GUÍA DE BUENAS PRÁCTICAS

CEPA BERNAL DÍAZ DEL CASTILLO

BIENESTAR DIGITAL

El bienestar digital hace referencia al equilibrio saludable entre el uso de la tecnología y el cuidado de nuestra salud mental y física. A medida que nuestra vida cotidiana se digitaliza, es fundamental gestionar de manera consciente cómo las tecnologías afectan nuestro bienestar, para evitar el agotamiento digital y mantener una relación saludable con los dispositivos.

1. Equilibrio entre Tecnología y Vida Personal

- **Desconexión Programada**: Establecer horarios específicos para desconectar de los dispositivos, como durante las comidas, antes de dormir o durante actividades familiares. Esto ayuda a reducir la dependencia de la tecnología y a mejorar la calidad del tiempo personal. Puedes utilizar aplicaciones que te ayuden a programar estos momentos de desconexión.
- **Actividades Sin Pantallas**: Dedicar tiempo a hobbies y actividades que no involucren tecnología, como leer, hacer ejercicio, practicar deportes, cocinar, o pasar tiempo en la naturaleza. Estas actividades pueden mejorar el bienestar general y reducir el estrés. Considera unirte a clubes o grupos locales que compartan tus intereses para fomentar la interacción social.

2. Uso Consciente de la Tecnología

- **Redes Sociales con Moderación**: Limitar el tiempo en redes sociales y ser selectivo con el contenido que consumimos. Utilizar herramientas de gestión del tiempo para monitorizar y controlar el uso de estas plataformas. Reflexiona sobre el propósito de tu uso de redes sociales y ajusta tus hábitos para alinearlos con tus objetivos personales.
- **Notificaciones**: Desactivar notificaciones innecesarias para reducir distracciones y mejorar la concentración. Configurar el móvil para recibir solo las notificaciones esenciales. Puedes establecer horarios específicos para revisar tus notificaciones y correos electrónicos, evitando así interrupciones constantes.

3. Salud Física y Ergonomía

- **Postura y Mobiliario**: Utilizar sillas ergonómicas y ajustar la altura de la pantalla para mantener una postura adecuada. Asegurarse de que la pantalla esté a la altura de los ojos y que los pies estén apoyados en el suelo. Considera la posibilidad de utilizar escritorios ajustables que te permitan trabajar de pie en algunos momentos del día.

- **Pausas Activas**: Hacer pausas regulares cada 30-60 minutos para estirarse y moverse. Realizar ejercicios de estiramiento y caminar un poco para evitar el sedentarismo y mejorar la circulación. Puedes utilizar aplicaciones o recordatorios que te avisen cuando sea el momento de tomar una pausa.

4. Interacciones Sociales Saludables

- **Comunicación Respetuosa**: Fomentar interacciones positivas y respetuosas en línea, evitando discusiones y comportamientos tóxicos. Practicar la empatía y el respeto hacia los demás usuarios. Participa en comunidades en línea que promuevan un ambiente positivo y constructivo.

- **Balance Online/Offline:** Mantener un equilibrio entre las interacciones en línea y las relaciones cara a cara. Participar en actividades sociales fuera de la pantalla para fortalecer las relaciones personales. Organiza encuentros presenciales con amigos y familiares para mantener conexiones significativas

CONTRASEÑAS SEGURAS

En la era digital actual, nuestras vidas están profundamente integradas con la tecnología, lo que nos expone a una variedad de riesgos cibernéticos. Desde operaciones bancarias hasta redes sociales, cada cuenta que poseemos contiene información personal valiosa y, en algunos casos, sensible. Las contraseñas actúan como la primera línea de defensa contra accesos no autorizados, y su fortaleza es crucial para proteger nuestra identidad digital y nuestros activos en línea. Una contraseña débil o fácilmente adivinable es como una puerta abierta para los ciberdelincuentes. Para evitar cualquier problema, debemos crear una contraseña segura.

