

CURSO E

HAZ TUS COMPRAS EN LÍNEA CON SEGURIDAD

NIVEL BÁSICO INICIAL

QUÉ APRENDERÁS

- Serás capaz de realizar búsquedas sencillas en internet a través de un dispositivo electrónico con ayuda del equipo docente.
- Podrás identificar nociones básicas de ciberseguridad y aplicarlas para navegar en internet de forma segura.
- Clasificarás mensajes de correo electrónico dentro de las diferentes carpetas de la aplicación y utilizarás el correo electrónico para comunicarse digitalmente con otras personas.
- Podrás identificar mensajes de correo sospechosos basándote en la verificación de indicadores de seguridad.
- Realizarás compras en línea seguras aplicando prácticas de ciberseguridad apropiadas.
- Serás capaz de resolver problemas sencillos relacionados con el dispositivo electrónico utilizado y la navegación en internet, así como con compras en línea seguras.

CÓMO APRENDERÁS

- Realizando las tareas personalmente con apoyo del equipo docente.
- Resolviendo enigmas y casos que te ayudarán a aprender practicando.
- Utilizando simulaciones con gafas 3D.
- Participando en juegos y dinámicas en grupo.

RECURSOS

- Portátil, tableta, gafas 3D, juegos.

DURACIÓN

- 10 horas repartidas en 5 días

CALENDARIO

DÍA 1: Introducción al curso.

Entrega de un cuaderno y un bolígrafo

DÍA 2: Navegación segura por internet.

Entrega de una bolsa de tela y un agarrador para el móvil

DÍA 3: Comunicación digital: el correo electrónico.

DÍA 4: Compras digitales seguras.

Entrega de un pen drive

DÍA 5: Realizar una compra digital.

Participación en el sorteo de un viaje si completas el curso





ANDROID BLOQUEO Y DESBLOQUEO



IDENTIFICA Y SELECCIONA LAS FORMAS DE BLOQUEO EXISTENTES

Código PIN: ve a Ajustes > Seguridad y Ubicación > Bloqueo de Pantalla y selecciona tu PIN

Contraseña alfanumérica: dirígete a Ajustes > Seguridad y Ubicación > Bloqueo de Pantalla > Contraseña. Te pedirá introducir una contraseña que contenga al menos cuatro caracteres

Patrón de desbloqueo: accede a Ajustes > Seguridad y Ubicación > Bloqueo de Pantalla (al igual que el PIN) y selecciona el patrón de desbloqueo

Huella dactilar: acude al menú anterior: Ajustes > Seguridad y Ubicación > Huella digital. Desde aquí, sigue los pasos necesarios para terminar de configurarla.

Desbloqueo por reconocimiento facial: ve a Ajustes > Seguridad y Ubicación > Smart lock > Reconocimiento Facial. A partir de aquí, el sistema te guiará para terminar la configuración



ANDROID BLOQUEO Y DESBLOQUEO



CREA CONTRASEÑAS SEGURAS

Crea contraseñas robustas difíciles de piratear. El **INCIBE** coMmparte buenas prácticas para hacerlo.



DOBLE FACTOR DE AUTENTICACIÓN

Añade una capa adicional de seguridad a tu **cuenta de Google**.

Es una medida de seguridad adicional a la contraseña que se utiliza para **proteger del acceso no autorizado** a las cuentas de los usuarios online.

Ve a Ajustes > Google > Gestionar tu cuenta de Google > Seguridad. En Inicio de sesión de Google pulsa Verificación en dos pasos > Empezar y sigue los pasos indicados.

Protege tus dispositivos para resguardar tus datos, tus ahorros y tu intimidad

Fuente:INCIBE





Apple BLOQUEO Y DESBLOQUEO



IDENTIFICA Y SELECCIONA LAS FORMAS DE BLOQUEO EXISTENTES

Código PIN: ve a Ajustes > TouchID/FaceID y código > activar tu código

Huella dactilar: dirígete a Ajustes > TouchID/FaceID y código > TouchID. Con el PIN puedes seleccionar la opción **Añadir huella**. *No todos los dispositivos cuentan con esta funcionalidad.

Reconocimiento facial: dirígete a Ajustes > TouchID/FaceID y código. Con el PIN puedes seleccionar **configurar Facial ID**. *No todos los dispositivos cuentan con esta funcionalidad.



