POLÍTICA DE USO ACEPTABLE DE CORREO ELECTRÓNICO, INTERNET, INTRANET y RED

1. INTRODUCCIÓN

Este documento se encuentra incluido dentro del Anexo “Gestión de Comunicaciones y Operaciones” de la Política General de Seguridad de la Información – SENASA.

2. OBJETIVO

El objetivo de la presente Política es el de definir las reglas de uso aceptable para los servicios de “Correo Electrónico”, “Internet”, “Intranet” y “Red”, para lo cual se emiten los siguientes lineamientos de cumplimiento obligatorio.

3. ALCANCE

Esta Política es de cumplimiento obligatorio para todo el personal del Organismo, independientemente de su situación de revista y de su asiento de funciones.

El uso de la “red”, así como los recursos de información del SENASA, están disponibles para fortalecer el flujo de información interna, la investigación, la capacitación, la administración y el apoyo a las diferentes tareas encomendadas, haciendo el trabajo más eficiente y productivo.

Se espera de todos los usuarios una actuación con altos principios morales y éticos al utilizar los recursos. El uso inapropiado de los mismos será sancionado y conllevado a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

4. GENERALIDADES

4.1. PROPIEDAD DE LOS RECURSOS

El SENASA define que todos los recursos relacionados con las tecnologías de la información (datos, sistemas, equipos e instalaciones) son de su propiedad y serán tratados como activos siendo, por lo tanto, sujetos de administración, monitorización y control.

En cuanto a los datos e información, los considera como activos estratégicos, por lo tanto deberán ser usados en función del trabajo asignado.

Para asegurar el correcto uso y detectar acciones indebidas, todos los recursos serán monitorizados mediante archivos de log, registros de ingresos, requerimientos realizados, cantidad de bytes transferidos y recibidos, éxitos y fracasos en las transferencias, fechas y horarios infrecuentes de accesos, rastreos de IP y por todo aquel control manual o automático implementado para tal fin.

Como consecuencia de ello, el personal que utilice los equipos del Organismo para acceder a los servicios de correo electrónico, Internet, Intranet y red, así como la información conservada en los equipos y la que está en tránsito, solicitada o enviada, está sujeta a ser monitorizada, controlada y reportada en sus actividades por el personal de la Dirección de Tecnología de la Información, administradora de los recursos.

En caso de detectarse comportamientos inadecuados o cualquier tipo de abuso que atente contra la seguridad e integridad de otros usuarios o recursos del Organismo, el agente en infracción será bloqueado en forma preventiva para acceder a los servicios prestados, debiendo el empleado solicitar la reincorporación del mismo, cuya autorización deberá elevar con la firma del Director Nacional de su área de trabajo.

Por su parte, la Dirección de Tecnología de la Información deberá informar a la Dirección de recursos humanos acerca del hecho para su intervención y que esta aplique la sanción correspondiente.

4.2. SOLICITUD DE SERVICIO

Toda solicitud de servicio de alta, baja, modificación y excepción deberá realizarse por GDE. En caso de no poseer acceso por algún motivo, podrá remitirse por medio del formulario correspondiente, firmado por el Director/Coordinador dependiendo del tipo de petición (todos los formularios se encuentran publicados en la Intranet) y remitidos a la Mesa de Ayuda para su tratamiento.

La Dirección de Recursos Humanos y Organización debe informar a la Dirección de Tecnología de la Información toda alta de personal para su incorporación como usuario de correo electrónico, Internet nivel básico e Intranet.

Dicha Dirección deberá hacerle firmar al nuevo personal el “Formulario de aceptación de términos de uso de recursos informáticos”, que se adjunta como Apéndice al presente, el que deberá ser guardado en su legajo.

La habilitación y desafectación de equipos a la red de datos debe ser solicitada a la Mesa de Ayuda para la posterior intervención de la Unidad de Ingeniería en Comunicaciones de la DTI.

Asimismo, debe informar a la Dirección de Tecnología de la Información toda baja de personal para su bloqueo de cuentas de usuario, teléfono y recursos informáticos asignados.

El Área de Seguridad Informática debe indicar la baja del agente al Área de Aplicaciones Centrales, Área de Soporte Técnico, a la Unidad de Ingeniería en Comunicaciones, al Área de Base de Datos y al Área de Telefonía para completar la baja de los recursos y cuentas de usuario que utilizaba.

4.3 NOMENCLATURA DE CUENTAS DE USUARIO

Son fijadas por el Área de Aplicaciones Centrales. Prioritariamente, las cuentas personales de usuario se conforman por la inicial del nombre, seguida por el primer apellido completo. De existir igualdad con otra cuenta, se procederá a modificarla de modo tal de generar una cuenta única.

Las cuentas institucionales o cuentas de grupo, deben hacer referencia al área específica, programa o curso solicitante, informando el nombre completo o la abreviatura que lo representa. El responsable de dicha cuenta es el titular a cargo de la cuenta a referenciar. Todos los usuarios pertenecientes al grupo recibirán el e-mail que lleguen a este destino pero la respuesta será individual, de manera de hacer un uso responsable, con nombre propio y no guarecerse detrás de un grupo.

4.4 CONTRASEÑAS

El uso de contraseñas (*password*) es necesario para mantener la *confidencialidad* de la información. Se define confidencialidad a la información accesible solo para aquellas personas (usuarios) autorizadas a tener acceso.

El criterio para componer una password debe utilizarse para todos los accesos en donde sea necesario ingresar contraseñas, como por ejemplo el correo electrónico, Internet, el acceso a la PC, sistemas informáticos, etc.

Una contraseña para que se la considere fuerte debe contener al menos:

- DIEZ (10) dígitos.
- Caracteres numéricos no consecutivos.
- Caracteres alfabéticos no consecutivos.
- Caracteres especiales como por ejemplo ° # &) ¡ / + % € @.
- No deben ser nombres propios, de familiares o mascotas.
- No deben ser nombres que se relacionen fácilmente con usted, como equipos de fútbol, bandas de música o números de teléfono.
- No deben ser fechas de nacimiento/cumpleaños/aniversarios.
- Recuerde cambiar la contraseña en períodos no prolongados [al menos una vez cada DOS (2) meses].
- Evitar repetir las contraseñas cada vez que las cambia, por lo menos en las últimas DIEZ (10) veces.
- No debe tildar o aceptar las opciones de “Recordar Contraseña”.
- No debe divulgar la contraseña ni la deje anotada en lugares inseguros. La contraseña no debe ser compartida ni por la secretaria ni por los compañeros de oficina.

5. RESPONSABILIDADES

5.1 RESPONSABLES DE AUTORIZACIÓN

Son responsables de la autorización, baja y modificación de perfil de usuario los Directores Nacionales. También son responsables de autorizar los cambios y restablecimientos de contraseñas.

Asimismo, tienen el compromiso de evaluar la necesidad de los usuarios de acceder al servicio de Internet para cumplir con sus funciones, solicitando el nivel de acceso adecuado y/o las excepciones web necesarias.

El criterio sugerido es que se autorice el nivel de acceso web, de acuerdo a la función específica de los usuarios dentro del Organismo.

Los Directores Nacionales deben notificar a los agentes a su cargo, las restricciones en el uso de los recursos del Organismo para acceder a los servicios de correo electrónico, Internet e Intranet y a la Red, y deben poner en conocimiento del personal, las sanciones por incumplimiento o uso indebido a las que están sujetos como consecuencia del quebrantamiento de esta Política.

5.2 RESPONSABLES DE HABILITACIÓN Y DESAFECTACIÓN

Son responsables de la habilitación/desafectación de los servicios de correo electrónico, Internet e Intranet el personal de las áreas informáticas de la Dirección de Tecnología de la Información.

Es responsable de la habilitación/desafectación/reparación del software y hardware de los equipos (PC, periféricos, etc.) el personal del Área de Soporte Técnico de la Dirección de Tecnología de la Información. Dicho personal solo está autorizado a instalar y configurar software legal y de uso en el Organismo, de la misma manera que el hardware, solamente equipos y dispositivos patrimoniados por el SENASA.

Es responsable de la habilitación/desafectación de los servicios y equipos de red, el personal de la Unidad de Ingeniería en Comunicaciones de la Dirección de Tecnología de la Información.

Cuando corresponda, serán responsables de cumplimentar todas las tareas aquí enunciadas, los Informáticos Regionales; esto es, en los Centros Regionales, en las Oficinas Locales, en las Delegaciones, en los Laboratorios y en cualquier otra dependencia del SENASA que la Dirección de Tecnología de la Información crea conveniente afectar.

Cualquier usuario que haga uso de las responsabilidades mencionadas podrá ser sancionado, ya que no posee competencia para ejecutar las tareas citadas.

5.3 RESPONSABILIDADES DE LOS USUARIOS

A) Conocer y aplicar lo establecido en la presente Política de Uso Aceptable.
B) Adoptar una forma de conducirse en el manejo de los activos y recursos que refleje positivamente la imagen del Organismo, de manera de reducir los problemas de seguridad de la información a los que se está expuesto.
C) Utilizar el correo electrónico, Internet, Intranet, la red de datos y todo servicio que tenga relación directa con la función que desempeña.
D) En caso de que a través de los servicios expuestos, se expresen opiniones personales, se deberá dejar constancia que las mismas corren por parte del usuario y "no representan la posición oficial del Organismo".

6. ESPECIFICACIONES DE LOS RECURSOS

6.1 CORREO ELECTRÓNICO

Se asignará UNA (1) cuenta de correo electrónico oficial por cada agente del Organismo y UNA (1) o varias cuentas de correo electrónico institucional oficial por cada área o sector que necesite utilizar este tipo de cuentas.

Los valores asignados de tamaño de casilla de correo y/o almacenamiento están sujetos a las limitaciones de infraestructura que posee el Organismo. Dichas capacidades serán publicadas en la Intranet de SENASA.

Tales descripciones de cantidades y recursos están exceptuadas para la Coordinación de Comunicación Institucional, dado el volumen de datos que administra y publica.