Buenas prácticas para crear contraseñas seguras:

- **Longitud adecuada:** Utiliza contraseñas de al menos 12 caracteres; cuanto más largas, más seguras serán.
- **Combinación de caracteres:** Incluye una mezcla de letras mayúsculas y minúsculas, números y símbolos especiales para aumentar la complejidad.
- **Evita información personal:** No uses datos fácilmente accesibles, como nombres, fechas de nacimiento o direcciones.
- **No reutilices contraseñas:** Cada cuenta debe tener una contraseña única para evitar que una brecha de seguridad comprometa múltiples servicios.
- **Frases de contraseña:** Considera usar frases de contraseña, combinando palabras aleatorias y símbolos, que sean fáciles de recordar, pero difíciles de adivinar.
- **Gestores de contraseñas:** Utiliza herramientas especializadas para generar y almacenar contraseñas de forma segura, facilitando la gestión de múltiples credenciales.
- **Autenticación de dos factores (2FA):** Habilita 2FA siempre que sea posible para añadir una capa adicional de seguridad.
- **Actualizaciones periódicas:** Cambia tus contraseñas regularmente y especialmente si sospechas que han sido comprometidas.

Conclusión

Implementar buenas prácticas en la creación y gestión de contraseñas es esencial para salvaguardar nuestra información personal y mantener la integridad de nuestras cuentas en línea. Al adoptar medidas como utilizar contraseñas largas y complejas, evitar la reutilización y emplear herramientas especializadas, podemos reducir significativamente el riesgo de accesos no

autorizados y protegernos contra diversas amenazas cibernéticas. Recuerda que la seguridad digital es una responsabilidad compartida; cada acción que tomamos contribuye a un entorno en línea más seguro para todos.

BÚSQUEDA DE INFORMACIÓN SEGURA Y DE CALIDAD.

En la era digital, el acceso a la información es más fácil que nunca, pero también lo es la proliferación de contenido falso o engañoso. Para garantizar que la información que consultamos y utilizamos es confiable, es fundamental seguir una serie de buenas prácticas que nos ayuden a navegar de manera segura y crítica. A continuación, se presentan los principales aspectos a considerar para una búsqueda efectiva y segura en internet.

1. Verificación de la Seguridad Web

Antes de interactuar con cualquier página web, es fundamental verificar su seguridad para evitar fraudes, robo de datos o acceso a información falsa. Para ello, sigue estas recomendaciones:

- **Comprueba el candado en la barra de direcciones:** Un candado cerrado indica que la conexión con la página es segura y encriptada, reduciendo el riesgo de interceptación de datos.
- **Asegúrate de que la URL comience con "HTTPS":** La "S" en HTTPS significa "seguro", lo que indica que la transferencia de datos está protegida contra accesos no autorizados.
- **Verifica los certificados SSL:** Al hacer clic en el candado, puedes comprobar si el sitio web tiene un certificado de seguridad válido. Los certificados SSL garantizan que el sitio web pertenece a una entidad legítima y no a un tercero malintencionado.

2. Fuentes Oficiales y Confiables

No toda la información en internet es fiable. Es fundamental priorizar fuentes oficiales y de prestigio que cuenten con rigor académico o institucional.

- **Sitios Gubernamentales**: Las páginas web de entidades gubernamentales (ej. ".gob.es") suelen ofrecer datos oficiales, estadísticas y documentos normativos actualizados.
- **Instituciones Académicas:** Universidades y centros de investigación publican estudios y artículos revisados por pares que garantizan su validez científica.
- **Organizaciones Internacionales:** Entidades como la ONU, la OMS, la UNESCO y otras instituciones reconocidas a nivel global proporcionan información basada en estudios y análisis verificables.

3. Identificación de Expertos Confiables

Para asegurarte de que la información proviene de una fuente legítima, es importante verificar la autoridad y credibilidad del autor.

- **Revisa las credenciales**: Asegúrate de que el autor tenga formación académica, experiencia en el tema y un historial de publicaciones relacionadas.
- **Evalúa su reputación:** Investiga si el experto es citado por otras fuentes de confianza y si su trabajo es reconocido dentro de su campo.
- **Consulta sus publicaciones:** Los expertos confiables suelen publicar artículos en revistas científicas, libros o plataformas de divulgación reconocidas.