CREA CONTRASEÑAS SEGURAS

Crea contraseñas robustas difíciles de piratear. El **INCIBE** comparte buenas prácticas para hacerlo.



Apple BLOQUEO Y DESBLOQUEO



DOBLE FACTOR DE AUTENTICACIÓN

Añade una capa adicional de seguridad a tu **cuenta de Apple**.

Es una medida de seguridad adicional a la contraseña que se utiliza para **proteger del acceso no autorizado** a las cuentas de los usuarios online.

Versión iOS 10.3 o superior. Ve a Ajustes > [nombre] > Contraseña y seguridad > Activar autentificación de doble factor > Continuar.

Versión iOS 10.2 o superior. Ve a Ajustes > iCloud > [Apple Id] > Contraseña y seguridad > Activar autentificación de doble factor > Continuar y seguir los pasos indicados.

Tienes más instrucciones de cómo hacerlo en [¿Cómo activar la autentificación de doble factor?](#)

Protege tus dispositivos para proteger tu datos, tus ahorros y tu intimidad

Fuente: Incibe





NAVEGACIÓN SEGURA EN INTERNET



Un navegador es una aplicación de software que nos permite acceder a toda la información de la World Wide Web, es decir internet

¿CÓMO ELEGIR EL NAVEGADOR?

- Tiene una buena experiencia de usuario: fácil de entender y cómodo.
- Se actualiza automáticamente para corregir vulnerabilidades
- Permite eliminar información almacenada en el caché, cookies e historial.
- Ofrece la opción de navegación de incógnito.
- Protege la privacidad de tus búsquedas.

¿QUÉ NAVEGADORES SE SUELEN UTILIZAR?



Google Chrome

- El navegador se actualiza automáticamente cada 6 semanas o cuando hay una nueva versión.
- Almacena información personal al poder enlazarse a una cuenta de Gmail.
- Incluye funcionalidades de seguridad para evitar sitios web peligrosos y protección predictiva frente a la suplantación de identidad.



Mozilla Firefox

- Por defecto, Firefox está configurado para actualizarse automáticamente.
- Permite controlar ajustes de privacidad, como por ejemplo, evitar que los sitios web rastreen tu actividad de navegación.
- En cuanto a seguridad, dispone de funcionalidades de protección contra software peligroso y contenido malicioso.

Fuente: INCIBE





NAVEGACIÓN SEGURA EN INTERNET



Microsoft Edge

- Permite eliminar los datos de búsqueda recopilados por el navegador como historial de navegación, cookies o contraseñas, entre otros.
- Incorpora el sistema SmartScreen de Windows Defender para bloquear automáticamente las descargas de sitios web y de contenidos que sean conocidos como malintencionados.
- El navegador se actualiza a través de Windows 10 Update Assistant de manera automática.
- Puede contar herramientas de Inteligencia Artificial (IA) integradas.



Safari

- El navegador se actualiza cuando sale una nueva versión del sistema operativo macOS.
- Dispone de funcionalidades de privacidad y seguridad integradas como navegación privada, antirrastreo inteligente o protección contra sitios dañinos.



¿QUÉ SON LAS DIRECCIONES HTTPS://?

- Son protocolos de comunicación de internet que protegen la integridad y la confidencialidad de todos los datos que se intercambian entre tu dispositivo y el sitio web que estás consultando o viceversa
- Cifra la información para que terceras partes no puedan tener acceso a ella aunque intercepten la comunicación.
- Los sitios con https aplican tres capas de seguridad a la aplicación para asegurar que toda tu información está segura.
- Los sitios http no son maliciosos o fraudulentos pero no protegen tu datos de forma eficaz. Por lo que puede que ciberdelincuentes accedan a tus datos en estos sitios.

Fuente: INCIBE



NAVEGACIÓN SEGURA EN INTERNET



¿QUÉ ES UN MOTOR DE BÚSQUEDA?

- Es un software cuya función es buscar contenidos en internet.
- Un buen buscador debe respetar tu información y no rastrearla ni guardarla.
- Los buscadores seguros muestran resultados de búsqueda objetivos y no influenciados por el posicionamiento web.

