Principios globales sobre seguridad nacional y el derecho a la información

("Principios de Tshwane")

Principios globales sobre seguridad nacional y el derecho a la información ("Principios de Tshwane")

Estos Principios globales sobre seguridad nacional y el derecho a la información, emitidos el 12 de junio de 2013, fueron redactados por 22 organizaciones durante un periodo de dos años, en el que se contó con la asesoría de más de 500 expertos de al menos 70 países. El proceso de redacción culminó con una reunión en la ciudad sudafricana de Tshwane, de la que estos Principios tomaron su nombre.

12 de junio de 2013

ISBN: 978-1-940983-26-4

Publicado por:
Open Society Foundations
Open Society Justice Initiative
224 West 57th Street
Nueva York, NY 10019 E.E.U.U.
www.opensocietyfoundations.org

Portada diseñada por Judit Kovács | Createch Ltd.
Diseño de texto e impresión de Createch Ltd.

Índice

Introducción		5
Preámbulo		9
Definiciones		13
Parte I:	Principios generales	17
Parte II:	Información que puede ser clasificada por razones de seguridad nacional e información que debería ser divulgada	23
Parte III.A:	Normas relativas a la clasificación y desclasificación de información	33
Parte III.B:	Normas sobre gestión de solicitudes de información	39
Parte IV:	Aspectos judiciales relativos a la seguridad nacional y al derecho a la información	45
Parte V:	Organismos que supervisan el sector de seguridad	49
Parte VI:	Divulgaciones de interés público por parte del personal de organismos públicos	55
Parte VII:	Límites a las medidas destinadas a sancionar o restringir la divulgación de información al público	65
Parte VIII:	Principio final	69
Anexo:	Organizaciones asociadas	71

Introducción

Estos Principios han sido formulados para orientar a quienes intervienen en la redacción, revisión o implementación de leyes o disposiciones relativas a la potestad del Estado para clasificar información por motivos de seguridad nacional o sancionar su divulgación.

Están basados en normas, estándares y buenas prácticas nacionales e internacionales (incluso regionales) y la doctrina especializada.

Abordan aspectos específicos de seguridad nacional, y no todos los supuestos en los cuales se podría retener información. Todos los demás motivos de interés público para limitar su acceso deberían, como mínimo, cumplir estos estándares.

Estos Principios fueron redactados por 22 organizaciones y centros académicos (que se enumeran en el Anexo) con la asesoría de más de 500 expertos procedentes de más de 70 países en 14 reuniones celebradas alrededor del mundo y moderadas por la Iniciativa Pro-Justicia de la Sociedad Abierta, y con la ayuda de los cuatro relatores especiales para la promoción y protección de la libertad de expresión y/o la libertad de prensa y el relator especial sobre la promoción y protección de los derechos humanos y libertades fundamentales en la lucha contra el terrorismo:

- el Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión,
- el Relator Especial de las Naciones Unidas (ONU) sobre la promoción y protección de los derechos humanos y libertades fundamentales en la lucha contra el terrorismo,
- la Relatora Especial de la Comisión Africana de Derechos Humanos y de los Pueblos sobre Libertad de Expresión y Acceso a la Información (ACHPR),

- la Relatora Especial de la Organización de los Estados Americanos (OEA) para la Libertad de Expresión y
- La Representante de la Organización para la Seguridad y la Cooperación en Europa (OSCE) para la libertad de los medios.

Antecedentes y Exposición de Motivos

La seguridad nacional y el derecho a saber de la sociedad a menudo se consideran objetivos contrapuestos. Si bien a veces puede haber cierto grado de tensión entre el interés de un gobierno por preservar el carácter reservado de cierta información por razones de seguridad nacional y el derecho de la población a acceder a información en poder de autoridades públicas, un examen exhaustivo del pasado reciente indica que los intereses legítimos de seguridad nacional, en la práctica, se ven favorecidos cuando la sociedad está bien informada sobre las actividades del Estado, incluidas aquellas llevadas a cabo para resguardar la seguridad nacional.

El acceso a la información, al facilitar el escrutinio público de los actos del Estado, no sólo previene abusos por parte de funcionarios públicos, sino que además permite que la población intervenga en la definición de las políticas del Estado y, por ende, constituye un elemento clave para la preservación efectiva de la seguridad nacional, la participación democrática y la formulación de políticas sólidas. Para proteger el pleno ejercicio de los derechos humanos, en ciertas circunstancias, podría ser necesario mantener información en secreto para salvaguardar intereses legítimos de la seguridad nacional.

Encontrar un punto de equilibrio adecuado se torna aún más difícil debido a que, en muchos países, los tribunales actúa con la menor independencia y la mayor deferencia frente a los reclamos del gobierno cuando este apela a argumentos de seguridad nacional. Esta deferencia se ve reforzada por disposiciones de las leyes sobre seguridad de numerosos países que prevén excepciones al derecho a la información y a las normas procesales comunes sobre prueba y derechos de los acusados ante la mínima demostración, o mera afirmación, por parte del gobierno de que existe un riesgo para la seguridad nacional. Cuando un gobierno apela excesivamente a argumentos de seguridad nacional, se pueden quebrantar las principales garantías institucionales contra el abuso gubernamental: la independencia de los tribunales, el estado de derecho, el control legislativo, la libertad de los medios de comunicación y el gobierno abierto.

Los presentes Principios se formulan en respuesta a los desafíos históricos descritos en líneas precedentes y a que, en los últimos años, una cantidad significativa de Estados de todo el mundo se han propuesto adoptar o reformar regímenes de clasificación de información y leyes relacionadas. Esta tendencia, a su vez, ha sido provocada por varios acontecimientos. El más significativo ha sido, quizás, la rápida adopción de leyes sobre acceso a la información desde la caída del Muro de Berlín, lo que ha tenido como consecuencia, que a la fecha de emisión de estos Principios, más de 5.200 millones de personas en 95 países del mundo gocen del derecho de acceso a la información—al menos por disposición legal, no siempre en la práctica. La población de estos países se enfrenta —a menudo por primera vez— con la pregunta de si la información ha de mantenerse en secreto, y bajo qué circunstancias. Otros acontecimientos que han contribuido a un aumento de la legislación propuesta en materia de secrecía están relacionados con las respuestas gubernamentales al terrorismo o la amenaza terrorista, además de un interés en mantener la secrecía regulada por la ley de las transiciones democráticas. ic transitions.