6.2 INTERNET

Niveles de navegación

Nivel Básico:
- Acceso a todos los sitios web.
- Restringido por sitios de chat, mensajería instantánea, redes sociales, webmail, pornografía, música en línea, juegos en línea, contenidos de racismo, violencia, sectas, drogas, sitios rosas, hackers, radio y televisión, evasiones de proxy, financieras o legales, apuestas, tarjetas digitales, descargas, nubes, telefonía internet, conexiones remotas y todo aquel sitio peligroso, deshonesto y/o ilegal.

Nivel Jerárquico:
- Acceso a todos los sitios web.
- Restringido por sitios de pornografía, música en línea, juegos en línea, contenidos de racismo, violencia, sectas, drogas, hackers, radio y televisión, evasiones de proxy, financieras o legales, apuestas, tarjetas digitales, nubes, telefonía internet, conexiones remotas y todo aquel sitio peligroso, deshonesto y/o ilegal.

Nivel Prensa:
- Acceso a todos los sitios web.
- Restringido por sitios de pornografía, música en línea, juegos en línea, contenidos de racismo, violencia, sectas, drogas, hackers, evasiones de proxy, financieras o legales, apuestas, tarjetas digitales, nubes, telefonía internet, conexiones remotas y todo aquel sitio peligroso, deshonesto y/o ilegal.
- Las redes sociales solo están permitidas para el área específica de la Coordinación de Comunicación Institucional que opera con este tipo de servicio web.
- Los servicios de almacenamiento y compartir archivos solo están permitidos para el área específica de la Coordinación de Comunicación Institucional que opera con este tipo de servicio web.
- Los servicios de radio y televisión en línea solo están permitidos para el área específica de la Coordinación de Comunicación Institucional que opera con este tipo de servicio web.

Excepciones web:

Todo aquel sitio necesario para el desarrollo de las tareas encomendadas, ya sean estos accesos temporales o permanentes.

También forman parte de la excepción los servicios de nube pagos, es decir que proporcionen un usuario y contraseña válido, una cuota garantizada, servicio de soporte técnico y servicio de *backup* -mínimamente- y sean estos utilizados con fines laborales, principalmente intercambio de trabajos con otros organismos y empresas.

Se podrá permitir el acceso a un solo servicio de webmail externo, siendo este debidamente aprobado por el Director Nacional, preferentemente Gmail de la empresa Alphabet Inc. Deberá recordarse que los correos electrónicos provenientes o enviados desde estos servicios externos carecen de valor institucional. Solamente son válidos los correos electrónicos con dominio @senasa.gob.ar.

6.3 INTRANET

Un único nivel de navegación web de Intranet total para todos los usuarios.

La página web de la Intranet SENASA debe estar configurada por defecto en el inicio del navegador web.

Esto además sirve para efectuar una nueva validación de ingreso a los recursos que se ejecutan en la PC/Notebook, ya que el agente deberá escribir el nombre de usuario (*login*) y contraseña (*password*) nuevamente.

6.4 RED

De acuerdo a la ubicación de los dispositivos PC, notebook, tableta, etc., tareas que desarrollan en ellas los usuarios y características técnicas, la numeración IP de cada recurso podrá establecerse por medio de direcciones estáticas o dinámicas (DHCP).

El enlace entre equipos estará dado por la utilización de medios de conectividad según corresponda, pudiendo utilizarse cableado de fibra óptica o UTP, inalámbrica (redes wireless), antenas satelitales, módems u otra, o cualquier otra tecnología acorde a las necesidades del sitio.

La sola mención del término "Red" en esta Política hacer referencia a "todo" tipo de red de datos utilizada en el Organismo independientemente de su topología, dispositivos, componentes, alcance y extensión, por lo tanto, los beneficios y prohibiciones afectan a todas las posibles redes encontradas y dispositivos componentes de ella.

7. NORMAS DE BUEN USO

En estas normas se detallan "buenas prácticas" en el uso y aprovechamiento de los recursos de información, tecnológicos e informáticos provistos por el SENASA para el desarrollo de las actividades.

La utilización de los recursos por parte de personal ajeno al Organismo está totalmente prohibida. Únicamente con la solicitud vía formulario se podrán -en caso de aprobarse- configurar accesos especiales y controlados VPN, por ejemplo- para el desarrollo de tareas específicas.

Las restricciones que surgen en la utilización de estos medios son solamente a efectos de evitar el uso inadecuado de los mismos y la minimización de todos aquellos riesgos que pueden comprometer las actividades y/o recursos del SENASA.

La demanda de servicios puede ocasionalmente exceder la disponibilidad, por lo que serán establecidas prioridades, dando las más altas de ellas a las actividades consideradas críticas para llevar a cabo la misión del Organismo.

Para todos los casos, deberán contactarse con la Mesa de Ayuda de la Dirección de Tecnología de la Información sobre cualquier deficiencia o funcionamiento irregular que se observe.

7.1 CORREO ELECTRÓNICO - DERECHOS Y OBLIGACIONES DE LOS USUARIOS

A) Acceder a la cuenta personal/institucional de correo electrónico oficial al menos UNA (1) vez al día (jornada laboral), de manera de evitar la acumulación de mensajes en ella. En este sentido, se advierte que debido a políticas internas relativas a la administración de los recursos informáticos, al exceder determinado volumen (cuota), los mensajes excedentes serán rechazados automáticamente y la cuenta bloqueada. Esto se realiza con el fin de no seguir generando tráfico de correos electrónicos no depositados en la casilla.

B) Tomar conciencia de que la cuenta asignada para el cumplimiento de las tareas es de propiedad del Organismo, independientemente del nombre de usuario y contraseña otorgada.
C) La única cuenta de correo electrónico válida para utilizar por los agentes para transmitir y/o recibir información es la oficial, de dominio @senasa.gob.ar.
D) Se debe evitar en todos los casos, la divulgación de la contraseña de acceso.
E) Jamás debe tildar o aceptar las opciones de "Recordar Contraseña".
F) Asumir una absoluta responsabilidad respecto del contenido de todo mensaje que se envíe 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, la moral y las buenas costumbres. Las personas que reciben mucho correo electrónico pueden no leer un mensaje mal hecho. No utilice letras en MAYÚSCULA, esto es considerado como gritar, en su lugar, estile usar símbolos para enfatizar algo, como el asterisco (*) para significar negrita o guión bajo (_) para subrayar. Por ejemplo: _El mercader de Venecia_ es mi libro *favorito*.
G) Se debe tener en cuenta que al utilizar las direcciones de correo electrónico del Organismo, se está actuando en su representación. Si las opiniones que se expresan son a título personal, se debe aclarar que las mismas no reflejan la "posición oficial del Organismo".
H) El correo electrónico es el mecanismo más común de transporte e ingreso de malware (virus informáticos). Por esta razón, se deberá cumplir con las siguientes reglas básicas:
- No se deben abrir NUNCA archivos extraños, anexos a los mensajes de correo electrónico provenientes de un remitente desconocido, sospechoso o poco confiable. Estos mensajes deben ser eliminados inmediatamente.
- Se deben suprimir los correos tipo SPAM (correos electrónicos de publicidad no solicitados y distribuidos a muchos destinatarios), cadenas (correos cuyo contenido invita a replicarlo varias veces a otras personas) y cualquier otro correo electrónico que no esté relacionado con las actividades propias del Organismo y que no haya sido solicitado por el usuario.
- Se debe ser estrictamente cuidadoso con su dirección electrónica, no la publique, ni participe en foros poco confiables o en cadenas de e-mail, ello ayudará a reducir considerablemente los ataques de virus electrónicos y el ingreso de SPAM.
I) Es obligatoria la utilización de carpetas personales para almacenar en forma local, los correos electrónicos que desea conservar. Elimine los mensajes innecesarios.
J) Su firma de correo electrónico al pie de un mensaje debe ser breve e informativa, no mayor de TRES (3) líneas y debería usarse solo cuando sea necesario.
K) Nunca debe incluir su dirección de correo electrónico en la firma, ya que esta fue incluida en la parte superior del mensaje.
L) Cuando reenvíe un mensaje, incluya el mensaje original para que el destinatario del mensaje conozca de qué se está tratando la respuesta enviada.
M) Se recomienda que la cantidad de destinatarios de un correo electrónico, en casos normales, no sea superior a DIEZ (10) direcciones.
N) Cada usuario es responsable de los archivos adjuntos que envía, se tomarán las medidas respectivas en caso de envío adrede con malware o información confidencial del Organismo.
O) El envío de mensajes a todo el personal se autoriza únicamente para asuntos oficiales:

- Se debe comunicar al Área de Aplicaciones Centrales de la DTI que se enviará un correo electrónico [mayor a CINCUENTA (50) direcciones de correo electrónico], la fecha y el horario (antes de las 8:45 o luego de las 16:45 horas de todo día laboral).
- Se podrá enviar un correo electrónico masivo siempre y cuando no sea posible presentar la información que se quiere transmitir a través de la página de Intranet del Organismo, pudiendo citarse como ejemplo:
    - Fechas de pago de sueldo, viáticos, etc.
    - Comunicaciones institucionales y de prensa.
    - Comunicaciones al personal.
- Asimismo, se deben crear grupos de envíos, de manera que la información sea precisa y llegue al destinatario que la espera. Por ejemplo, presentaciones de agentes en radio o TV o cable local de determinadas zonas del país, por distancia imposibles de escuchar o ver por otros.
- Estas listas de grupos deben "cotejarse" o "verificarse" periódicamente, de modo de tener los listados actualizados y no generar correo electrónico basura.
- A partir de esto, se establece que todo el material por divulgar, en forma institucional, debe ser publicado en la página de Intranet del Organismo, la cual es de uso obligatorio como página principal del navegador web y debe ser visitada al menos una vez al día.

P) Cuando envía o publica información, respete los derechos de autor en el material que reproduzca, ya sea en forma parcial o en su totalidad. Casi todos los países -incluida la REPÚBLICA ARGENTINA-, poseen leyes de derecho de autor y sus penalidades.

Q) Al igual que la información que se publica, la declaración que se redacta a través del correo electrónico debe ser concreta, coherente, exacta, clara y ágil en su lectura y comprensión.

