## DIRECCIÓN PROVINCIAL DE INFORMÁTICA Y COMUNICACIONES

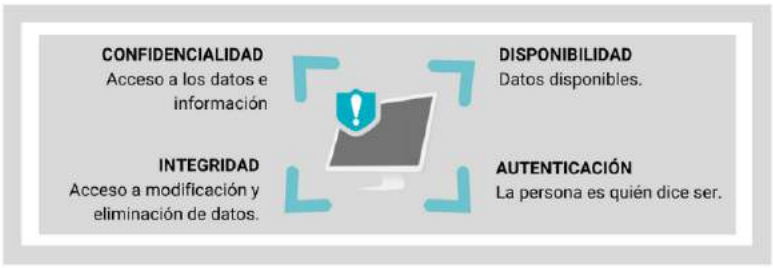
- ¿Qué es la **SEGURIDAD INFORMÁTICA**?

Es un conjunto de prácticas que incluye:

- El **uso responsable** del equipamiento tecnológico,
- Mantenerse **alerta** para **identificar** y **prevenir riesgos**.


- ¿Por qué es **IMPORTANTE**?

Porque **resguarda** los datos de las personas, archivos, información sensible y/o confidencial y **protege** los equipos de trabajo.




## CONSEJOS útiles

- **No compartas** información personal con otras personas (identificación y clave).
- Navegá siempre en páginas seguras, verificá que el dominio sea **https://www.**
- **No descargues ni ejecutes archivos** de fuentes no confiables.
- **Analizá** los archivos antes de descargarlos con un **antivirus**.

Ante cualquier duda, nos podes escribir a **soporte@mjus.gba.gob.ar**

¡Nos mantenemos en comunicación!

**Dirección Provincial de Informática y Comunicaciones**

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

GOBIERNO DE LA PROVINCIA DE BUENOS AIRES

DIRECCIÓN PROVINCIAL DE INFORMÁTICA Y COMUNICACIONES

# CONTRASEÑAS

## Seguras

Tener contraseñas seguras es muy importante para proteger tus cuentas y dispositivos.

- ¿Cómo configurar una contraseña **SEGURA** ?

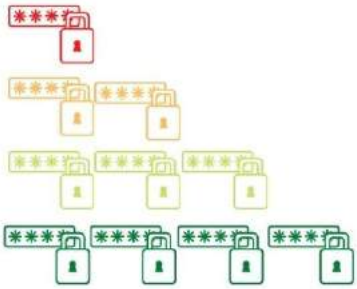
Para obtener un nivel **ÓPTIMO** de Seguridad, la contraseña debe contener por los menos **8 CARACTERES** y combinar los siguientes elementos (no importa el orden):

**minúsculas**

**MAYÚSCULAS**

**1234567890** números

*%$#"%$ símbolos



**N0lOh4Ga$f@C¡!**

## prácticas **SEGURAS**

- **NO** uses la **MISMA CONTRASEÑA** para todas tus cuentas o dispositivos (correo electrónico, redes sociales, cuentas bancarias).
- **NO** utilices **DATOS PERSONALES** (fecha de nacimiento, nombres o apellidos).
- **NO** es recomendable utilizar **secuencia de números** ni de **letras.**
- **CAMBIALAS PERIÓDICAMENTE** (aun cuando los sistemas no lo soliciten).
- **NUNCA COMPARTAS** tus contraseñas.

Ante cualquier duda, nos podés escribir a **soporte@mjus.gba.gob.ar**

¡Nos mantenemos en comunicación!

**Dirección Provincial de Informática y Comunicaciones**

## DIRECCIÓN PROVINCIAL DE INFORMÁTICA Y COMUNICACIONES

# PHISHING

### Correo fraudulento

Son correos que se envían desde **remitentes falsos,** habitualmente indican un **problema con la cuenta,** por ej.: límite de buzón excedido, cuenta desactualizada o desactivada, actualización de base de datos.

Incluyen **un enlace** en el cuerpo del mail y **alertan con la posibilidad de baja** de tu casilla de correo.

- ¿Cómo darte cuenta si un link es **MALICIOSO**?

| **Chequeá estos ítems** | **Es Seguro** | **No es Seguro** |
|---|---|---|
| Revisar autenticidad del **remitente.** | soporte@mjus.gba.gob.ar | soporte@mjus.gba.com.ar |
| Pasar el mouse sobre el LINK para **verificar la dirección del enlace.** | http://www.gba.gob.ar/justicia_y_ddhh | http://www.gba.gob.ar/justicia_y_ddhh<br>http:/cas.dowload.net |
| Si comienza con **https://** es un buen indicio. Prestá atención al mensaje de **alerta** del sistema. | https://www.gba.gob.ar/justicia_y_ddhh | La conexión no es privada |
| Comprobar si la **información de los archivos adjuntos corresponde** (y no está vinculado a un sitio sospechoso). | Tipo: Documento Adobe Acrobat<br>Tamaño: 240 KB<br>Fecha de modificación: 23/2/2022 10:58 | http:/cas.dowload.net |

Recordá **NO** abrir, responder ni reenviar **SPAMs** o mails dudosos.

