

JORNADA DE CONCIENTIZACIÓN EN CIBERSEGURIDAD

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Seguridad Informática



Agencia de Administración
de Bienes del Estado

TÉCNICAS DE ESTAFAS Y ROBO DE DATOS



Los ataques de **phishing** son correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos diseñados para manipular personas para que descarguen [malware](#), compartan información confidencial (p. ej., números de tarjetas de crédito, números de cuentas bancarias, credenciales de inicio de sesión, etc.), o realicen otras acciones que los exponga a ellos mismos o a sus organizaciones al ciberdelito.



El **smishing** o fraude por mensaje de texto, es una variante del [phishing](#) en la que un atacante usa un atractivo mensaje de SMS o WhatsApp para convencer al destinatario de que haga clic en un enlace, que le envía al atacante información privada o descarga programas malintencionados a un teléfono móvil o smartphone.






El **vishing** es un ataque diferente, que está dentro de la misma clasificación que el phishing y tiene objetivos en común. Los vishers usan números telefónicos fraudulentos, software de modificación de voz, mensajes de texto e ingeniería social para convencer a los usuarios de que divulguen información delicada. En el vishing generalmente se usa la voz para engañar a los usuarios.



Ransomware, es un tipo de [malware](#) que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Las primeras variantes de ransomware se crearon al final de la década de los 80 y el pago debía efectuarse por correo postal. Hoy en día los creadores de ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito.



¿QUÉ ES LA INGENIERIA SOCIAL?

-  La ingeniería social basa su comportamiento en una premisa básica: **es más fácil manejar a las personas que a las máquinas**. Para llevar a cabo este tipo de ataque se utilizan técnicas de manipulación psicológica con el objetivo de conseguir que los usuarios revelen información confidencial o realicen cualquier tipo de acción que pueda beneficiar al ciberdelincuente.
-  Los ciberdelincuentes engañan a sus víctimas haciéndose pasar por otra persona. Por ejemplo, se hacen pasar por familiares, personas de soporte técnico, compañeros de trabajo o personas de confianza. El objetivo de este engaño es apropiarse de datos personales, contraseñas o suplantar la identidad de la persona engañada.
-  Los ataques de ingeniería social son notoriamente difíciles de impedir porque se basan en la psicología humana en lugar de vías tecnológicas. La superficie de ataque también es significativa: en una gran organización, basta con el error de un empleado para comprometer la integridad de toda la red empresarial.

CONCIENTIZACIÓN SOBRE PHISHING

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Seguridad Informática



**Agencia de Administración
de Bienes del Estado**

PREVENCIÓN EN CORREOS ELECTRÓNICOS



Los **riesgos** derivados de estas técnicas son el robo de identidad y datos confidenciales, pérdida de productividad y consumo de recursos de las redes corporativas. Los métodos utilizados para la realización del **phishing** no se limitan exclusivamente al correo electrónico, sino que también utilizan SMS (**smishing**), telefonía IP (**vishing**), **redes sociales**, mensajería instantánea a través del móvil, **Whatsapp** etc.



Para evitar estos riesgos es recomendable adoptar unas buenas prácticas principalmente en el uso del correo electrónico corporativo.



Aprende a identificar correctamente los correos electrónicos sospechosos de ser phishing, en general mensajes que solicitan información confidencial (contraseñas, datos bancarios, número de teléfono móvil, etc.).



Verifica la fuente de información de tus **correos entrantes** . Tu banco no te va a solicitar tus datos o claves bancarias a través del correo electrónico.

PREVENCIÓN EN OTROS MEDIOS



En lugar de utilizar los enlaces incluidos en los correos electrónicos, escribe la dirección directamente en el navegador.



Mantén **actualizado tu equipo** y todas las aplicaciones, sobre todo el antivirus y anti-spam. Aplica los parches de seguridad facilitados por los fabricantes.



Antes de introducir información confidencial en una página web, **asegúrate que es segura**. Han de empezar con <<https://>> y tener un candado cerrado en el navegador.



El **smishing** se realiza a través un mensaje de texto intentando convencerte de que visites un enlace fraudulento.



El **vishing** se realiza a través de una llamada telefónica que simula proceder de una entidad bancaria solicitándote verificar una serie de datos.

EJEMPLOS DE PHISHING

Buscar en correo electrónico

Actualizacion bancaria, Urgente

Carpetas

Entrada

Correo no deseado

Borradores

Enviados

Eliminados

BBVA Bancocontinental. (noreply@sonico.com) Agregar a contactos 05/07/2 Acciones

Para: [redacted].com

De: **BBVA Bancocontinental** (noreply@sonico.com) Has movido este mensaje a su ubicación actual.

