Bloque I. La seguridad cibernética es un tema crucial en la cultura digital actual. Guía básica sobre seguridad cibernética:

1. Concienciación y Educación

- **Educación básica en seguridad cibernética:** Entender los conceptos básicos como contraseñas seguras, phishing, malware, etc.
- **Concienciación:** Promover una cultura de seguridad entre empleados, familiares y amigos.

2. Uso de Contraseñas Seguras

- **Longitud y complejidad:** Utilizar contraseñas largas, combinando letras, números y caracteres especiales.
- **Autenticación de dos factores (2FA):** Activar siempre que sea posible para una capa adicional de seguridad.

3. Actualizaciones y Parches

- **Software actualizado:** Mantener el sistema operativo, aplicaciones y software de seguridad actualizados para protegerse contra vulnerabilidades conocidas.

4. Protección contra Malware y Virus

- **Software antivirus/antimalware:** Instalar y mantener actualizado un programa de protección contra virus y malware.
- **Descargas seguras:** Evitar descargar archivos de fuentes no confiables o desconocidas.

5. Navegación Segura

- **Navegador seguro:** Utilizar navegadores web actualizados y configurar la privacidad y seguridad según sea necesario.
- **Sitios web seguros:** Verificar que los sitios web utilizan conexiones seguras (HTTPS).

6. Seguridad en Dispositivos Móviles

- **Seguridad móvil:** Utilizar bloqueo de pantalla, cifrado de datos y software de seguridad en dispositivos móviles.
- **Aplicaciones seguras:** Descargar aplicaciones solo de fuentes confiables y revisar los permisos que solicitan.

7. Redes Wi-Fi Seguras

- **Redes Wi-Fi públicas:** Evitar realizar transacciones financieras o compartir información sensible en redes Wi-Fi públicas no seguras.
- **Uso de VPN:** Considerar el uso de una red privada virtual (VPN) para cifrar la conexión en redes Wi-Fi públicas.

8. Copias de Seguridad

- **Respaldo regular:** Mantener copias de seguridad de datos importantes en dispositivos externos o en la nube.

9. Privacidad de Datos

- **Configuración de privacidad:** Revisar y ajustar la configuración de privacidad en redes sociales y otros servicios en línea.
- **Mínima divulgación:** Limitar la cantidad de información personal que se comparte en línea.

10. Gestión de Incidentes

- **Plan de respuesta:** Desarrollar y practicar un plan de respuesta ante incidentes de seguridad cibernética.
- **Reporte de incidentes:** Saber a quién reportar incidentes de seguridad, tanto en el ámbito personal como profesional.

Bloque II. la ética digital y la comunicación en línea son aspectos fundamentales en la cultura digital contemporánea. Guía básica sobre ética digital y comunicación en línea:

Ética Digital

1. Respeto y Responsabilidad

- **Trato respetuoso:** Tratar a los demás en línea con el mismo respeto que se esperaría cara a cara.
- **Responsabilidad por acciones:** Ser consciente de las consecuencias de tus acciones en línea, tanto en el ámbito personal como profesional.
- **Protección de datos:** Respetar la privacidad y proteger los datos personales de otros.

2. Honestidad y Transparencia

- **Veracidad de la información:** Verificar la exactitud de la información antes de compartirla.
- **Transparencia en comunicaciones:** Ser claro y transparente sobre la identidad y propósito al comunicarse en línea.

3. Educación y Concienciación

- **Alfabetización digital:** Promover la educación y concienciación sobre el uso responsable de la tecnología y la información en línea.
- **Capacitación en ética digital:** Proporcionar formación y recursos para entender y aplicar principios éticos en entornos digitales.

4. Derechos y Libertades

- **Derechos digitales:** Defender los derechos fundamentales en el entorno digital, como la libertad de expresión y el acceso a la información.
- **Lucha contra la discriminación:** Evitar comportamientos discriminatorios y respetar la diversidad en línea.