Preámbulo

Las organizaciones e individuos que intervinieron en la redacción de los presentes Principios:

Recordando que el acceso a la información en poder del Estado es un derecho de toda persona y que, por tanto, se trata de un derecho que ha de ser protegido por leyes formuladas con precisión y que contemplen excepciones claramente delimitadas, y la tutela del derecho por tribunales independientes, organismos de control parlamentario y otras instituciones independientes;

Reconociendo que los estados tienen el derecho legítimo de clasificar cierta información, incluso por razones de seguridad nacional, y destacando que encontrar un punto de equilibrio adecuado entre la divulgación y la clasificación de información resulta indispensable para una sociedad democrática y su seguridad, progreso, desarrollo y bienestar, así como para el pleno goce de los derechos humanos y las libertades fundamentales;

Ratificando que resulta imperativo, para que las personas puedan monitorear la conducta de su gobierno y participar plenamente en una sociedad democrática, que tengan acceso a información en poder de autoridades públicas, incluida información relativa a seguridad nacional;

Observando que estos Principios están basados en normas y estándares internacionales sobre el derecho público de acceso a la información en poder de autoridades estatales y otros derechos humanos, la evolución de las prácticas de los Estados (según se refleja, entre otras medidas, en las sentencias de los tribunales nacionales e internacionales), los principios generales del derecho reconocidos por la comunidad de naciones, y la doctrina de los expertos;

Teniendo en cuenta también la Declaración de Principios sobre Libertad de Expresión de la Comisión Inter-Americana de Derechos Humanos; la ley Modelo Interamericana sobre Acceso a la Información Pública; la Declaración de Principios sobre Libertad de Expresión en África, y la ley Modelo sobre Acceso a la Información Pública en África;

Recordando la Declaración Conjunta de 2004 del Relator Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión, la Representante de la OSCE para la Libertad de los Medios de Comunicación y el Relator Especial de la OEA para la Libertad de Expresión; las Declaraciones Conjuntas emitidas en 2006, 2008, 2009 y 2010 por estos tres expertos y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos; la Declaración Conjunta sobre WikiLeaks de los Relatores Especiales de la ONU y la Comisión Interamericana, de diciembre de 2010; y el Informe sobre Medidas contra el Terrorismo y Derechos Humanos, adoptado por la Comisión de Venecia en 2010;

Recordando asimismo los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información adoptados por un grupo de expertos convocados por la organización Artículo 19 en 1995 y los Principios sobre Control y Rendición de Cuentas de los Servicios de Seguridad en una Democracia Constitucional elaborados en 1997 por el Centro de Estudios sobre Seguridad Nacional (Centre for National Security Studies, CNSS) y la organización polaca Helsinki Foundation for Human Rights;

Teniendo en cuenta que existen principios internacionales — como los incluidos en la Ley Modelo sobre Acceso a la Información Pública en África, los Principios de la ONU sobre Empresas y Derechos Humanos (Ruggie Principles), el Tratado de Comercio de Armas, las Líneas Directrices de la OCDE para Empresas Multinacionales y el Documento de Montreal sobre las obligaciones legales y las buenas prácticas de los Estados en relación con las operaciones de empresas militares privadas y empresas de seguridad durante un conflicto armado —que reconocen la importancia de acceder a información sobre, o en relación con, empresas en ciertas circunstancias; y que algunos abordan específicamente la necesidad de que las empresas militares privadas y las empresas de seguridad que trabajen dentro del sector de la seguridad nacional hagan pública cierta información;

Observando que estos Principios no contemplan estándares sustantivas sobre recopilación de inteligencia, manejo de información personal o intercambio de inteligencia, los cuales son adecuadamente abordados en las "buenas prácticas relativas a marcos jurídicos e institucionales para los servicios de inteligencia y su supervisión", emitidas en 2010 por Martin Scheinin, el entonces Relator Especial de la ONU sobre la promoción y la protección de los

derechos humanos y las libertades fundamentales en la lucha contra el terrorismo a petición del Consejo de los Derechos Humanos de las Naciones Unidas.

Reconociendo la importancia del intercambio eficaz de inteligencia entre Estados, tal como se insta en la Resolución 1373 del Consejo de Seguridad de la ONU;

Reconociendo asimismo que los obstáculos al control público e independiente interpuestos en nombre de la seguridad nacional agravan el riesgo de que se produzcan comportamientos ilícitos, corruptos y fraudulentos y de que tales actos no sean descubiertos, y que con frecuencia se cometen violaciones a la privacidad y otros derechos individuales bajo el manto de la reserva por razones de seguridad nacional;

Preocupados por los costos que supone para la seguridad nacional la clasificación excesiva de información como reservada, incluidos los obstáculos al intercambio de información entre organismos gubernamentales y aliados, la imposibilidad de resguardar información clasificada legítima y de identificar datos importantes entre el gran volumen de información, la recopilación repetitiva de información por parte de distintos organismos, y la asignación excesiva de responsabilidades a directores de seguridad;

Destacando que los Principios se centran en el derecho de la sociedad a la información, y que abordan los derechos a la información de personas detenidas, víctimas de violaciones de los derechos humanos y otros cuya situación requiere de manera especial acceso a cierta información, únicamente en la medida en que tales derechos se vinculen directamente con el derecho de la población a la información;

Reconociendo que cierta información que no debería ser clasificada por motivos de seguridad nacional podría igualmente ser clasificada por otras razones reconocidas por el derecho internacional, incluyendo por ejemplo las relaciones internacionales, la imparcialidad de los procedimientos judiciales, el derecho de las partes litigantes y la privacidad de las personas, sujetas siempre al principio según el cual no podrá clasificarse información cuando el interés público en acceder a ella sea mayor al interés público en mantener su clasificación;

Manifestando nuestra intención de ofrecer orientación práctica a gobiernos, organismos legislativos y reguladores, autoridades públicas, legisladores, tribunales, otros organismos de supervisión y la sociedad civil, con respecto a algunos de los desafíos más importantes que plantea la convergencia de la seguridad nacional con el derecho a información en esta, especialmente aquellos vinculados con el respeto de los derechos humanos y la rendición de cuentas democrática;

Esforzándonos por formular Principios de aplicación y valor universal;

Reconociendo que los Estados enfrentan múltiples desafíos al procurar encontrar un equilibrio entre el interés público en la divulgación y la necesidad de la clasificación para proteger intereses legítimos de la seguridad nacional, y que toda vez que estos Principios son universales, su puesta en práctica debería tomar en cuenta las distintas realidades en el ámbito local, incluyendo la diversidad de sistemas jurídicos;

Recomendamos que los órganos pertinentes a nivel nacional, regional e internacional adopten medidas para difundir y debatir estos Principios, y los avalen, adopten o implementen en la mayor medida posible, a fin de contribuir progresivamente al pleno goce del derecho a la información conforme se establece en el Principio 1.