R) Antes de enviar un mensaje (comunicaciones a otros Organismos, citaciones, formalidades, temas de agenda, etc.), revise los destinatarios, el *subject*, asunto o título y pase el corrector ortográfico sobre el texto. Una buena práctica de uso es componer el escrito en un procesador de texto -MS Word, Notepad, Wordpad, etc.-, pasar el corrector ortográfico para luego copiar y pegar la redacción en el cuerpo del mensaje a enviar.

S) Si el mensaje que va a enviar es extenso [más de SETENTA (70) líneas], agregue la palabra "extenso" o "largo" en el título del mensaje, para que la persona que lo va a leer sepa de las características del mismo.

T) Los mensajes de correo electrónico deben tener un título que refleje el contenido del mismo.

U) Límite el largo del mensaje a SESENTA Y CINCO (65) caracteres y presione la tecla <ENTER> al terminar cada línea.

V) No utilice tabuladores, ya que mucho software administrador de correo electrónico no interpreta este tipo de caracteres y puede acarrear correo basura en el mensaje original.

W) Cuando envíe un correo electrónico a otra zona del país o del exterior, sea cuidadoso con los vulgarismos o acrónimos locales.

X) Todo usuario debe respetar la naturaleza confidencial del acceso de una persona o cualquier otra información que pueda caer en su poder, ya sea como parte de su trabajo o por accidente, en este caso la información recibida deberá ser eliminada inmediatamente.

Y) Cuide el medio ambiente. Antes de imprimir un correo electrónico, piense bien si es necesario hacerlo. Una tonelada de papel implica la tala de DIECISIETE (17) árboles. Si va

a imprimir, utilice la opción de “Versión Rápida, Baja Calidad o Económica” después de seleccionar la opción “imprimir”. Esta práctica de “no impresión innecesaria” debiera aplicarse para cualquier tipo de documento.

7.2 CORREO ELECTRÓNICO - PROHIBICIONES O USOS INACEPTABLES

Todos los enunciados que se proclaman en este punto penan las actividades que no sean laborales, o laborales sin ser anunciadas o fuera de horario estipulado.

A) Utilizar los servicios de comunicación, en este caso el correo electrónico, para intimidar, insultar, difamar, ofender, acosar a otras personas o interferir en el trabajo de otros usuarios.
B) Utilizar el servicio para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o negocio particular.
C) Distribuir o divulgar cualquier información o material inapropiado, sacrílego, ilícito, obsceno, xenofóbico, indecente o ilegal.
D) Utilizar o ingresar a otra cuenta de usuario que no sea la propia, excepto con autorización expresa del titular de la cuenta, en cuyo caso caerá bajo su responsabilidad toda consecuencia legal, administrativa o judicial emanada de dicha autorización.
E) Revelar la contraseña de acceso a otro usuario o compartirla.
F) El envío de información autorizada y oficial en forma masiva, dentro del horario laboral (8:45 h - 16:45 h).
G) El envío de información masiva en general (publicidad, propaganda, comercial, particulares, etc.).
H) El envío de información crítica del Organismo o información privada de usuarios del mismo.
I) El envío o retransmisión de cadenas de ayuda, chistes, leyendas urbanas, pensamientos, pornografía, promesas de premio por reenvío de e-mail o cualquier temática de cadena; la creación de sucesos de discusión y contestación. El envío de correo electrónico en donde se solicita ayuda a personas será únicamente permitido si es canalizado por los medios correspondientes. El envío, participación y retransmisión de cadenas es considerado ilegal y fuente principal de SPAM.
J) Transmitir material en violación de derechos de autor, marcas, información protegida por secreto comercial o en violación de cualquier regulación de la REPÚBLICA ARGENTINA o del resto de los países.
K) La modificación o falsificación de cualquier parte del encabezado de un mensaje de correo electrónico, del asunto o del cuerpo del mismo.
L) Enviar mensajes en formato HTML o imágenes que por sus características de extensión, forma, dimensión, tamaño o configuración puedan generar daños en la cuenta de correo electrónico del destinatario (Ejemplo: publicidad, animaciones, multimedia, etc.).
M) A través del envío de virus, gusanos, troyanos o archivos adjuntos, se puede provocar deliberadamente el mal funcionamiento de computadoras, servidores, equipos y periféricos de sistemas o redes, el sabotaje o el ingreso de software malicioso al Organismo.
N) No utilice las opciones de confirmación de entrega y lectura, a menos que sea un mensaje muy importante, ya que de esta forma provoca mucho tráfico innecesario en la red.

O) Antes de abrir un correo electrónico, lea atentamente el nombre del remitente y el asunto del mensaje. Si desconfía, elimínelo. Asimismo, asegúrese que los mensajes que responda vayan dirigidos hacia usted.
P) No responda mensajes en donde se solicitan datos particulares o privados, contraseñas, números o nombres de identificación. Ningún medio solicita este tipo de información a través del correo electrónico, ni siquiera personal del SENASA, y menos aún Administradores o Soporte Técnico de correo electrónico, Internet, computadoras o redes.
Q) Los mensajes contenidos en los correos electrónicos no pueden ser contrarios a las disposiciones del orden público, la moral, las buenas costumbres nacionales e internacionales y los usos y costumbres aplicables en Internet, y el respeto de los derechos personalísimos de terceras personas.
R) Si recibe un mensaje por error, este no se debe revelar, copiar, distribuir o usar su contenido, esto es por la naturaleza confidencial de la información de todo usuario.
S) Cada buzón de correo electrónico tiene un tamaño máximo de capacidad disponible tomando en cuenta los mensajes depositados en la bandeja de entrada, en la de borradores, enviados, papelera y cualquier otra carpeta que sea creada dentro de este buzón. Una vez que este espacio es consumido, no será posible enviar o recibir mensajes hasta que sea liberado el espacio suficiente en el buzón (cuota).
T) El costo de la entrega del mensaje es compartido entre quien lo manda y quien lo recibe. Esta es una razón económica fundamental por la cual el correo no solicitado (SPAM) no es bienvenido y prohibido en muchas formas.
U) El uso de cuentas de correo electrónico no oficiales para la transmisión y/o recepción de información. Los datos contenidos en estos mensajes carecen de valor institucional. Solo son reconocidos por el Organismo los mensajes con dominio @senasa.gob.ar.
V) Por último, el personal del Organismo debe concientizarse en leer y borrar o almacenar en carpetas locales los correos electrónicos sistemáticamente, ya que de no hacerlo se consume innecesariamente el espacio de almacenamiento en los servidores.

Las presentes citas no se limitan solo a prohibiciones o usos inaceptables.

IMPORTANTE: el registro de correos electrónicos enviados y recibidos utilizando los recursos informáticos del Organismo, está sujeto a su monitorización por parte del personal responsable de la seguridad y administración de este servicio. Se deja constancia que de ninguna manera se procederá a la comprobación o intercepción de los contenidos de los e-mails de los agentes si no existen razones de amenaza para el funcionamiento y/o seguridad del Organismo al cual representan o bien razones de orden judicial.

7.3 INTERNET - DERECHOS Y OBLIGACIONES DE LOS USUARIOS

Estos puntos se elaboraron con base en que el servicio Internet es compartido por todos los usuarios, con lo cual, el abuso por parte de unos imposibilita la utilización de otros.

A) El Servicio web es necesario para el uso de las tareas diarias y está disponible para fortalecer la investigación, la capacitación (ya sea por medios virtuales o en línea), la búsqueda de información, así como herramienta de apoyo para el desarrollo de la actividad de

cada sector del Organismo. La comunicación entre los agentes del servicio e investigadores, académicos, profesionales y personas del exterior relacionadas con las labores desempeñadas por el SENASA, tanto en el ámbito nacional como internacional.

B) Es responsabilidad de todos los usuarios, seguir las políticas y procedimientos de seguridad existentes para el uso de este servicio y evitar toda práctica que pueda dañar los recursos informáticos y la información del Organismo. Como ejemplo, se podría citar descargar archivos con malware, burlar los controles de navegación permitidos, ingresar a sitios de hacking, deep web y similares.
C) Los mensajes que se envíen vía Internet serán de completa responsabilidad del usuario emisor y, en todo caso, deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses de personas individuales, de otras Instituciones o en contra del propio Organismo.
D) Conducirse de forma tal que se refleje positivamente la imagen del SENASA, ya que se encuentran identificados como usuarios del mismo.
E) El usuario y quien lo autoriza serán responsables por los sitios web visitados desde cada cuenta de Internet. Por ello, se debe tener cuidado con "proporcionar" la cuenta de acceso y contraseña a otros usuarios de menor nivel de acceso.
F) Jamás debe tildar o aceptar las opciones de "Recordar Contraseña".
G) Todo usuario tiene derecho a solicitar mediante GDE y/o formulario de "Excepciones Web", los sitios web inaccesibles por el nivel de navegación otorgado y que le son necesarios para desarrollar sus tareas.
H) Todo usuario tiene derecho a solicitar el ingreso a cualquier sitio web laboral que haya sido bloqueado por los controles automáticos de contenido web.
I) Todo usuario que observe cualquier deficiencia o funcionamiento anómalo deberá comunicarlo a la Mesa de Ayuda.

7.4 INTERNET - PROHIBICIONES O USOS INACEPTABLES

A) Cualquier actividad que sea lucrativa o comercial de carácter individual, privado para negocio particular o propaganda política.
B) El uso del servicio web para propósitos que puedan influir negativamente en la imagen del SENASA, de sus autoridades y agentes.
C) La realización de cualquier actividad que pueda comprometer la seguridad de los servidores y recursos electrónicos del Organismo.
D) Accesos a lugares obscenos, que distribuyan, emitan o promocionen material pornográfico, o bien material ofensivo que pueda ofender la moral de terceros.
E) Usar el servicio en relación a sitios de juegos y actividades recreativas o de promoción de intereses personales tales como redes sociales, hobbies, chat, webmail, encuestas, concursos, mensajes no solicitados (spamming), mensajes duplicativos, etc.
F) La transmisión de amenazas, material indecente o de hostigamiento. Así como intimidar, insultar, difamar, ofender, acosar a otras personas o interferir en el trabajo de otros usuarios.
G) Utilizar el servicio web para distribuir material que se encuentran en las cadenas de e-mail como pensamientos, leyendas urbanas, chistes, deporte, música, pornografía, etc.