4. Consulta de Múltiples Fuentes

Una buena práctica es no depender de una única fuente de información. Para asegurarte de que los datos son correctos y objetivos, sigue estos pasos:

- **Contrasta información en varias fuentes:** Si una noticia o dato aparece en múltiples sitios reconocidos, es más probable que sea cierta.
- **Busca consistencia:** Compara cómo distintos medios o investigadores abordan el mismo tema y detecta posibles discrepancias.
- **Evalúa la objetividad:** Considera si la fuente tiene un sesgo político, comercial o ideológico que pueda afectar la información.

5. Actualización de la Información

El conocimiento evoluciona constantemente, por lo que es importante asegurarse de que la información consultada es actual y sigue siendo relevante.

- **Revisa la fecha de publicación:** Verifica cuándo fue escrito o actualizado el contenido. La información desactualizada puede no reflejar la realidad actual.
- **Asegúrate de que la información siga vigente:** Algunos datos pueden volverse obsoletos con el tiempo, especialmente en temas científicos, tecnológicos o jurídicos.
- **Evalúa su relevancia temporal:** En algunos casos, información antigua puede seguir siendo válida, pero es clave analizar si se han producido cambios recientes en el tema.

6. Creación de un Directorio de Fuentes Seguras

Para facilitar futuras búsquedas, es útil mantener un registro de fuentes fiables y actualizadas.

- **Añade sitios de confianza a una lista personal de recursos en línea para tener siempre a mano información verificada.**

- **Mantén la lista actualizada:** Agrega nuevas fuentes conforme las descubras y elimina aquellas que pierdan credibilidad o dejen de estar activas.

CIBERACOSO

El ciberacoso es una forma de acoso que ocurre a través de medios digitales como redes sociales, mensajes de texto, correos electrónicos y otras plataformas en línea. Se caracteriza por el hostigamiento, la intimidación o la humillación de una persona a través de tecnologías de la información y comunicación.

Tipos de Ciberacoso

- **Insultos y humillaciones:** Comentarios ofensivos o degradantes dirigidos a una persona con la intención de dañar su autoestima o reputación.
- **Difusión de rumores:** Compartir información falsa o comprometedora sobre una persona con el propósito de dañar su imagen.
- **Exclusión de grupos:** Bloquear, aislar o excluir intencionalmente a alguien de comunidades en línea, grupos de chat o redes sociales.
- **Suplantación de identidad:** Crear perfiles falsos o robar la identidad de otra persona para realizar acciones perjudiciales en su nombre.
- **Acoso sexual en línea:** Envío de mensajes, imágenes o videos de contenido sexual sin el consentimiento de la persona afectada.
- **Ciberpersecución:** Seguimiento constante y no deseado a una persona a través de medios digitales con la intención de intimidarla o manipularla.

Impacto Psicológico del Ciberacoso

El ciberacoso puede tener graves consecuencias emocionales y psicológicas en las víctimas, afectando su bienestar y calidad de vida. Entre los principales efectos se encuentran:

- **Ansiedad y depresión:** La constante exposición a ataques y humillaciones genera altos niveles de estrés, tristeza y angustia.
- **Baja autoestima:** La víctima puede desarrollar inseguridad y una percepción negativa de sí misma debido a las críticas y el rechazo en línea.
- **Aislamiento social:** El miedo al acoso puede llevar a la víctima a evitar interacciones tanto en línea como en la vida real, afectando su desarrollo social.

- **Problemas de concentración y rendimiento académico o laboral:** El estrés causado por el ciberacoso puede interferir en la capacidad de concentración y desempeño en estudios o trabajo.
- **Pensamientos autodestructivos:** En casos graves, la víctima puede desarrollar ideas suicidas debido a la presión y la desesperación.