Definiciones

En estos Principios, y a menos que el contexto requiera algo distinto:

"**Compañías dentro del sector de la seguridad**" es una persona jurídica que lleva a cabo o ha llevado a cabo transacciones o negocios en el sector de la seguridad nacional, y solamente en tal calidad; ya sea como contratista o proveedor de servicios, instalaciones, personal o productos incluyendo, aunque sin limitarse a, armamento, equipos e inteligencia. Esto incluye empresas militares y de seguridad privadas (PMSCs). No incluye a personas jurídicas constituidas como organizaciones sin ánimo de lucro o no gubernamentales.

"Independiente" significa la libertad institucional, financiera y operativa respecto de la influencia, la dirección y el control del poder ejecutivo, incluidas todas las autoridades del sector de seguridad.

"Información" significa cualquier material documental, ya sea original o copia, independientemente de sus características físicas y cualquier otro material tangible o intangible, con independencia de la forma o el medio en que se contenga. Incluye, sin carácter restrictivo, registros, correspondencia, hechos, opiniones, asesorías, memorándums, datos, estadísticas, libros, ilustraciones, planos, mapas, diagramas, fotografías, grabaciones en audio o vídeo, documentos, mensajes de correo electrónico, cuadernos de bitácora, muestras, modelos e información en cualquier formato electrónico.

"Información de interés público" se refiere a información que resulta relevante o beneficiosa para el público, y no simplemente de interés individual, y cuya divulgación es "en interés del público", por ejemplo, debido a que resulta útil para que la sociedad comprenda las actividades que lleva a cabo el gobierno.

"Interés legítimo de seguridad nacional" hace referencia a un interés cuyo verdadero objeto y principal efecto sea proteger la seguridad nacional, de forma consistente con el derecho interno e internacional. (En el Principio 9 se establecen categorías de información cuya confidencialidad podría ser necesaria para proteger un interés legítimo de seguridad nacional.) Un interés de seguridad nacional no será legítimo cuando su objetivo real o su principal efecto sea resguardar un interés que no esté vinculado con la seguridad nacional, tal como evitar que se ridiculice o señale a gobiernos o funcionarios por irregularidades; ocultar información sobre violaciones de los derechos humanos, otras violaciones a la ley o el funcionamiento de las instituciones públicas; fortalecer o perpetuar un determinado interés político, ideología o partido político; o reprimir protestas legales.

"**Seguridad nacional**" no se define en estos Principios. El Principio 2 recomienda que la "seguridad nacional" se defina con precisión en el derecho nacional de forma coherente con las necesidades de una sociedad democrática.

"Autoridades públicas" incluye a todos los organismos de los poderes ejecutivo, legislativo y judicial en todos los niveles del gobierno, las autoridades creadas por la constitución y las leyes, incluyendo autoridades del sector de seguridad, y los organismos que no pertenecen al Estado pero son controlados o son propiedad del gobierno, o actúan como agentes del mismo. Las "autoridades públicas" también incluyen a entidades privadas o de otra naturaleza que desempeñan funciones o servicios públicos, u operan con fondos o beneficios públicos significativos, pero únicamente en lo que respecta a la ejecución de tales funciones, prestación de servicios, o uso de fondos o beneficios públicos.

"Personal público" o "**funcionario público**" hace referencia a empleados públicos actuales y anteriores, contratistas y subcontratistas de autoridades públicas, incluido el sector de seguridad. Con " personal público" o "funcionario público" también se hace referencia a personas contratadas por órganos no estatales que pertenecen o están bajo el control del gobierno o que sirven como agentes del gobierno; y empleados de entidades privadas de otra naturaleza que realizan funciones públicas o que prestan servicios u operan con fondos o ayudas públicos substanciales, pero sólo en lo que concierne a la realización de dichas funciones, o la prestación de esos servicios, o el uso de fondos o ayudas públicas.

"**Sanción**" usado como sustantivo refiere a cualquier forma de penalización o perjuicio, incluidas las medidas criminales, civiles o administrativas. En forma de verbo, **"sancionar"** significa hacer efectiva dicha forma de penalización o perjuicio.

"Sector de seguridad" comprende: (i) agentes de seguridad, incluyendo pero sin limitarse a las fuerzas armadas, la policía y otros organismos encargados de vigilar el cumplimiento de la ley, fuerzas paramilitares, y servicios de inteligencia y seguridad (tanto militares como civiles); y (ii) todos los órganos ejecutivos, departamentos y ministerios responsables de la coordinación, el control y la vigilancia de los agentes de seguridad.

Parte I: Principios generales

Principio 1: Derecho a la información

(a) Todas las personas tienen derecho a buscar, recibir, usar y difundir información que esté en poder de autoridades públicas u otros órganos que actúen en su representación, o cuyo acceso haya sido reconocido legalmente a las autoridades públicas.

(b) Los principios internacionales también reconocen que las empresas dentro del sector de seguridad nacional, incluidas las empresas militares y de seguridad privadas, tienen la responsabilidad de divulgar información con respecto a situaciones, actividades o conductas que razonablemente se puede esperar que tengan un impacto en el ejercicio de los derechos humanos.

(c) Aquellos que tengan la obligación de divulgar información, de acuerdo con los Principios 1(a) y 1(b), deben proporcionar la información que se solicite y tienen una obligación positiva de publicar información de interés público, salvo las limitadas excepciones previstas en la legislación que sean necesarias para prevenir perjuicios concretos e identificables a intereses legítimos, incluida la seguridad nacional.

(d) Sólo las autoridades públicas cuyas responsabilidades específicas incluyan la protección de la seguridad nacional podrán hacer valer la seguridad nacional como fundamento para clasificar información.