H) La distribución por Internet de material que cause daños, como la piratería, el sabotaje y más específicamente la distribución de software dañino.
I) Descargar archivos e instalar archivos descargados vía Internet. Únicamente se podrá llevar a cabo esta tarea en situaciones previamente convenidas con el área de Soporte Técnico, Aplicaciones Centrales o Seguridad Informática según corresponda (si es que no cuenta con el nivel de acceso web permitido). En caso de aprobarse la descarga de archivos, el agente solicitante deberá contactarse con el Área de Soporte Técnico, indicando el enlace (link) de descarga y dónde deberá recoger el/los archivos/s solicitados. Para esta función, el Área de Soporte Técnico cuenta con una salida a Internet por fuera de la red de datos del Organismo, de manera de no mezclar las redes (internas y externas) para no exponer al Organismo a la intromisión de malware.
J) Cualquier acción condenada por las políticas de uso del sitio web en el cual el usuario se encuentra navegando.
K) Cualquier conducta ilegal contraria a la legislación local vigente o a la aplicable en los países a los que se pueda tener acceso por Internet.
L) No se puede congestionar, afectar, interferir o paralizar el uso del servicio.
M) La instalación de dispositivos (como podrían ser módems con cualquier componente -entre ellas módem PC, módem USB-, antenas, tecnología wireless, telefónicos, USB, tabletas, etc., y tecnologías como GSM, ADSL, DSL, 2G, 3G, 4G, 5G, n/G, etc.) para ganar acceso a Internet, servicio web, correo electrónico u otras redes, aplicaciones o servicios.
N) La instalación o uso de programas P2P (este tipo de programas, utiliza una red común para comunicar entre sí las computadoras de los usuarios, donde se encuentran los archivos a intercambiar), como por ejemplo: Ares, Torrent, uTorrent, BitTorrent, Blubster, Computwin, E-Donkey, Emule, FreeWire, Grokster, Imesh, KaZaa, Kiwi Alpha, Warez P2P, Xolox, etc; o sitios como The Pirate Bay y similares.
O) Uso o descarga recreativa de material multimedia: radio, TV, video o cualquier tipo de *streaming* (sin necesidad de descargas, ver o escuchar un archivo directamente en una página web).
P) Uso de programas de descargas masivas automáticas, como: Black Widow, GetRight, Wget, Teleport Pro, etc.
Q) Descargas prescindibles de manuales, música, fotos, videos, etc., de gran tamaño que congestionen la red y el servicio web.

Las presentes citas no se limitan solo a prohibiciones o usos inaceptables.

7.5 INTRANET - DERECHOS Y OBLIGACIONES DE LOS USUARIOS

El recurso Intranet es una herramienta para fortalecer el flujo de información interna. Está disponible para mejorar las comunicaciones entre el Organismo y los agentes y entre los agentes mismos. Refuerza y apoya a las distintas tareas, tanto administrativas y educativas como las de investigación.

Por su llegada a todos los agentes, permite la interrelación y comunicación entre los distintos usuarios que se encuentran diseminados en todo el país y no se limita solo al ámbito nacional,

sino que su presencia es internacional para todos los agentes del Organismo, en cualquier lugar del planeta en donde se encuentren.

Por lo expuesto:

A) Se establece que "TODO MATERIAL (gacetillas no generadas por la Coordinación de Comunicación Institucional, fechas de pago, avisos gremiales, etc.) POR DIVULGAR EN FORMA INSTITUCIONAL DEBE SER PUBLICADO EN LA INTRANET SENASA", de esta manera, mantener información actualizada y accesible a través del servicio de Intranet ha probado ser una herramienta efectiva para agilizar la gestión y circulación de información en las Organizaciones.
B) Toda área, sector o dependencia que necesite publicar su información podrá contar con un apartado, marco o espacio definido dentro de la página de Intranet para su utilización.
C) Actividades de capacitación por medios virtuales o en línea.
D) Todas las áreas, a través de la Dirección/Coordinación correspondiente, deberán difundir sus servicios, estructura y función, logrando de esta manera una integración de sectores y usuarios. Esto mejora la calidad de comunicación institucional, a partir de las ventajas otorgadas por la rápida evolución de esta tecnología digital.
E) Con el fin de poder realizar autogestión, ahorro de canales de comunicación y minimización de errores de presentación, deberán ser publicados: documentos, formularios, encuestas, consultas, servicios, normativa actualizada, novedades, noticias, preguntas frecuentes, "libros" de sugerencias y quejas; propiciar la interacción con los agentes teniendo en cuenta sus opiniones como recursos para el mejoramiento continuo mediante mecanismos como sondeos o foros que permitan conocer el grado de plenitud personal y laboral alcanzado.
F) Es obligación para todos los usuarios del Organismo, dejar configurada la página de Intranet SENASA como página por defecto del navegador principal y "navegarla" aunque sea una vez al día, ya que en la misma se deberá dar aviso a los agentes de las fechas de cobro de sueldos, depósitos de viáticos, demás información contable, noticias de prensa, información del personal, gremiales, anuncios, novedades o servicios nuevos y datos propios del Organismo.
G) Los mensajes que se envíen vía Intranet, serán de completa responsabilidad del usuario emisor y, en todo caso, deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses de personas individuales o en contra del propio Organismo.
H) Asumir una absoluta responsabilidad respecto del contenido de todo mensaje o información que se publique. Los datos deben ser explícitos y concisos y la comunicación a difundir concreta, coherente, exacta, clara y ágil en su lectura y comprensión, escritos en un tono amable y utilizando un lenguaje adecuado, que no exceda los límites del buen gusto, la moral y las buenas costumbres.
I) Cuando envía o publica información, respete los derechos de autor en el material que reproduzca, ya sea en forma parcial o en su totalidad. Casi todos los países, incluida la REPÚBLICA ARGENTINA, poseen leyes de derecho de autor y sus penalidades.
J) Antes de publicar un mensaje o información, revise el contenido y pase el corrector ortográfico sobre el texto (una buena práctica de uso es componer el escrito en un procesador

de texto -MS Word, Notepad, Wordpad, etc.-, pasar el corrector ortográfico para luego copiar y pegar la redacción en el cuerpo del mensaje a difundir).

K) Se debe dilucidar cuidadosamente la información que se publicará. Debe prevalecer siempre la necesidad de información de quien consultará la página.
L) Se debe minimizar la información general y no específica, esto atentaría contra futuros ingresos a un espacio específico de publicación.
M) Se debe tener especial cuidado al citar información que depende de otros sectores, con el fin de evitar la duplicación de datos.
N) Los foros y cualquier servicio de concurrencia de usuarios, se deben utilizar siempre que sea necesario y útil para las tareas generales que se realizan o para determinadas interrelaciones temporales. En estas listas de discusión, debe prevalecer el trato amable y el lenguaje apropiado para la comunicación.
O) Todo usuario que observe cualquier deficiencia o funcionamiento anómalo deberá comunicarlo a la Mesa de Ayuda.

7.6 INTRANET - PROHIBICIONES O USOS INACEPTABLES

A) El uso del servicio Intranet para propósitos que puedan influir negativamente en la imagen del SENASA, de sus autoridades o agentes.
B) La realización de cualquier actividad que pueda comprometer la seguridad de los servidores y recursos electrónicos del Organismo.
C) La transmisión de amenazas, material indecente o de hostigamiento. Así como intimidar, insultar, difamar, ofender, acosar a otras personas o interferir en el trabajo de otros usuarios.
D) Utilizar el servicio Intranet para distribuir o exhibir material que se encuentra en las cadenas de e-mail como pensamientos, chistes, deporte, música, pornografía, etc.
E) Subir información que infrinja los derechos de los demás.
F) Subir información que sea confidencial.
G) La distribución de material que cause daños, como la piratería, el sabotaje y más específicamente la distribución de software dañino.
H) La corrupción o destrucción de datos o cualquier acción que pueda impedir el acceso legítimo a la información, incluyendo la carga intencional de malware (virus) o de software dañino.
I) El otorgamiento de autorizaciones o permisos a terceros no conectados a la red de datos del Organismo para que la utilicen ilegalmente e invadan la privacidad de un sitio resguardado solo al personal del SENASA.
J) Congestionar, afectar, interferir o paralizar el uso del servicio.
K) Utilizar o ingresar a otra cuenta de usuario que no sea la propia, excepto con la autorización expresa del titular de la cuenta, en cuyo caso caerá bajo su responsabilidad toda consecuencia legal, administrativa o judicial emanada de dicha autorización.
L) Intentar o ganar acceso a otros sitios, sistemas o recursos informáticos para los cuales no se tiene permiso de ingreso.
M) Exportar por cualquier medio, información del Organismo con fines no laborales o laborales sin autorización del dueño de datos.

Las presentes citas no se limitan solo a prohibiciones o usos inaceptables.

7.7 RED - DERECHOS Y OBLIGACIONES DE LOS USUARIOS

El uso de la red y dispositivos que la misma utiliza, están disponibles para fortalecer el flujo de la información, para compartir recursos e intercambiar y acceder a datos y aplicaciones, de manera de hacer que el trabajo sea eficiente y productivo.
Se deberá trabajar en función a las políticas y procedimientos de seguridad existentes para el buen uso de los servicios de la red de datos y evitar toda práctica que pueda dañar los sistemas informáticos, datos y demás equipos conectados a la misma.

