las que son personales, secretas e intransferibles. El/la usuario/a será responsable exclusivo en caso de su divulgación y de los perjuicios que pudiese ocasionar a terceros o al Sistema, siendo pasible de ser sancionado/a, sin perjuicio de las acciones civiles o de otra naturaleza que le pudiesen corresponder.
6. Las transacciones efectuadas y firmadas por el/la usuario/a utilizando su respectiva clave, se consideran realizadas por él/ella. A tal efecto, se considera que las mismas son válidas, legítimas y auténticas, sin necesidad de realizar o tomar ningún otro resguardo, de cualquier índole.
7. El/la usuario/a es responsable por el uso indebido o inadecuado de los recursos informáticos y de los daños y perjuicios que puedan resultar a causa de cualquier presentación falsa o incorrecta efectuada al usar el Sistema.
8. Los/as usuarios/as se comprometen a notificar inmediatamente a los/as Administradores/as de los Sistemas internos y externos de ANMaC, dependientes de la Dirección de Sistemas –o dependencia que en un futuro la reemplace-, de la pérdida de su contraseña o del acceso no autorizado por parte de terceros a su cuenta. Además, se comprometen a enviar información sobre las vulnerabilidades detectadas en el Sistema a la siguiente dirección de contacto: informatica@anmac.gob.ar.
9. El/la usuario/a tiene el deber de respetar la confidencialidad y la integridad de cualquier información o dato al que tenga acceso, y es personalmente responsable de proteger y salvaguardar estos recursos.
10. Al utilizar el Sistema, el/la usuario/a reconoce y acepta que los/as Administradores/as del Sistema y los Auditores/as miembro de la Unidad de Auditoria Interna de la ANMaC podrán solicitar el acceso a la información presente en su cuenta, preservarla y/o divulgar su contenido o cualquier contenido asociado a la misma, en el caso de ser necesario por razones estrictamente legales o, si

existiese razones fundadas que permitan suponer que el acceso, conservación o divulgación de dicha información es necesario para:

a) Cumplir con leyes, regulaciones, procesos legales o solicitudes administrativas efectuadas por autoridad competente o judiciales exigibles;

b) Aplicar estos términos y condiciones, incluida la investigación de posibles infracciones a los mismos;

c) Detectar, prevenir y/o abordar, de cualquier modo, los casos o situaciones relativas a la seguridad del Sistema o de sus usuarios/as;

d) Proteger contra todo daño inminente los derechos, propiedad o seguridad de los Sistemas ANMaC y de sus usuarios/as en la manera prevista o permitida por todas las normas, especialmente de conformidad a lo previsto en el artículo 11 de la Nº Ley 25.326 y sus modificatorios;

e) Utilizarla con el fin de auditar y evaluar el desempeño de la gestión electrónica ofrecida;

f) Utilizarla para responder a los pedidos de acceso a la información pública, en el marco de lo establecido en la Ley Nº 27.275, sus modificatorias y complementarias;

g) Optimizar las respuestas de pedidos de acceso a la información pública, en los términos señalados en el punto anterior;

h) Ayudar a obtener métricas de uso y niveles de servicio del Sistema;

11. La información de identificación que el/la usuario/a provea para acceder y operar dentro del Sistema, se mantendrá en servidores ubicados en un ambiente controlado y seguro, protegidos del acceso, uso o divulgación no autorizados.

12. Es responsabilidad del/la usuario/a mantener sus datos personales actualizados en todo momento, informando a la Coordinación de Recursos Humanos y en su defecto a la Coordinación de Informática.

13. Si el/la usuario/a proporcionara datos falsos, inexactos o incompletos, o los/as Administradores/as del Sistema tuvieren motivos fundados para sospechar tal conducta, la cuenta del/la usuario/a podrá ser cancelada por el/la Administrador/a de los Sistemas, denegándole el acceso y uso de los Sistemas.

14. Queda expresamente prohibido por parte del/la usuario/a:

I. Modificar, alterar y/o borrar, sin las autorizaciones correspondientes, la información o las configuraciones del Sistema y aplicativos instalados;

II. Interferir, sin autorización, el acceso de otros/as usuarios/as al Sistema;

III. Transgredir o eludir las verificaciones de identidad establecidos en los Sistemas;

IV. Realizar actos maliciosos o que atenten contra el Sistema, que impacte directamente en el funcionamiento adecuado del mismo, o que de alguna forma puedan llegar a dañar, inutilizar, sobrecargar, deteriorar, limitar o inutilizar el normal funcionamiento de los Sistemas o la utilización de todas o algunas de las funcionalidades de los mismos, entre ellos: cargar archivos que contengan malware, archivos dañados o cualquier otro software o programas similares o introducir a los Sistemas cualquier tipo de virus, gusano, o programa de computación cuya intención sea hostil, destructiva y que impidan, inutilicen, puedan dañar o efectivamente causen daños a los Sistemas y/o a sus usuarios/as y/o inferir cualquier otro daño a los equipos o a la información, las configuraciones del sistema operativo o los aplicativos que se encuentren instalados en los Sistemas;