DIFERENCIAS CON UN NAVEGADOR

Mientras que el navegador es el software que te permite consultar información de cualquier página de internet a través de una **dirección web o URL**, el motor de búsqueda te permite **encontrar información precisa** que necesitas entre todos los contenidos disponibles.

¿QUÉ MOTORES DE BÚSQUEDA SON MÁS UTILIZADOS?



Google Search: es el buscador de Google. El más utilizado con diferencia. Es algo más que un buscador, ya que ofrece un gran volumen de “servicios gratuitos” puestos a disposición de los usuarios al poseer una cuenta.



Bing: es el buscador de Microsoft. Ofrece igualmente servicios propios de Microsoft (Outlook o paquete Office) a cambio de tus datos personales. Cuenta además con herramientas de IA integradas.



Yahoo! Search: es el buscador de Yahoo!. Da acceso a servicios gratuitos, como al servicio de correo o a su comunidad de imágenes Flickr. Es el tercero más utilizado. También se basa en políticas de cesión de datos.



DuckDuckGo

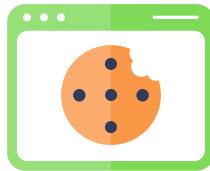
DuckDuckGo: es el buscador de DuckDuckGo. Esta compañía aboga por la privacidad de los usuarios: ni recopilará información personal que identifique a un usuario, ni la compartirá con nadie. Permite utilizar Google Search sin ser rastreado.

Fuente: INCIBE





NAVEGACIÓN SEGURA EN INTERNET



¿QUÉ INFORMACIÓN ALMACENA CUANDO NAVEGAMOS?

Cookies: Son pequeños archivos que se guardan en tu ordenador cuando navegas y que almacenan información sobre los sitios que visitas, preferencias y otra información personal.

Historial de navegación: es el registro completo de toda nuestra actividad en Internet. Cualquier persona que tenga acceso a nuestro navegador podrá ver qué hemos estado haciendo y cuándo.

Registro de las credenciales: muchos navegadores permiten la memorización del usuario y contraseña de los sitios usualmente visitados.

Caché: son archivos temporales (se eliminan con el tiempo) que se guardan para que nuestra navegación vaya más rápida, como por ejemplo imágenes, para no tener que cargarlas cada vez que accedamos.

Recuerda borrar periódicamente el rastro que dejas al usar el navegador para proteger tus datos

Fuente: INCIBE



EL USO DEL CORREO ELECTRÓNICO



¿QUÉ ES Y PARA QUÉ SIRVE?

El correo electrónico o email en inglés es una herramienta básica de **comunicación digital**. Un servicio en línea que, al igual que ocurre con el correo postal tradicional, nos permite enviar y recibir mensajes a través de un servicio de red a múltiples destinatarios.

Utilidad:

- **Identificarnos a través de Internet y registrarnos** en diferentes servicios en línea. Como por ejemplo para aprovechar los cursos de la Fundación Integra.
- **Asociar uno o varios dispositivos** y sincronizar toda la información almacenada, como contactos, agenda, localizaciones guardadas, etc., entre ellos.
- **Realizar compras en línea:** las plataformas de compra online requieren nuestro correo electrónico para verificar nuestra cuenta, enviarnos notificaciones y como parte de la información personal que nos solicitan.

Recuerda que para proteger tu cuenta de correo y la información que compartes en las plataformas y servicios en los que te inscribas debes crear contraseñas seguras

Fuente: INCIBE



EL USO DEL CORREO ELECTRÓNICO



PARTES IMPORTANTES DE TU CUENTA DE CORREO ELECTRÓNICO

La bandeja de entrada es la parte del correo donde podrás ver los mensajes recibidos. Es la página que aparece cuando abres la cuenta.

Panel o barra de navegación lateral es la parte del servidor que te muestra sus diferentes carpetas y funcionalidades. Suele estar a la izquierda de la pantalla.

Carpetas En ellas podrás encontrar los diferentes correos que clasifica el servidor: recibidos, enviados, spam, borradores...

Carpeta de SPAM donde el servidor clasifica automáticamente todos los correos que le parecen sospechosos. Es una de las funcionalidades de seguridad de tu servidor de correo electrónico.

Configuración o settings es la parte del servidor en la que tienes las opciones de configuración de tu cuenta, como tus datos personales o cómo quieres que el servidor clasifique tus correos o te apoye en la redacción de los mensajes.