Ante cualquier duda, nos podés escribir a **soporte@mjus.gba.gob.ar**

¡Nos mantenemos en comunicación!

**Dirección Provincial de Informática y Comunicaciones**

DIRECCIÓN PROVINCIAL DE INFORMÁTICA Y COMUNICACIONES

# USO SEGURO DE LA COMPUTADORA LABORAL

Te pasamos algunos tips para trabajar de forma segura en tu ámbito laboral y evitar exponer tus datos, documentos o equipo informático.

Navegá en **páginas seguras**.

No **repitas contraseñas**.

Habilitá el **uso compartido** de archivos únicamente cuando sea necesario y **con clave**.

Si trabajaste desde un equipo en una sala de reunión:

- **Deslogueate.**
- **Borrá** los **archivos** que hayas **descargado**.
- **Vaciá la papelera** de reciclaje.

**Bloqueá la PC** al ausentarte, o configurá el bloqueo automático.

**Apagá la PC** cuando finalice tu jornada laboral.

Además:

Configurá las **actualizaciones automáticas** del sistema operativo.

**No instales programas** por tu cuenta, consultalo con el área de SOPORTE.

Hacé copias de seguridad con regularidad, ya sea en la nube, disco rígido o USB.

Utiliza **antivirus**, **anti-spyware** y **antitroyanos**, combinados o como programas independientes.

Ante cualquier duda, nos podés escribir a **soporte@mjus.gba.gob.ar**

¡Nos mantenemos en comunicación!

**Dirección Provincial de Informática y Comunicaciones**

## DIRECCIÓN PROVINCIAL DE INFORMÁTICA Y COMUNICACIONES

Uso responsable del

# CORREO ELECTRÓNICO

¿Sabías que el **CORREO ELECTRÓNICO** es uno de los **principales canales** a través de los cuáles podemos **exponer** nuestra información, datos personales e infraestructura informática?

- ¿Cuáles son los **RIESGOS**?
  - Robo de información sensible
  - Publicidad engañosa
  - Virus que afectan el funcionamiento de los equipos

## RECOMENDACIONES

- No uses la casilla de **correo oficial** para correos no laborales.
- **Eliminá** los correos electrónicos de **destinatarios desconocidos.**
- **No abras archivos adjuntos ni accedas a links** de correos sospechosos.
- **No reenvies** ni **respondas** correos **SPAM** (envío masivo).
- Si el **asunto** del correo electrónico no concuerda con tu temática laboral **no lo abras ni lo respondas**.

Ante cualquier duda, nos podés escribir a **soporte@mjus.gba.gob.ar**

¡Nos mantenemos en comunicación!

**Dirección Provincial de Informática y Comunicaciones**

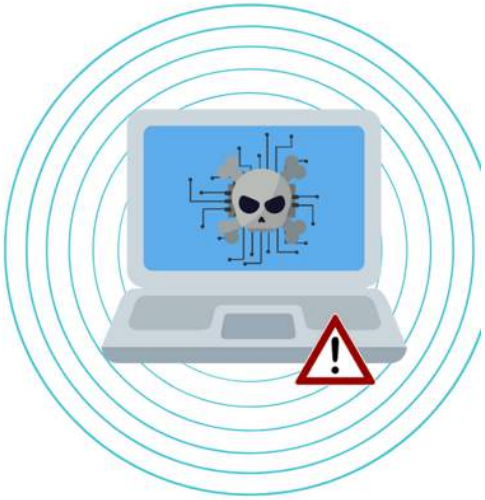
MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

GOBIERNO DE LA PROVINCIA DE BUENOS AIRES

## DIRECCIÓN PROVINCIAL DE INFORMÁTICA Y COMUNICACIONES

Archivos

# MALICIOSOS o MALWARE



Existen una serie de archivos que afectan todo tipo de dispositivos y sistemas operativos, como los **virus**, **gusanos**, **troyanos**, **rootkits**, **ramsomware** (secuestro de archivos), **spyware** (espía)

- ¿Cómo se **ACTIVAN** ?

Clickeando en links maliciosos.
Conectando dispositivos como pen drives o discos externos.
Descargando programas (software) de páginas no oficiales.

## CONSEJOS útiles

- Instalar un **antivirus** y mantenerlo actualizado.
- **No conectar ni abrir archivos** de un **dispositivo externo** sin chequearlo previamente.
- Tener **precaución** al clickear links desconocidos (correos, banners, etc.).
- Solo descargar archivos o **software** de **fuentes confiables**.

Ante cualquier duda, nos podés escribir a **soporte@mjus.gba.gob.ar**

¡Nos mantenemos en comunicación!

**Dirección Provincial de Informática y Comunicaciones**

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

GOBIERNO DE LA PROVINCIA DE BUENOS AIRES