

# HABILIDADES DIGITALES

Cartilla informativa para  
fortalecer el emprendedurismo.





## **HABILIDADES DIGITALES**

Cartilla informativa para  
fortalecer el emprendedurismo.

### **Equipo Editorial**

ONG Centro de Fomento a  
Iniciativas Económicas FIE

### **Contenido**

María del Carmen Ostria  
ONG FIE

### **Diseño y Diagramación**

Paola Rivero Salas

### **Depósito Legal**

4-2-4046-2022

### **Primera edición**

Impreso en  
Art Graf Color S.R.L.

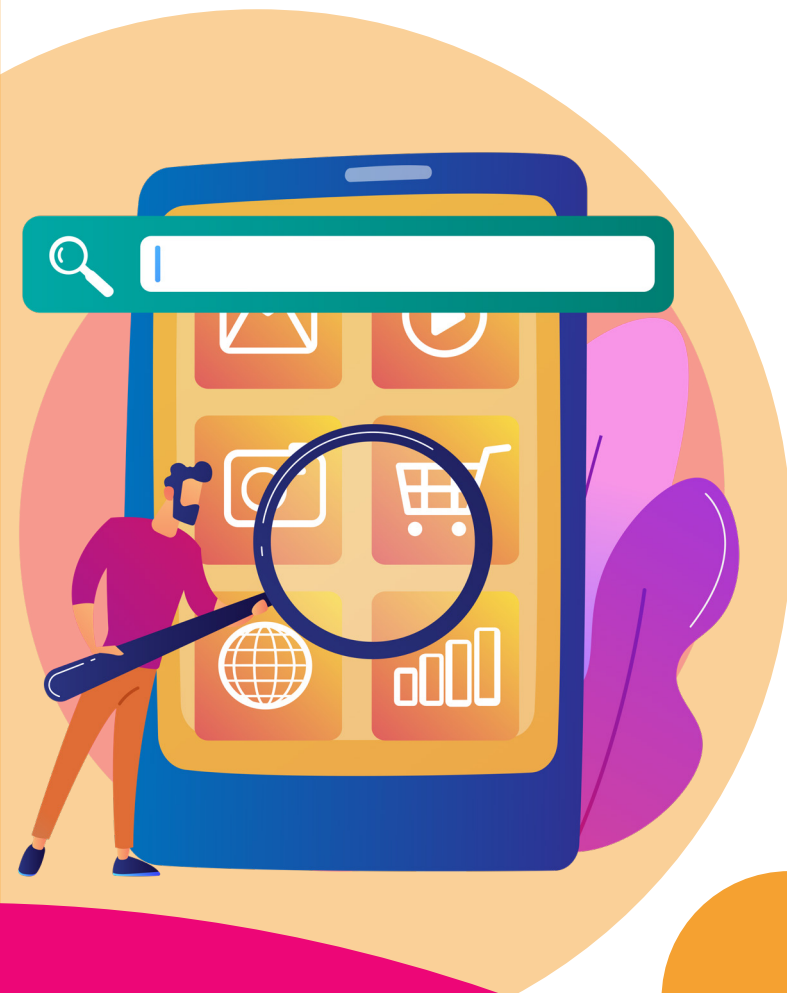
### **La Paz, Bolivia**

2022

## INTRODUCCIÓN

Esta cartilla es parte de la intervención “Mujeres, Jóvenes y Adolescentes acelerando la ruta 20-30 PostCovid-19” para promover la reactivación de emprendimientos mediante el fortalecimiento de sus capacidades empresariales y para promover una educación integral e inclusiva.

Su objetivo es brindar herramientas a quienes lideran sus emprendimientos, a través del fortalecimiento de sus capacidades digitales, las cuales implican el uso creativo, crítico y seguro de las tecnologías de la información y la comunicación.



# CAPACIDADES DIGITALES Y TECNOLÓGICAS

Son la suma de conocimientos, destrezas, actitudes y estrategias que se requieren para el uso de las tecnologías y del Internet.

Ingresar al mundo digital te permitirá tener una ventaja competitiva importante, porque podrás crear contenido digital, llegando a más personas interesadas en tu producto o servicio, además de ayudarte a gestionar tu negocio con mayor seguridad.