Enviado: viernes, 05 de julio de 2013 04:38:56 p.m.

Para: [redacted].com

BBVA Continental

Estimado Cliente:

CUENTA SUSPENDIDA TEMPORALMENTE
Codigo de bloqueo : 3418L67-001KL

Le informamos que su clave internet ha vencido el día 29/06/2013. Para una mayor seguridad su cuenta se encuentra temporalmente suspendida hasta validar sus datos, una vez realizada la validación automáticamente su cuenta será activada obteniendo los beneficios de banca por internet.

Recuerde que tiene solo 48 horas hábiles después de la fecha de vencimiento para realizar este proceso mediante el enlace que se le proporciona nuestra Banca por Internet, de lo contrario su cuenta será inhabilitada y tendrá que acercarse a la sucursal más cercana para su verificación y activación respectiva.

Solicitamos que acceda al enlace que a continuación le facilitamos **VALIDACION AQUI** para la activación de su cuenta de manera segura.

Para mayor información, por favor comuníquese con nosotros al 01 595 0000.

bbvabancocontinental.cicbla.com/personas/ Términos Privacidad Desarrolladores Español

De: vahid.shahabi@srbiau.ac.ir <vahid.shahabi@srbiau.ac.ir>
Enviado el: miércoles, 13 de septiembre de 2023 8:38
Asunto: RE

La contraseña de su casilla de correo electrónico caducará en 2 días. para guardar su contraseña., [HAGA CLIC AQUI](#), para actualizar y enviar inmediatamente

hjuibopde-drdxw.formstack.com/forms/mx

ERROR: This form is not available for public access. Please [login](#) or contact the account owner. (Error ID: 86376b97a3ba2fa55d33)

Back

BLOQUEOS EN EL FILTRO ANTISPAM DE LA AGENCIA

Puede definir reglas de mensajes personalizadas que pueden hacer que el filtro de spam acepte o rechace los mensajes que coincidan sin tener en cuenta la puntuación asignada por el filtro de spam, o aumentar o disminuir la pu

Encabezado	Tipo	Contenido	Acción	Descripción	Última utilización antes de
<input checked="" type="checkbox"/>	From	Dirección maihtaiwo@gmail.com	Rechazar	maihtaiwo@gmail.com	No utilizado
<input checked="" type="checkbox"/>	From	Dominio al.ce.gov.br	Rechazar	al.ce.gov.br	No utilizado
<input checked="" type="checkbox"/>	From	Dirección aishaaadams44@gmail.com	Rechazar	aishaaadams44@gmail.com	No utilizado
<input checked="" type="checkbox"/>	From	Dirección capacitasaludigital@msal.gov.ar	Rechazar	capacitasaludigital@msal.gov.ar	No utilizado
<input checked="" type="checkbox"/>	From	Dominio mailprime12.seuentregadorbrasileirossverde.com	Rechazar	mailprime12.seuentregadorbrasileirossverde.com	No utilizado
<input checked="" type="checkbox"/>	From	Dominio facturacion.com	Rechazar	facturacion.com	No utilizado
<input checked="" type="checkbox"/>	From	Dominio enersa.com.ar	Rechazar	enersa.com.ar	No utilizado
<input checked="" type="checkbox"/>	From	Dirección alejandrromero@ccorporativa.com	Rechazar	alejandrromero@ccorporativa.com	No utilizado
<input checked="" type="checkbox"/>	From	Dirección info@notificados.com	Rechazar	info@notificados.com	7 días, 21 horas, 28 minutos
<input checked="" type="checkbox"/>	Subject Subcadena	Factura Electrónica protocolo	Rechazar	Factura Electrónica protocolo	No utilizado
<input checked="" type="checkbox"/>	From	Dirección mrssuzan45@gmail.com	Rechazar	mrssuzan45@gmail.com	No utilizado
<input checked="" type="checkbox"/>	From	Dirección annakiirabo@gmail.com	Rechazar	annakiirabo@gmail.com	No utilizado
<input checked="" type="checkbox"/>	From	Dirección fabriceakakpo77@gmail.com	Rechazar	fabriceakakpo77@gmail.com	No utilizado
<input checked="" type="checkbox"/>	From	Dominio iting.com.ar	Permitir	iting.com.ar	12 días, 20 horas, 30 minutos
<input checked="" type="checkbox"/>	From	Dominio ix.com.ar	Permitir	ix.com.ar	No utilizado
<input checked="" type="checkbox"/>	From	Dirección m.munoz@gmail.com	Rechazar	m.munoz@gmail.com	No utilizado
<input checked="" type="checkbox"/>	From	Dominio lacargogroup.com	Rechazar	lacargogroup.com	No utilizado
<input checked="" type="checkbox"/>	From	Dirección facturas@seredecom.com	Rechazar	facturas@seredecom.com	No utilizado
<input checked="" type="checkbox"/>	From	Dirección mandatarios.dgai@buenosaires.gob.ar	Rechazar	mandatarios.dgai@buenosaires.gob.ar	19 días, 1 hora, 18 minutos
<input checked="" type="checkbox"/>	Subject Subcadena	Your personal data has leaked due to suspected harmfu...	Rechazar	Your personal data has leaked due to suspected harmful activities.	No utilizado
<input checked="" type="checkbox"/>	From	Dominio ziftextile.com	Rechazar	ziftextile.com	No utilizado