V. Realizar acciones que impongan una carga irrazonable o desproporcionadamente grande sobre la infraestructura del Sistema;

VI. Intentar acceder, mediante los Sistemas, a datos restringidos sin la debida autorización y/o transgredir las barreras de seguridad de los Sistemas para llegar a ellos;

VII. Realizar búsquedas de vulnerabilidades o explotación de las mismas, a través de los Sistemas, para cualquier fin, sin la debida autorización efectuada por el Administrador del Sistema;
VIII. Divulgar información acerca de la detección de vulnerabilidades encontradas en el Sistema a terceros no autorizados;
IX. Difundir, publicar, distribuir o difundir dentro del Sistema material o información difamatorio, transgresor, obsceno, indecente o ilegal;
X. Cargar al Sistema archivos que contengan software u otro material protegido por derechos de propiedad intelectual, o que transgreda el derecho a la privacidad, a menos que el Organismo Implementador o el/la Usuario/a sea el/la propietario/a o controle dichos derechos, o haya recibido las autorizaciones necesarias;
XI. Eliminar las atribuciones de autor, los avisos legales o las designaciones o etiquetas de propiedad de cualquier archivo que se cargue al Sistema;
XII. Difundir, a través del Sistema, ideas políticas, lograr la adhesión a campañas o movilizaciones, captar el voto, enviar o reenviar comunicaciones masivas o realizar cualquier otro tipo de práctica de políticas partidarias;
XIII. Enviar cualquier transmisión de datos en forma fraudulenta a través del Sistema;
XIV. Distribuir, permutar o intercambiar con fines comerciales la información contenida dentro de los Sistemas.
XV. Modificar, copiar, transmitir, vender, ceder, distribuir, exhibir, publicar, licenciar, crear trabajos derivados, o usar, en general, el contenido disponible en o a través de los Sistemas para fines comerciales y otros sin la previa autorización, entre otros:
a) copiar, modificar, adaptar, traducir, realizar ingeniería inversa, descompilar o desensamblar cualquier parte del contenido y/o de los Sistemas;
b) reproducir y/o comunicar por cualquier medio el contenido con fines prohibidos;
c) interferir o interrumpir el funcionamiento de los Sistemas;
d) vender, ceder, licenciar o explotar el contenido y/o cualquier tipo de acceso y/o uso de los Sistemas;
e) utilizar los Sistemas con fines ilícitos o inmorales; e
f) infringir de cualquier modo los presentes TyC.

XVI. El/la usuario/a, es responsable de tomar los recaudos necesarios para proteger sus credenciales de acceso e información personal suministrada dentro de los Sistemas.
XVII. En el desarrollo de sus funciones, los/as usuarios/as deberán utilizar los Sistemas para mejorar la eficacia y eficiencia administrativa. Su utilización no podrá constituirse en obstáculo para el cumplimiento de las funciones encomendadas al/la usuario/a.
XVIII. El/la usuario/a se compromete a cerrar su cuenta al final de cada sesión.
XIX. Los/as usuarios/as de los Sistemas declaran conocer y aceptar la circunstancia relativa a que el Administrador de los Sistemas puede, en cualquier momento, modificar en todo o en parte los presentes términos y condiciones.

USO ACEPTABLE DE LOS SISTEMAS

Se acepta que los/las usuarios/as aprovechen en forma limitada los Sistemas para un uso personal que derive en su mayor y/o mejor jerarquización y/o especialización en sus conocimientos, prácticas y habilidades y/o para aprovechar los beneficios de la información y el conocimiento para el mejor desarrollo y cumplimiento de las

funciones asignadas, previa autorización por escrito otorgada por el funcionario que corresponda.
No obstante, tal uso no podrá interferir con las funciones y tareas que el/la usuario/a cumple en la ANMaC ni en las competencias del mismo.

El uso aceptable se encuentra sujeto al estricto control del Administrador de los Sistemas y del/la funcionario/a a cargo de cada área.

El uso aceptable puede ser controlado, revocado o limitado en cualquier momento.

No se considera uso aceptable aquel que demande un gasto adicional para la ANMaC, excepto aquel que derive del uso normal de los recursos informáticos.

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2022-44098269-APN-DNAAJYM#ANMAC

CIUDAD DE BUENOS AIRES
Miércoles 4 de Mayo de 2022

Referencia: ANEXO I DIRECTRICES PARA LA AUTENTICACIÓN, AUTORIZACIÓN Y CONTROL DE ACCESO A LOS SISTEMAS QUE UTILIZA LA AGENCIA NACIONAL DE MATERIALES CONTROLADOS

El documento fue importado por el sistema GEDO con un total de 4 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.05.04 16:41:40 -03:00

Miguel Alfredo La Scalea
Coordinador
Dirección Nacional de Administración, Asuntos Jurídicos y Modernización
Agencia Nacional de Materiales Controlados

Digitally signed by Gestion Documental Electronica
Date: 2022.05.04 16:41:40 -03:00