(e) Cualquier argumentación de seguridad nacional hecha por una empresa para justificar la clasificación de información ha de ser explícitamente autorizada o confirmada por una autoridad pública cuyas responsabilidades incluyan la protección de la seguridad nacional.

Nota: El gobierno, y sólo el gobierno, es responsable, en última instancia, de la seguridad nacional, y por lo tanto sólo el gobierno podrá determinar que cierta información no sea publicada si pudiere redundar en perjuicio de la seguridad nacional.

(f) Las autoridades públicas también tienen la obligación explícita de publicar, de forma proactiva, cierta información de interés público.

Principio 2: Aplicación de los Principios

(a) Estos Principios se aplican al ejercicio del derecho de acceso a información tal y cómo se identifica en el Principio 1, cuando el gobierno asevera o confirma que la divulgación de dicha información podría redundar en perjuicio de la seguridad nacional.

(b) Dado que la seguridad nacional es uno de los argumentos públicos de mayor peso para restringir la información, cuando las autoridades públicas invocan otros motivos de interés público para limitar su acceso —incluidos motivos de relaciones internacionales, orden público, salud y seguridad públicas, aplicación de la ley, emisión futura de una opinión libre y abierta, formulación de políticas efectivas e intereses económicos del Estado— estos deberán, como mínimo, cumplir los estándares relativos a la imposición de restricciones en el derecho del acceso a la información establecidos en estos Principios como pertinentes.

(c) Se considera buena práctica para la seguridad nacional, cuando la misma es empleada para limitar el derecho a la información, que se defina con precisión en el ordenamiento jurídico de un país de forma consistente con una sociedad democrática.

Principio 3: Requisitos para restringir el derecho a la información por razones de seguridad nacional

No podrán aplicarse restricciones al derecho a la información invocando razones de seguridad nacional a menos que el gobierno demuestre que: (1) la restricción (a) está establecida en una ley y (b) resulta necesaria en una sociedad democrática (c) para proteger un interés legítimo de seguridad nacional; y (2) la ley establece garantías adecuadas contra la posibilidad de abuso, incluido el escrutinio oportuno, pleno, accesible y efectivo de la

validez de las restricciones por una autoridad supervisora independiente y su revisión exhaustiva por los tribunales.

(a) *Establecida en una ley*. La ley debe ser accesible, inequívoca y redactada de forma acotada y precisa para permitir que las personas comprendan qué información puede ser clasificada, cuál debería ser divulgada y qué actos relativos a la información pueden ser objeto de sanción.

(b) *Necesaria en una sociedad democrática*.

(i) La divulgación de la información debe representar un riesgo real e identificable de perjuicio significativo para un interés legítimo de seguridad nacional.

(ii) El riesgo de perjuicio que supondría la divulgación debe superar al interés público de difundir la información.

(iii) La limitación debe adecuarse al principio de proporcionalidad y representar el medio menos restrictivo disponible para evitar el perjuicio.

(iv) La restricción no debe atentar contra la esencia misma del derecho a la información.

(c) *Protección de un interés legítimo de seguridad nacional*. Las restringidas categorías de información que pueden clasificarse con base en argumentos relativos a la seguridad nacional deberían establecerse claramente en la ley.

Notas: ver la definición de "interés legítimo de seguridad nacional" en la sección de Definiciones. El Principio 3 (b) es aún más importante si la seguridad nacional no se define claramente en la legislación tal y como se recomienda en el Principio 2.

"Interés público" no se define en estos Principios. En el Principio 10 se incluye una lista de categorías de interés público especialmente relevantes que deberían publicarse de forma proactiva y que nunca deberían clasificarse. En el Principio 37 se incluye una lista de categorías de irregularidades de alto interés para la sociedad y que los funcionarios públicos deberían y podrían publicar sin miedo a las represalias.

Al ponderar el riesgo de perjuicio y el interés público en la divulgación, debería considerarse la posibilidad de mitigar los perjuicios causados por la difusión, incluso a través de medios que requieran una erogación razonable de fondos. A continuación se incluye una lista enunciativa de factores que deben ser tenidos en cuenta al determinar si el interés público en la divulgación supera el riesgo de perjuicio:

- *factores que favorecen la divulgación: es razonablemente esperable que la divulgación (a) fomente la discusión abierta de asuntos públicos, (b) incremente la rendición de cuentas por parte del gobierno, (c) contribuya al debate positivo e informado sobre cuestiones importantes o asuntos de interés relevante, (d) promueva el control efectivo de los recursos públicos, (e) permita revelar los motivos de una decisión gubernamental, (f) contribuya a la protección del medioambiente, (g) exponga amenazas a la salud o seguridad públicas, o (h) exponga o favorezca la rendición de cuentas respecto de violaciones a derechos humanos o derecho internacional humanitario.*
- *factores que favorecen que no se divulgue información: la divulgación podría causar un riesgo de perjuicio real e identificable para un interés legítimo de seguridad nacional;*
- *factores que son irrelevantes: es razonablemente esperable que la divulgación (a) ridiculice al gobierno o a un funcionario, o menoscabe la confianza en ellos, o (b) debilite a una ideología o partido político.*

El hecho de que la divulgación pueda causar perjuicio a la economía de un país tendría relevancia a efectos de determinar si resulta conveniente clasificar información por este motivo, pero no por razones de seguridad nacional.

Principio 4: Corresponde a la autoridad pública establecer la legitimidad de las restricciones

(a) Corresponde a la autoridad pública que pretenda que no se divulgue determinada información demostrar la legitimidad de cualquier restricción que se aplique.

(b) El derecho a la información debería interpretarse y aplicarse en sentido amplio, mientras que la interpretación de las restricciones debería ser acotada.

(c) Al demostrar esta legitimidad, no bastará con que la autoridad pública simplemente afirme que existe un riesgo de perjuicio; sino que debe proporcionar razones específicas y sustanciales que respalden sus afirmaciones.

Nota: Cualquier persona que pretenda acceder a la información debería tener una oportunidad genuina de impugnar la base de la evaluación del riesgo ante autoridades administrativas y judiciales, de acuerdo con los Principios 26 y 27.

(d) En ningún caso se considerará un argumento concluyente la mera afirmación de que la divulgación causaría un riesgo para la seguridad nacional, por ejemplo, la emisión de un certificado en ese sentido por un ministro u otro funcionario.