EJEMPLOS DE MAIL VALIDO

De Dirección de Tecnologías de la Información <dti@bienesdelestado.gob.ar>

A [REDACTED]@bienesdelestado.gob.ar

Asunto **Su contraseña expirará en 6 días.**

Estimado/a [REDACTED],

Su contraseña de la Red y Mail de AABE expirará en 6 días.

Por favor cambie la contraseña desde su PC presionando las teclas "CTRL + ALT + Suprimir" y seleccionando "Cambiar contraseña"

Si usted no se encuentra dentro de la Red de AABE o se encuentra fuera del Agencia puede cambiar la contraseña mediante el Webmail.


Por favor ingrese en el [Webmail](#) y haga click en "Opciones" y luego en "Cambiar Contraseña".

Por favor no olvide actualizar la contraseña en sus dispositivos móviles (ej: teléfonos celulares y tablets).

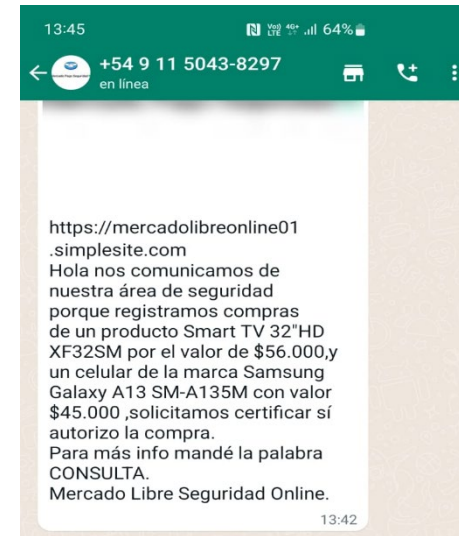
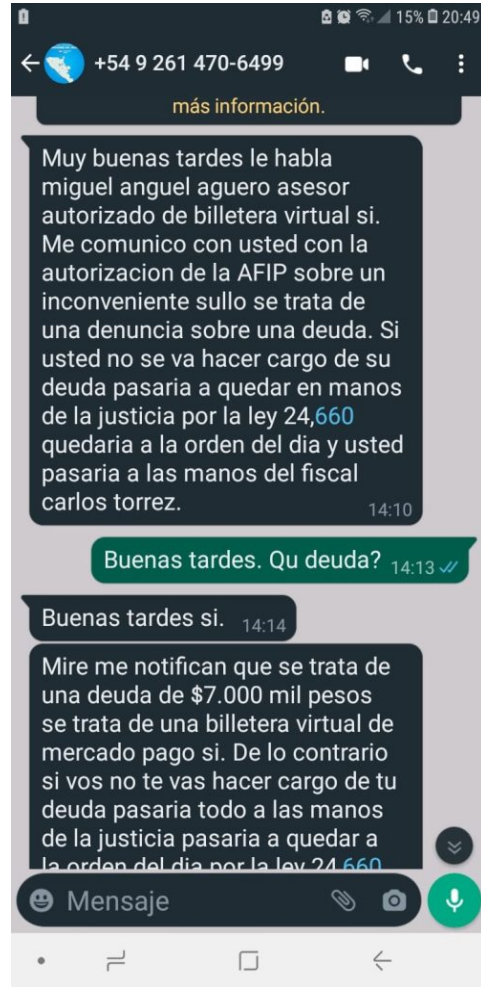
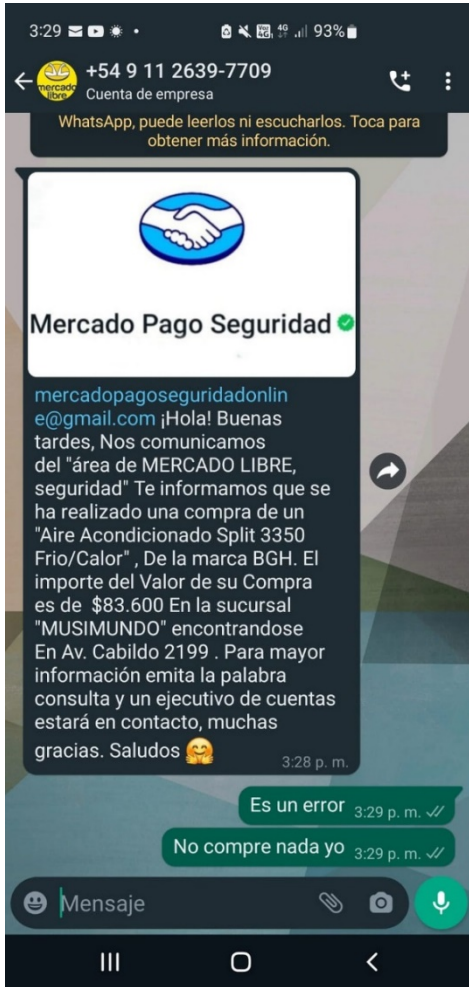
Este es un mail automático, por favor no lo responda.