Comunicación en Línea

1. Claridad y Precisión

- **Comunicación clara:** Expresar ideas de manera clara y comprensible, evitando ambigüedades.
- **Verificación de información:** Confirmar la exactitud de la información antes de compartirla o citarla.

2. Cortesía y Respeto

- **Tono respetuoso:** Mantener un tono cortés y respetuoso en las interacciones en línea, incluso en situaciones de desacuerdo.

- **Empatía:** Intentar comprender las perspectivas de los demás y responder de manera empática.

3. Seguridad y Privacidad

- **Protección de la privacidad:** Respetar la privacidad de la información personal y utilizar medidas de seguridad adecuadas al comunicarse en línea.
- **Seguridad de la información:** Evitar compartir información confidencial en canales no seguros.

4. Gestión de Conflictos

- **Resolución pacífica:** Resolver conflictos de manera constructiva y pacífica, evitando confrontaciones públicas o ataques personales.
- **Mediación y negociación:** Utilizar herramientas de mediación y negociación para llegar a acuerdos en disputas en línea.

Prácticas Éticas y Seguras

- **Autoevaluación:** Reflexionar periódicamente sobre tus prácticas en línea y ajustarlas según los principios éticos.
- **Liderazgo ético:** Promover y ejercer un liderazgo ético en entornos digitales, inspirando a otros a seguir prácticas similares.

Bloque II. Guía básica sobre el uso de redes sociales dentro del contexto de la cultura digital:

Uso Responsable de Redes Sociales

1. Privacidad y Configuración de Perfiles

- **Configuración de privacidad:** Revisar y ajustar la configuración de privacidad para controlar quién puede ver tus publicaciones, información personal y fotos.
- **Información sensible:** Evitar compartir información sensible como números de teléfono, dirección exacta o detalles financieros públicamente.

2. Gestión de la Identidad Digital

- **Imagen pública:** Ser consciente de que lo que compartes en redes sociales forma parte de tu identidad digital y puede influir en cómo te perciben los demás.
- **Reputación en línea:** Mantener una imagen positiva cuidando el contenido que publicas y cómo interactúas con otros.

3. Interacciones y Comportamiento

- **Respeto y cortesía:** Mantener un tono respetuoso en las interacciones con otros usuarios, incluso en debates o discusiones.
- **Verificación de información:** Evitar difundir información no verificada o falsa que pueda causar confusión o daño.

4. Administración del Tiempo

- **Uso consciente:** Controlar el tiempo dedicado a las redes sociales para evitar distracciones excesivas y mantener un equilibrio con otras actividades.
- **Bienestar digital:** Estar atento a cómo el uso de redes sociales afecta tu bienestar emocional y mental.

5. Seguridad y Protección

- **Contraseñas seguras:** Utilizar contraseñas robustas y cambiarlas regularmente para proteger tu cuenta.
- **Phishing y fraudes:** Estar alerta ante posibles intentos de phishing u otros fraudes que podrían comprometer tu seguridad.

6. Educación y Alfabetización Digital

- **Capacitación:** Mantenerse informado sobre las últimas prácticas de seguridad y ética en redes sociales.
- **Educación continua:** Participar en programas de alfabetización digital para aprender a utilizar las redes sociales de manera segura y efectiva.

7. Conciencia sobre el Impacto Social

- **Responsabilidad social:** Considerar el impacto social y ético de tus acciones en redes sociales, como el efecto de compartir noticias falsas o participar en bullying en línea.
- **Activismo digital:** Utilizar las redes sociales para promover causas sociales y participar en debates constructivos.

Recomendaciones Finales

- **Actualización:** Mantener las aplicaciones de redes sociales actualizadas para beneficiarse de las últimas características de seguridad y privacidad.
- **Revisión periódica:** Revisar periódicamente tus perfiles y ajustar la configuración de privacidad según sea necesario.