

Guía de la COP28 Sobre la Legislación de los Emiratos Árabes Unidos y la Seguridad Integral en la COP

Seguridad para los activistas que asisten a la COP 28

Esta Guía está diseñada para los activistas y defensores del clima que asistan a la COP28 en los Emiratos Árabes Unidos (EAU), y proporciona información básica sobre el marco jurídico y los recursos disponibles para navegar por el panorama jurídico local en los EAU; y una visión general de las cuestiones de seguridad de la información/digital, con sugerencias sobre cómo proteger su información y permanecer seguro antes, durante y después de la COP.

Esperamos que esta guía permita a los activistas, defensores y otros asistentes a la COP28 tomar decisiones informadas sobre sus acciones durante su estancia en los EAU.



Lista de Control Para los Asistentes a la COP 28

Antes de partir hacia los EAU, consulte esta lista de control de seis puntos para tomar decisiones informadas y mantenerse seguro durante su estancia en Dubai.

- Elabore y prepárese para aplicar un plan de comunicación segura durante su estancia en los EAU (que puede incluir la descarga de Signal si aún no dispone de ella).
- Establece una red de seguridad personal que permita a los demás encontrarte y localizar a otros activistas. Verifica los números de seguridad en Signal de los miembros de tu red de seguridad personal antes de ir a los EAU.
- Asegúrate un compañero o “amigo” con el que viajar, idealmente en todo momento, dentro de los EAU, pero especialmente hacia, desde y fuera de la Zona Azul de la conferencia. Este compañero puede ayudarle a evitar problemas y también a solucionarlos en caso de que surjan. Verifique el número de seguridad de Signal de su compañero antes de viajar a los EAU.
- Elabore y lleve consigo una lista de recursos críticos:
 - Información de contacto de la embajada/servicios consulares de tu país en los EAU
 - Números de teléfono de los contactos de tu red de seguridad
 - Línea directa de protección jurídica para asesoramiento jurídico urgente:
Señal o mensajes de WhatsApp +41 767 635 765
(Abierta entre el 28 de noviembre y el 14 de diciembre)
 - Correo electrónico: cop@climatelegaldefense.org
(Email open November 28 - December 14)
 - Correo electrónico del Centro de seguridad: safetyhub@proton.me
(Fully operational November 23-December 19)
- Revise sus declaraciones publicadas en línea o en las redes sociales; las que sean críticas con los EAU, así como con otros Estados, pueden violar las leyes de los EAU que restringen la expresión.
- Revise las medidas y configuraciones de seguridad digital en la [página 14](#).

Para saber más sobre la iniciativa de protección jurídica de CliDef, visite:

www.climatelegaldefense.org/COP28

La línea directa de protección jurídica de CliDef estará disponible entre el 28 de noviembre y el 14 de diciembre a través de la línea gratuita Signal o WhatsApp text (las llamadas telefónicas pueden estar bloqueadas) en el +41 767 635 765, y por correo electrónico en cop@climatelegaldefense.org.

La línea directa del Centro de Seguridad estará disponible una semana antes y una semana después de la COP 28 (del 23 de noviembre al 19 de diciembre) en el +49 177 684 4896, y por correo electrónico en safetyhub@proton.me.

Contenido de esta Guía

PRIMERA PARTE: Conozca la Ley

I. Breve resumen de las leyes importantes de los EAU y consideraciones relacionadas

1. Controles, registros personales y detenciones
2. Libertad de expresión
3. Libertad de prensa
4. Detención preventiva
5. Protestas públicas
6. Seguridad nacional
7. Libertad de circulación
8. Derecho a un abogado y a protección consular
9. Recaudación de fondos y actividades conexas

II. Cómo cumplir la ley y mantenerse a salvo

III. Preguntas más frecuentes

1. Cuestiones relativas a la entrada y salida de los EAU
2. Cuestiones relacionadas con protestas, reuniones y manifestaciones públicas
3. Sus derechos en caso de registro y detención
4. Tus derechos en relación con casos LGBTQ

SEGUNDA PARTE: Información y seguridad digital

I. Comprender los riesgos de seguridad “de referencia”

II. Antes de viajar

Paso 1: Sentar las bases de la seguridad de la información

Paso 2: Tome medidas de seguridad de la información con respecto a sus datos

Paso 3: Asegúrese de que su documentación personal está en regla

Paso 4: Considere la posibilidad de contratar un seguro de viaje

Paso 5: Embalaje y ropa seguros

Paso 6: Establezca su red de apoyo

Paso 7: Prepárese para hacer frente a preguntas basadas en la identidad y abordar las sensibilidades culturales

III. A su llegada

Conozca la Ley

La legislación de los EAU relativa al tipo de cuestiones que podrían preocupar a los asistentes a la COP -búsquedas, arrestos y detenciones, libertad de expresión, identidad personal y seguridad- se complica por el hecho de que algunas de las leyes están publicadas y otras no. Además, algunas de las leyes más relevantes, como la Ley de Seguridad del Estado (que se ocupa de los delitos y el terrorismo) y el Código Penal, contienen lenguaje que a menudo es interpretado de forma amplia por las autoridades.

Es importante saber que **la legislación de EAU está plenamente vigente en todo el país, excepto en la Zona Azul, regulada por la ONU**. En otras palabras, la Zona Verde (“el eje central de la acción... abierto al público, al sector privado, a los medios de comunicación, a los jóvenes, a las ONG, así como a los delegados e invitados de la Zona Azul gestionada por la CMNUCC”) se rige por la legislación de EAU. Por lo tanto, **cualquier actividad que los participantes lleven a cabo fuera de la Zona Azul, incluida la Zona Verde, estará sujeta a las restricciones y consideraciones descritas en esta Guía**.

Aunque los activistas y defensores de la CP dispondrán de asesoramiento jurídico a través de la Línea Directa de Protección Jurídica, el apoyo jurídico local sobre el terreno para los activistas es extremadamente limitado. Debido a que los visitantes de los EAU están sujetos a sus leyes, esta Guía pretende explicar el contexto legal, que esperamos permita a los participantes de la COP tomar decisiones informadas sobre las acciones que toman y cómo van a participar durante su estancia en los EAU.

I. Breve resumen de las leyes importantes de los EAU y consideraciones relacionadas

1. Controles, registros personales y detenciones

En circunstancias normales, un agente de policía típico en los EAU tiene estrictamente prohibido registrar o detener a una persona sin permiso judicial previo. Sin embargo, los miembros del Aparato de Seguridad del Estado (SSA) tienen poderes únicos que los agentes de policía normales no tienen en virtud de la Ley del Servicio de Seguridad del Estado. Esta ley permite a los agentes del SSA detener y registrar a personas y sus domicilios y detenerlas durante largos periodos de tiempo.

En concreto, los agentes del SSA (incluido el jefe del SSA) tienen autoridad para

- Registrar y detener a personas sin autorización judicial para ello.
- Autorizar la detención de un sospechoso más allá de unos días; si interviene el jefe de la SSA, puede ordenar la detención hasta 3 meses antes de obtener una orden judicial.
- Ordenar la expulsión de un sospechoso extranjero.
- Investigar casos relacionados con cualquier actividad de una persona, organización, partido o asociación que pretenda perjudicar la seguridad y protección del Estado de los EAU; se trata de un mandato amplio y la SSA lo interpreta en sentido amplio.

¿Qué significa esto para los participantes en la COP?

- **Antes de partir:** Lee la Ley de Servicios de Seguridad del Estado, disponible en <https://en.edacrights.com/post/108>, antes de salir de casa, para que conozcas tus derechos si te paran.
- **Antes de salir:** Protege los datos de tus dispositivos en la medida de lo posible adoptando las medidas para datos en reposo y datos en uso de la [Parte II, Paso 2](#) de esta Guía.
- **Mientras estés en la COP (o en los EAU, incluido el aeropuerto):**
 - ▶ **Si te paran**, intenta averiguar si es un agente de policía normal o un miembro de la SSA quien te ha parado.
 - Los policías ordinarios suelen llevar uniformes grises, verdes o caquis.
 - Los agentes de la SSA llevan uniformes completamente negros y máscaras negras que les cubren la cara, pero también pueden vestir de paisano.
 - ▶ **Si no está seguro de quién le ha parado, o si le para alguien vestido de paisano**, pida respetuosamente que verifiquen su identidad. Esta es una práctica común, y puede ayudarle a confirmar si la persona que se le acerca es realmente un agente legítimo de la ley.
 - ▶ Sepa que siempre puede solicitar un intérprete.
 - ▶ **Si te para un agente de policía normal**, puedes hacer valer respetuosamente tu derecho a no ser registrado ni detenido sin una orden judicial. Sin embargo, considera si es posible acceder fácilmente al registro, ya que las consecuencias de la negativa pueden agravar el encuentro. Si te detienen, debes llamar inmediatamente a tu embajada o servicios consulares

si puedes, y también enviar un mensaje de texto a la línea directa de protección jurídica y a tu red de seguridad para informarles de lo ocurrido.