Principio 5: No se aplican excepciones para autoridades públicas

(a) Ninguna autoridad pública estará exenta de los requerimientos de divulgación, incluyendo al poder judicial, legislativo, instituciones supervisoras, servicios de inteligencia, fuerzas armadas, policía, otros cuerpos de seguridad, los jefes de Estado y de gobierno y las dependencias que integren los anteriores.

(b) No se podrá clasificar información por motivos relativos a la seguridad nacional simplemente con el argumento de que fue generada por, o transmitida a un Estado extranjero o un organismo intergubernamental, determinada autoridad pública o unidad dentro del ámbito de una autoridad.

Nota: Ver el Principio 9(a)(v) relativo a la información generada por un Estado extranjero u organismo intergubernamental.

Principio 6: Acceso a información por parte de organismos supervisores

Todos los organismos de supervisión, defensa del pueblo y apelación, incluidos los tribunales, deben tener acceso a todo tipo de información —incluso la información sobre seguridad nacional y con independencia de su nivel de confidencialidad— que resulte relevante para el desempeño de sus funciones.

Nota: Este Principio se detalla en el Principio 32. No se refiere a la divulgación pública por parte de los organismos supervisores. Los organismos supervisores deberían mantener la confidencialidad de toda la información que haya sido legítimamente clasificada de acuerdo con estos Principios tal y cómo se establece en el Principio 35.

Principio 7: Recursos

Los Estados deben destinar recursos suficientes y adoptar otras medidas necesarias, como emitir reglamentaciones y manejar los archivos de forma adecuada, para asegurar que estos Principios se cumplan en la práctica.

Principio 8: Estados de emergencia

En una situación de emergencia pública que suponga una amenaza para la vida de la población de un país y cuya existencia haya sido reconocida en forma oficial y legítima conforme al derecho nacional e internacional, un Estado podrá establecer excepciones a sus obligaciones relativas al derecho a buscar, recibir y difundir información, únicamente en la medida en que resulte indispensable por las exigencias de la situación y solamente cuando y por el tiempo que dichas excepciones sean congruentes con las demás obligaciones que corresponden al Estado de conformidad con el derecho internacional, y no implique ningún tipo de discriminación.

Nota: Ciertos aspectos del derecho a buscar, recibir y difundir información e ideas son tan fundamentales para el disfrute de los derechos no derogables que siempre habrían de ser plenamente respetados incluso en períodos de emergencia pública. Como ejemplo no exhaustivo, alguna o la totalidad de la información contenida en el Principio 10 sería de este carácter.

Parte II: Información que puede ser clasificada por razones de seguridad nacional e información que debería ser divulgada

Principio 9: Información que puede ser clasificada en forma legítima

(a) Las autoridades públicas podrán restringir el derecho del público de acceder a información cuando existan razones de seguridad nacional, pero únicamente cuando tales restricciones cumplan todas las demás disposiciones establecidas en estos Principios, la información obre en poder de una autoridad pública y la información esté comprendida en una de las siguientes categorías:

(i) Información sobre planes de defensa en curso, operaciones y cuestiones sobre capacidad durante el período en que la información resulte de utilidad operativa.

Nota: Debe entenderse que la frase "durante el período en que la información resulte de utilidad operativa" exige divulgar la información una vez que esta ya no suponga revelar datos que podrían ser aprovechados por enemigos para conocer la capacidad de reacción del Estado, su capacidad, sus planes, etc.

(ii) Información sobre la producción, capacidades, o uso de los sistemas de armamentos y otros sistemas militares, incluidos los sistemas de comunicaciones.

Nota: Dicha información incluye datos e inventos tecnológicos, e información sobre su producción, capacidad o uso. La información sobre partidas presupuestarias relativas a armamento y otros sistemas militares deberían encontrarse disponibles para el público. Ver los Principios 10C(3) y 10F. El que los Estados mantengan y publiquen una lista de control de armamento supone una buena práctica alentada por el Tratado sobre el Comercio de Armas en lo que concierne a armas convencionales. La publicación de información relativa a armas, equipos y números de tropas también es una buena práctica.

(iii) Información sobre medidas específicas destinadas a resguardar el territorio del Estado, infraestructura crítica o instituciones nacionales fundamentales (*institutions essentielles*) contra amenazas, uso de la fuerza o sabotaje, cuya efectividad depende de su confidencialidad;

Nota: "Infraestructura crítica" hace referencia a recursos estratégicos, activos y sistemas, ya sea físicos o virtuales, de tal importancia para el Estado que su destrucción o incapacidad tendría un impacto debilitador en la seguridad nacional.

(iv) Información perteneciente a, o derivada de, operaciones, fuentes y métodos de los servicios de inteligencia, siempre que conciernan a asuntos relativos a la seguridad nacional; e

(v) Información relativa a asuntos de seguridad nacional suministrada por un Estado extranjero u organismo intergubernamental con una expectativa expresa de confidencialidad; y otras comunicaciones diplomáticas en tanto tengan que ver con asuntos relativos a la seguridad nacional.

Nota: Se considera buena práctica dejar constancia de estas expectativas por escrito.

Nota: en la medida en que la información relativa a terrorismo y a medidas para la lucha contra el terrorismo esté comprendida en una de las categorías expuestas anteriormente, el derecho del público al acceso de dicha información podría estar sujeta a restricciones por motivos de seguridad nacional de acuerdo con estas y otras disposiciones de los Principios. A su vez, alguna información relacionada con terrorismo, o con medidas para la lucha contra el terrorismo podría ser de alto interés público: ver ej. Principios 10A, 10B y 10H(1).

(b) Se considera buena práctica que la legislación nacional establezca una lista exclusiva de categorías de información limitadas, como las categorías anteriores.

(c) Un Estado podría añadir una categoría de información a la lista anterior de categorías, pero únicamente si dicha categoría está específicamente identificada y definida

de forma limitada y la preservación de la confidencialidad de la información es necesaria para proteger un interés legítimo de seguridad nacional establecido por ley, tal y cómo se sugiere en el Principio 2(c). Al proponer la categoría, el Estado debería explicar que la divulgación de la información contenida en la misma supondría una amenaza para la seguridad nacional.

