CHECKLIST PARA EVALUAR Y VERIFICAR TU SEGURIDAD DIGITAL

*Esta lista de verificación debe completarse solo después de leer la **Guía de seguridad digital para todos.***

Seguridad Digital

- ○ Comprendo la diferencia entre seguridad digital y ciberseguridad, y reconozco la importancia de ambas para mi protección general en línea.
- ○ Soy consciente de la creciente digitalización de nuestras vidas y de los riesgos que conlleva.
- ○ Me aseguro de que mi software se actualiza regularmente para parchear las vulnerabilidades conocidas, reduciendo el riesgo de explotación por parte de los ciberdelincuentes.
- ○ Me mantengo informado y actualizado sobre las tendencias en seguridad digital a través de fuentes acreditadas.
- ○ Presto atención a mi presencia en línea comprobando regularmente las aplicaciones, los programas y la información personal que tengo en línea.

Software

- ○ Reconozco que una huella digital es un registro de mis actividades en línea, que da forma a mi identidad en línea incluso cuando no utilizo activamente Internet.
- ○ Entiendo que acciones como publicar, buscar o compartir en línea contribuyen a crear un rastro de datos que puede revelar aspectos de quién soy.
- ○ Soy consciente de que el uso de Internet deja un rastro de datos que recogen los motores de búsqueda, las redes sociales y las empresas, lo que plantea riesgos como el fraude potencial y la invasión de la privacidad.
- ○ Sigo buenas prácticas de ciberseguridad, incluido el uso de programas antivirus y su actualización periódica.
- ○ En caso necesario, conozco los pasos para borrar mi huella digital, incluida la desactivación de cuentas en redes sociales y la presentación de solicitudes de eliminación de información personal.

Contraseñas

- ○ Comprendo los criterios para crear una contraseña segura, incluido el uso de palabras, frases y combinaciones de letras, números y símbolos poco habituales.
- ○ Soy consciente de la existencia de diversos métodos utilizados por los piratas informáticos para descifrar contraseñas.
- ○ Nunca utilizo la misma contraseña en varios sitios para evitar la vulnerabilidad de las cuentas vinculadas.
- ○ Tengo por costumbre cambiar las contraseñas con regularidad para añadir una capa adicional de seguridad.
- ○ Utilizo métodos de seguridad adicionales como la autenticación de dos factores (2FA), la autenticación multifactor (MFA) y las contraseñas de un solo uso (OTP) para mejorar la protección de las cuentas.

DOCUMENTO ELABORADO POR
cameco+
Communication Consultancy for the Common Good

CHECKLIST PARA VERIFICAR LA SEGURIDAD DIGITAL

*Esta lista de verificación debe completarse solo después de leer la **Guía de seguridad digital para todos.***

Inteligencia artificial generativa (IA generativa)

- ○ Comprendo que la IA generativa crea texto, imágenes y contenidos diversos utilizando los conocimientos adquiridos con la formación.
- ○ Me mantengo informado sobre los avances de la IA generativa y sus riesgos potenciales.
- ○ Soy consciente de los riesgos en materia de seguridad digital, como las imitaciones convincentes para estafas, el malware sofisticado y los problemas de seguridad de los datos.
- ○ Verifico la información procedente de múltiples fuentes fiables para contrarrestar la desinformación generada por IA.
- ○ Informo de los contenidos sospechosos generados por IA a las plataformas y autoridades pertinentes.
- ○ Actualizo regularmente la configuración de privacidad de mis cuentas en línea.

Aspectos socioculturales de la seguridad digital

- ○ Entiendo que el contexto, ya sea individual, comunitario u organizativo, puede dar forma a las percepciones y prácticas de seguridad digital.
- ○ Soy consciente de que determinadas personas, por motivos de raza, etnia, sexo, nacionalidad o credo, pueden ser más vulnerables en línea.
- ○ Entiendo las diversas formas de acoso en línea, incluyendo difamación, suplantación de identidad, extorsión, acecho, vigilancia sexual, hostigamiento, daño emocional y amenazas de violencia.
- ○ Reconozco que los problemas de bienestar, la cultura de la cancelación y la autocensura son amenazas que afectan a la seguridad en línea de todos.
- ○ Promuevo la empatía digital, fomentando la comprensión y denunciando el acoso en línea para crear un espacio en línea más seguro.