- ▶ **Si un miembro de la SSA te da el alto o te detiene**, debes llamar inmediatamente a tu embajada o a tus servicios consulares para pedir ayuda, si puedes, y también enviar un mensaje de texto a la Línea Directa de Protección Jurídica y a tu red de seguridad para informarles de lo ocurrido. Al notificar rápidamente a otros tu situación, creas un registro de lo que ha sucedido, lo que permite la intervención legal (en caso necesario).

2. Restricciones a la libertad de expresión e información

Las leyes de los EAU contienen amplias restricciones a la libertad de expresión y tipifican como delito que alguien:

- Criticar al gobierno de los EAU, sus instituciones o dirigentes;
- Criticar a otros Estados;
- Publicar “noticias falsas” que perturben la seguridad pública o inciten a la opinión pública;
- Publicar cualquiera de los anteriores en línea (en cuyo caso se convierte en un delito cibernético).

Los EAU también cuentan con un cortafuegos nacional que bloquea los sitios web prohibidos, limitando el acceso a la información contenida en ellos. Utilizar una VPN para acceder a estos sitios es ilegal y no siempre crea una conexión continuamente segura.

¿Qué significa esto para los participantes en la COP?

- **Antes de ir:** piense si ha publicado declaraciones en línea o en las redes sociales que sean críticas con los EAU, así como

con otros Estados, ya que pueden violar las restricciones de los EAU a la libertad de expresión y/o pueden constituir un delito cibernético si esas declaraciones se relacionan con usted después de entrar en los EAU.

- **Mientras esté allí:**

- ▶ Antes de utilizar una VPN para eludir la censura local, pregúntese si vale la pena correr el riesgo de acceder al contenido inmediatamente. Las pruebas del contenido al que ha accedido pueden permanecer en su dispositivo y estar a disposición de las autoridades si acceden al mismo. No utilizar una VPN puede exponer los datos comunicados, pero el cortafuegos debería impedirle acceder a contenidos ilícitos.
- ▶ El uso de una VPN no garantiza una conexión continuamente segura. Si ignora las advertencias de seguridad al conectarse, es posible que no establezca una conexión segura con su proveedor de VPN en primer lugar. Su conexión a un proveedor de VPN puede caerse debido a errores o interferencias y su dispositivo puede ignorar esto y continuar enviando y recibiendo datos sin la VPN. Por último, es posible que no haya configurado la VPN para garantizar que todo el tráfico se envía a través de la conexión, dejando expuestos algunos datos muy sensibles, como una lista de todos los sitios a los que accede.
- ▶ Si utiliza una VPN para acceder a contenidos web prohibidos (y sabrá si están prohibidos si intenta acceder a ellos sin la VPN y choca con un cortafuegos), puede ser perseguido penalmente por infringir la legislación de los EAU.
- ▶ Piensa en cómo podrás comunicarte en privado durante la COP. Se recomienda utilizar Signal text, con WhatsApp como

segunda mejor opción. (Asegúrate de verificar el número de seguridad de tus contactos en Signal antes de ir al COP). Las videollamadas y las llamadas de voz en Signal pueden estar bloqueadas. Las llamadas de voz normales y los mensajes de texto SMS se interceptarán de forma rutinaria y se conservarán durante meses o años. Telegram no es recomendable, ya que tiene su sede en los EAU y es probable que esté vigilado.

- ▶ Tenga en cuenta que si hace comentarios que violen las restricciones descritas anteriormente, ya sea de forma oral y en público donde sea escuchado por funcionarios de los EAU, o en línea o a través de las redes sociales, podría ser arrestado, detenido y procesado.

3. Restricciones a la libertad de prensa

Según la [estrategia de los medios de los EAU publicada en el sitio web de su gobierno](#), los medios deben operar con moderación y cumplir con lo siguiente:

- No criticar ni insultar al presidente o a los gobernantes de los EAU, al sistema de gobierno de los EAU, al jefe de otro Estado árabe o islámico, ni a ningún otro Estado.
- No publicar nada que atente contra la unidad nacional, la cohesión social y la moneda nacional.
- No publicar nada que incite o insulte al Islam o a otras creencias religiosas o que avive luchas sectarias o tribales.
- No difundir rumores ni noticias malintencionadas, engañosas o falsas.
- Respetar el patrimonio cultural de los EAU.
- No publicar información que ofenda a los niños, las mujeres y otros grupos sociales, o viole la inviolabilidad de la moral pública o la privacidad.

- No publicar noticias, fotos o comentarios relacionados con la vida privada o familiar de las personas.
- No cuestionar la labor de un funcionario público o de una persona con capacidad de acusación pública.

¿Qué significa esto para los participantes en la COP?

- Los periodistas de fuera de los EAU que cubran la COP deben familiarizarse con el contenido prohibido en los medios de comunicación y ser conscientes de que la violación de estas prohibiciones puede dar lugar a arrestos y detenciones.
- Tenga cuidado al publicar contenidos. Las leyes de los Emiratos Árabes Unidos dan a las autoridades amplia discreción para censurar o prohibir el contenido que cae dentro de las prohibiciones de formulación amplia.
- Averigüe si se le considera un medio de comunicación a efectos de “noticias falsas”. La ley de los EAU penaliza a cualquiera que difunda, publique, reedite, circule o recircule noticias o declaraciones falsas... o que publique contenidos que se desvíen o violen “lo que se ha anunciado oficialmente”. También es ilegal “difundir cualquier propaganda sensacionalista que pueda incitar o provocar a la opinión pública, perturbar la seguridad pública, sembrar el terror entre la población o perjudicar el interés público, la economía nacional, el orden público o la salud pública.”

4. Detención preventiva

Si una persona es detenida y acusada de violar uno de los delitos o restricciones descritos en la lista no exhaustiva anterior, la Fiscalía puede ordenar que esa persona permanezca detenida durante un máximo de 21 días, tras los cuales el fiscal debe obtener una orden judicial si desea prorrogar la detención. La legislación de los EAU no establece un límite máximo para el periodo

de detención preventiva, ya que el tribunal puede renovar la detención del acusado cada 30 días.

¿Qué significa esto para los participantes en la COP?

- Sepa que siempre puede solicitar un intérprete.
- No firme ningún documento que no pueda leer y entender.
- Si te detienen, debes pedir que confirmen la identidad de la persona que te detiene y acudir inmediatamente a tu embajada o servicios consulares, a la Línea de Protección Jurídica y a tu red de seguridad.

5. Protestas públicas

La legislación de los EAU restringe la protesta pública de las siguientes maneras:

- Es ilegal protestar sin permiso, y rara vez se conceden permisos.
- No se pueden llevar a una protesta armas, fuegos artificiales ni nada que pueda dañar a personas, edificios o propiedades.
- Los manifestantes no pueden obstruir el tráfico rodado ni impedir que otros realicen su trabajo al protestar (ya que esto atenta contra la seguridad pública).
- Los participantes u organizadores de una concentración de cinco o más personas que perturbe la seguridad pública pueden ser castigados con penas de prisión.
- Quien utilice medios digitales para planear u organizar una protesta sin permiso de “la autoridad competente” se expone a penas de prisión y multas.

¿Qué significa esto para los participantes en la COP que participen en protestas públicas?

- La Zona Azul se rige por la ONU. La Zona Verde se rige por la legislación de los EAU. Esto significa que SI participas en una

protesta, importa DÓNDE sea esa protesta.

- Considere seriamente **no participar** en una manifestación o protesta pública fuera de la Zona Azul de la conferencia, ya que estará sujeto a la legislación de los EAU..
- Si participa en una protesta incluso dentro de la Zona Azul, actúe con cuidado y discreción.
- Si decide participar en una protesta fuera de la Zona Azul de la conferencia -lo cual no se recomienda-, asegúrese de no obstruir el acceso ni formar un piquete frente a un edificio gubernamental.