A) Está totalmente prohibida la divulgación del nombre de usuario y de las claves de acceso a cualquier servicio de red de datos.
B) Jamás debe tildar o aceptar las opciones de "Recordar Contraseña".
C) Asumir una absoluta responsabilidad respecto de los archivos y del contenido de datos que se transmiten utilizando los recursos o medios proporcionados por la red, se tomarán las medidas respectivas en caso de envío adrede con malware o información confidencial del Organismo.
D) Se permiten todas las transmisiones internas de información para actividades de investigación, trabajo grupal, capacitación, resguardo de datos, etc., siempre y cuando exista un intercambio mutuo y en condiciones recíprocas. En cuanto a las trasmisiones externas, se permiten siempre que existan convenios específicos de intercambio de información con el adecuado nivel de seguridad.
E) La demanda de servicios puede ocasionalmente exceder la disponibilidad de los recursos, por lo que serán establecidas prioridades, siendo las más altas las actividades más esenciales para llevar a cabo la misión del Organismo.
F) Los agentes tendrán que dar aviso al área que administra la red de datos, por toda mudanza o baja de PC y/o equipo conectado a la red para que dicha área reconecte al usuario en el nuevo puesto de trabajo, habilitando el servicio de red en el dispositivo "switch" u otro, donde está conectado e inhabilite el puerto que quedó en desuso.
G) Todo usuario debe respetar la naturaleza confidencial del acceso de una persona o cualquier otra información que pueda caer en su poder, ya sea como parte de su trabajo o por accidente, en este caso la información recibida deberá ser eliminada inmediatamente.
H) Todo usuario que observe cualquier deficiencia o funcionamiento anómalo deberá comunicarlo a la Mesa de Ayuda.

7.8 RED - PROHIBICIONES O USOS INACEPTABLES

A) Utilizar los servicios de comunicación, en este caso, aquellos que utilizan la red de datos como medio de propagación, para intimidar, insultar, difamar, ofender o acosar a otras personas o interferir en el trabajo de otros usuarios.
B) Utilizar los servicios de la red de datos para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o negocio particular.
C) Distribuir o divulgar cualquier información o material inapropiado, sacrílego, ilícito, obsceno, indecente o ilegal.

D) Revelar la contraseña de acceso de los servicios de red a otro usuario o compartirla.
E) Enviar y/o compartir información masiva en general (publicidad, propaganda, comercial, particulares, música, hobbies, etc.).
F) Enviar y/o compartir información crítica del Organismo o información privada de usuarios.
G) El envío o retransmisión de cadenas de ayuda, leyendas urbanas, chistes, pensamientos, pornografía, promesas de premio o cualquier temática de cadena.
H) Transmitir material en violación de derechos de autor, marcas, información protegida por secreto comercial o en violación de cualquier regulación de la REPÚBLICA ARGENTINA o del resto de los países.
I) Enviar y/o compartir virus, gusanos, troyanos o cualquier tipo de malware, puede provocar deliberadamente el mal funcionamiento de computadoras, servidores, equipos y periféricos de sistemas o redes, el sabotaje o permitir el ingreso de malware y/o software malicioso al Organismo.
J) La realización de cualquier actividad que pueda comprometer la seguridad de los servidores y recursos electrónicos del Organismo.
K) Usar el servicio para juegos y actividades recreativas como pensamientos, leyendas urbanas, chistes, deporte, música, hobbies, pornografía, etc.
L) La distribución de material que cause daños en dispositivos como la piratería, sabotaje y más específicamente la distribución de software dañino hacia o dentro del Organismo.
M) Monopolizar el uso de los recursos de red en perjuicio de otros usuarios.
N) Congestionar, afectar, interferir, deteriorar o paralizar el uso del servicio.
O) Descargas prescindibles de manuales, música, fotos, videos, etc., de gran tamaño que congestionen la red de datos.
P) Transmitir y/o distribuir información que infrinja los derechos de los demás, también todas aquellas actividades que tengan por misión vulnerar el secreto de las comunicaciones ya sean estas de voz, datos y/o imágenes.
Q) La corrupción o destrucción de datos o cualquier acción que pueda impedir el acceso legítimo a la información.
R) El otorgamiento de autorizaciones o permisos y la utilización de terceros no conectados a la red de datos del Organismo para que la utilicen ilegalmente e invadan la privacidad de equipos y sitios resguardados solo al personal del SENASA.
S) Intentar o ganar acceso a otros equipos, sistemas o recursos informáticos para los cuales no se tiene permiso de ingreso, ya sean accesos locales o remotos.
T) Exportar por cualquier medio, información del Organismo con fines no laborales o información confidencial.
U) Cambiar la dirección o identificador IP asignado.
V) Modificar los protocolos de red establecidos en cada recurso y/o la falsificación de cualquier parte de un encabezado de paquete TCP/IP.
W) Modificar el hardware y/o configuraciones de red para recursos asignados u otros, así como incorporar sin autorización a la red dispositivos tales como hubs, switchs, routers, puntos de accesos wireless, cámaras, filmadoras, antenas, teléfonos IP, tarjetas de red, módems (de cualquier tecnología), impresoras, PC, Notebook, Netbook, tabletas, Smartphones, consolas de videojuegos, otros.

X) Difundir (por cualquier y en cualquier medio -foros, portales, etc.-) la dirección o identificador IP de los recursos asignados al usuario, de otros usuarios o recursos del Organismo y/o de la red SENASA.
Y) Utilizar la red para cometidos prejuiciosos contra usuarios, dispositivos y/o equipos, entre ellos las prácticas de hacking, cracking, phreaking, spamming, phishing, ransomware, ingeniería social, entre otras.
Z) Utilizar en la red programas de spyware, adware, sniffer, denegación de servicio, man in the middle, spoofing, backdoors, minería de Bitcoins y monedas virtuales similares, drones entre otros.

Las presentes citas no se limitan solo a prohibiciones o usos inaceptables.

El servicio de nube SENASA está regido por los derechos y prohibiciones contemplados en los puntos Internet y Red de la presente PUA.

8. SANCIONES

El incumplimiento de las Políticas de Buen Uso establecidas en el presente documento acarrea distintos tipos de penalidades, las cuales serán dispuestas por la Dirección de Recursos Humanos y Organización.

Cada instancia deberá ser registrada en el legajo del agente. Asimismo, se establece que las acciones disciplinarias no impiden que se incorporen procedimientos administrativos para aplicar sanciones disciplinarias mayores -dependiendo del grado de trasgresión efectuado-, así como someter al agente que esté incumpliendo esta Política al rigor de la Justicia Penal Argentina y/o Justicia Penal del país en donde se produzca la infracción o delito.

9. GLOSARIO

A-W
A.

ADSL (*Asymmetrical Digital Subscriber Line* - Línea Asimétrica de Suscripción Digital): es una forma de DSL que permite transmitir información digital con un elevado ancho de banda sobre líneas telefónicas y que ofrece distintos servicios, como el acceso a Internet. Puede tomar más velocidad cuando el usuario recibe datos (bajada) que cuando los envía (subida).

Adware: (contracción de ADvertisement + softWARE) son tipos de aplicaciones que incluyen alguna forma de publicidad mostrada cuando son ejecutados.
Los desarrolladores usan el adware como recurso para lograr ingresos económicos de sus programas, que usualmente son gratuitos.

B.

Backdoor: (en castellano, puerta trasera) defecto en un software o página web que permite ingresar a un recurso que usualmente está restringida a un usuario ajeno. No siempre es un defecto (bug), también puede ser una entrada secreta de los programadores con diversos fines.

Bit: cifra binaria; número en notación binaria. Es la cantidad de información más pequeña que puede transmitirse. En el sistema de numeración binario los números se representan utilizando solamente las cifras 0 y 1. Es el que se utiliza en las computadoras, pues trabajan internamente con DOS (2) niveles de voltaje, por lo que su sistema de numeración natural es el sistema binario (encendido 1, apagado 0).

Buzón o bandeja de correo electrónico: depósito o recipiente dentro del Webmail o cliente de correo que sirve para almacenar correos electrónicos.

Bytes: conjunto de 8 bits, el cual es equivalente a un carácter.
C.

Cable de fibra óptica: cable de comunicación compuesto por filamentos de vidrio (u otros materiales transparentes) de pequeñísimo diámetro a través de los cuales se pueden transmitir enormes cantidades de información a largas distancias. La señal transmitida es un haz de luz láser, exclusivamente. Este tipo de transmisión tiene la ventaja de que prácticamente no se pierde señal pese a la distancia (la señal no se debilita) y que no le afectan las posibles interferencias electromagnéticas que sí afectan a la tecnología de cable de cobre clásica.

Chat: conversación interactiva en tiempo real, en Internet. Cuando incorporan servicios de video y audio se los conoce como Videochat.

Confidencialidad: es la propiedad de la información, por la que se garantiza que esta será accesible únicamente a personal autorizado a acceder a la misma. La confidencialidad ha sido definida por la Organización Internacional de Estandarización (ISO) en la norma ISO-17799 como “garantizar que la información es accesible solo para aquellos autorizados a tener acceso” y es una de las piedras angulares de la seguridad de la información.

Contraseña o clave: también llamada *password*; es una forma de autenticación que utiliza datos secretos para controlar el acceso hacia algún recurso, como puede ser la PC, carpetas o archivos compartidos, sistemas, correo electrónico, etc., y es un método de seguridad que se utiliza para identificar a un usuario.

Correo electrónico o e-mail: del inglés *electronic mail*, por medio del protocolo de comunicación TCP/IP, permite el intercambio de mensajes entre las personas conectadas a la red de datos de manera similar al correo tradicional. Para ello es necesario tener una dirección de correo electrónico, compuesta por el nombre del usuario, el símbolo arroba “@” y el nombre del servidor de correo. Por ejemplo, jsalguiero@senasa.gob.ar, en donde “jsalguiero” es el usuario y senasa.gob.ar es el nombre del host o servidor.

Cracking: conjunto de técnicas cuyo objetivo es crear “cracks” para desproteger programas y evitar pagar licencias de uso o comprarlos. Un *crack* informático es un parche, creado sin conocer el código fuente del programa, cuya finalidad es la de modificar el comportamiento del software original.

Criticidad: propiedad de la información que la describe de mayor o menor riesgo para los objetivos del Organismo.

Cuenta de usuario: conjunto de caracteres que identifica a cada usuario en el proceso de acceso a los sistemas o recursos.

D.

Denegación de servicio: un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés *Denial of Service*), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red o sobrecarga de los recursos computacionales del sistema de la víctima. Un ataque mayor o a gran escala se denomina DDoS (de las siglas en inglés *Distributed Denial of Service*),

DHCP (*Dynamic Host Configuration Protocol*): es un protocolo de configuración dinámica de host que utilizan las computadoras para obtener información de configuración. El DHCP permite asignar una dirección IP a una computadora sin requerir que un administrador configure la información sobre la computadora o equipo. Sin DHCP, cada dirección IP debe configurarse manualmente (IP Fija o estática).