Factores que Contribuyen al Ciberacoso

El ciberacoso se ve favorecido por diversos factores que facilitan su ocurrencia y prolongación:

- **Anonimato en internet:** La posibilidad de ocultar la identidad hace que los agresores se sientan protegidos y actúen sin miedo a las consecuencias.
- **Falta de empatía:** La comunicación digital reduce la percepción del daño emocional que se causa a la víctima, ya que no se observan sus reacciones en tiempo real.
- **Presión de grupo:** En algunos casos, las personas participan en el ciberacoso para ganar aceptación en su círculo social o evitar ser ellas mismas el blanco de ataques.
- **Accesibilidad y permanencia de la información:** Los mensajes, imágenes o videos compartidos en línea pueden mantenerse en internet durante mucho tiempo, amplificando el daño.
- **Falta de regulación o control parental:** La ausencia de supervisión y la falta de normas claras en el uso de dispositivos digitales pueden propiciar conductas de acoso en menores y adolescentes.

Estrategias de Prevención del Ciberacoso

Para reducir el impacto del ciberacoso y prevenir su ocurrencia, es fundamental adoptar medidas educativas y de control:

- **Educación y concienciación:** Enseñar a niños, adolescentes y adultos sobre los riesgos del ciberacoso y sus consecuencias.
- **Uso responsable de la tecnología:** Promover buenas prácticas en internet, como evitar compartir información personal y respetar la privacidad de los demás.
- **Supervisión y control parental:** Establecer normas claras sobre el uso de dispositivos digitales y monitorear la actividad en línea de menores.

- **Fomentar el respeto y la empatía:** Crear conciencia sobre la importancia de tratar a los demás con respeto en cualquier entorno, incluyendo el digital.
- **Reportar y bloquear agresores:** En caso de ser víctima de ciberacoso, es recomendable bloquear al agresor y denunciar su comportamiento en la plataforma correspondiente.

Marcos Legales y Denuncia

El ciberacoso es un delito en muchos países, y existen diversas leyes para sancionarlo y proteger a las víctimas:

- **Legislación contra el ciberacoso**: Cada país cuenta con normativas específicas que penalizan el acoso digital y establecen sanciones para los agresores.
- **Canales de denuncia:** Las víctimas pueden reportar el ciberacoso a plataformas digitales, centros de ayuda especializados o autoridades policiales.
- **Protección de las víctimas:** Las leyes buscan garantizar la seguridad de las víctimas mediante medidas de restricción contra los agresores y asesoramiento legal.
- **Responsabilidad de las plataformas digitales:** Redes sociales y aplicaciones deben establecer políticas claras para prevenir y sancionar el ciberacoso.

Apoyo y Recursos para Víctimas

Las víctimas de ciberacoso deben buscar apoyo emocional y ayuda profesional para afrontar la situación de manera adecuada:

- **Apoyo emocional:** Contar con el respaldo de amigos, familiares y profesionales de la salud mental es fundamental para superar el impacto del ciberacoso.
- **Recursos en línea:** Existen líneas de ayuda, foros de apoyo y páginas web que brindan información y orientación a las víctimas.
- **Grupos de apoyo**: Compartir experiencias con otras víctimas puede ser útil para afrontar la situación y recibir consejos de personas que han pasado por lo mismo.
- **Asesoramiento legal:** En caso de que el ciberacoso sea grave, se recomienda buscar ayuda de un abogado para tomar acciones legales contra el agresor.

SOBREEXPOSICIÓN EN LA RED

La sobreexposición en la red se refiere a la divulgación excesiva de información personal en plataformas digitales, como redes sociales o blogs. Esta práctica puede incluir detalles íntimos, imágenes, opiniones o ubicaciones, lo que aumenta la vulnerabilidad de la persona. Socialmente, genera preocupaciones sobre la privacidad, la seguridad y el acoso en línea. Además, puede fomentar una cultura de comparación, estrés y ansiedad debido a la presión de mostrar una vida "ideal". La sobreexposición también puede tener consecuencias a largo plazo, como la pérdida de control sobre la información compartida.

1. Protege tu privacidad

- **Revisa y ajusta las configuraciones de privacidad:** Asegúrate de que tu información personal solo sea accesible para quienes realmente necesitas que la vean. Configura las redes sociales para que solo tus amigos o contactos aprobados puedan ver tus publicaciones.
- **Evita compartir detalles sensibles:** Datos como tu dirección, número de teléfono, número de tarjeta de crédito o ubicación exacta pueden ser utilizados para suplantar tu identidad o exponerte a riesgos.