6. Seguridad nacional

La ley de los EAU define ampliamente el delito de terrorismo como cualquier acto que aterrorice o mate a personas, cause daños corporales graves o daños a la propiedad, y perturbe la seguridad del Estado. El terrorismo también incluye la posesión de materiales que contradigan o critiquen los principios en los que se basa la religión islámica o sus enseñanzas, o cualquier acción que amenace la estabilidad, la unidad o la soberanía del Estado. Cualquiera que declare públicamente su hostilidad al Estado o a su régimen o su deslealtad a sus dirigentes corre el riesgo de ser encarcelado.

¿Qué significa esto para los participantes en la COP?

- Infórmese sobre la definición ampliada de organizaciones terroristas en los EAU y considere las graves consecuencias si se descubre que protesta contra el gobierno de los EAU durante su estancia en el país. La ley define las “organizaciones terroristas” como grupos de dos o más personas que trabajan para causar un “resultado terrorista directo o indirecto” y prevé penas severas para cualquiera que establezca, financie, organice, gestione o dirija una organización terrorista. Con estas definiciones, los grupos políticos o las organizaciones de derechos humanos que

protestan contra el gobierno pueden correr el riesgo de ser procesados como terroristas.

7. Libertad de circulación

Aunque la Constitución de los EAU garantiza a los ciudadanos emiratíes la libertad de circulación y residencia dentro de los límites de la ley, también permite a los Servicios de Seguridad impedir a cualquier persona entrar o salir del país.

¿Qué significa esto para los participantes en la COP?

- **Si le dan el alto**, intente averiguar si es un agente de policía normal o un miembro de los SSA quien le ha parado.
 - ▶ Los agentes de policía ordinarios suelen llevar uniformes grises, verdes o caquis.
 - ▶ Los agentes de la SSA llevan uniformes completamente negros y máscaras negras que les cubren la cara, pero también pueden vestir de paisano.
- **Si no está seguro de quién le ha parado, o si le para alguien vestido de paisano**, pida respetuosamente que verifiquen su identidad. Esta es una práctica habitual y puede ayudarle a confirmar si la persona que se le acerca es realmente un agente legítimo de las fuerzas del orden.
- **Si te para un agente de policía normal**, puedes hacer valer respetuosamente tu derecho a no ser registrado ni detenido sin una orden judicial. Si te detienen, debes llamar inmediatamente a tu embajada o servicios consulares si puedes, y también enviar un mensaje de texto a la línea directa de protección jurídica y a tu red de seguridad para informarles de lo ocurrido.
- **Si un miembro de la SSA te da el alto o te detiene**, debes llamar inmediatamente a tu embajada o a tus servicios consulares para pedir ayuda, si puedes, y también enviar

un mensaje de texto a la Línea Directa de Protección Jurídica y a tu red de seguridad para informarles de lo ocurrido. Al notificar rápidamente tu situación a otras personas, creas un registro de lo que ha ocurrido, lo que permite la intervención legal (en caso necesario).

8. Derecho a un abogado y a protección consular

Según la legislación de los EAU, una persona acusada de un delito grave puede pedir al tribunal que le asigne un abogado que le defienda si no puede pagar. Sin embargo, este acceso a un abogado sólo está disponible durante un juicio, y no permite la designación de un abogado para delitos menos graves. La ley de EAU también establece que los detenidos extranjeros tienen derecho a comunicarse con sus autoridades consulares tras obtener el permiso del fiscal competente.

¿Qué significa esto para los participantes en la COP?

- Sepa que siempre puede solicitar un intérprete.
- Si le detiene alguna autoridad de los EAU, pida respetuosamente hablar con su embajada o servicios consulares y siga preguntando si no le permiten hacerlo de inmediato. Durante la COP, también debe enviar un mensaje de texto a la línea directa de protección jurídica y a su red de seguridad para informarles de su situación.
- No firme ningún documento que no pueda leer y comprender.

9. Recaudación de fondos y actividades relacionadas

Según la legislación de los EAU, las actividades de recaudación de fondos sólo pueden ser

llevadas a cabo por organizaciones benéficas, ONG o entidades gubernamentales que tengan licencia y/o autorización del gobierno de los EAU para hacerlo, y los particulares tienen prohibido por ley recaudar fondos. Además, cualquier organización sin ánimo de lucro que pretenda recaudar fondos en los EAU debe hacerlo a través de una entidad autorizada de los EAU y debe seguir una serie de pasos. Quienes infrinjan estas restricciones pueden ser castigados con penas de prisión o fuertes multas.

¿Qué significa esto para los participantes en la COP?

- Hay que tener en cuenta que la legislación de los EAU está vigente en todas partes fuera de la Zona Azul. Dentro de la Zona Azul, las actividades están reguladas por la ONU.
- Comprenda que la legislación de los EAU limita estrictamente las actividades legales de recaudación de fondos, y lo que se califica como tal puede ser interpretado de manera amplia por las autoridades de los EAU. Se recomienda llevar a cabo actividades que puedan interpretarse como recaudación de fondos -debates sobre propuestas y subvenciones, organización de donantes, recaudación de fondos- únicamente dentro de la Zona Azul, ya que esta área está regulada por la ONU.
- Si lleva a cabo actividades que podrían considerarse recaudación de fondos, dentro de una definición amplia, dentro de la Zona Azul, se recomienda que lo haga en privado y con cuidado y atención a su entorno.
- Tenga en cuenta que las actividades digitales de recaudación de fondos, si se llevan a cabo en los EAU, someten a la persona u organización que las realiza a la legislación de los EAU. Por ejemplo, un participante en la COP que tuitee sobre recaudación de fondos mientras está en la COP se expone

a ser sancionado por la legislación de los EAU. Incluso los esfuerzos de recaudación de fondos destinados a obtener apoyo para actividades fuera de los EAU, si se realizan a través de medios digitales, están regulados por la legislación de los EAU.

- Incluso si se realizan esfuerzos digitales de recaudación de fondos dentro de la Zona Azul o fuera del país, puede ser difícil demostrarlo a las autoridades de los EAU. Por lo tanto, considere que si un participante en la COP está asociado o acreditado por una organización dedicada a la recaudación de fondos en línea o a través de las redes sociales mientras dicho participante asiste a la COP, esto puede crear un riesgo adicional para dicho participante.

II. Cómo cumplir la ley y mantenerse seguro durante la COP

- **Establezca una red de seguridad personal:** Asegúrese de que dispone de una red de apoyo activa y accesible mientras esté en la COP. Esto incluye desarrollar métodos de comunicación seguros y un sistema seguro para rastrear a otros activistas y ser rastreado, por la seguridad de todos. (Véase la sección Información/Seguridad digital, Parte II de esta guía). Asegúrate de haber verificado los números de seguridad de tu red de seguridad personal en Signal antes de entrar en los EAU.
- **Tenga un acompañante o “amigo”:** Viajar a cualquier lugar fuera de la Zona Verde es más seguro si no se está solo. Esto puede ayudar a evitar problemas y a afrontarlos en caso de que surjan.
- **Elabore y lleve consigo su lista de recursos críticos:** Estos incluyen
 - ▶ El número/email de la embajada/servicios consulares de su país en los EAU

- ▶ El número/correo electrónico de la línea directa de protección jurídica
- ▶ Los números de los contactos de su red de seguridad

- **Acceso a contenidos y comunicaciones en Internet:** Ten en cuenta que puedes estar infringiendo la ley si utilizas una VPN. La señal de texto o WhatsApp es tu mejor método de comunicación.
- **Llevar identificación:** Lleva siempre contigo un documento de identidad, preferiblemente una copia de tu pasaporte y visado, ya que es posible que se realicen controles aleatorios.
- **Absténgase de llevar o consumir drogas:** Sepa que las penas por posesión o consumo de drogas ilegales, incluso en pequeñas cantidades, pueden ser muy severas. Traiga recetas para todos los medicamentos. Tenga en cuenta que se requiere un permiso especial para los antidepresivos.
- **Tenga cuidado al hacer fotos con su teléfono:** La ley de los EAU regula estrictamente la toma de fotos y exige permiso para hacerlo sin sanciones. Cuando se encuentre fuera de la Zona Azul de la conferencia, se recomienda no hacer fotos con el teléfono ni con una cámara. Nunca haga fotos a la policía ni a los agentes de seguridad.
- **Tenga cuidado con las redes sociales:** Sepa que si utiliza su presencia en las redes sociales como medio para que su red de apoyo esté al tanto de su paradero, otras personas ajenas a su red estarán igualmente informadas. Por lo tanto, se recomienda que utilice su red de seguridad personal e, idealmente, el sistema de amigos, para informar a otros de su paradero en lugar de las redes sociales. Además, ten cuidado con lo que publicas; algunos influencers de TikTok han sido procesados por contenido obsceno.
- **Ten en cuenta las normas locales sobre la vestimenta:** Para los hombres, esto significa

llevar pantalones largos y evitar las camisas sin mangas en lugares públicos. En el caso de las mujeres, suele significar cubrirse los hombros, el escote y las rodillas. Aunque la ropa de estilo occidental es aceptable en muchas zonas, en los barrios rurales o tradicionales predomina un atuendo más conservador.