DSL (*Digital Subscriber Line* o Línea de Abonado Digital): tecnología que permite una conexión a una red con más velocidad a través de las líneas telefónicas. La diferencia entre ADSL y otras DSL es que las velocidades de bajada y las de subida no son iguales; por lo general permiten una mayor bajada que subida.

E.

Equipos: recursos informáticos físicos para el procesamiento, transmisión y/o conservación de datos.

F.

Foro: en Internet, un foro, también conocido como foro de mensajes, foro de opinión o foro de discusión, es una aplicación web que da soporte a discusiones u opiniones entre sus participantes.

G.

GSM: (*Global System for Mobile Communications* - Sistema Global para Comunicaciones Móviles): es un sistema telefónico digital difundido en Europa usado especialmente por telefonía móvil. Puede funcionar en todo el mundo.

H.

Hacker: aficionado a la informática cuya afición es buscar defectos de programación para entrar en los sistemas y, sobre todo, a entrar ilegalmente en redes de computadoras y sitios web. El término hacker es siempre muy mal utilizado, y se lo confunde con el de delincuente informático.

Hacking: técnicas y procedimientos utilizados por un hacker para cumplir un determinado objetivo. Suele asociarse esta palabra a procedimientos ilegales o malignos.

Hardware: se refiere a todos los componentes físicos, aquellos que se pueden tocar, en el caso de una computadora personal serían el disco rígido, la compactera, el monitor, el teclado, la memoria, etc.

HTML (*HyperText Markup Language* o Lenguaje de marcado de Hipertexto): es el lenguaje estándar para describir el contenido y la apariencia de las páginas en la WWW.

Hub: también llamado Concentrador, es un equipo de redes que permite conectar entre sí otros equipos o dispositivos retransmitiendo los paquetes de datos desde cualquiera de ellos hacia todos los demás. Han dejado de utilizarse por la gran cantidad de colisiones y tráfico de red que producen.

I.

IP: acrónimo de *Internet Protocol* (Protocolo de Internet), permite identificar unívocamente dispositivos (PC, notebook, impresoras, routers, smartphones, etc.) en la red. Una vez identificados o direccionados, estos dispositivos se pueden conectar entre sí. Una dirección IP esta compuesta de cuatro octetos como por ejemplo, 172.27.57.58.

IP fija: es una dirección IP estática, es decir, no cambia con el tiempo, solo puede cambiarse manualmente.

Incidente de seguridad: cualquier hecho o evento que puede afectar a la seguridad del personal o a la seguridad de los equipos/dispositivos e información del Organismo.

Información: se considera información a todo dato relacionado con el logro de los objetivos del Organismo, cualquiera sea su forma y medio de conservación:

- Formularios/comprobantes propios y/o de terceros.
- Información en los sistemas y/o reportes impresos.
- Otros soportes magnéticos móviles y/o fijos.

Ingeniería social: significa persuadir o manipular a una persona para obtener datos útiles sobre ellos mismos o las empresas en donde trabajan. Suelen utilizarse métodos de engaños para obtener contraseñas o información útil. Pueden emplearse páginas web falsas, programas en-

gañosos o incluso simplemente chatear con una persona ignorante del tema. Increíblemente, la mayoría de las personas son lo suficientemente ilusas como para dar contraseñas a un extraño. La ingeniería social es muy empleada en el *phishing*.

Internet: INTER (Internacional) NET (Red), es un conjunto de redes conectadas entre sí, una red mundial de redes de computadoras unidas por el protocolo TCP/IP. Internet empezó a funcionar en el año 1962 como una red de uso militar llamada ARPANet. Sobre esta "red de redes" se pueden utilizar múltiples servicios como por ejemplo el e-mail, la WWW, los grupos de noticias, etc.

Intranet: INTRA (Interna) NET (Red), es una red privada dentro de una compañía u organismo que se visualiza a través del navegador web. Generalmente utilizada para comunicaciones al personal, calendario de actividades, repositorio de archivos y presentación de normativas internas, entre otros temas.

L.

Leyendas urbanas: son relatos pertenecientes al folclore contemporáneo que, pese a contener elementos sobrenaturales o inverosímiles, se presentan como crónica de hechos reales sucedidos en la actualidad. Algunos parten de hechos reales, pero estos son exagerados, distorsionados o mezclados con datos ficticios.

Una misma leyenda urbana puede llegar a tener infinidad de versiones, situadas generalmente en el entorno de aquellos que las narran y reciben. Están muy extendidas las leyendas urbanas relacionadas con el tráfico de órganos. La mayoría tratan de personas que han sido secuestradas con el único fin de extirparles un riñón después de asistir a una fiesta o de consumir alguna droga, generalmente en un lugar poco recomendable. Hay numerosas leyendas acerca de la Coca-Cola y sus propiedades. De este producto se ha dicho que su fórmula secreta es capaz de descomponer trozos de carne, dientes, que desatasca las tuberías, que sirve para aflojar los tornillos, limpia las manchas de grasa en la ropa y es un poderoso espermicida.

Log: (*log file* o archivo de log), archivo que registra movimientos y actividades de un determinado programa, sitio web, dispositivo, etc.

M.

Malware: son todos aquellos programas diseñados para causar daños al hardware, software, redes, etc.; como los virus, troyanos o gusanos. Es un término común que se utiliza al referirse a cualquier programa malicioso.

Man in the middle: en criptografía, un ataque *man-in-the-middle* o JANUS (MitM o intermediario, en español) es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas. El ataque MitM es particularmente significativo en el protocolo original de in-

tercambio de claves de Diffie-Hellman, cuando este se emplea sin autentificación. Hay ciertas situaciones donde es bastante simple, por ejemplo, un atacante dentro del alcance de un punto de acceso WIFI sin cifrar, donde este se puede insertar como *man-in-the-middle*.

Megabyte: (Mega-octeto o MByte) equivale a 1024 KByte o 1.024.000 bytes. Otros valores son:

1 TB (Terabyte) = 1024 GB
1 GB (Gibabyte) = 1024 MB
1 MB (Megabyte) = 1024 KB
1 KB (Kbyte) = 1024 bytes
1 byte = 8 bits
1 bit = 1 señal eléctrica 0 y 1

Mensajería instantánea: *Instant Messaging* (IM), en inglés, es un sistema de intercambio de mensajes entre personas, escritos en tiempo real a través de las redes.

Módem: acrónimo de modulador/demodulador. Designa al aparato que convierte las señales digitales en analógicas, y viceversa, y que permite la comunicación entre DOS (2) computadoras o equipos a través de una línea telefónica normal o una línea de cable (módem para cable).

N.

Notepad (Bloc de notas): es un editor de texto simple incluido en los sistemas operativos de Microsoft de 1985. Su funcionalidad es muy sencilla.

P.

Proxy: es un programa que realiza la tarea de encaminador o enrutador de peticiones web. Las aplicaciones que están en la red local jamás se conectan con la red externa, la única aplicación que conecta con la red externa es el proxy. Cuando se lo utiliza para salir a Internet, el único que sale afuera es el proxy.

Periférico: es un dispositivo electrónico físico que se conecta o acopla a una computadora, pero no forma parte del núcleo básico (CPU, memoria, placa madre) de la misma. Los periféricos son parte del hardware de la computadora y forman parte de los accesorios o complementos de la misma. Ejemplos de periféricos son: teclado, mouse, micrófono, escáner, impresora, monitor, etc.

Phishing: es un tipo de engaño creado con el objetivo de obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc. El objetivo más común, suele ser la obtención de dinero del usuario que cae en la trampa. Por lo general, el engaño se basa en la ignorancia del usuario al ingresar a un sitio que presume legal o auténtico.

Phreaking: es un término utilizado para denominar la actividad de aquellos individuos que orientan sus estudios y ocio hacia el aprendizaje y comprensión del funcionamiento de teléfonos de diversa índole, tecnologías de telecomunicaciones, funcionamiento de compañías telefónicas, sistemas que componen una red telefónica y por último, electrónica aplicada a sistemas telefónicos.

El término "Phreak" es una conjunción de las palabras *phone* (teléfono en inglés), *hack* y *freak* (monstruo en inglés). También se refiere al uso de varias frecuencias de audio para manipular un sistema telefónico, ya que la palabra *phreak* se pronuncia de forma similar a *frequency* (frecuencia).

Protocolos de red: son reglas de comunicación que permiten el flujo de información entre equipos que manejan lenguajes distintos -por ejemplo-, DOS (2) computadoras conectadas en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma, por tal sentido el protocolo TCP/IP, que fue creado para las comunicaciones en Internet, es necesario para que cualquier computadora se conecte a Internet.
Otra definición es: "Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes".

R.

Ransomware: del inglés *ransom* (rescate) y *ware* (software), es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.

Se hicieron populares en Rusia y su uso creció internacionalmente en junio del 2013. Normalmente un ransomware se transmite tanto como un troyano como un gusano, infectando el sistema operativo, por ejemplo, con un archivo descargado o explotando una vulnerabilidad de software. En este punto, el ransomware se iniciará y cifrará los archivos del usuario con una determinada clave, que solo el creador del ransomware conoce y proveerá al usuario que la reclame a cambio de un pago, normalmente en Bitcoins.
Redes sociales: se conoce como Web 2.0 a la segunda generación de desarrollo de tecnología web y que está basada en comunidades de usuarios interconectados a través de redes sociales (usuarios con intereses en común).

Ejemplos de redes sociales son: *Facebook* (contactos), *Instagram* (fotos) *Myspace* (interacción social), *Flickr* (folk-fotos y videos), *Youtube* (videos), *43 Things* (folk-objetivos y deseos), *Linkedin* (profesionales), *Periscope* (transmisión de video en línea), *Sonico* (Social latinoamericana), *Del.icio.us* (folk-enlaces), *Hi5* (contactos), *Twitter* (microblogging), *Microsiervos* (blog), *Denken Über* (blog), *Wikipedia* (enciclopedia libre), *Wikiquote* (frases célebres), *Wikitravel* (viajes), etc.

Router: también llamado Enrutador o Encaminador, es un dispositivo para interconexión de redes de computadoras. El router interconecta segmentos de red o redes enteras, toma decisiones (basado en diversos parámetros) con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuado.