Para lograrlo, es importante desarrollar conocimientos y destrezas en torno a:

## Manejo de Plataformas

Existen distintos canales de comunicación que se puede integrar en la estrategia de tu emprendimiento para hacer llegar tu mensaje y posicionar el nombre de tu negocio. La comunicación digital es fundamental en este caso.

Involucra la comunicación digital en tu empresa, haciendo uso de las redes sociales, correos electrónicos, blogs y otro tipo de plataformas digitales, que te permitan llegar a más personas interesadas en tu producto o servicio.

## ¿Cuáles son las herramientas que debemos conocer?



### Sitio web/blog

La página web es un espacio virtual de presentación de tu empresa. A través de este espacio logras atraer clientes potenciales, demostrar tu expertiz o calidad; crear una identidad digital; ganar imagen y reputación.

El Blog es una herramienta destinada a brindarles información de interés a tus clientes, que te permite posicionarte como un referente en tu rubro.



## Redes Sociales

Son comunidades relacionadas por los mismos intereses, donde puedes captar a potenciales clientes a través de tu contenido. Las más conocidas son: Facebook, LinkedIn, Instagram o TikTok. Dentro de la clasificaciones de redes sociales se incluye la de mensajería instantánea como Whatsapp o Telegram, que te permite escribir de forma personalizada y directa a tu público objetivo.



## Newsletter

Es un tipo de correo que se envía de forma periódica a una lista de contactos o una base de datos propia. Es una forma directa de llegar a tu público. El contenido que se envíe deberá ser del interés de los receptores, de los contactos o suscritos en nuestra lista de correo.



## Podcast

Es una especie de blog en audio al cual se puede suscribir y escuchar asincrónicamente desde una computadora o dispositivo móvil, en cualquier momento. Estos pueden ser grabados en diferentes formatos, como por ejemplo entrevistas o conversatorios sobre un tema específico.

## Creación de Contenido

El contenido de tu micro y/o pequeña empresa está orientado a realzar tu marca, mostrar tu valor o captar la atención de tu público objetivo a través de la comunicación. Para ello es importante cuidar el lenguaje que usas. Imagínate a la persona que está leyendo tu contenido, debes tener presente sus gustos, sus preferencias, si es alguien a quien debes dirigirte con formalidad o es alguien a quien deseas hablarle cercana e informalmente. Recuerda que es tan importante lo que se dice como el cómo se dice.

Usa textos, imágenes, vídeos y cualquier otro elemento que permita la transmisión de tu mensaje de forma fácil y concreta.

**Es importante usar herramientas y plataformas para mostrar tu negocio, pero también es importante dedicar tiempo para capacitarte y desarrollar nuevas habilidades y desarrollar tu potencial, esto permitirá crear un contenido que destaque.**



# ¿QUÉ HABILIDADES TECNOLÓGICAS DEBO APRENDER?

**Manejo de programas de computación:** Dentro de las habilidades tecnológicas más importantes hoy en día es el manejo de programas de computación (softwares) los cuales dependerán del área del conocimiento a desempeñar. Ej.: un diseñador gráfico, debe contar con habilidades en el manejo de softwares como Illustrator, Photoshop, etc.

**Programas o herramientas de Office,** minimamente estar familiarizado con: Word, Excel, y Power Point (documentos, hojas de cálculo y presentaciones).

**Herramientas colaborativas:** Las herramientas colaborativas son servicios informáticos diseñados para mejorar el trabajo en equipo, transferencia de archivos y la comunicación. Los primeros programas para este fin fueron los emails y los servicios de mensajería instantánea. Pero con el tiempo, han ido surgiendo nuevos productos y servicios.

Las herramientas de trabajo más sencillas pueden ser los servicios de mensajería instantánea como **WhatsApp o Telegram y el servicio de Google Drive.**

Plataformas como **Zoom, Skype, Microsoft Teams, Google Meet** son buenos ejemplos de plataformas colaborativas. A través de estas aplicaciones puedes reunirte virtualmente con tu equipo o clientes, mostrando video, sonido, compartir tu pantalla, hacer encuestas virtuales entre otros.

Las herramientas colaborativas resultan esenciales para desarrollar nuestro día a día en nuestro emprendimiento o negocio, investiga cuál es la mejor para tu empresa.

# Seguridad Digital

La seguridad digital es un término amplio que se refiere a las diferentes formas de protección de infraestructura tecnológica de una organización y la información que contiene de posibles ataques maliciosos u otro tipo de riesgos.