- **Respete las normas culturales locales:** Las muestras públicas de afecto, como besos y abrazos, no son culturalmente aceptables, independientemente del sexo o la orientación sexual. También es costumbre abstenerse de las muestras públicas de afecto. Los apretones de manos entre hombres y mujeres suelen ser aceptables en entornos profesionales, pero el contacto físico más allá de eso no se considera aceptable.
- **Identidad LGBTQIA+:** Las identidades sexuales y de género distintas de la heteronormativa/binaria son ilegales o no están reconocidas. Dadas las restricciones legales, la expresión abierta de la identidad LGBTQIA+ en público (incluso a través de la vestimenta, los símbolos, el comportamiento o las acciones) crea riesgos legales. Las expresiones públicas de identidad de género pueden estar penalizadas en virtud de la ley de moralidad pública.
- **Debates políticos:** Dadas las estrictas prohibiciones de la libertad de expresión, los debates políticos por parte de visitantes extranjeros suponen un riesgo. Criticar al gobierno o sus políticas puede acarrear importantes problemas legales.
- **Idioma:** Aunque mucha gente en los EAU habla inglés, aprender algunas frases básicas en árabe puede ser útil y apreciado. En general, si sabe inglés, no necesita ir acompañado de un hablante de árabe. Sin embargo, si le para un funcionario o policía que no habla un idioma que usted pueda entender, sepa que siempre puede pedir un intérprete.

III. Preguntas frecuentes

Cuestiones de entrada y salida de los EAU

1. ¿Puede el gobierno impedirme entrar o regresar al país y puede deportarme?

Sí, el gobierno puede impedirle entrar o regresar al país, incluso sin una decisión judicial. Si un funcionario le impide la entrada o le ordena salir, lo mejor es acatar la orden. Discutir o resistirse a tales decisiones podría acarrearle más complicaciones o problemas legales. Las leyes de los EAU permiten a sus autoridades expulsarle del país si supone una amenaza para su seguridad sin que medie una decisión judicial.

2. ¿Qué documentos necesito para entrar en el país?

Su pasaporte debe tener una validez mínima de seis meses a partir de la fecha en que viaje a los EAU. Asegúrese de obtener un visado para los EAU si es ciudadano de un país que exige visado.

3. Si me paran en el aeropuerto, ¿tiene derecho un agente de la ley a registrar mi teléfono u ordenador?

No tienen derecho a registrar su teléfono móvil u ordenador sin permiso del fiscal o del juez. Sin embargo, tenga en cuenta que pueden separarle de sus pertenencias, incluidos el teléfono y el ordenador portátil, y esto puede darles la oportunidad de copiar los datos o introducir algo en el dispositivo. Si te paran, pide comunicarte en un idioma que entiendas. Pide que verifiquen la identidad de la persona que te ha parado. Si piden registrar tu teléfono u ordenador portátil, pide ver el documento que les permite hacerlo. Considera si es posible acceder fácilmente al registro, ya que las consecuencias de la negativa pueden agravar el encuentro. Si los funcionarios insisten en registrarte sin una orden judicial, debes solicitar ayuda a la embajada o consulado, ponerte en contacto con la Línea Directa de Protección Jurídica y notificarlo a

tu red de seguridad. Sea cual sea la situación, es vital mantener la compostura y mostrar respeto al interactuar con las autoridades. Evite la confrontación y [absténgase de tocar a las autoridades](#). Y recuerda que siempre puedes pedir un intérprete.

4. ¿Qué debo hacer si me detienen y me interrogan en el aeropuerto?

Si te hacen preguntas sobre algo que no sea información básica (tu pasaporte, por qué has venido a los EAU), ponte en contacto con la embajada/servicios consulares de tu país y con la línea directa de protección jurídica. Si consigues contactar con su embajada, explique que necesita ayuda de un abogado, intérprete y/o representante de su embajada. No es útil proporcionar más información que la básica a los agentes de seguridad emiratíes sin la presencia de un abogado o representante de su embajada.

Cuestiones relacionadas con protestas, concentraciones y manifestaciones públicas

1. ¿Cuáles son los requisitos legales para organizar una marcha durante la COP 28?

La constitución de los EAU reconoce el derecho de reunión y manifestación pacífica de acuerdo con la ley (lo que significa que, entre otras cosas, se requiere un permiso para una protesta), aunque hay que tener en cuenta las importantes limitaciones a la libertad de expresión que crean un riesgo legal si la manifestación tiene un propósito político. Las protestas o marchas que se produzcan sin permiso son ilegales donde se aplica EAU, que es en todo el país excepto en la Zona Azul (regulada por la ONU). Si utilizas medios en línea (sitios web, redes sociales, redes de correo electrónico) sin permiso de las “autoridades competentes”, puedes ser acusado de un delito cibernético.

2. ¿Qué debo hacer para cumplir la legislación

de los EAU durante una manifestación/marcha/manifestación?

Antes de participar en una manifestación/marcha/reunión en los EAU fuera de la Zona Azul de la ONU, ten muy en cuenta los riesgos que conlleva. No se recomienda protestar fuera de la Zona Azul, y considere la importancia de comportarse con cuidado incluso dentro de la Zona Azul.

3. ¿Es legal que la policía de los EAU disperse una manifestación/marcha/reunión?

Sí, la concentración puede ser dispersada si los manifestantes se comportan de un modo que la policía considere un delito punible, o si la manifestación deja de ser pacífica. Las fuerzas de seguridad están obligadas a pedir a los participantes que se marchen voluntariamente mediante repetidas advertencias verbales que les indiquen cómo hacerlo. Si los manifestantes no se marchan pacíficamente, la ley de EAU les permite usar la fuerza.

Sus derechos en caso de registro y detención

1. ¿Es necesaria una orden de la fiscalía o de la judicatura para detenerme?

La policía puede detenerte durante 48 horas sin orden judicial ni de la fiscalía, tras lo cual debes comparecer ante la judicatura. Si le detiene el Cuerpo de Seguridad del Estado, puede permanecer detenido hasta 90 días sin orden judicial.

2. ¿Qué debo hacer si me registra o detiene la policía o los agentes de seguridad de los EAU?

Si un agente de policía te detiene, debes pedirle que verifique tu identidad. Sólo tiene derecho a pedirle que demuestre su identidad personal, por qué se encuentra en ese lugar y adónde se dirige. No tiene derecho a registrarte sin permiso de la fiscalía ni a registrar tu teléfono móvil u ordenador. Si a pesar de todo intenta registrarte,

debes considerar si la negativa a someterte al registro creará más problemas que si te sometes. En cualquier caso, mantenga la calma. Si te niegas a ser registrado, o si la policía insiste en registrarte, debes llamar a tu embajada/ servicios consulares y enviar un mensaje de texto a la línea directa de protección jurídica. Recuerde que siempre puede pedir un intérprete si lo necesita para entender lo que le piden.

3. Si me detienen y no soy emiratí, ¿qué debo hacer?

Mantenga la calma y diga inmediatamente que desea ayuda de su embajada. Pida a su embajada que le proporcione un representante, un intérprete y un abogado. Si no puede ponerse en contacto con su embajada, envíe un mensaje de texto a la línea directa de protección jurídica. Es posible que las autoridades de los EAU no le permitan comunicarse con nadie, por eso es importante ir siempre acompañado de otra persona, que pueda ponerse en contacto con la embajada o con la línea directa en su nombre.

4. Si me detienen, ¿tengo derecho a hablar en privado con un abogado antes de ser interrogado?

Sí, tiene derecho a estar a solas con su abogado en privado sin que nadie esté presente antes de que comience la investigación, aunque la legislación de los EAU permite a los servicios de seguridad impedirle estar a solas con un abogado si consideran que ha infringido la ley de Servicios de Seguridad (antiterrorista).