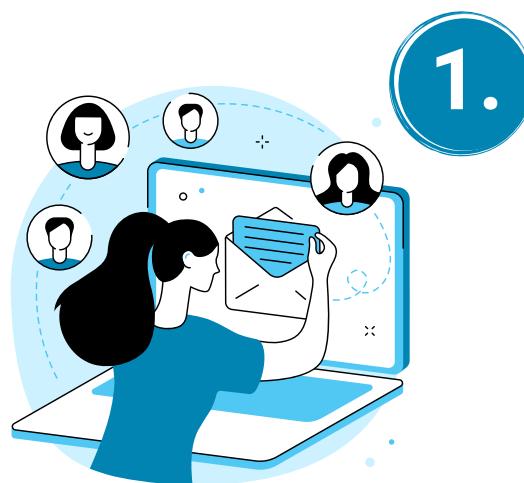
IDENTIFICA UN MENSAJE MALICIOSO



¿QUÉ ES EL PHISHING?

El **phishing** es una técnica que consiste en el envío de un correo electrónico en el que los ciberdelincuentes suplantan la identidad de entidades públicas, una empresa reconocida o un servicio que utilicemos, para obtener toda nuestra información personal y bancaria y realizar compras con nuestro dinero.

¿CÓMO DETECTARLO?



1.

REVISA EL REMITENTE

¿Esperabas una comunicación de esta entidad o persona? Identifica que la **dirección** que lo envía existe realmente y que corresponde a la entidad.

Fuente: Incibe



2.

ANALIZA EL OBJETIVO DEL MENSAJE

Una entidad que ofrece servicios nunca pide información personal o bancaria por correo, ya que es información sensible. Atención a los **premios, promociones muy atractivas o amenazas**, suelen ser phishing.



IDENTIFICA UN MENSAJE MALICIOSO



3.

VERIFICA LOS ENLACES

Sitúa el ratón encima del enlace para que te salga la dirección URL. Revisa si es la URL oficial de la entidad. ¡Cuidado!, **nunca abras el enlace antes de la verificación.**

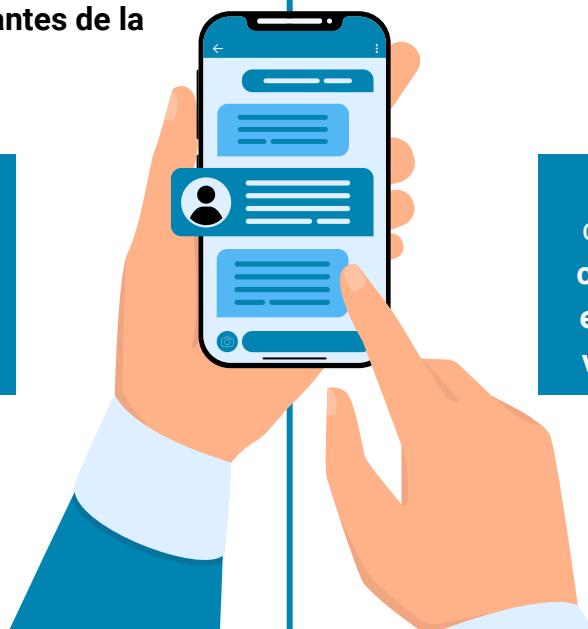
Fíjate en si tiene **errores de ortografía y gramática, o el asunto es llamativo** (puede poner urgente, importante, has ganado, etc.)



4.

ANALIZA LOS ARCHIVOS ADJUNTOS

¿Estabas esperando alguna documentación de esta entidad? Siempre **analiza con un antivirus el archivo antes de abrirlo.**



Si tienes dudas de si un correo es malicioso o no, **contacta por teléfono a la entidad que lo envía para verificar su autenticidad.**

Fuente: INCIBE

OFERTA

COMPRAS SEGURAS EN LÍNEA



Una **compra en línea** es la acción voluntaria de adquirir un producto o contratar un servicio a través de internet y realizando el pago a través de procesos telemáticos.



¿QUÉ VENTAJAS TIENEN?

1. Nos ahorraremos en desplazamiento.
2. Recibimos el pedido cómodamente en casa o recibimos los papeles del servicio por correo electrónico.
3. Es más fácil comparar precios y ofertas.
4. Puedes hasta planificar un viaje sin salir de casa

¿QUÉ PRECAUCIONES HAY QUE TOMAR?