Recursos informáticos: conjunto de elementos de hardware y software que conforman un sistema.

Red: una red de computadoras es una interconexión de computadoras para compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico (cables) o inalámbrico (wireless). Básicamente se describen DOS (2) tipos de redes, dependiendo de su tamaño y alcance; a las redes chicas se las conoce como LAN (*Local Area Network* o red de área local) y a las redes medianas/grandes como WAN (*Wide Area Network* o red de área extensa). Un tipo de red más chica aún se denomina PAN (*Personal Area Network* o red de área personal).

S.

Sabotaje informático: comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Básicamente, se puede diferenciar DOS (2) grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

Seguridad de la información: conjunto de medidas físicas y técnicas que permiten proteger la información del Organismo de los riesgos de su uso indebido.

Servicio: software particular que se utiliza para la ejecución de ciertas funciones.

Servidor/Server: genéricamente, dispositivo de un sistema que resuelve las peticiones de otros elementos del sistema, denominados clientes.
También se define como una computadora conectada a una red que pone sus recursos a disposición del resto de los integrantes de la red. Suele utilizarse para mantener datos centralizados o para gestionar recursos compartidos.

Sitios rosas: sitios web dedicados a revistas del corazón, parejas, entretenimientos, salidas, rumores, en general, periodismo sobre la vida privada de celebridades y de la farándula.

Sniffer: programa encargado de obtener datos que circulan por una red. Puede usarse ilegalmente para recibir datos privados como nombres de usuarios y contraseñas, además son difíciles de detectar.

Software: es intangible, existe como información; es el conjunto de programas y procedimientos necesarios para hacer posible la realización de una tarea específica, esto incluye sistemas aplicativos, sistemas operativos, base de datos, planilla de cálculos, etc.

Spam o SPAM: se llaman así los mensajes de correo electrónico no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor.

Spamming: es el abuso de cualquier tipo de sistema de mensajes electrónicos y, por extensión, cualquier forma de abuso en otros medios como SPAM en mensajería instantánea, en foros, blogs, buscadores, mensajes en smartphones, etc. Actualmente, cualquier tipo de *spamming* está mal visto tanto por personas como por empresas y gobiernos, incluso algunos tipos llegan a ser ilegal en algunos países.

Spoofing: se refiere al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Existen diferentes tipos dependiendo de la tecnología a la que nos refiramos, como el IP Spoofing (quizás el más conocido, que suplanta la dirección IP), Web Spoofing o E-mail Spoofing, entre otros.

Streaming: término que hace referencia al hecho de transmitir video o audio remotamente a través de una red (como Internet) en tiempo real sin necesidad de descargar el archivo completo. Se hace *streaming*, por ejemplo, cuando se transmite una radio, o un canal de televisión en vivo por Internet.

Switch: también llamado conmutador, es un dispositivo digital de interconexión de redes de computadoras. Su función es interconectar DOS (2) o más segmentos de red, pasando datos de un segmento a otro de acuerdo con direcciones de red que maneja.

T.

Tabulador: la tecla Tab o Tabulador en un teclado se utiliza para avanzar hasta el siguiente “tab stop”. Tab es la abreviatura de Tabulador. Tabular significa poner algo en forma de tabla.

TCP/IP: este nombre proviene de dos protocolos importantes, el *Transmission Control Protocol* (TCP) y el *Internet Protocol* (IP). En español, Protocolo de Control de Transmisión y Protocolo de Internet, respectivamente. Es la forma de comunicación básica que usa Internet, la cual hace posible que cualquier tipo de información (mensajes, gráficos o audio) viaje en forma de paquetes sin que estos se pierdan y siguiendo cualquier ruta posible.

U.

USB (Universal Serial Bus): es un puerto que sirve para conectar distintos dispositivos a una computadora como teclados, mouse, escáner, cámaras digitales, parlantes, teléfonos celulares, impresoras, etc.

Es un estándar de conectores y su principal característica es que los pueden conectarse y desconectarse con la computadora en funcionamiento, configurándose de forma automática.

Usuario: persona física que utiliza los sistemas o equipos.

UTP (*Unshielded Twisted Pair* o par trenzado sin blindaje): tipo de cableado estructurado con un cable de cobre para redes interiores de comunicaciones.

V.

Virus: un virus informático es un programa que se copia automáticamente y que tiene por finalidad alterar el normal funcionamiento de una computadora, un grupo de ellas o la red.
Se ejecuta en el ordenador sin previo aviso y puede corromper el resto de los programas, datos e, incluso el mismo sistema operativo.
Algunos ejemplos de virus son:
Worms o gusanos: se utilizan para ejecutarse cuando se inicia el sistema operativo ocupando la memoria y volviendo lento al ordenador, pero no se adhieren a otros archivos ejecutables. Utilizan medios masivos como el correo electrónico para esparcirse de manera global.

Troyanos: suelen ser los más peligrosos, ya que no hay muchas maneras de eliminarlos. No son virus en sí mismo, acostumbra ser un programa alojado dentro de una aplicación, una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene. Una vez instalado parece realizar una función útil pero internamente realiza otras tareas de las que el usuario no es consciente.

Jokes o virus de broma: no son realmente virus, sino programas con distintas funciones, pero todas con un fin de diversión, nunca de destrucción, aunque pueden llegar a ser muy molestos.

Hoaxes o falsos virus: son mensajes con una información falsa; normalmente son difundidos mediante el correo electrónico, su común denominador, es pedirle al usuario que los distribuya “a la mayor cantidad posible de conocidos”. Suelen ser cadenas de mensajes por enfermos, solidarios, denuncias, premios excesivos, etc.

VPN: una red privada virtual, en inglés: *Virtual Private Network* (VPN), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

W.
WEB: por este término se suele conocer a WWW (*World Wide Web* o Trama Mundial), creado por el centro de investigación suizo CERN por el científico británico Tim BARNES-LEE en el año 1992, como un sistema de intercambio de información y que Internet ha estandari-

zado. Supone un medio cómodo y elegante, basado en multimedia e hipertexto, para publicar información en la red.

Inicial y básicamente se compone del protocolo HTTP y del lenguaje HTML.

Webmail: servicio que permite gestionar el correo electrónico desde un sitio Web.

WI-FI (*Wireless Fidelity*): la expresión Wi-Fi (actualmente wifi) se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11, que permite la creación de redes de trabajo sin cables (conocidas como WLAN, *Wireless Local Area Netwok*).

Wireless: La comunicación inalámbrica (del inglés *wireless*, sin cables) es el tipo de comunicación en la que no se utiliza un medio de propagación físico alguno entre los equipos. En este sentido, los dispositivos físicos solo están presentes en los emisores y receptores de la señal, como por ejemplo antenas, notebooks, teléfonos celulares, tabletas, PDA, etc.
WordPad: es un procesador básico de texto que se incluye con casi todas las versiones de Microsoft Windows desde Windows 95 hacia arriba. Es más avanzado que el *Bloc de notas* pero más sencillo que el procesador de textos *Microsoft Word*.

2G o 2-G: se conoce como 2G a la segunda generación de telefonía móvil. La telefonía móvil 2G no es un estándar o un protocolo sino que es una forma de marcar el cambio de protocolos de telefonía móvil analógica a digital.

Permite integrar otros servicios, que anteriormente eran independientes, en la misma señal, como es el caso del envío de mensajes de texto o *paging* en un servicio denominado *Short Message Service* o SMS y una mayor capacidad de envío de datos desde dispositivos de fax y módem.

3G o 3-G: es la abreviación de tercera generación en telefonía móvil. Los servicios asociados con la tercera generación proporcionan la posibilidad de transferir tanto voz y datos (una llamada telefónica) y datos no-voz (como la descarga de programas, intercambio de e-mail y mensajería instantánea).

4G o 4-G: es la abreviación de cuarta generación en telefonía móvil. Está basada completamente en el protocolo IP, siendo un sistema y una red, que se alcanza gracias a la convergencia entre las redes de cable e inalámbricas. Esta tecnología podrá ser usada por módems inalámbricos, móviles inteligentes y otros dispositivos móviles. La principal diferencia con las generaciones predecesoras es la capacidad para proveer velocidades de acceso mayores de 100 Mbit/s en movimiento y 1 Gbit/s en reposo, manteniendo una calidad de servicio (QoS) de punta a punta de alta seguridad que permitirá ofrecer servicios de cualquier clase en cualquier momento, en cualquier lugar, con el mínimo coste posible. La videoconferencia es una de sus principales actividades.

5G o 5-G: es la abreviación quinta generación en telefonía móvil. Actualmente se encuentra sin estandarizar y las empresas de telecomunicación están desarrollando sus prototipos.

SÍMBOLOS

@ (arroba): este símbolo es uno de los componentes de las direcciones de correo electrónico y separa el nombre del usuario de los nombres de dominio del servidor de correo (ejemplo: nombre@senasa.gob.ar); el origen de su uso en Internet se origina en su frecuente empleo como abreviatura de la preposición inglesa *at* (en).

Fuentes del glosario:

- wikipedia.org
- panamacom.com
- glosarium.com
- mallorcaweb.net
- lawebdelprogramador.com
- alegsa.com.ar
- blog.segu-info.com.ar

APÉNDICE

SERVICIO NACIONAL DE SANIDAD
Y CALIDAD AGROALIMENTARIA

DIRECCION DE TECNOLOGIA DE LA INFORMACION

Formulario de aceptación de términos
de uso de recursos informáticos

ANEXO

FORMULARIO DE ACEPTACION DE TERMINOS DE USO DE RECURSOS INFORMATICOS

Apellido y Nombres: ……

CUIT/CUIL N°……

En mi carácter de usuario de elementos informáticos de propiedad del SENASA - o licenciados por éste organismo, con motivo de mis tareas desarrolladas, manifiesto conocer:

1 - La existencia de un área de Dirección de Tecnología de la Información (DTI) mail: soporte@senasa.gob.ar y de un Área de Seguridad de la Información mail: seguridad@ senasa.gob.ar), ambas se encuentran a disposición para asesorarme con las dudas que pudieran devenir de las clausulas presentes en este formulario, como así también para colaborar con las inquietudes que pudieran ocasionarse durante mi trabajo diario con temáticas de índole informáticas-tecnológicas y de seguridad.