5. ¿Tengo derecho a que esté presente un abogado durante mi interrogatorio?

Sí, tiene derecho a solicitar la presencia de su abogado durante el interrogatorio. Sin embargo, la ley de los EAU permite que se le interroge sin la presencia de un abogado si el “interés de la investigación” así lo requiere.

6. ¿Tengo derecho a guardar silencio?

Sí, tiene derecho a guardar silencio y a negarse a firmar una declaración. Aunque tiene estos derechos, considere las circunstancias y las preguntas que le están haciendo. En algunos casos, si simplemente le hacen preguntas básicas (su nombre, por qué está en los EAU), puede decidir que responder resolverá la cuestión. Sin embargo, si le preguntan algo más que información básica, debe pedir hablar con su embajada/servicios consulares y/o solicitar un abogado.

7. ¿Puedo no abrir mi teléfono u ordenador para las investigaciones de la fiscalía si así lo solicitan?

Sí, tiene derecho a no entregar su contraseña; la constitución de los EAU le garantiza este derecho basándose en el principio constitucional de que el acusado es inocente hasta que se demuestre su culpabilidad. Si las autoridades insisten, pregunte educadamente sobre la base legal de la solicitud, exprese su voluntad de cooperar dentro de los límites de la ley y solicite asesoramiento jurídico para proteger sus derechos e intereses. Es esencial mantener la calma y el respeto al tratar con las fuerzas del orden o de seguridad.

Tus derechos en relación con los casos LGBTQ

1. ¿Protege la Constitución de los EAU a las personas que forman parte de la comunidad LGBTQIA+?

No, el código penal de los EAU penaliza las relaciones homosexuales entre varones adultos y las mujeres trans, en particular, corren un alto riesgo de criminalización. Las personas también pueden ser detenidas por una amplia gama de comportamientos que violan la legislación de los EAU, como la expresión pública de emociones, las expresiones incompatibles con el género y las campañas en favor de los derechos LGBTQIA+. Expresión pública de emociones” y “expresiones incompatibles con el género”

se refieren a acciones o comportamientos que se perciben como una violación de las normas tradicionales de género o expresiones que se consideran no conformes con las normas de comportamiento socialmente aceptadas. Esto puede incluir demostraciones públicas de afecto o emociones entre individuos del mismo género, vestirse o presentarse de una manera que no se alinea con el género asignado o percibido, o abogar por los derechos y la igualdad LGBTQIA+.

2. ¿Cómo puedo reducir la probabilidad de que se violen mis derechos por motivos de género real o percibido, identidad de género, expresión sexual y orientación sexual?

Considera las consecuencias de llevar y exhibir/

llevar pancartas, banderas, carteles, camisetas u otras formas de expresión en lenguaje pro-LGBT. En general, es útil adoptar un perfil bajo (evitar comportamientos que llamen la atención, abstenerse de demostraciones públicas de afecto, ser discreto en la elección de la ropa). Participar en cualquier reunión o acto excepto en el lugar designado a tal efecto por las autoridades de los EAU también puede exponerte a una atención policial no deseada.

Segunda Parte

Información y Seguridad Física

En esta sección se describen los riesgos y las medidas de seguridad que los asistentes que viajen a los EAU para asistir a la COP28 tal vez deseen tener en cuenta y adoptar antes, durante y después de la conferencia. Se ha diseñado teniendo en cuenta tanto los riesgos digitales / de información como los de seguridad física, reconociendo las interconexiones entre ambos.

La gestión de los riesgos de seguridad en la COP28 no debe verse como un esfuerzo de “todo o nada”. Cualquier medida de seguridad que adopten los asistentes deberá equilibrar los riesgos con otros objetivos que los asistentes pretendan alcanzar en la COP 28.

I. Comprender los riesgos de seguridad “de referencia”

En los meses y semanas previos a la COP 28, dedique tiempo a comprender los riesgos de seguridad “básicos” a los que puede enfrentarse

cuando viaje a los EAU para asistir a la COP 28. Esto es importante, ya que determina la base de las medidas y estrategias de seguridad que aplicará.

Comprender sus riesgos de seguridad “de referencia” cuando asista a la COP28 requiere (1) pensar en lo que podría salir mal y (2) determinar lo expuesto o susceptible que está.

Las principales amenazas a la seguridad que hay que tener en cuenta en el contexto de los EAU y la COP28 pueden ser:

- Ser arrestado o detenido y obligado a proporcionar acceso a información sobre dispositivos o servicios.
- Que le roben o pierda sus dispositivos o pertenencias
- Interferencias en sus dispositivos sin su conocimiento
- Interferencias en sus comunicaciones sin su

conocimiento

- Bloqueo del acceso a servicios seguros
- Ser acosado o intimidado (en línea o físicamente)
- Ser condenado o multado por actividades delictivas
- Ser deportado
- Agresión o intimidación por parte de las autoridades o agentes de la ley
- Sufrir ataques contra su reputación, como campañas de desprestigio y difamación
- Ser sometido a cualquiera de las situaciones anteriores al regresar a su país de origen.

Para comprender hasta qué punto puede estar expuesto a estas amenazas contra su seguridad, debe tener en cuenta lo siguiente:

- ¿Quiénes son **los actores** que están detrás de cada una de estas amenazas a la seguridad, y cuáles son sus capacidades y motivaciones para infligirle daño?
- Si tu identidad / **perfil individual o colectivo** (por ejemplo, género / género percibido, orientación sexual u otras características protegidas) te hace más o menos susceptible a estas amenazas a la seguridad.
- Si su **papel o las actividades previstas** en la COP 28 y en los EAU le hacen más o menos susceptible a estas amenazas a la seguridad.
- ¿Cuáles son las posibles **consecuencias** de estas amenazas a la seguridad para usted y sus aliados o socios, y hasta qué punto serían aceptables para usted y/o sus aliados/socios?

Al considerar lo anterior, no debe asumir:

- Que las mismas medidas de seguridad, acciones o comportamientos que aplicarías en tu país serían eficaces o legales en los EAU.

- Que las leyes o prácticas de los EAU son las mismas que en su país de origen.
- Que por el hecho de asistir a una conferencia internacional de la ONU estás protegido de cualquier riesgo o incidente.
- Que sus acciones y comunicaciones son inmunes a la vigilancia y el escrutinio de las autoridades y otros actores clave.

II. Antes de viajar

Una vez establecidas las medidas de seguridad “de referencia”, éstas deben servir de base para las medidas de seguridad que desee aplicar antes de viajar. Usted tendrá el máximo control sobre las medidas de seguridad que adopte antes de subir a un avión; una vez allí, su control disminuye. Por ello, se recomienda encarecidamente tomarse un tiempo antes de viajar para prepararse adecuadamente.

Paso 1: Sentar las bases de la seguridad de la información

Una seguridad de la información eficaz implica establecer una estrategia de seguridad básica y, a continuación, superponer medidas de seguridad específicas.

La estrategia básica de seguridad de la información de menor riesgo que podría adoptar para viajar a la COP28 sería viajar sin ningún dispositivo o forma de información. Sin embargo, esto puede no ser factible, o incluso recomendable, dada la importancia de mantener la comunicación y acceder a información crítica durante el viaje, especialmente en caso de emergencia.

Teniendo esto en cuenta, otras estrategias alternativas de seguridad de la información incluyen:

- **Opción 1:** Llevar dispositivos “quemadores”

(si los recursos lo permiten).

- **Opción 2:** Borrar todos los dispositivos antes de viajar y sólo tener acceso a la información que se necesita
- **Opción 3:** Limpiar manualmente de tus dispositivos las copias de información que no necesites
- **Opción 4:** Llevarte toda la información que tengas en tus dispositivos y a la que puedas acceder desde ellos

Al considerar estas opciones, tenga en cuenta:

- Cuál es su **objetivo principal**: ¿Es preservar la confidencialidad, integridad, disponibilidad o anonimato de tu información?
- Cuáles son las posibles **consecuencias negativas** de las distintas opciones (como el coste o el esfuerzo), y cuáles son los riesgos de seguridad que persisten aunque tomes determinadas medidas. (como que otras personas graben información sobre usted en la COP 28).