Existen diversas herramientas para proteger los datos e información, desde la instalación de firewalls y antivirus en las computadoras, dispositivos móviles, servidores y diferentes hardwares hasta el cifrado de los discos duros y el uso de contraseñas seguras.

Es decir, la seguridad digital es la protección del contenido de los dispositivos conectados a Internet de intrusos, que podrían caer en piratería, virus, malware, phishing, suplantación de identidad y otras, por lo que es una práctica fundamental de protección de información personal, como los datos privados y datos sensibles.





# La importancia de la Seguridad Digital en las organizaciones

En definitiva, la seguridad digital es un campo de rápido crecimiento que tiene como objetivo proteger los datos para que no sean vulnerados. Por lo mismo, es tan importante tomar precauciones contra los ciberataques, principalmente por los altos costos en los que se incurre, que incluyen la pérdida de productividad, las fallas de cumplimiento y la imagen y reputación de nuestros emprendimientos.

## Tipos de datos vulnerables para la seguridad digital

**Datos personales:** La información asociada a la identificación personal, es considerada de riesgo. Por ejemplo, datos como el nombre, número de teléfono, dirección, correo electrónico, dirección IP y dependiendo del país, números relacionados a seguros sociales con los que es posible abrir cuentas de tarjetas de crédito fraudulentas, son datos que siempre hay que proteger. Estos datos de identificación personal son considerados de riesgo ya que por lo general incluyen información que potencialmente indica la localización de la víctima.

**Datos financieros:** Si de transacciones se trata, podemos decir con total seguridad que los datos personales de pago son considerados los más buscados por los ciberdelincuentes. Información que incluye números de tarjetas de crédito y débito (incluidas las fechas de vencimiento y códigos), números bancarios online (cuenta y ruta) y códigos PIN, es información que en definitiva se tiene que proteger para evitar robos y fraudes financieros.

**Datos de salud:** Este tipo de datos considerados como datos sensibles, engloba información relevante acerca de la salud de las personas, historiales de visitas médicas, medicamentos, y suscripciones a seguros de salud. Este tipo de información es de alto interés para los ciberdelincuentes ya que tienen la posibilidad de utilizar su información de salud para exponer reclamos de seguros falsos u ordenar y revender medicamentos.

## Errores frecuentes que cometemos:

- Usar contraseñas triviales o muy simples (Ej.: 12345; Juan1987).
- Reutilizar contraseñas en distintos servicios.
- Compartir contraseñas con personas no autorizadas.
- Caer en estrategias de phishing. Es decir, ingresar a correos electrónicos que suplantando una identidad y te invitan a hacer click en un enlace de una página web falsa por la que se roban datos de usuario y contraseña de la víctima.
- Instalar programas no autorizados, pudiendo dar lugar a robo de información o secuestro de datos.
- Revelar información sensible en redes sociales o compartirla con personas ajenas a la organización.

# Consejos de Seguridad Digital

Instala aplicaciones y programas únicamente de fuentes seguras. En dispositivos móviles a través de AppStore, PlayStore o los programas de antivirus instalados para computadora.

Usa contraseñas únicas que combinen números, letras y símbolos y si es posible utiliza un segundo dispositivo para la autenticación

Ten cuidado con ventanas emergentes, enlaces y archivos adjuntos que pueden llevarte a sitios falsos, virus y/o programas que roben la información a tu dispositivo.

Protege tu identidad digital. La configuración de privacidad de los servicios que utilizamos es muy importante. Y recuerda no dar información personal en los espacios virtuales que no conozcas.

# BANCA ELECTRÓNICA

Es una plataforma virtual que las entidades financieras implementan para sus clientes y se utiliza por medios electrónicos (cajeros electrónicos, teléfonos y otras redes de comunicación), permite realizar operaciones y transacciones con sus productos en tiempo real de forma autónoma, independiente, segura y rápida.

A través de la Banca Electrónica se pueden realizar operaciones bancarias de manera inmediata (24/7) y en cualquier lugar.

## ¿Cuáles son los dispositivos por los cuales se puede acceder a la Banca Electrónica?



### DISPOSITIVO MÓVIL

Permite realizar una serie de transacciones financieras de forma remota mediante un dispositivo móvil.