1 Busca indicadores de seguridad: revisa que la dirección empiece por HTTPS, que tenga certificado de seguridad (el candado al lado de la dirección) y sellos de confianza (al pie o a los laterales de la página principal).

2 Verifica los métodos de pago que admite: no es buena señal que solo se pueda pagar con tarjeta de crédito o que no nos redirija a la pasarela de pago del banco.

Fuente: INCIBE



Plan de Recuperación
Transformación
y Resiliencia

OFERTA

COMPRAS SEGURAS EN LÍNEA



3 Comprueba la valoración y comentarios de otros usuarios: puedes consultar páginas especializadas para ello o mirar en foros o en redes sociales.

4 Desconfía de las ofertas demasiado atractivas: ya que es una de las técnicas utilizadas por los ciberdelincuentes.

5 Asegúrate de que se trata de la página oficial de la empresa : para evitar caer en páginas falsas comprueba que los datos de la empresa en esa web coinciden con la empresa real consultando sitios de información sobre las empresas (NIF, dirección, etc.). Desconfía si no aparece información de contacto.

6 Consulta la política de privacidad y de envío y devolución: deben estar accesibles, actualizadas, ser claras y que informen cómo van a ser tratados nuestros datos o cómo funcionan los envíos, devoluciones y reembolsos.

7 Comparte solo los datos que sean necesarios: si te piden datos de otras personas o lugar de nacimiento no hagas la compra y revisa que estás en la web correcta.

8 Revisa periódicamente los movimientos de tu cuenta: para comparar los cargos con las compras reales y estar alerta si ves algún cargo que no corresponde.

Fuente: INCIBE



Plan de Recuperación
Transformación
y Resiliencia



fundación
Integra
digital

OFERTA

COMPRAS SEGURAS EN LÍNEA



MÉTODOS DE PAGO EN LÍNEA

A la hora de efectuar un pago, hay varios métodos en línea disponibles que cumplen con diversas medidas de seguridad, como cifrado de datos, autenticación de dos factores y sistemas de detección de fraudes.

PAGOS DE FORMA SEGURA

1 Tarjetas de crédito: es muy importante comprobar que el sitio web nos redirige a la pasarela de pago segura de nuestro banco, abriendose una nueva ventana del navegador, donde es necesario confirmar la transacción realizando los pasos adicionales como introducir un código numérico recibido por SMS, acceder a la app del banco para confirmar la compra, etc.

2 PayPal: Es un sistema que te permite realizar pagos online de forma segura creando una cuenta de usuario. Selecciona PayPal como método de pago y serás redirigido a la página de inicio de sesión de PayPal, abriendose una nueva ventana.

3 Bizum: Permite a los usuarios realizar pagos en línea a través de una aplicación móvil. Para utilizar Bizum debes vincular tu número de teléfono móvil con tus datos financieros y es autorizado por casi todos los bancos.