2 - En materia de Equipamiento Informático-Tecnológico:

2.1) Que el equipamiento informático-tecnológico que se me otorga (PC, Netbook, Notebook, Impresora, Scanner, Teléfono fijo, smartphone, etc.) es propiedad exclusiva de SENASA y me es asignado en forma temporaria y con el único fin de cumplimentar los proyectos y tareas que me sean asignadas.

2.2) – Que las tareas de instalación, segurización, mudanzas y trasladados del equipamiento informático-tecnológico como aquellas vinculadas con la configuración y parametrización de periféricos y software de base, deberán ser realizadas en forma exclusiva por personal informático autorizado quedando prohibidas estas tareas a los usuarios quienes no podrán cambiar de lugar, manipular o sustraer equipamiento o piezas de ningún tipo.

3 – En materia de SOFTWARE:

3.1) Que el software es una creación, una obra intelectual y como tal se encuentra tutelado por las leyes.

3.2) Que toda reproducción de software que no cuente con la expresa autorización de su autor, significa una infracción a sus derechos y constituye un delito severamente sancionado.
3.3) Que SENASA rechaza todo tipo de uso no autorizado de software.
3.4) Que SENASA como titular de los derechos o licencias sobre el software y hardware empleado, tiene derecho a controlar y auditar su uso conforme a criterios de razonabilidad,

atendiendo a los principios de privacidad pero a la vez resguardando la seguridad de la información y el buen uso de las herramientas provistas por esta cartera ministerial.

3.5) Que lo expuesto en el punto anterior incluye al correo electrónico dirigido a mi cuenta asignada por SENASA, como emitido desde la misma, y los datos contenidos en aquella, los que, en caso de mi retiro de SENASA– por la causa que fuese - permanecerán en propiedad de éste último, no teniendo el usuario derecho a los mismos.

4 – En materia de Seguridad de la Información:

4.1) Me comprometo a no revelar, divulgar o facilitar –bajo cualquier forma– información adquirida con motivo del ejercicio de mis funciones a ninguna persona física o jurídica, sea esta pública o privada, salvo en caso que la Información así lo permita o mediase su aprobación previa y por escrito.

4.2) Me comprometo a no utilizar información adquirida con motivo del ejercicio de mis funciones, para mi propio beneficio o para beneficio de cualquier otra persona física o jurídica, pública o privada, sea o no con fines de lucro.

4.3) Me comprometo a no realizar actividades maliciosas que puedan comprometer la confidencialidad, integridad y disponibilidad de la información y/o que me permitan obtener mayores privilegios que los otorgados por el SENASA

4.4) Las contraseñas de las cuentas de usuarios de acceso a los diferentes sistemas informáticos que se me asignan, son personales, secretas, intransferibles y modificables sólo por su titular. De esta manera, toda actividad registrada con dichas cuentas se entenderá como efectuada por su propietario.

4.5) En el caso de utilizar la modalidad de acceso remoto, me comprometo a no utilizar esta funcionalidad desde un sitio público con equipos de uso compartido, como puede ser un cibercafé o locutorio.

4.6) Me comprometo a detener las acciones que estaba realizando e informar al Área de Seguridad, al detectar un fallo de seguridad.

4.7) Conozco que en las estaciones de trabajo, que son de propiedad del SENASA, sólo podrá instalarse software incluido en el Listado de software estándar de PC, con la autorización correspondiente y la instalación del área de Dirección de Tecnología de la Información. La instalación y/o la ejecución de cualquier aplicación, programa o ejecutable no autorizado serán consideradas una grave infracción.

4.8) Utilizaré los recursos que me asigna la Dirección de Tecnología de la Información para el desempeño de mis funciones de manera racional, evitando su abuso, derroche o desaprovechamiento, y aceptando a tales fines las actividades de monitoreo.

4.9) Bloquearé la terminal cuando me levante de mi escritorio y cerraré la sesión cuando termine la jornada laboral.

5 – **En materia de Seguridad de Password:**

5.1) El uso del sistema, dominio y recursos que se encuentren protegidos mediante una contraseña, está restringido a la persona a la que se le ha dado permiso y una contraseña para ingresar a dicho servicio y/o recursos autorizados.

5.2) La contraseña no puede ser distribuida a otros y la Parte Autorizada es responsable de cualquier y todos los daños que sufra el sistema como resultado de la distribución de su contraseña.

5.3) Si más de una persona necesita la contraseña única que le pertenece a la Parte Autorizada, tal Parte Autorizada deberá solicitar permiso por escrito fundamentándolo, quedando entendido que el área de Dirección de Tecnología de la Información no tendrá obligación alguna de aprobar dicha solicitud.

5.4) La contraseña otorgada inicialmente es solo temporal. El sistema pedirá que la cambie en el primer inicio de sesión

5.5) La contraseña caduca periódicamente. El sistema le avisará con 5 días de anticipación solicitándole el cambio.

5.6) La cuenta se bloqueará al 5to intento fallido. Para su reactivación es necesario informar al área de Dirección de Tecnología de la Información para su desbloqueo.

5.7) Es importante que usted cambie su contraseña o perderá temporalmente el acceso a su computadora y correo electrónico.
5.8) Evite mantener un registro (por ejemplo papeles, archivos de software o dispositivos portátiles) de contraseñas.

5.9) Las contraseñas deben cumplir los siguientes criterios:
* No debe coincidir con las últimas 5 contraseñas utilizadas.
* Por lo menos 8 caracteres.
* No debe contener su nombre de cuenta o nombre completo.
* Contiene al menos una letra mayúscula (A - Z).
* Contiene al menos un dígito (0 a 9).
* Contiene al menos un carácter especial

5.10) Si usted no recuerda la contraseña deberá seguir el proceso de blanqueo de la misma, informando al área de Dirección de Tecnología de la Información, mail: soporte@senasa.gob.ar.

Por lo tanto, me obligo por esta vía, a:
1.- Utilizar solamente el software que me sea autorizado por el SENASA y a no efectuar copias del mismo o de los datos procesados por dicho software que no sea ordenado por un superior jerárquico.
2.- Usar dicho software exclusivamente para los fines para los cuales fuera instalado en los equipos, absteniéndome de aplicarlo para uso personal.
3.- Deslindar a SENASA de toda responsabilidad legal que mi obrar pudiere generarle en tal sentido.
4.- Adquirir el compromiso formal de no divulgar ni destinar a mi uso particular o de terceros, ni reproducir, transmitir o suministrar parcial o totalmente, toda información y/o datos que sean de la actividad propia de SENASA y que se adquieran en el ejercicio de mis funciones.
Asimismo tomo conocimiento de que se encuentra totalmente prohibido copiar, reproducir o facilitar a terceros los programas que utiliza la jurisdicción, así como cualquier otra parte o elemento del software al que tengo acceso con motivo de mis tareas.
Respecto de las modificaciones, variaciones, nuevas aplicaciones o desarrollos que pueda realizar a los programas y software utilizados, y en cuanto los mismos pudieran ser conceptuados como invenciones, descubrimientos, o procedimientos registrables, entiendo que los mismos son derivados de los procedimientos y actividades de SENASA y en consecuencia le pertenecen en exclusividad.
5 - Que los servicios informáticos-tecnológicos que de SENASA brinda, son para uso laboral y deberán utilizarse de manera responsable quedando prohibidas las siguientes prácticas:
Spamming (envío masivo de e-mails no solicitados). Uso de software y / o técnicas de Hacking o robo de información. Alojamiento de música y / o vídeos personales en discos de trabajo de red .La obligación de confidencialidad asumida en virtud del presente compromiso seguirá vigente después de finalizadas las tareas encomendadas y aún después de la rescisión o resolución de la relación de empleo o rescisión o resolución del servicio que me vincula con el SENASA, haciéndome responsable de los daños y perjuicios que pudiere irrogar la difusión de datos o informes no publicados.
Que la violación a las obligaciones impuestas por este documento podrá ser causal de sanciones internas de acuerdo con las normas de carácter disciplinario aplicables al personal de la Administración Pública Nacional (Ley N° 25.164 y su reglamentación aprobada por el Decreto N° 1.421/02; el Reglamento de Investigaciones Administrativas aprobado por el Decreto N° 467/99; y normas complementarias y concordantes)

En la Ciudad Autónoma de Buenos Aires, a los .... días del mes de …….. del año …..

…… ……
FIRMA ACLARACION

ANEXO

FORMULARIO DE ACEPTACION DE TERMINOS DE USO DE RECURSOS INFORMATICOS

ANEXO: DATOS PERSONALES Y LABORALES

Datos Personales:

Nombres: -

Apellidos: -

CUIL: - **DNI:** -

SERVICIO NACIONAL DE SANIDAD Y CALIDAD AGROALIMENTARIA
Ministerio: Agroindustria

Dependencia: Dirección de Tecnología de la Información

Teléfono: - - - - - - - - - - - - - - - -- **mail:** -

Modalidad de Contratación:

- ☐ Autoridades Políticas
- ☐ Asistencia Técnica
- ☐ Artículo 9°
- ☐ Personal SINEP
- ☐ Designaciones Transitorias
- ☐ Decreto N° 1421/02
- ☐ FUNDACIÓN ARGENINTA
- ☐ Decreto N° 1109/17

Mail Institucional: - - - - - - - - - - - - -@senasa.gob.ar

Firma: - Aclaración: -

República Argentina - Poder Ejecutivo Nacional
2018 - Año del Centenario de la Reforma Universitaria

Hoja Adicional de Firmas
Anexo

Número: IF-2018-39450179-APN-DTINF#SENASA

CIUDAD DE BUENOS AIRES
Miércoles 15 de Agosto de 2018

Referencia: E 8422/2017 ANEXO PUA

El documento fue importado por el sistema GEDO con un total de 36 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2018.08.15 11:35:44 -03'00'

Hector Anselmo Bilbao
Director
Dirección de Tecnología de la Información
Servicio Nacional de Sanidad y Calidad Agroalimentaria

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2018.08.15 11:36:14 -03'00'