Desde ya muchas gracias,

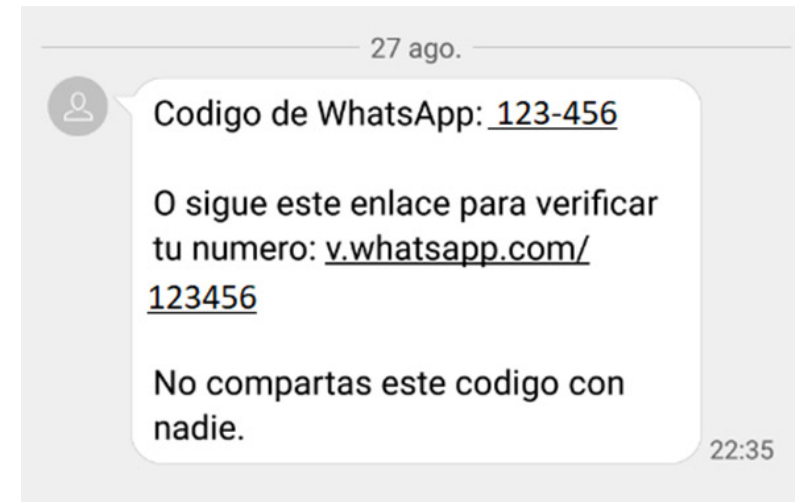
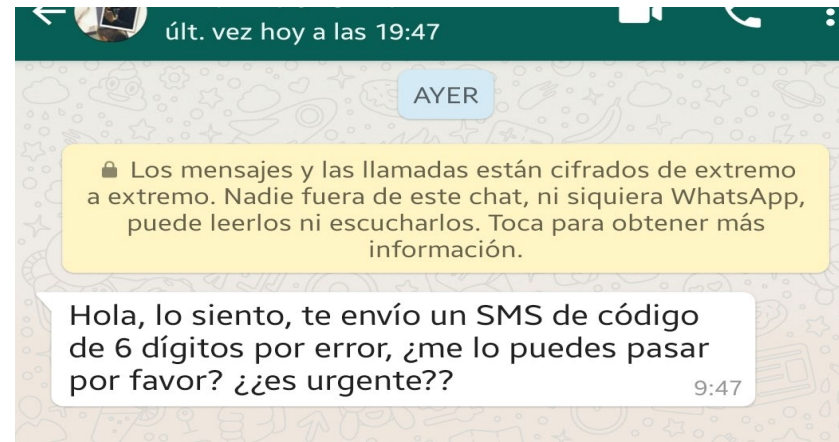
Dirección de Tecnologías de la Información
mesadeayuda@bienesdelestado.gob.ar | 011-4318-3668