2. Sé consciente de la información que compartes

- **Piensa antes de publicar:** Reflexiona sobre el contenido que vas a compartir y si es apropiado para que quede disponible en internet de forma pública, incluso a largo plazo.
- **Evita la sobreexposición emocional:** Publicar constantemente sobre tus sentimientos o problemas puede atraer a personas con intenciones dañinas o crear un ambiente negativo para tu bienestar emocional.

3. Cuida tus imágenes y vídeos

- **Ten cuidado con las fotos y videos personales:** Imágenes que pueden parecer inofensivas en un principio pueden ser compartidas y utilizadas sin tu consentimiento, llegando a exponerte a situaciones incómodas o peligrosas.
- **Piensa en las implicaciones de compartir imágenes:** Antes de publicar fotos de tus hijos, familiares o amigos, asegúrate de que todos estén de acuerdo y que no se comprometa la privacidad de ninguna de las personas involucradas.

4. Controla tu presencia en redes sociales

- **No compartas en exceso tu ubicación:** Evita publicar fotos o información en tiempo real que puedan revelar dónde te encuentras, especialmente si estás en lugares privados o sensibles.
- **Evita conectar con desconocidos:** Aceptar solicitudes de amistad o seguir a personas que no conoces bien puede ponerte en riesgo. Es mejor limitar tu red a personas que realmente conoces y confías.

5. Gestiona las interacciones con los demás

- **Protege tu bienestar emocional**: Si te sientes invadido por la sobreexposición o el contacto constante en redes sociales, es importante saber poner límites. Limita el tiempo en redes sociales y usa herramientas de gestión de tiempo para evitar la fatiga digital.
- **Desactiva o bloquea cuentas y personas tóxicas:** Si alguien está invadiendo tu espacio digital o causando angustia emocional, no dudes en bloquear o reportar la cuenta. Tu bienestar es lo más importante.

6. Sé responsable con el uso de datos

- **No compartas información de otras personas sin su consentimiento:** Si vas a publicar algo que involucra a otras personas, asegúrate de que están de acuerdo con ello, especialmente cuando se trata de información personal.
- **Comprende el alcance de tus publicaciones:** Lo que publicas hoy puede ser visto por miles de personas, o incluso ser compartido fuera de tu círculo de confianza. Piensa si ese contenido sería apropiado para una audiencia mucho más amplia.

7. Considera las implicaciones legales

- **Infórmate sobre las leyes de protección de datos:** Existen leyes que protegen tus derechos digitales, como el GDPR en Europa. Conocer tus derechos sobre cómo se maneja tu información personal es fundamental para proteger tu privacidad en la red.
- **Sé consciente de los derechos de autor y la propiedad intelectual:** No compartas contenido que no te pertenece sin dar los créditos apropiados o sin tener los derechos necesarios.

DOBLE FACTOR DE AUTENTICACIÓN (2FA)

1. ¿Qué es 2FA y cómo funciona?

La Autenticación de Doble Factor (2FA) es un sistema de seguridad que añade una segunda comprobación para entrar en una cuenta. Así, aunque alguien tenga tu contraseña, no podrá acceder sin el segundo paso. Los factores de autenticación pueden ser:

- **Algo que sabes:** Una contraseña o un PIN.
- **Algo que tienes: Un móvil, una tarjeta o una llave de seguridad.**
- **Algo que eres:** Huella dactilar, rostro o voz.
- **Consejo:** Usa siempre dos factores diferentes, por ejemplo, contraseña + código en tu móvil.

2. ¿Qué método de 2FA elegir?

Hay varios métodos de 2FA, pero no todos son igual de seguros:

- **Más seguros:** Aplicaciones como Google Authenticator o Authy y llaves físicas como YubiKey.
- **Menos seguros:** Códigos enviados por SMS o correo electrónico (pueden ser interceptados).
- **Otros métodos:** Huella dactilar o reconocimiento facial.
- **Consejo:** Prefiere apps de autenticación o llaves de seguridad en lugar de SMS.

3. ¿Dónde activar 2FA?