### COMPUTADORA

Plataforma que permite a los clientes de una institución de intermediación financiera realizar operaciones financieras desde una computadora mediante internet.

A través de la Banca Electrónica se pueden realizar muchos procesos los 7 días de la semana.

Aunque cada banco tiene su aplicación con sus características propias, la mayoría te permite realizar procesos, como:

- Consulta de saldos y movimientos
- Cambiar contraseñas (claves)
- Realizar giros
- Pago de créditos
- Transferencias
- Pago de servicios
- Manejo de tarjetas de débito
- Apertura de cuenta de ahorro
- Pago Simple - QR



## DESCARGA TU BANCA ELECTRÓNICA

Primero busca el nombre de la aplicación móvil de tu banco en AppStore o Play Store, asegúrate que sea el nombre correcto (Ej. FIE móvil es el nombre de la app de Banco FIE).

Sí es la primera vez que ingresas acude a la atención al cliente de tu banco para obtener el usuario y password o contraseña inicial. La mayoría de los bancos tienen tutoriales de ingreso en Youtube.

Generalmente podrás ingresar un método de verificación adicional como el uso de huella digital, reconocimiento facial o un código enviado a través de SMS.

Cada que cambies de teléfono celular, deberás volver a instalar la aplicación, solicitando el acceso o verificación a tu banco.



## Cajero automático (ATM):

Máquinas dispensadoras de dinero activadas mediante una tarjeta y una clave secreta personal, que identifica a un usuario. Permite realizar operaciones financieras utilizando una tarjeta de plástico con banda magnética o un chip (tarjeta de débito o tarjeta de crédito).

Dependiendo del cajero automático y la entidad bancaria se puede:

- Retirar y depositar dinero en efectivo en cualquier momento del día.
- Transferencias de dinero entre cuentas bancarias.
- Recargas de tarjetas telefónicas.

## POS:

Dispositivo usado en establecimientos comerciales que permite cobrar/pagar a través de tarjetas de débito o crédito, la creación e impresión del ticket de venta, gestionar el inventario o generar informes que ayudan en la gestión del negocio.



- El punto de venta mejora en velocidad y disminuye el riesgo de un "error humano" al ser una herramienta que procesa las peticiones mucho más rápido.
- Control de stock: puede gestionar el stock del negocio en tiempo real.
- Ahorro de tiempo y dinero: por la operación automática y precisa que realizará la aplicación por ti.
- Seguridad: disminución en el riesgo por robo.

A través de estos dispositivos POS existe la facilidad de pagar/cobrar con solo la proximidad de la tarjeta de débito/crédito (Contact Less) y en compras igual o menores a 100 Bs. no se requiere introducir el PIN.

## Pago Simple QR:

Es un sistema que facilita las transacciones electrónicas (cobrar, pagar) a través de un código y que está presente en todas las apps de los bancos.

Un Código QR, es una imagen segura que contiene información codificada, en este caso información del número de cuenta titular, tipo de cuenta, banco, moneda y monto. Es así que ya no es necesario llenar cada vez la información personal, evitando así errores de llenado. A través de este sistema podrás realizar cobros y/o pagos de hasta Bs. 5.000 y la verificación de movimientos, escaneando el código QR.



Para poder realizar el pago o cobro por QR, se debe contar con la app del banco descargada en tu teléfono móvil.

En el menú general encontrarás la opción de “Pago/Cobro QR” la cual cuenta con tres opciones: cobro, pago y movimiento.

## Cobro QR:

- Ingresa a la opción cobro, selecciona la cuenta a la que se abonará o ingresará el dinero del cobro.
- \* Se puede elegir si la validez del QR (imagen generada) es por uno o varios días.
- Llena el monto a cobrar o déjalo en blanco para que la persona que pague ingrese el monto.
- Finalmente, selecciona la opción “generar código QR”, para guardarlo como imagen en tu teléfono o compartirlo directamente con la persona que debe pagar.

## Pago QR:

- Al seleccionar en el menú el Pago QR, se habilitará la pantalla para escanear el código QR.
- Escanea el código QR.
- Te aparecerá la cuenta de destino a la que se realizará el abono del dinero.
- Sí el monto es fijo, aparecerá el monto a pagar, de lo contrario debes introducirlo tú.
- Selecciona la cuenta desde la cual se realizará el pago y dale click a confirmar el pago.
- \*Se puede enviar el comprobante realizado a tu contacto.