 <https://mail.bienesdelestado.gob.ar/>

EJEMPLOS DE SMISHING

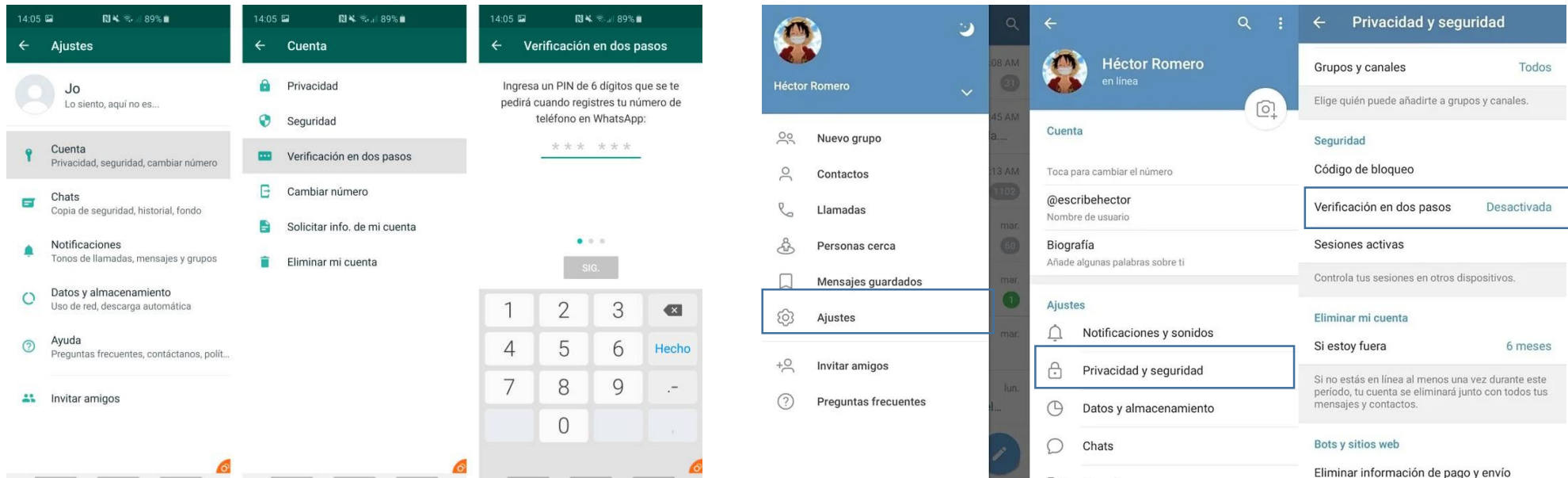


EJEMPLO DE CLONACIÓN DE WHATSAPP



CLONACIÓN DE WHATSAPP – RECOMENDACIONES

- Ante el incremento de casos de clonación de Whatsapp, es recomendación de la DTI, que los usuarios de las distintas aplicaciones de mensajería (Whatsapp, Telegram, Etc.) activen la autenticación en dos pasos y de esta forma evitar estafas para los propios usuarios y sus contactos.
- Muchas veces al clonar una cuenta, los atacantes activan esta autenticación en dos pasos para asegurarse que el usuario no recupere su cuenta.



CONCIENTIZACIÓN SOBRE EL USO DE CONTRASEÑAS

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Seguridad Informática



Agencia de Administración
de Bienes del Estado

ASPECTOS ESENCIALES DE LAS CONTRASEÑAS



Las contraseñas son un tipo de **información personal e intransferible** , nadie a excepción de su propietario debe conocerlas.



Las contraseñas deben ser **gestionadas de forma segura en todo su ciclo de vida** : desde su creación, pasando por su almacenamiento y terminando por la destrucción.



Deben cumplir una serie de requisitos para que sean **robustas** como **tamaño, tipos de caracteres** a incluir o su **periodo de validez**.



En la Agencia la **política actual de contraseñas**, establece un largo de 9 caracteres alfanuméricos, con mayúsculas, minúsculas y símbolos. Se bloquean luego de tres intentos inválidos y su validez es de 60 días.

SEGURIDAD DE LAS CONTRASEÑAS



Es recomendable utilizar **una contraseña para cada servicio**, de esta manera en caso de robo solamente se comprometerá un servicio y no todos.



Cambiar las **contraseñas por defecto por otras consideradas robustas** siempre es recomendable.



Los mecanismos de **doble factor de autenticación "2fa"** aumentan la seguridad de la **cuenta**, son especialmente indicados para acceder a información sensible o servicios críticos.