Es importante activar 2FA en todas tus cuentas importantes:

- **Correo electrónico** : Gmail, Outlook.
- **Bancos y apps de pago**: PayPal, Bizum.
- **Redes sociales:** Instagram, TikTok, Facebook.
- **Almacenamiento en la nube:** Google Drive, Dropbox.
- **Cuentas del trabajo o la escuela**
- **Consejo:** Activa 2FA en todas tus cuentas importantes.

4. ¿Cómo saber si 2FA funciona bien?

Cada cierto tiempo, revisa que todo esté funcionando correctamente:

- Prueba que tu aplicación de autenticación genera códigos.

- Intenta iniciar sesión en otra computadora para ver si 2FA funciona.
- Asegúrate de no perder acceso a tu método de autenticación.
- **Consejo:** Haz pruebas cada pocos meses para evitar problemas.

5. ¿Cómo recuperar una cuenta con 2FA?

Si pierdes el acceso a 2FA, puedes recuperarlo con:

- Códigos de respaldo (te los dan cuando activas 2FA).
- Correo de recuperación.
- Contactando al soporte de la plataforma.
- **Consejo:** Guarda los códigos de respaldo en un lugar seguro (pero no en tu móvil).

6. ¿Cómo proteger los dispositivos que usas con 2FA?

Si alguien accede a tu móvil u ordenador, podría robarte los códigos de 2FA. Para evitarlo:

- Usa contraseñas seguras y bloqueo de pantalla.
- No compartas tu dispositivo con otras personas.
- Activa el cifrado del móvil para proteger tus datos.
- **Consejo:** Protege bien tu móvil, ya que muchas cuentas dependen de él.

7. Evita caer en engaños y ataques

Los ciberdelincuentes intentarán robarte tus códigos de 2FA con trampas como:

- **Phishing**: mensajes falsos que piden tu código.
- Páginas falsas que parecen reales.
- Personas que te piden códigos por WhatsApp o redes sociales.
- **Consejo:** Nunca compartas tus códigos de 2FA con nadie.

8. Mantén seguras tus cuentas y dispositivos

Para mejorar tu seguridad:

- Mantén actualizados tus programas y apps.
- Revisa las configuraciones de seguridad de tus cuentas.
- Desactiva dispositivos que ya no uses.
- **Consejo:** Configura bien cada cuenta para evitar riesgos.

9. No uses métodos inseguros

Algunos métodos de 2FA pueden ser hackeados fácilmente:

- Los códigos por SMS pueden ser robados con ataques llamados SIM swapping.
- Es mejor usar aplicaciones de autenticación o llaves de seguridad físicas.
- **Consejo:** Evita los SMS y usa apps de autenticación siempre que sea
- posible.

CONEXIONES SEGURAS:

1. Reglas básicas para navegar seguro

- **Usa páginas web seguras (HTTPS)**
  - Asegúrate de que las páginas que visitas empiezan por **https://**. Esa "s" significa que tu conexión está cifrada y es más difícil que alguien la intercepte.
  - Evita entrar en páginas que no muestren el candado en la barra de direcciones.

- **Protege tus datos con contraseñas seguras**
  - - Usa contraseñas largas, mezclando letras, números y símbolos. Ej.: **Gato3Azul!7**
  - No repitas la misma contraseña en diferentes sitios.
  - Activa la **verificación en dos pasos** (MFA) siempre que puedas. Es como una doble cerradura.

- **Conéctate con seguridad, especialmente en redes públicas**:
  - Si usas Wi-Fi en cafeterías o aeropuertos, activa una **VPN (Red Privada Virtual)** para cifrar tu conexión.
  - En casa, usa **WPA3** para tu red Wi-Fi y evita dejar la contraseña por defecto.

- **Mantén tu dispositivo actualizado**
  - Actualizar tu móvil o portátil no solo te da nuevas funciones, también corrige errores que los hackers pueden aprovechar.

- **Ojo con los correos sospechosos**
  - Si recibes un correo que te pide datos o tiene enlaces raros, **¡no hagas clic!**. Puede ser **phishing** (intento de engaño para robarte información).

2. ¿Cómo saber si te han hackeado?