Principio 10: Categorías de información sobre las cuales existe una fuerte presunción o un interés preponderante a favor de su divulgación

Algunas categorías de información, incluyendo las enumeradas a continuación, revisten un interés público especialmente significativo o preponderante por su relevancia extraordinaria para el proceso de control democrático y el Estado de derecho. En consecuencia, existe una fuerte presunción, y en algunos casos una necesidad imperiosa, de que tal información debería ser pública y divulgarse en forma proactiva.

La información contenida en las siguientes categorías debería, al menos, gozar de una elevada presunción a favor de su divulgación, y podría clasificarse por motivos de seguridad nacional, únicamente en circunstancias absolutamente excepcionales y en concordancia con los demás Principios, sólo por un plazo estrictamente limitado, en forma acorde con la ley y cuando no exista un medio razonable para limitar el perjuicio que provocaría la divulgación. Para el caso de ciertas categorías de información que se especifican a continuación como sujetas de forma inherente a un interés público preponderante en su divulgación, la clasificación por motivos de seguridad nacional no puede justificarse nunca.

A. Violaciones de los derechos humanos internacionales y del derecho internacional humanitario

(1) Existe un interés público preponderante en la divulgación de información sobre violaciones graves de los derechos humanos o violaciones serias del derecho internacional humanitario, incluidos los crímenes de derecho internacional, y violaciones sistemáticas o generalizadas de los derechos a la libertad y seguridad personales. Dicha información no podrá ser clasificada por razones de seguridad nacional bajo ninguna circunstancia.

(2) La información relacionada con otras violaciones de los derechos humanos o el derecho humanitario está sujeta a una alta presunción de divulgación, y en ningún caso podrá ser clasificada invocando razones de seguridad nacional de forma tal que se evitara la rendición de cuentas por dichas violaciones, o se despojara a la víctima de la oportunidad de acceder a una reparación efectiva.

(3) Cuando un Estado está sometido a un proceso de justicia transicional durante el cual se ve especialmente obligado a garantizar la verdad, justicia, reparación y garantías de no repetición, existe un interés público preponderante en cuanto a la divulgación a la sociedad en su conjunto de la información sobre violaciones de los derechos humanos cometidas bajo el régimen pasado. El gobierno sucesor debería, inmediatamente, dedicarse a proteger y preservar la integridad de todos los documentos que contengan dicha información oculta por el gobierno anterior, y publicarlas inmediatamente.

Nota: Ver el Principio 21(c) relativo al deber de buscar o reconstruir la información relativa a las violaciones de los derechos humanos.

(4) Cuando la existencia de violaciones se refute o se sospeche en lugar de haberse establecido, este Principio se aplica a la información que, por sí sola, o en conjunto con otra información, pudiere arrojar alguna luz sobre la verdad relativa a las supuestas violaciones.

(5) Este Principio se refiere a la información sobre violaciones que hayan tenido lugar o estén teniendo lugar, y se aplica independientemente de que las violaciones hayan sido cometidas por el Estado que posee la información, u otros Estados.

(6) La información relativa a las violaciones cubiertas por este Principio incluyen, sin límite alguno, la siguientes:

(a) Descripción completa de los actos u omisiones que constituyan las violaciones, y los registros que den cuenta de las mismas, además de las fechas y circunstancias en las que dichas violaciones hayan tenido lugar, y cuando corresponda, la ubicación de las personas desaparecidas o del lugar donde se encuentran los restos mortales.

(b) La identidad de todas las víctimas, congruente con la privacidad y otros derechos de las víctimas, de sus familiares, y testigos; y los datos generales o anónimos referentes a su número y características que pudieran ser relevantes para la salvaguarda de los derechos humanos.

Nota: Se podrá impedir la divulgación al público en general de los nombres y otros datos personales de las víctimas, de sus familiares y de testigos en la medida necesaria para evitar que éstos sufran un mayor perjuicio, cuando las personas afectadas o, en el caso de personas fallecidas, sus familiares, soliciten expresa y voluntariamente, que no se divulgue dicha información, o, de otra forma, la confidencialidad de la información corresponda con los deseos de la persona o con las necesidades particulares de grupos vulnerables. En el caso de las víctimas de violencia sexual, se solicitará expresamente su consentimiento para divulgar sus nombres u otros datos personales. Las víctimas infantiles (menores de 18 años) no deberán ser identificables por el público en general. Este Principio debería interpretarse, sin embargo, teniendo en cuenta la realidad de que ciertos gobiernos han protegido información relativa a violaciones de los derechos humanos invocando el derecho a la privacidad, incluyendo el de las víctimas que han sufrido violaciones graves, sin tener en cuenta los deseos reales de las mismas. Estas salvedades, sin embargo, no deberían impedir la publicación de datos generales o anónimos.

(c) Los nombres de las agencias e individuos que perpetraron o fueron, de algún modo, responsables de las violaciones, y de forma más genérica, de cualquier unidad del sector seguridad que estuviera presente al momento de las mismas, o implicada de otro modo, en dichas violaciones, al igual que sus superiores y comandantes, así como la información sobre el alcance de su mando y control.

(d) Información sobre las causas de las violaciones y la incapacidad de impedirlas.

B. Garantías relativas al derecho a la libertad y seguridad de la persona, la prevención de la tortura y otros abusos y el derecho a la vida

La información cubierta por este Principio comprende:

(1) Las leyes y reglamentos que autorizan la privación de la vida de una persona por parte del Estado, y las leyes y reglamentos que se refieren a la privación de la libertad, incluyendo aquellos que tengan que ver con los motivos, procedimientos, transferencias, tratamiento, o condiciones de detención de las personas afectadas, incluyendo los métodos de interrogatorio. La divulgación de estas leyes y reglamentos es de un interés público preponderante.

Notas: "Leyes y reglamentos" hace referencia a la forma de usar dichos términos en el Principio 10, e incluyen: toda legislación primaria o secundaria, estatutos, reglamentos y

ordenanzas, y también decretos u órdenes ejecutivas emitidos por un presidente, primer ministro u otra autoridad pública, y órdenes judiciales con fuerza de ley. Incluyen, además, cualquier normativa o interpretación de la ley consideradas como obligatorias por parte de los funcionarios ejecutivos.

La privación de la libertad incluye cualquier forma de arresto, detención, encarcelamiento o internamiento.