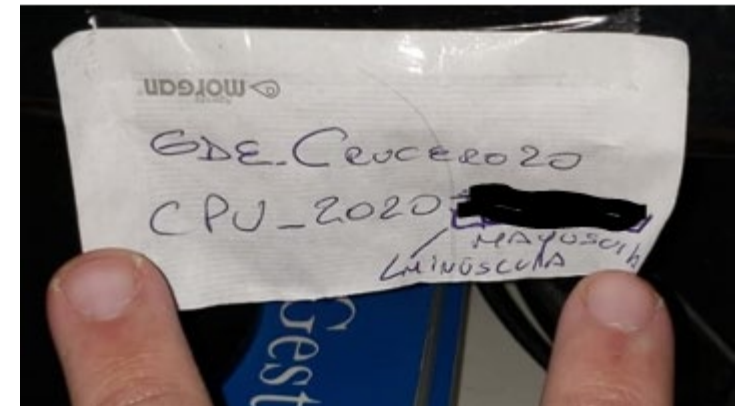
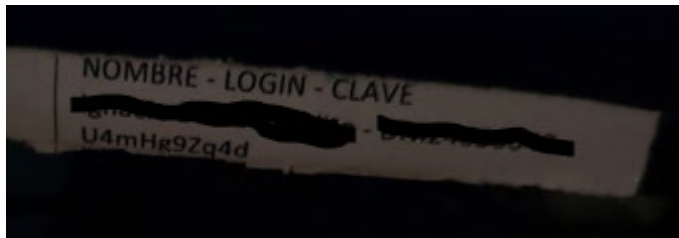
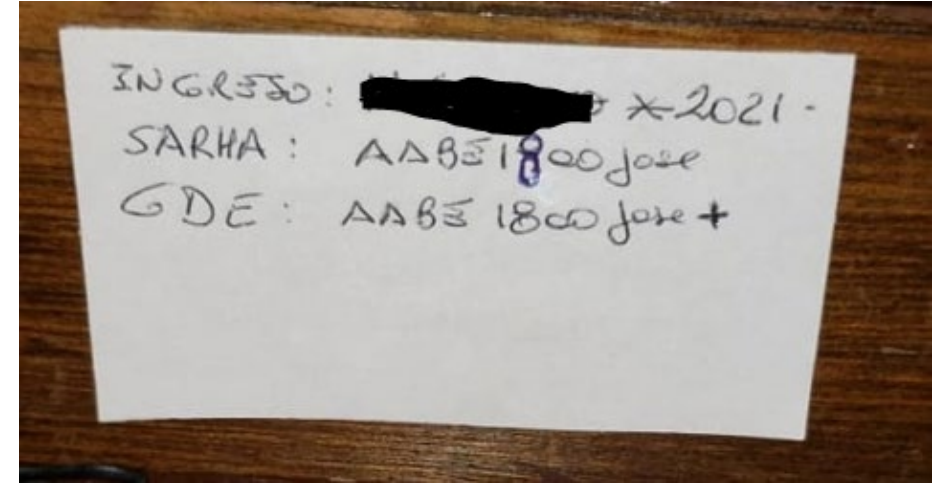
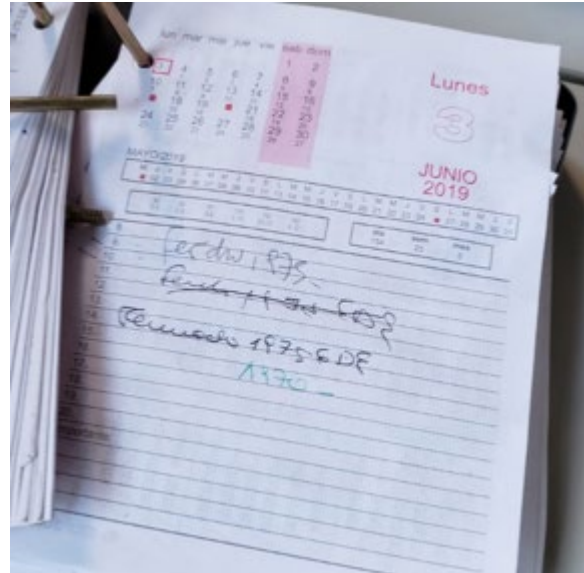
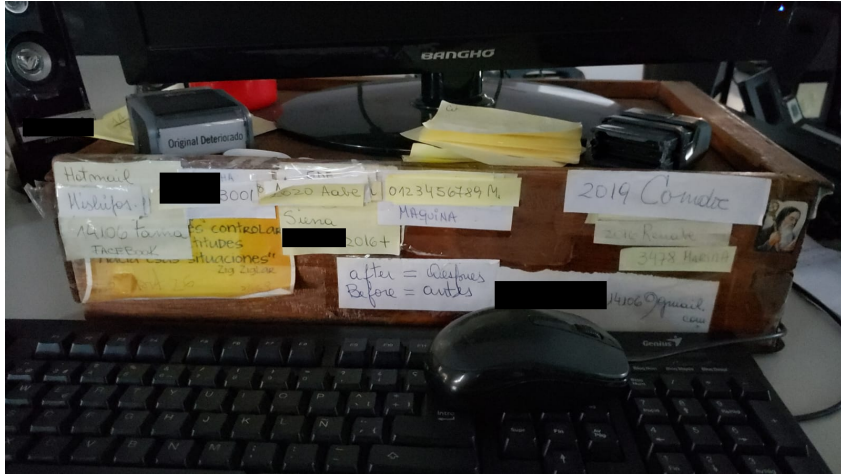


Los **gestores de contraseñas** son un tipo de herramienta que **ayuda a su administración de forma segura**, especialmente útiles cuando el número de contraseñas es elevado.