Opción 1: Dispositivos “quemadores”

Si está pensando en llevar un dispositivo “quemador” (Opción 1), se recomienda:

- Restablecer la configuración de fábrica del dispositivo antes de utilizarlo (tenga en cuenta que no todos los restablecimientos de fábrica consiguen un dispositivo totalmente “limpio”).
- Asegúrese de que tiene instalado el software mínimo para que el dispositivo funcione correctamente.
- Instale y configure en su dispositivo sólo las aplicaciones que sean imprescindibles durante su viaje y que estén permitidas en los EAU.
- Considere qué información pone en el dispositivo y pone a disposición del dispositivo desechable (como cuentas en la nube).

- Considere cómo registrará y almacenará la información que recopile durante la COP 28.

Opción 2: Restablecer dispositivos

Si estás considerando borrar todos tus dispositivos antes de viajar y sólo tener acceso a la información que necesitas (Opción 2), considera los consejos dados para la Opción 1, así como lo siguiente:

- Asegúrese de que cualquier restablecimiento que se realice afecte a todo el dispositivo, no sólo a los datos que contiene o a su sistema operativo. Cabe señalar que puede que sólo sea posible restablecer el dispositivo al sistema operativo que se instaló originalmente en el momento de la compra del dispositivo.
- Si tu dispositivo no está cifrado, puedes intentar “llenar” el dispositivo con archivos no sensibles y de gran tamaño y borrarlos cuando alcance su capacidad. Esto ayudará a borrar datos antiguos u ocultos que puedan permanecer en el dispositivo, incluso después de haberlo borrado. Asegúrate de que el dispositivo está cifrado durante el restablecimiento.
- Si su dispositivo no está cifrado, es probable que haya cantidades significativas de datos que no podrá borrar manualmente. Los dispositivos modernos utilizan unidades SSD en lugar de discos duros. Los SSD tienen una cantidad significativa de capacidad de almacenamiento adicional a su máximo declarado. Utilizan este almacenamiento extra para aumentar la vida útil del dispositivo, sin embargo, usted no puede acceder a este almacenamiento extra para borrar los datos, pero sus adversarios sí. Puedes seguir los consejos anteriores para forzar la sobrescritura, pero tendrás que hacerlo repetidamente.

Opción 3: Limpiar dispositivos

Si la opción de limpiar manualmente la información de tus dispositivos es la única disponible, ten en cuenta lo siguiente:

- Generalmente no será posible eliminar todas las copias de información valiosa y sensible. Los sistemas modernos escanean tus datos, crean índices de búsqueda y pueden guardar copias de seguridad de tus datos en ubicaciones distintas de los archivos en los que trabajas.
- No será posible eliminar todas las pruebas de las cuentas en línea utilizadas anteriormente, ya que es probable que las cachés y el historial incluyan datos de las cuentas con las que inició sesión.
- Los archivos que actualmente pueden parecer de bajo riesgo pueden contener cambios rastreados, comentarios y metadatos. Los adversarios pueden comprar (o desarrollar) herramientas capaces de realizar un escaneo exhaustivo de todo lo disponible en su dispositivo.
- También puedes limpiar la información sensible y valiosa de tus servicios teniendo en cuenta la eficacia de lo anterior.

Paso 2: Tome medidas de seguridad de la información con respecto a sus datos

Con una estrategia fundacional de seguridad de la información en marcha, puede empezar a pensar en las medidas de seguridad específicas que tomará cuando su información esté:

- **En reposo** (por ejemplo, en un dispositivo apagado)
- **En uso** (por ejemplo, en un dispositivo encendido)
- **En movimiento** (por ejemplo, cuando se envía o comparte entre dispositivos)

Esta sección se centra específicamente en la protección de la confidencialidad de los datos. Pero tenga en cuenta que las herramientas

y la tecnología por sí solas no protegerán su información; también es fundamental su forma de actuar y la de los demás.

Confidencialidad de los datos en reposo (cuando no se utilizan)

Para proteger la confidencialidad de la información en reposo, debería considerar:

- Instalar un cifrado de disco completo como primera línea de defensa (el cifrado de disco completo para tu portátil y teléfonos dependerá de la marca, el modelo y la versión del sistema operativo).
- Utilizar una contraseña segura para tus dispositivos y cuentas seleccionando de 3 a 6 palabras al azar o el título/letra de una canción y a continuación:
 - ▶ Poner en mayúsculas algunas de las palabras
 - ▶ Sustituir algunas letras por números
 - ▶ Añadir símbolos como `_`, `-` y `!` entre algunas palabras
- Mantener los dispositivos apagados con la mayor frecuencia posible.
- Asegúrate de que tus dispositivos están actualizados con el software oficial.
- Utilizar plataformas cifradas de extremo a extremo para las comunicaciones y el almacenamiento de datos, y familiarizarse con lo que está cifrado y lo que no en estas plataformas.

Confidencialidad de los datos en uso

Cuando se trata de proteger la confidencialidad de la información en uso, debe considerar:

- Desactivar (o saber cómo desactivar rápidamente) la lectura biométrica u otros dispositivos wearables que puedan desbloquear tus dispositivos sin contraseña
- Utilizar software actualizado

- Configurar correctamente el software antimalware y cortafuegos
- Utilizar una contraseña segura
- Activar la autenticación de dos factores
- Prestar atención a las advertencias y alertas de su dispositivo o software que puedan indicar que se está produciendo un ataque
- Prestar atención al entorno en el que se utiliza el dispositivo (por ejemplo, saber que otras personas pueden estar mirando la pantalla en espacios públicos).

Confidencialidad de los datos en movimiento

Cuando se trata de proteger la confidencialidad de la información en movimiento, debe tener en cuenta:

- Investigar las medidas de seguridad que tiene cualquier característica del Sistema Operativo, aplicaciones o servicios que uses en tus dispositivos, particularmente asegurarte de que están comunicando tu información de forma encriptada y que están asegurando cualquier dato requerido para establecer una comunicación segura con el servicio.
- Considere la posibilidad de no instalar, desinstalar o no utilizar aplicaciones o servicios durante la COP 28 de los que no esté seguro que utilizan la máxima seguridad.
- Investigar las limitaciones del cifrado de extremo a extremo al utilizar plataformas de comunicación como Signal, WhatsApp o iMessage. Por ejemplo, estos servicios no sólo cifrarán sus datos hacia y desde sus dispositivos, sino también en el hardware del proveedor de servicios. Sin embargo, los metadatos necesarios para encaminar tu comunicación por el sistema no pueden cifrarse y esto puede poner en peligro el anonimato si un adversario accede a los datos en estas plataformas.

- Los servicios cifrados de extremo a extremo no protegen la información de tu dispositivo ni de los dispositivos con los que te comunicas. Para solucionarlo, tenga en cuenta los consejos anteriores relativos a la información en uso y en reposo.

Paso 3: Asegúrese de que su documentación personal está en regla

- Asegúrese de que su pasaporte tiene una validez mínima de 6 meses desde el momento de su llegada, y de que le queda al menos una página en blanco / sin utilizar para el sello de entrada.
- Compruebe los requisitos de visado para entrar en los EAU según su nacionalidad y el motivo de su visita.
- Solicite su visado con antelación para evitar inconvenientes, sobre todo teniendo en cuenta que las solicitudes de visado y los plazos de tramitación pueden aumentar debido a la COP 28.
- Asegúrese de que se le han expedido o solicitado las tarjetas de acreditación o documentos similares que demuestren su participación en la COP 28, que podrían ser necesarios para su solicitud de visado / entrada en los EAU o el acceso a zonas restringidas en el lugar de celebración de la conferencia.
- Asegúrese de que dispone de los billetes de avión de ida y vuelta, alojamiento y fondos suficientes para la duración de su estancia, ya que podrían solicitársele tanto para la tramitación del visado como para el control de inmigración/fronteras, como prueba de que no tiene previsto prolongar su estancia en los EAU.
- Lleve todos los documentos pertinentes en su equipaje de mano y tenga fotocopias de seguridad o escaneados digitales en una carpeta segura.

Paso 4: Considere la posibilidad de contratar un seguro de viaje

- Contrate un seguro de viaje y de accidentes personales que, como mínimo, cubra el tratamiento médico de urgencia (idealmente hasta un importe limitado), la repatriación médica, la evacuación política, cualquier gasto médico a largo plazo que se produzca al regresar a su país de origen (como consecuencia de un accidente ocurrido durante el viaje), la pérdida de equipaje y la cancelación o retraso de vuelos.
- Asegúrese de que entiende y ha aceptado las exclusiones que invalidarían su póliza de seguro de viaje y accidentes personales (por ejemplo, exclusiones geográficas, actividades prohibidas).
- Trate de disponer de fondos para cubrir cualquier emergencia, situaciones no aseguradas o en las que pueda ser necesario depositar dinero en efectivo para tratamientos médicos.
- Lleve siempre consigo una copia de la póliza de seguro y tenga el número de emergencia guardado en sus dispositivos y anotado en algún lugar seguro.