Otros aspectos

- ○ Me aseguro de tener un teléfono u ordenador portátil exclusivamente para el trabajo con el fin de mejorar la seguridad.
- ○ Soy consciente de las normativas específicas de cada país sobre prácticas digitales, como el uso prohibido de VPN personales en algunos lugares.
- ○ Reconozco que, a pesar de no ser famoso, puedo seguir siendo un objetivo para las amenazas digitales.
- ○ Comprendo que acciones sencillas, como la actualización periódica del software y el uso de contraseñas más seguras, pueden mejorar significativamente la seguridad digital.
- ○ Reconozco que alcanzar el 100% de seguridad digital es imposible debido a la evolución de las amenazas y a los factores humanos.

DOCUMENTO ELABORADO POR
cameco+
Communication Consultancy for the Common Good

CHECKLIST PARA VERIFICAR LA SEGURIDAD DIGITAL

*Esta lista de verificación debe completarse solo después de leer la **Guía de seguridad digital para todos.***

Navegadores o *browsers*

- ○ Entiendo que el uso de un navegador web inseguro puede exponerme a riesgos como la piratería informática, el robo de datos, el rastreo, el malware y otras amenazas.
- ○ Reconozco que incluso los navegadores seguros no proporcionan una seguridad absoluta, por lo que es esencial adoptar buenas prácticas de higiene web.
- ○ Mantengo mi navegador actualizado con regularidad y utilizo un número mínimo de extensiones para reducir el riesgo de comprometer la información.
- ○ Instalo un adblocker fiable para bloquear los anuncios maliciosos, las molestias, las amenazas a la privacidad y los rastreadores.
- ○ Bloqueo las ventanas emergentes para evitar exponerme a contenidos molestos y peligrosos de sitios web maliciosos.
- ○ Elimino regularmente las cookies no deseadas para evitar el rastreo y proteger la privacidad.
- ○ Deshabilito la función de autorrelleno para evitar introducir información confidencial en formularios potencialmente maliciosos.

Redes privadas virtuales (VPN)

- ○ Reconozco que una VPN, o "red privada virtual", protege mi conexión a Internet, garantizando la privacidad en línea a través de un túnel de datos cifrado.
- ○ Reconozco la importancia de utilizar una VPN personal, especialmente cuando me conecto a redes Wi-Fi públicas, accedo a contenidos restringidos, protejo mis datos personales y oculto mi dirección IP.
- ○ Evalúo regularmente mis actividades en línea para determinar si es necesaria una VPN para mejorar mi seguridad y privacidad.

Redes sociales

- ○ Reconozco la doble naturaleza de las redes sociales, sus ventajas para el aprendizaje y la comunicación y sus riesgos potenciales, como el ciberacoso y la adicción.
- ○ Organizo activamente mi configuración de privacidad para controlar la audiencia de mis publicaciones en las redes sociales.
- ○ Soy consciente de la permanencia de las publicaciones en línea y protejo mi reputación seleccionando cuidadosamente los contenidos compartidos.
- ○ Adapto mi presencia en Internet, absteniéndome de compartir en exceso en entornos que puedan plantear riesgos.
- ○ Doy prioridad a la privacidad de la información personal para evitar el robo de identidad.
- ○ Conozco las medidas apropiadas en determinadas situaciones, como eliminar y bloquear a los acosadores, informar a los administradores del sitio e implicar a las autoridades cuando sea necesario.
- ○ Actúo con cautela en las redes sociales y me mantengo alejado de mensajes, enlaces o intentos de suplantación de identidad sospechosos.
- ○ Evito compartir información sensible a través de sistemas de mensajería para mitigar los riesgos de piratería informática, violación de datos e interceptación.

DOCUMENTO ELABORADO POR
cameco+
Communication Consultancy for the Common Good