CONSEJOS DE SEGURIDAD

AREA DE SEGURIDAD INFORMATICA• COORDINACION DE GESTION TECNICA

En los siguientes párrafos podrá encontrar información útil para el buen uso del Webmail Senasa, el correo electrónico en general e Internet a través del servicio Web.

Evite acceder al sitio Web del Senasa utilizando links. Siempre escriba en el navegador la dirección correspondiente: www.senasa.gov.ar y desde allí, sí, haga clic en el botón de Webmail. También puede ingresar directamente en https://senasamail.senasa.gov.ar/

Recuerde su contraseña de acceso, no la divulgue ni la deje anotada en lugares vistosos, la misma es personal e intransferible. Tampoco debe compartirla con nadie, ya que al compartir dicha clave, usted está perdiendo el derecho que tiene toda persona sobre la **"razonable expectativa de privacidad".**

Al momento de pensar una nueva **contraseña**, utilice caracteres especiales como +-*/$, combine letras mayúsculas con minúsculas y una longitud de no menos de 10 (diez) caracteres. Jamás tilde o acepte las opciones que le proponen "recordar" la contraseña.

Acuérdese que siempre puede consultar sus dudas, llamando a la mesa de ayuda del Organismo, al **teléfono (011) 4121-5005 o #1200.** Allí le informarán y aconsejarán detalladamente de cómo utilizar el servicio de Webmail, cómo realizar el cambio de contraseña y demás opciones presentadas en el correo electrónico y demás aplicaciones Web.

Senasa, a través de cualesquiera de sus áreas, **"JAMAS"** le solicitará que informe o confirme sus claves o datos a través de un correo electrónico o llamado telefónico. Sea precavido con las llamadas o correos electrónicos no solicitados. Estos correos electrónicos no los conteste y reenvíelos al área de Seguridad Informática, a la dirección: seguridad@senasa.gov.ar.

En general, desconfíe y no responda todo mensaje que solicite datos confidenciales. Nunca responda E-mails donde le requieran información personal o claves, tampoco en donde le avisen de un supuesto problema y/o pretendan actualizar la información correspondiente a sus datos, envíen links de descargas de archivos de actualizaciones, fotos, videos o presentaciones. Estas técnicas, denominadas **"Phishing" e "Ingeniería Social"** tienen como único objetivo obtener su información personal y si es posible, la de todos sus contactos.

Si usted no está seguro de la **legitimidad** de un correo electrónico, trate de verificarlo telefónicamente contactando directamente a la persona, Empresa o Institución que lo envió, ya sea, enviando un correo al contacto o llamando telefónicamente a la mesa de entrada del lugar. Para reconocer estos tipos de engaños, no es necesario poseer muchos conocimientos técnicos, por ejemplo: -Un correo electrónico que nos llega proveniente de la empresa XYZ, tiene que tener una dirección de correo electrónico que se corresponda con el dominio de dicha empresa. Entonces, la mesa de ayuda de ésta empresa, debería tener una cuenta mesadeayuda@XYZ.com.ar y no: mesadeayudaXYZ@yahoo.com, ayudaXYZ@gmail.com o XYZtayuda@niemals.com

Universalmente, las grandes y medianas empresas, los Organismos e Instituciones, utilizan cuentas de correo electrónico formadas por el nombre del empleado o el sector más el dominio de la entidad en que desarrollan sus actividades, y éstas se pueden comprobar ingresando al Sitio Web del emisor del E-mail. Es muy poco probable que dichos Entes, envíen correos electrónicos desde cuentas como @rapidito, @hotmail, @yahoo o @gmail.

Si de todos modos, abrió el correo electrónico que creyó **sospechoso**, y el mismo le "invita" a un link de una página sospechosa, no debe hacer clic en el vínculo que contiene la dirección Web a donde se redireccionará, sólo debe pasarle (NO presionar!) el puntero del mouse por encima del link. En la barra inferior del navegador, sobre la parte izquierda aparecerá la verdadera dirección a donde lo llevará el hacer clic en el vínculo engañoso que se encuentra en el cuerpo del mensaje, entonces, si son distintas ambas direcciones, inmediatamente cierre el E-mail y elimínelo.

En general, para direcciones de correo electrónico y sitios Webs que usted crea inciertos o inseguros, un simple consejo para estimar la veracidad de los mismos, es **copiar y pegar** (direcciones de E-mail o páginas Web) en Google o cualquier otro buscador conocido (Bing, Yahoo, AltaVista, etc.) y ver los resultados acercados.

Al ingresar a sitios donde se solicita el ingreso de password, generalmente Bancos, Webmails, sitios de compras, etc.; en la barra del navegador, el sitio Web deberá estar precedido por el protocolo **HTTPS**, en vez de http; significando Secure/Seguro la S final.

Los sitios seguros (https) visualizan un **candado**. Haciendo clic en el mismo se puede ver el certificado de sitio seguro emitido por la empresa certificante. Dicho certificado, brinda certeza sobre la identidad del sitio que estamos visitando, garantiza la privacidad de la información transmitida entre éste y el usuario, además cerciora que dicha información no ha sido modificada por un tercero. Dependiendo del navegador que utilicemos, el candado de seguridad aparecerá en la parte superior (Internet Explorer y Google Chrome) o en la parte inferior (Mozilla Firefox).

El escribir rápido o sin mirar el teclado o la pantalla, hace que escribamos mal el nombre del sitio y de este "error" se valen los hackers. Por ejemplo el **descuido** de tipear www.googkle.com en vez de www.google.com, hace que el usuario ingrese en una página cuyo objetivo real es infectar la PC, robar contraseñas o contactos.

Hay que tener cuidado con **"omitir"** el punto (.) que separa el nombre de dominio del prefijo www. Un mal ejemplo sería tipear http://wwwsenasa.gov.ar.

Debe prestar especial atención al teclear **URL largas** o difíciles de escribir.

En cada uno, de uno o varios **re-direccionamientos de páginas**, siempre verifique si "está" en el sitio que pretendía visitar. Algunas pautas son:
Si el sitio que desea visitar es un sitio del gobierno, ¿termina la URL en .gov o gob, y no en .com?;
Si la página a visitar es de Egipto, el dominio termina en eg?.

Acerca de la Ley de Protección de Datos Personales - Ley 25.326

Algunos artículos son:

ARTICULO 13. — (Derecho de Información).
Toda persona puede solicitar información al Organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables.
El registro que se lleve al efecto será de consulta pública y gratuita.

ARTICULO 14. — (Derecho de acceso).
1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.
2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.
Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.
3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.
4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.
Más información en **www.jus.gov.ar/dnpdp/**