Fuente: INCIBE



Plan de Recuperación
Transformación
y Resiliencia

OFERTA

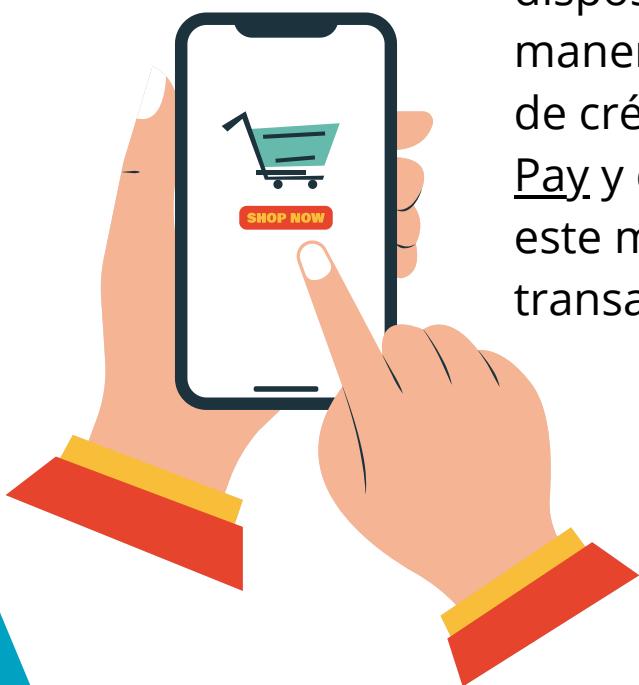
COMPRAS SEGURAS EN LÍNEA



4 Apple Pay: Es una forma de pago móvil que está disponible en dispositivos Apple. Puedes agregar tus tarjetas de crédito o débito a la aplicación Wallet en Apple y, en el momento de pagar en una tienda online o aplicación móvil, simplemente seleccionarlo como método de pago. Verifica la transacción con el sistema Touch ID (huella) o Face ID (rostro).



5 Google Pay: Es una plataforma de pago móvil que permite a los usuarios de dispositivos Android comprar online de manera segura. Puedes vincular tus tarjetas de crédito o débito a la aplicación Google Pay y cuando vayas a pagar, seleccionar este método de pago y confirmar la transacción con tu huella digital o PIN.



Fuente: INCIBE





EL USO DEL CORREO ELECTRÓNICO



¿QUÉ ES Y PARA QUÉ SIRVE?

El correo electrónico o email en inglés es una herramienta básica de **comunicación digital**. Un servicio en línea que, al igual que ocurre con el correo postal tradicional, nos permite enviar y recibir mensajes a través de un servicio de red a múltiples destinatarios.

Utilidad:

- **Identificarnos a través de Internet y registrarnos** en diferentes servicios en línea. Como por ejemplo para aprovechar los cursos de la Fundación Integra.
- **Asociar uno o varios dispositivos** y sincronizar toda la información almacenada, como contactos, agenda, localizaciones guardadas, etc., entre ellos.
- **Realizar compras en línea:** las plataformas de compra online requieren nuestro correo electrónico para verificar nuestra cuenta, enviarnos notificaciones y como parte de la información personal que nos solicitan.

Recuerda que para proteger tu cuenta de correo y la información que compartes en las plataformas y servicios en los que te inscribas debes crear contraseñas seguras

Fuente: INCIBE



EL USO DEL CORREO ELECTRÓNICO



PARTES IMPORTANTES DE TU CUENTA DE CORREO ELECTRÓNICO

La bandeja de entrada es la parte del correo donde podrás ver los mensajes recibidos. Es la página que aparece cuando abres la cuenta.

Panel o barra de navegación lateral es la parte del servidor que te muestra sus diferentes carpetas y funcionalidades. Suele estar a la izquierda de la pantalla.

Carpetas En ellas podrás encontrar los diferentes correos que clasifica el servidor: recibidos, enviados, spam, borradores...

Carpeta de SPAM donde el servidor clasifica automáticamente todos los correos que le parecen sospechosos. Es una de las funcionalidades de seguridad de tu servidor de correo electrónico.

Configuración o settings es la parte del servidor en la que tienes las opciones de configuración de tu cuenta, como tus datos personales o cómo quieres que el servidor clasifique tus correos o te apoye en la redacción de los mensajes.

CREA TU CUENTA EN FORM@CARM



¿QUÉ ES FORM@CARM ?

Tu plataforma de cursos gratuitos de la Región de Murcia
con más de 125 cursos disponibles para
seguir mejorando tus habilidades.

No hay requisitos, solo debes crear una cuenta para
inscribirte en los cursos que te interesen.

PASOS PARA CREAR TU CUENTA

1

Entra en la página de
<https://www.formacarm.es/portal/>

Selecciona el botón

ACCESO A CURSOS

2

que encontrarás arriba a la
derecha de la página

3

En la siguiente página tienes dos opciones:
Acceder o Registrarse. Selecciona Registrarse
como usuario y pulsa el botón

Crear nueva cuenta

CREA TU CUENTA EN FORM@CARM



4

Rellena todos los datos personales que se solicitan, como el nombre, DNI o dirección

En esa misma páginas debes crear una contraseña segura para el sitio

5

También deberás marcar las casillas que correspondan al final de la página.

[Entiendo y estoy de acuerdo*](#)



[Validación automática](#)



Por último debes presionar el botón

[Crear cuenta](#)

7

para que la cuenta sea creada

Mejora tus habilidades digitales disfrutando de los cursos gratuitos de la Región de Murcia