(2) La ubicación de todos los sitios donde se mantiene a personas privadas de su libertad y que sean administrados por el Estado o en representación de éste, así como la identidad de todas las personas privadas de su libertad, los motivos de su detención y los cargos en su contra, incluso durante conflictos armados.

(3) Información sobre el fallecimiento de detenidos, e información sobre cualquier privación de la vida de la que sea responsable un Estado, incluyendo la identidad de la persona/s fallecidas, las circunstancias de su muerte y la ubicación de sus restos mortales.

Nota: En ningún caso se podrá clasificar información invocando razones de seguridad nacional cuando ello pudiera redundar en la detención clandestina de una persona o la creación y gestión de centros de detención y ejecuciones clandestinos. Asimismo, bajo ninguna circunstancia puede resultar admisible que por acción del Estado, o con su autorización, asistencia o aquiescencia, se oculte el destino o paradero de personas privadas de su libertad a familiares u otras personas que tengan interés legítimo en el bienestar de esa persona.

Los nombres y otros datos personales de las personas que hayan sido privadas de su libertad, y que hayan muerto mientras estaban detenidos, o cuyos fallecimientos hayan sido provocados por agentes del Estado, podrían no divulgarse al público general en la medida necesaria para proteger el derecho a la privacidad si las personas afectadas, o sus familiares en caso de que los afectados hayan fallecido, solicitan la no divulgación de dichos datos expresa y voluntariamente, y si dicha clasificación es congruente con los derechos humanos. Las identidades de niños privados de su libertad no serán divulgadas al público general. Estas salvedades, sin embargo, no deberían impedir la publicación de datos generales u anónimos.

C. Estructuras y poderes de gobierno

La información cubierta por este Principio incluye, sin limitación, lo siguiente:

(1) La existencia de autoridades militares, de policía, seguridad e inteligencia, así como las subunidades.

(2) Las leyes y reglamentos aplicables a dichas autoridades, sus organismos de supervisión y mecanismos internos de rendición de cuentas, así como los nombres de los funcionarios a cargo.

(3) Información necesaria para evaluar y controlar la erogación de fondos públicos, incluidos presupuestos generales, principales rubros e información básica sobre los gastos de tales autoridades.

(4) La existencia y términos de acuerdos bilaterales o multilaterales que se hayan celebrado, así como otros compromisos internacionales importantes asumidos por el Estado en materia de seguridad nacional.

D. Decisiones relativas al uso de la fuerza militar o a la adquisición de armas de destrucción masiva

(1) La información cubierta por este Principio incluye la información relevante para la toma de una decisión relativa a enviar tropas de combate o emprender acciones militares, incluyendo la confirmación de dichas acciones, su tamaño general y alcance, y una explicación de su justificación, además de cualquier información que demuestre que un hecho establecido como parte de la justificación pública fue erróneo.

Nota: La referencia al tamaño "general" de una acción y su alcance reconoce que debería, por norma general, poder satisfacerse el alto interés del público en obtener información relevante sobre la decisión de enviar tropas de combate sin que se revelen todos los detalles de los aspectos operativos de la acción militar en cuestión (Principio 9).

(2) La posesión o adquisición de armas nucleares, u otras armas de destrucción masiva, por parte de un Estado, aunque no necesariamente sobre su fabricación o capacidades operativas, es un asunto de interés público preponderante y no deberá mantenerse como información clasificada.

Nota: este subprincipio no deberá ser leído como una manifestación de apoyo a la adquisición de dichas armas.

E. Vigilancia

(1) El marco jurídico general en materia de vigilancia de todo tipo, así como los procedimientos a seguir para su autorización, la selección de los objetivos y el uso, intercambio, almacenamiento y destrucción del material interceptado, debería ser accesible para la sociedad.

Nota: Esta información incluye: (a) las leyes que rigen todos los tipos de vigilancia, tanto abierta como encubierta, incluidas las técnicas de vigilancia indirecta tales como la generación de perfiles y la minería de datos, y todas las medidas de vigilancia que puedan usarse; (b) los objetivos permisibles de vigilancia; (c) el umbral de presunción requerido para iniciar o continuar la vigilancia; (d) limitaciones en la duración de las medidas de vigilancia; (e) procedimientos para la autorización y revisión del uso de dichas medidas; (f) los tipos de datos personales que podrán recopilarse y/o procesarse por motivos relativos a la seguridad nacional; y (g) los criterios que se aplican al uso, retención, eliminación y transferencia de dichos datos.

(2) El público también deber tener acceso a la información sobre las entidades autorizadas para llevar a cabo acciones de vigilancia, y a las estadísticas relativas al uso de dichas acciones.

Notas: Esta información incluye la identidad de cada entidad gubernamental con autorización específica para llevar a cabo vigilancias específicas cada año; el número de autorizaciones para realizar vigilancias otorgadas cada año a dichas entidades; la mejor información disponible sobre el número de individuos y el número de comunicaciones sujetos a vigilancia cada año; y si se llevaron a cabo acciones de vigilancia sin autorización específica, y si es así, por parte de qué entidad.

El derecho de la sociedad a ser informada no se extiende, necesariamente, a los detalles fácticos u operativos de las vigilancias efectuadas con arreglo a la ley y en consonancia con las obligaciones relativas a los derechos humanos. Dicha información podría ser clasificada, tanto para el público como para aquellos que se encuentran sujetos a vigilancia, al menos hasta que el período de vigilancia haya concluido.

(3) Adicionalmente, la sociedad debería ser plenamente informada acerca de cualquier vigilancia ilegal. La información acerca de este tipo de vigilancias debería ser hecha pública en la mayor medida posible, sin violar los derechos de privacidad de las personas vigiladas.

(4) Estos Principios abordan el derecho de la sociedad a acceder a la información y se entienden sin perjuicio a los derechos sustantivos y procesales adicionales de los individuos que han sido, o creen haber sido, sujetos a vigilancia.

Nota: Se considera como una buena práctica el que se solicite a las autoridades que notifiquen a las personas que han sido sujetas a vigilancia encubierta (facilitando, como mínimo, información sobre el tipo de medida que se tomó, las fechas y el órgano responsable de autorizar la medida de vigilancia) en la medida en que esto se pueda hacer sin poner en peligro las operaciones en curso o las fuentes y métodos.