## ¿Es seguro el uso de la Banca Electrónica?

Sí. La seguridad de los usuarios de banca electrónica es una prioridad al momento del desarrollo de las diferentes plataformas por parte de las entidades financieras (Bancos, Fondos Financieros y otros), debiendo cumplir la normativa y estándares establecidos a nivel nacional e internacional.

Existen estándares de seguridad a ser cumplidos por todas las entidades financieras como la encriptación de los datos de los usuarios y la certificación de seguridad de los servidores. Indicar que toda la seguridad esta normada y supervisada por la Autoridad de Supervisión del Sistema Financiero (ASFI).







# GLOSARIO

**Capacidades Digitales:** Son las competencias que facilitan el uso de los dispositivos digitales, las aplicaciones de comunicación y las redes para acceder a la información y llevar a cabo una mejor gestión de éstas.

Es la suma de conocimientos, capacidades, destrezas, actitudes y estrategias que se requieren para el uso de las tecnologías e Internet.

**Capacidades Tecnológicas:** La definición de capacidades tecnológicas implica conocimientos y habilidades para adquirir, usar, absorber, adaptar, mejorar y generar nuevas tecnologías.

**Banca electrónica:** Plataforma virtual que las entidades financieras implementan para sus clientes y se realizan por medios electrónicos (cajeros electrónicos, teléfonos y otras redes de comunicación) y permite a sus clientes realizar operaciones y transacciones con sus productos en tiempo real de forma autónoma, independiente, segura y rápida.

**Malware:** Es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas. Está conformado por todo tipo de software malicioso, incluidos los virus, troyanos, gusanos, spyware y adware y se usa por muchos motivos, tales como: Infectar computadoras y usarlas para extraer bitcoins u otras criptomonedas.

**Phishing:** Es un ataque informático de ingeniería social que usa medios de comunicación digitales, como el correo electrónico, para engañar y estafar a las personas, utiliza el fraude, el engaño y el timo para manipular a sus víctimas y hacer que revelen información personal confidencial.

**Seguridad Digital:** Es aquella que se encarga de proteger elementos tales como ordenadores, servidores, teléfonos móviles, infraestructuras de red y cualquier otro sistema informático conectado, por el que circule o en el que se almacene información valiosa para la empresa o usuario.

**Virus:** Un virus informático es un tipo de malware, es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo, diseñado para propagarse de un equipo a otro y tiene el potencial para provocar efectos inesperados o dañinos, como perjudicar el software del sistema, ya sea dañando o destruyendo datos.

# REFERENCIAS

Alianza del Pacífico. (2022). Competencias Digitales. Alianza del Pacífico – El poder de la integración. <https://capacitacion.alianzapacifico.net/index.php/competencias-digitales/>

Bell y Pavitt, 1995; Lall, 1992 en Lugones et al, 2007

Conecta Software. S.f. Conecta Software. Qué es la competencia digital. <https://conectasoftware.com/analytics/que-son-las-habilidades-o-competencias-digitales/>

Redacción Redestelecom. (2022). Recomendaciones para protegernos en el mundo digital. RyT Redes y Telecom. <https://www.redestelecom.es/seguridad/noticias/1131271002503/recomendaciones-protecternos-mundo-digital.1.html>

Pereda, T. (2020). 5 competencias digitales esenciales para tu empresa. Lemon. <https://lemon.digital/5-competencias-digitales-esenciales-para-tu-empresa/>

Soto, L. (2021). ¿Qué es la seguridad digital? Signaturit Blog. <https://blog.signaturit.com/es/que-es-seguridad-digital>

Lugones et al. (2007). Indicadores de Capacidades Digitales en América Latina. Series Estudios y Perspectivas. [https://repositorio.cepal.org/bitstream/handle/11362/5014/1/S0700876\\_es.pdf](https://repositorio.cepal.org/bitstream/handle/11362/5014/1/S0700876_es.pdf)

Morduchowicz, R. (2021). Competencias y habilidades digitales. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000380113.locale=en>

Competencias y habilidades digitales UNESCO Office Montevideo and Regional Bureau for Science in Latin America and the Caribbean Morduchowicz, Roxana.



Financiado por  
la Unión Europea



# Aprender y fortalecer para **EMPRENDER**