CONSIDERACIONES GENERALES

- **Deshabilita** la sincronización de tu dispositivo con “la nube” cuando manejes información sensible.
- Nunca permitas que el navegador guarde o recuerde tus credenciales de acceso corporativo. **Desactiva también** la opción de auto-completado de formularios.
- Utiliza **una conexión 3G o 4G** para conectarte a tu red corporativa en lugar de WiFi y si está habilitada utiliza la VPN.
- Protege tu información y la del organismo estableciendo en tu **dispositivo móvil** una clave de acceso y la opción de bloqueo automático.
- Debemos **diferenciar** las contraseñas de acceso al entorno personal del profesional.
- Utiliza sólo las tiendas oficiales para descargar las aplicaciones que quieras instalar en tu móvil. No utilices **aplicaciones ilegítimas** en ninguno de tus dispositivos.
- Nunca dejes tus **equipos desatendidos** en lugares públicos o en tu vehículo. Ponlos también a salvo de riesgos domésticos cuando no los estés utilizando.

ASPECTOS ESENCIALES DE LAS CONTRASEÑAS



CONCIENTIZACIÓN SOBRE EL USO DE EQUIPOS PERSONALES EN EL TRABAJO (BYOD)

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Seguridad Informática



Agencia de Administración
de Bienes del Estado

ASPECTOS ESENCIALES



Byod o “Bring Your Own Device”, es una política de empresa que permite que los empleados hagan uso de sus dispositivos personales para acceder a recursos corporativos.



Los **riesgos** más habituales para tu empresa, de esta política, son la integridad física del dispositivo (pérdida, robo, rotura) y el acceso no autorizado al mismo (físicamente o a través de virus informáticos).



Para evitar estos riesgos es recomendable adoptar unas pautas de seguridad **cuando utilicemos el dispositivo móvil**.



Para **conocer y cumplir la política** de la AABE en cuanto al uso de BYOD, podrá visualizarse desde la Intranet.



Configura correctamente el dispositivo móvil y protégelo de forma adecuada. El departamento de informática te puede ayudar a hacerlo correctamente.

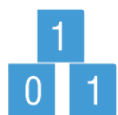


En un entorno BYOD debemos **diferenciar** claramente el correo personal del profesional.

SEGURIDAD



El **cifrado de las conexiones** para el acceso a la información corporativa es una de las medidas más eficaces a la hora de proteger la información cuando los dispositivos se utilizan fuera de la red corporativa.



Cifrar los dispositivos móviles reducirá el impacto en el caso de que se produzca una pérdida o un robo. Además esta medida ayuda a proteger tu información personal.



Haz uso del modo de **navegación de incognito** que incluye la mayoría de los navegadores.



Mantén el sistema operativo y todas tus aplicaciones **siempre actualizadas**.



CONECTIVIDAD SEGURA



No es recomendable hacer uso de redes **wifi públicas** si vamos a tratar información sensible, acceder a cuentas bancarias, a la red corporativa, etc.



Si necesitamos conectividad fuera de nuestras oficinas, es conveniente usar **alternativas de conexión** a redes **wifi** públicas como son el **3g** o el uso de **VPNs**.



Los dispositivos móviles (portátiles, tablets,...) permiten habilitar y deshabilitar las funciones de **geoposicionamiento** . Su objetivo es obtener la ubicación geográfica del dispositivo.

Es recomendable **desactivar** las funciones de **geoposicionamiento** de los dispositivos móviles, para evitar difundir más información de la necesaria.

CONECTIVIDAD SEGURA EN AABE

En la Agencia contamos con dos redes inalámbricas separadas:



- La red wifi **AABE** es donde se conectan todos los dispositivos (notebooks, impresoras, etc.) propiedad de AABE y que además están autorizados para la conexión.
- La red wifi **AABE-INVITADO** tiene reglas de bloqueo de acceso a los datos sensibles de AABE, es de uso libre y su función principal es la de proveer internet a dispositivos personales como smartphones, notebooks, tablets, etc. Estos bloqueos además previenen la propagación de malware/virus ante la conexión de un dispositivo infectado.
- Para conectar un dispositivo personal a la red AABE, se deberá proveer datos del mismo, de su propietario y firmar un formulario de consentimiento.