- El dispositivo va más lento sin razón.
- Aparecen apps que no recuerdas haber instalado.
- Tus amigos te dicen que les envías mensajes extraños.
- Si te pasa algo de esto, avisa a un adulto o experto en informática.

3. Protégete también en las redes sociales

- No compartas información personal como tu dirección, teléfono o contraseñas.
- Revisa quién puede ver lo que publicas (configura la privacidad).
- Acepta solo solicitudes de amistad de personas que conozcas.

IDENTIDAD DIGITAL:

1. Reglas básicas para navegar seguro

En la actualidad, la identidad digital es un aspecto esencial de nuestra vida personal y profesional. Nuestra identidad digital está conformada por diversos factores, incluyendo la información que publicamos y compartimos, lo que otros dicen de nosotros y la información que existe en internet sobre nuestra persona.

A continuación se muestran unas recomendaciones fundamentales para gestionar de manera adecuada nuestra identidad digital.

- **Ejercer la ciudadanía digital de forma responsable y activa:** Se nos anima a ser ciudadanos digitales comprometidos, lo que implica no solo participar activamente en las plataformas en línea, sino también denunciar actividades ilícitas o inadecuadas cuando sea necesario. Contribuir a una comunidad digital segura es una responsabilidad compartida.

- **Aportar contenidos de calidad:** Publicar información útil, veraz y relevante fortalece nuestra reputación en línea. Evitar la difusión de noticias falsas o contenido dañino ayuda a mantener un entorno digital confiable y positivo.

- **Respetar los derechos de autor y las licencias de uso:** Antes de compartir contenido ajeno, es fundamental verificar si está protegido por derechos de autor. Utilizar imágenes, textos y recursos con licencias adecuadas demuestra respeto por el trabajo de los demás y evita problemas legales.

- **Seleccionar cuidadosamente los avatares e imágenes asociados al perfil:** Las imágenes que elegimos para representarnos en internet influyen en la percepción que los demás tienen de nosotros. Es importante seleccionar fotografías y avatares adecuados, evitando aquellos que puedan ser inapropiados o comprometer nuestra privacidad.

- **Utilizar nombres de usuario o de registro adecuados:** El nombre de usuario que elegimos en plataformas digitales debe reflejar una identidad

profesional y respetuosa. Evitar nombres ofensivos o demasiado informales es clave para proyectar una imagen confiable.

- **Seleccionar con cuidado las amistades en redes sociales:** No todas las solicitudes de amistad o conexión en redes sociales deben ser aceptadas sin un análisis previo. Es recomendable añadir solo a personas conocidas o que aporten valor a nuestra red, evitando así posibles riesgos de seguridad.

- **Conocer y gestionar la privacidad en las redes donde se participa:** Cada plataforma tiene configuraciones de privacidad distintas. Es importante revisar y ajustar estos parámetros para controlar quién puede ver nuestra información y con quién compartimos nuestros datos personales.

- **Participar de forma respetuosa y expresarse con educación:** La convivencia digital debe basarse en el respeto. Al interactuar en línea, es fundamental utilizar un lenguaje adecuado, evitando insultos, comentarios ofensivos o actitudes agresivas.

- **Pensar antes de subir cualquier cosa a internet:** Una vez que se publica algo en internet, puede ser difícil eliminarlo por completo. Antes de compartir información, imágenes o comentarios, es importante reflexionar sobre sus posibles consecuencias.

- **Practicar el egosurfing periódicamente:** Realizar búsquedas de nuestro nombre en internet nos permite conocer qué información existe sobre nosotros. Esto facilita la gestión de nuestra identidad digital y nos ayuda a eliminar o modificar contenido que pueda afectar nuestra reputación.

> Además de estos puntos clave, es importante resaltar a la identidad digital como un elemento que influye en nuestras interacciones y deja una huella permanente en la red. Ser conscientes de cómo nos presentamos en el entorno digital nos permite tomar decisiones informadas y proteger nuestra privacidad.

RECUERDA:

La ciberseguridad no es solo cosa de expertos. Tú puedes protegerte siguiendo estos consejos. Internet es un lugar increíble, pero hay que usarlo con precaución.

¡Navega seguro!