Paso 5: Embalaje y ropa seguros

- Piense en lo que lleva consigo: ¿Hay algo que pueda considerarse sospechoso o que pueda percibirse como un ataque a los valores religiosos y morales de los EAU (como alcohol, libros o revistas de contenido político, activista, sexual o religioso, y productos que contengan cannabis, aunque tengas receta para ello). Tenga en cuenta que la ley prohíbe ampliamente todo lo que no se adhiera a los valores de los EAU, lo que deja margen para que los agentes migratorios de aduanas interpreten la ley y actúen según su criterio.
- Esté al tanto de las restricciones actuales y de los artículos prohibidos, como todo lo que

pueda considerarse un arma o equipo militar o para hacer cumplir la ley (lo que podría incluir también herramientas y artículos decorativos).

- Ten en cuenta tu atuendo. La ropa con mensajes o simbolismos políticos puede atraer una atención no deseada y provocar la desaprobación y el cuestionamiento social.
- Respete las costumbres locales y las sensibilidades culturales a la hora de elegir la ropa que va a llevar. La ropa que pueda percibirse como inmodesta (como los tejidos transparentes, la ropa ajustada o los atuendos que dejan al descubierto los hombros, el escote y las piernas) también puede llamar la atención.
- Lleve toda la medicación necesaria acompañada de sus recetas.

Paso 6: Establezca su red de apoyo

Una red de apoyo es una lista de aliados con los que puede ponerse en contacto en caso de que necesite ayuda inmediata en caso de incidente o emergencia, o que pueden actuar en su nombre cuando usted no pueda hacerlo (por ejemplo, si queda incapacitado debido a un incidente médico o por estar detenido).

Considere una red con tres tipos de contacto dentro de su red de apoyo:

1. Personas de confianza fuera de los EAU

Podría tratarse de colegas, amigos o familiares que no están físicamente presentes en los EAU y que estarían al tanto de tus horarios y movimientos. Se recomienda tener un contacto de confianza fuera de los EAU con el que se comunique regularmente (una vez al día), ya que estará mejor posicionado para responder a un incidente, tomar medidas para limitar las consecuencias de un incidente, o activar el apoyo externo de los proveedores internacionales / comunidad, si esto no se puede hacer desde los EAU.

Asegúrese de que cualquier acuerdo de check-in con contactos fuera de los EAU sea claramente entendido por ambas partes, y que las personas externas que sepan qué hacer en caso de que se pierda un check-in y hayan fracasado los repetidos intentos de establecer comunicación con usted. Dichas acciones pueden aumentar con urgencia cuanto más tiempo pase sin que se pueda establecer comunicación con usted.

2. Personas de confianza entre los asistentes a la COP28

Podría tratarse de colegas, amigos o compañeros delegados que asistan a la COP28, con los que mantendrá una comunicación regular a lo largo de la conferencia, incluso antes y después de actividades fuera de la COP28 (como hacer turismo o ir a un restaurante).

Si forma parte de una delegación, puede optar por comunicarse colectivamente (como parte de un grupo de Signal o WhatsApp), o emparejarse individualmente con un “compañero”. Estas comunicaciones pueden utilizarse para confirmar movimientos seguros y dar cuenta de los delegados o “compinches”, así como para alertarles de amenazas o incidentes de seguridad específicos.

3. Proveedores externos de apoyo

Es importante conocer los proveedores externos con los que se puede contactar en caso de emergencia (y tener sus datos de contacto programados en los dispositivos y en una copia física). Esto puede incluir, pero no se limita a:

- Proveedor de seguros de viaje y accidentes personales (+ cualquiera de sus proveedores de asistencia)
- Asistencia o representación jurídica
- Apoyo y acompañamiento para el bienestar
- Centros médicos locales
- Asesoramiento y apoyo en materia de riesgos de seguridad

Paso 7: Prepárese para hacer frente a preguntas basadas en la identidad y abordar las sensibilidades culturales

- Prepárese para preguntas sobre quién es y a qué se dedica. Considere que puede correr riesgos al revelar cosas personales sobre usted que pueden ser aceptables y legales en otros lugares. Piensa en lo que vas a revelar.
- Los activistas LGBTQIA+ deben ser especialmente conscientes de las leyes y costumbres conservadoras de los EAU. Ten en cuenta los riesgos que pueden conllevar las expresiones explícitas de tu sexualidad o las muestras públicas de afecto.

III. A su llegada

Seguridad de la información

- Apaga todos los dispositivos antes de salir del avión: dependerás de tu estrategia de seguridad de la información básica hasta que llegues a tu destino.
- Una vez en su destino, encienda sus dispositivos y compruebe que las aplicaciones y servicios que ha elegido funcionan según lo previsto.

Control fronterizo

- Prepárese para el control fronterizo, incluyendo posibles preguntas sobre su ruta, países que ha visitado antes y por qué, duración de su estancia, alojamiento en los EAU, su trabajo y actividades en su país de origen, dinero y preguntas personales sobre cosas como su religión u orientación sexual.
- Prepárese para responder con calma, de manera convincente y sin llamar la atención si le hacen preguntas personales.
- Tenga en cuenta que, independientemente de haber obtenido un visado, sólo se le permitirá la entrada en los EAU a discreción del funcionario de inmigración.

- Tenga a mano los documentos pertinentes (pasaporte y visado, carta de invitación, prueba de fondos y alojamiento, billetes de avión de ida y vuelta y seguro de viaje).
- Mantenga la calma, responda sólo a lo que se le pregunte y proporcione lo que se le pida.

DURANTE LA CONFERENCIA

Seguridad de la información

- Mantenga todos sus dispositivos apagados, bloqueados y en un lugar seguro en la medida de lo posible, especialmente cuando los esté cargando y cuando no los utilice.
- Evite utilizar cargadores que no sean los suyos y no enchufe otros periféricos o dispositivos de almacenamiento.
- Mantén desactivadas todas las funciones inalámbricas si no son necesarias, ya que pueden utilizarse para rastrearle de forma pasiva y vincularle con quienes te rodean.
- No te conectes a redes WiFi públicas a menos que sea necesaria una comunicación de emergencia.
- Si es posible, utilice la itinerancia internacional en lugar de comprar u obtener una tarjeta SIM local, ya que los EAU aplican el registro de tarjetas SIM que requiere documentos de identidad y datos biométricos. No hacerlo puede suponer un delito penal. Si no es posible utilizar la itinerancia internacional, probablemente sea mejor tener un teléfono con una tarjeta SIM local que no tener ningún teléfono. Cuando participe en cualquier tipo de medio de comunicación social o tradicional, ten en cuenta que estás difundiendo información ampliamente. Esta comunicación puede servir para proporcionar pruebas contra usted de un delito penal, o el acto de expresar la información específica puede ser en sí mismo un delito penal en los EAU. (Véase la Parte 1:

Conozca la Ley de esta Guía).

- Puede ser delito acceder a sitios web prohibidos y recibir contenidos ilícitos. Los EAU disponen de un cortafuegos nacional para bloquear las fuentes en línea prohibidas. Sin embargo, no pueden bloquear contenidos específicos en plataformas de medios sociales directamente de los propietarios de esos sitios.
- Aunque una VPN puede ser una herramienta útil para eludir el bloqueo de los EAU de las fuentes en línea prohibidas, el uso de una VPN para este fin es un delito penal. Si hay pruebas de que este contenido está presente en su dispositivo, esto proporciona munición adicional a los adversarios contra usted. Si no utiliza una VPN, no podrá acceder a estos contenidos durante la COP28.
- Además, tenga en cuenta que el uso de una VPN no garantiza una conexión siempre segura. Si ignora las advertencias de seguridad al conectarse, es posible que no establezca una conexión segura con su proveedor de VPN en primer lugar. Su conexión a un proveedor de VPN puede caer debido a errores o interferencias y su dispositivo puede ignorar esto y continuar enviando y recibiendo datos sin la VPN. Por último, es posible que no haya configurado la VPN para garantizar que todo el tráfico se envía a través de la conexión dejando expuestos algunos datos muy sensibles, como una lista de todos los sitios a los que accede, así que no se haga la ilusión de que conectarse a sitios ilegales es “seguro”.