CONCIENTIZACIÓN SOBRE SOPORTES DE ALMACENAMIENTO

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Seguridad Informática



Agencia de Administración
de Bienes del Estado

RESGUARDO Y SEGURIDAD DE LA INFORMACIÓN



Soportes de información son todos los dispositivos que nos permiten almacenar información en formato electrónico.

Los soportes **más utilizados** son: discos duros, unidades USB, tarjetas de memoria, cintas y discos de copias de seguridad, ordenadores portátiles, smartphones y tablets .



Los riesgos más habituales que puede sufrir un soporte son pérdida, robo, rotura, destrucción o avería.



Debemos evitar estos riesgos mediante **las medidas de seguridad** oportunas.



En lugar de las memorias USB, utilizacarpetas compartidas como método para compartir información (Red, Teams, One Drive).



USO SEGURO DE SOPORTES DE ALMACENAMIENTO - RECOMENDACIONES



El **cifrado** de nuestros soportes es una de las medidas más eficaces a la hora de evitar que nuestra información se vea comprometida.



Es necesario realizar un **borrado seguro** de los soportes antes de reutilizarlos. Así evitamos accesos no autorizados a la información almacenada.



Debemos **documentar** el proceso de borrado seguro de los soportes.



Debemos usar un proceso de **destrucción segura** para nuestros soportes cuando finalice su vida útil. Así, garantizamos que nuestra información deja de ser accesible. A la hora de destruir de forma segura un soporte, podemos hacerlo nosotros mismos o delegar en un tercero. Utiliza destructoras de oficina siempre que sea posible.



Documenta el proceso seguro de destrucción de los soportes.



Si delegamos el proceso de destrucción, debemos establecer los **acuerdos de confidencialidad** oportunos.

BUENAS PRÁCTICAS PARA EL RESGUARDO Y SEGURIDAD DE LA INFORMACIÓN

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Seguridad Informática



Agencia de Administración
de Bienes del Estado

CONSIDERACIONES FINALES



Debemos conocer y concientizarnos de las **medidas de seguridad** implementadas por la Agencia, para la adecuada protección de la información a la hora de desempeñar nuestra actividad profesional.



Debemos proteger nuestro **puesto de trabajo** y mantener la mesa “limpia” de papeles que contengan información sensible.



Es recomendable establecer en tu **dispositivo móvil** una clave de acceso y la opción de bloqueo automático.



No hagas uso de **equipos no corporativos** . Si es necesario, no manejes información corporativa en este tipo de equipos.



Evita las **fugas de información** . No mantengamos conversaciones confidenciales en lugares donde puedan ser oídas por terceros.

CONSIDERACIONES FINALES



Las **contraseñas** deben de ser secretas y únicas, no debemos anotarlas, compartirlas o reutilizarlas. No utilices tus **credenciales de acceso** corporativas en aplicaciones de uso personal.



Se debe realizar una **navegación segura** y evitar acceder a páginas web no confiables.



Utiliza el **correo electrónico** de forma segura, informa a la Dirección de Tecnologías de la Información todo correo sospechoso que recibas y elimínalo. Evita los correos en cadena.



Protege **la información** y realiza copias de seguridad de la información sensible que solo esté en nuestro equipo.



Cuando **viajes**, no mandes información sensible a través de redes WIFI no confiables.



Todos somos seguridad. Aprende a detectar los ataques de ingeniería social y como defenderte. Avisa a la Dirección de Tecnologías de la Información si detectas cualquier actividad sospechosa.



CONSIDERACIONES FINALES



No modifiques la configuración de tus **dispositivos móviles** ni instales aplicaciones no autorizadas.



Destruye la información sensible en formato papel. No te limites a tirarla a la papelera y evita una **fuga de información**.



No dejes las impresiones que contengan **información sensible**, en la bandeja de la impresora de piso.



Bloquea la sesión de tu equipo cuando abandones tu **puesto de trabajo**. En AABE los puestos de trabajo se bloquean automáticamente luego de 15 minutos de inactividad.



CANALES DE ATENCIÓN

Les recordamos que los Canales de Atención de la Dirección de Tecnologías de la Información son los siguientes:



Para solicitudes informáticas **vía mail** a mesadeayuda@bienesdelestado.gob.ar



Para atención por **vía telefónica** comunicarse al interno **3668** o **3482**



Para asuntos de **Seguridad Informática** enviar un mail a la casilla dtiseguridad@bienesdelestado.gob.ar



Esta presentación podrá ser consultada y descargada desde la Intranet de la Agencia <https://aabenet.bienesdelestado.gob.ar/>



¡MUCHAS GRACIAS!

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Seguridad Informática



**Agencia de Administración
de Bienes del Estado**