Seguridad personal

- Si es posible, evite estar solo. Hay más seguridad en grupos con otros asistentes de confianza a la COP28.
- Tenga en cuenta las normas culturales y evite expresiones que puedan considerarse

ofensivas o incendiarias.

- Recuerde que los EAU son un país musulmán y que el Islam prohíbe el consumo de alcohol, por lo que los EAU tienen normas estrictas al respecto. Aunque no está totalmente prohibido (ya que los extranjeros pueden comprar y consumir alcohol en determinadas circunstancias), tenga en cuenta que está prohibido beber en lugares públicos y que existen zonas libres de alcohol.
- Guarde sus objetos de valor en los bolsillos delanteros o en bolsillos con cremallera o botón dentro del bolso (que siempre deben estar cerrados con cremallera o broche).
- Si se encuentra en el hotel, considere la posibilidad de utilizar una caja fuerte para guardar cualquier objeto o pertenencia de valor que no vaya a necesitar fuera del hotel.
- Manténgase informado en todo momento de cualquier novedad y preste atención a su entorno para detectar cualquier cosa fuera de lo normal.
- Familiarícese con los lugares clave de los edificios en los que vaya a pasar tiempo (salidas de emergencia del hotel, lugar de la conferencia, restaurantes)
- Tenga en cuenta que asistir a actos no oficiales fuera de la Zona Azul oficial, como reuniones públicas y manifestaciones, supone un riesgo considerablemente mayor para los asistentes a la COP. Las reuniones y manifestaciones públicas fuera de la Zona Azul están muy reguladas en los EAU, son ilegales sin permiso, y los agentes del orden tienen autoridad para utilizar la fuerza en determinadas circunstancias si la protesta se considera ilegal.
- Lleve consigo en todo momento un documento de identidad con fotografía y sus tarjetas de acreditación.

Seguridad en el alojamiento

- Elija hoteles seguros y de buena reputación (tenga en cuenta la proximidad al lugar de celebración, las calificaciones y reseñas de antiguos clientes, y las medidas de seguridad, como recepción 24 horas, tarjeta de acceso a la habitación, caja fuerte).
- Mantenga la confidencialidad del número de su habitación de hotel y la tarjeta de acceso oculta y con usted en todo momento.
- Asegura tu habitación cada vez que salgas comprobando puertas y ventanas. Considere la posibilidad de utilizar un cartel de “No molestar” para impedir el acceso a su habitación tanto cuando esté ocupada como cuando no lo esté.

Transporte / Viajes por carretera

- Utilice únicamente el transporte recomendado u organizado por su delegación, su hotel o los organizadores del evento.
- Uber tiene licencia en los EAU, pero es más caro que un taxi. Si utiliza Uber, asegúrese de comprobar las opiniones y calificaciones de los conductores.
- Es ilegal compartir coche o utilizar servicios de viaje compartido en los EAU y es ilegal que un conductor sin la licencia adecuada transporte pasajeros.
- Evite estar solo durante los actos oficiales, pero sobre todo fuera de la Zona Azul. Intente siempre formar pareja con un colega o amigo, o moverse en grupo.
- Regístrese con un compañero de evento o con su delegación a la salida, a la llegada y al regreso.

AL REGRESAR

Seguridad de la información

- Si utiliza dispositivos “quemadores” o dispositivos de limpieza, deberá realizar el restablecimiento al final de la conferencia y

antes de salir hacia el aeropuerto.

- Si ha limpiado manualmente los dispositivos, deberá disponer de tiempo suficiente para hacerlo antes de salir hacia el aeropuerto.
- En todos los casos, deberá pasar el control de seguridad o fronterizo con los dispositivos apagados y los accesos biométricos desactivados.
- Cuando regrese a su país de origen, podrá restablecer la configuración de sus dispositivos anterior a la COP 28; no obstante, puede aprovechar la oportunidad para limitar la información que contienen y a la que se puede acceder desde ellos en el futuro.

Reevaluación del riesgo de seguridad “de referencia” en casa

- Reevalúe su riesgo de seguridad “de referencia” en casa y cómo su participación en la conferencia puede haber elevado su perfil y/o exposición a determinadas amenazas de seguridad. Preste especial atención a las situaciones que puedan producirse en su domicilio y que indiquen que corre un mayor riesgo (llamadas no solicitadas, amenazas directas, vigilancia física o digital).
- Cuando crea que su perfil de riesgo ha aumentado, considere la posibilidad de limitar temporalmente las actividades públicas, incluidas las manifestaciones y los casos judiciales que puedan agravar la demanda.
- Refuerce las medidas de seguridad, especialmente en su domicilio y para los niños que van al colegio.
- Si cree que existe una amenaza creíble por parte de un actor capaz, no desestime la posibilidad de una escalada. Considere la posibilidad de hibernar o el traslado temporal o la evacuación.

QUÉ HACER SI:

Sus dispositivos son confiscados y posteriormente le son devueltos:

- Compruebe si la carcasa ha sido manipulada físicamente
- No encienda ni utilice el dispositivo
- Notifíquelo a sus colegas, socios y compañeros por medios alternativos
- Intente conseguir un nuevo dispositivo si es posible

Sus dispositivos son robados o perdidos y posteriormente devueltos a usted:

- Restablezca todas las contraseñas de los servicios en línea
- Notifique a cualquier persona que pudiera verse afectada por los datos del dispositivo o accesibles desde el mismo
- No dé por sentado que los adversarios no podrán acceder a los datos cifrados de sus dispositivos porque puedan tener su contraseña, por ejemplo, a partir de imágenes de CCTV en las que se le vea entrar o mediante vigilancia física

Sus medidas previstas para proteger la confidencialidad de la información digital en reposo, en uso y en movimiento no funcionan:

- No seleccione alternativas inseguras sin antes considerar el riesgo y la probabilidad de que esto sea exactamente lo que un adversario quiere que haga
- Determina a través de los demás si esto sólo te afecta a ti o también a todos los que utilizan la aplicación o el servicio; en esta situación, la gente puede interpretarlo erróneamente como un ataque dirigido
- Acude a tu red de apoyo para identificar alternativas
- Considera seriamente la opción de realizar la actividad a tu regreso si puede esperar

Cree que otra persona puede haber intentado acceder a sus redes sociales, plataformas tecnológicas o herramientas digitales:

- Asegúrate de que este intento de acceso no ha sido, de hecho, tuyo;
- Revise su actividad anterior en relación con otros servicios, ya que también pueden haber tenido un intento de acceso y no habérselo notificado,
- Cambia tu(s) contraseña(s) de los servicios afectados sólo si estás seguro de que tus comunicaciones con el servicio son seguras.

Sospecha que están a punto de detenerle:

- Desactiva los controles biométricos y otros controles de acceso a tu información para que se requieran contraseñas reales. En algunos dispositivos, mantener pulsado el botón de encendido durante 10 segundos lo conseguirá en caso de emergencia.

Sufres ataques a tu reputación como campañas de desprestigio y difamación

- No respondas directamente a los mensajes o

contenidos difamatorios, ya que podrías dar más visibilidad al autor.

- Si procede, considere la posibilidad de participar en una campaña positiva en colaboración con aliados que refuerce su reputación y su buen trabajo, pero sin abordar el ataque.
- Documenta los ataques y reúne pruebas: podrían ser útiles en el futuro, ya sea con fines legales o para pedir a las plataformas y medios sociales utilizados que retiren el contenido.
- Supervisar la situación para identificar una escalada o nuevos ataques.
- Buscar apoyo en materia de bienestar, si procede
- Busca apoyo en los medios de comunicación y periodistas oficiales

Si sufres algún ataque o represalia (o estás en riesgo inmediato de ataque o represalia) al regresar a tu país de origen, puedes ser elegible para recibir apoyo holístico de seguridad totalmente financiado a través de Open Briefing. Puede remitir a Open Briefing una solicitud de apoyo holístico en materia de seguridad rellenando el formulario de remisión que aparece al final de [esta página web](#).

Si es elegible, recibirá el contacto de un consultor asignado dentro de las 72 horas siguientes a su remisión, quien discutirá su situación con usted (por ejemplo, riesgos, necesidades de apoyo, etc.) y las posibles opciones de apoyo.

Encontrará más información [aquí](#).