(5) Las altas presunciones a favor de la divulgación reconocida por este Principio no aplican al respecto de la información relacionada únicamente con la vigilancia de las actividades de gobiernos extranjeros.

Nota: La información obtenida a través de vigilancia encubierta, incluyendo la relativa a las actividades de gobiernos extranjeros, habrán de divulgarse en las circunstancias identificadas en el Principio 10A.

F. Información financiera

La información cubierta por este Principio incluye información suficiente para permitir que el público entienda las finanzas del sector de la seguridad, así como las reglas que las rigen. Dicha información deberá incluir, pero no limitarse a:

(1) Presupuestos de los departamentos y las agencias con los principales rubros;

(2) Estados de cuentas a cierre de ejercicio con los principales rubros;

(3) Reglas de gestión financiera y mecanismos de control;

(4) Reglas de contratación; y

(5) Informes redactados por instituciones supremas de auditoria y otros órganos responsables de la revisión de aspectos financieros del sector de la seguridad, incluyendo los resúmenes de las secciones clasificadas de dichos informes.

G. Responsabilidad relativa a violaciones constitucionales y estatutarias y otros abusos de poder

La información cubierta por este Principio incluye la relativa a la existencia, carácter y escala de las violaciones constitucionales y estatutarias y otros abusos de poder por parte de las autoridades o el personal público.

H. Salud pública, seguridad pública o medioambiente

La información cubierta por este Principio incluye:

(1) En el caso de una amenaza inminente o actual a la salud pública, a la seguridad pública o al medioambiente, toda la información que permita que el público entienda o tome las medidas pertinentes para evitar o mitigar el daño procedente de dicha amenaza, tanto si ésta deriva de causas naturales como de actividades humanas, incluyendo por acciones del Estado o de compañías privadas.

(2) Cualquier otra información, actualizada regularmente, sobre la explotación de recursos naturales, contaminación e inventarios de emisiones, los impactos medioambientales derivados de grandes obras públicas existentes o propuestas, o de la extracción de recursos, y evaluación de riesgos y planes de gestión de las instalaciones especialmente peligrosas.

Parte III.A: Normas relativas a la clasificación y desclasificación de información

Principio 11: Obligación de exponer las razones para clasificar información

(a) Con independencia de que un Estado cuente o no con un proceso de clasificación formal, las autoridades públicas están obligadas a expresar las razones por las cuales se clasifica la información.

Nota: La "clasificación" es el proceso por el cual los documentos que contienen información sensible se revisan y se marcan para indicar quién puede acceder a los mismos y la forma en la que han de ser manejados. El establecimiento de un sistema formal de clasificación para reducir la arbitrariedad y la clasificación excesiva supone una buena práctica.

(b) Las razones deberían indicar en qué categoría acotada, de las enumeradas en el Principio 9, queda comprendida la información, y describir cuál sería el perjuicio que se causaría con su divulgación, incluido el nivel de gravedad y probabilidad.

(c) Los niveles de clasificación, si se usan, deberían corresponder a los niveles y probabilidades de perjuicio identificadas en la justificación.

(d) Cuando se clasifica la información, (i) una marca protectora debe incorporarse al documento indicando el nivel, si procede, y la duración máxima de la clasificación, y (ii) debe incluirse una declaración en la que se justifique la necesidad de clasificar la información a ese nivel y por ese período.

Nota: Se recomienda la inclusión de una declaración que justifique cada decisión de clasificación ya que hace que los funcionarios presten atención al perjuicio específico que podría derivar de la divulgación de la información, y porque facilita el proceso de desclasificación y divulgación. Las marcas párrafo a párrafo facilita aún más la coherencia de las partes no clasificadas de los documentos.

Principio 12: Acceso público a las normas sobre clasificación

(a) El público debe tener la posibilidad de comentar los procedimientos y las normas que se aplican a la clasificación antes de que entren en vigor.

(b) El público debe tener acceso a las normas y procedimientos escritos que se aplican a la clasificación.

Principio 13: Potestad para clasificar información

(a) Únicamente los funcionarios específicamente autorizados o designados, según se prevea en la ley, podrán clasificar información. Cuando un funcionario sin esta potestad considere que cierta información debería tener carácter clasificado, ésta podrá ser considerada como clasificada durante un período breve y expresamente establecido, hasta tanto un funcionario designado haya revisado la recomendación sobre clasificación.

Nota: en ausencia de disposiciones legales que controlen la potestad para clasificar información, se considera buena práctica, al menos especificar la delegación de potestad en un reglamento.

(b) La identidad de la persona responsable de una decisión sobre clasificación deberá ser localizable, o indicada en el documento, a menos que existan razones de peso para clasificar la identidad, a fin de garantizar la rendición de cuentas.

(c) Los funcionarios públicos designados por la ley deben delegar su potestad original de clasificación a la menor cantidad de subordinados jerárquicos que resulte viable desde el punto de vista administrativo.

Nota: Se considera buena práctica publicar información sobre la cantidad de personas que tienen potestad para clasificar información, y la cantidad de personas que tienen acceso a información clasificada..

Principio 14: Facilitar la impugnación interna de la clasificación de información

Los funcionarios públicos, incluidos aquellos que pertenezcan a autoridades del sector de seguridad, que consideren que se ha clasificado indebidamente información podrán impugnar dicha clasificación.

Nota: El personal del sector de seguridad es considerado como especialmente adecuado para impugnar la clasificación debido a la arraigada cultura de secretismo existente en las agencias de seguridad, el hecho de que la mayor parte de los países no ha establecido o designado un órgano independiente para la recepción de quejas por parte del personal de seguridad, y que la divulgación de información sobre seguridad a menudo tiene como consecuencia mayores sanciones que la divulgación de otro tipo de información.

Principio 15: Obligación de archivar, gestionar y conservar adecuadamente información y documentos sobre seguridad nacional

(a) Las autoridades públicas tienen la obligación de archivar, gestionar y conservar adecuadamente documentos e información de conformidad con lo establecido en las normas internacionales.[I] Solamente podrán quedar exentos de archivo, gestión

1. Estos incluyen: Consejo Internacional de Archivos (CIA), *Principios sobre Acceso a los Archivos* (2012); CIA, Declaración Universal sobre los Archivos (2010; adoptada por la UNESCO); Consejo Europeo, *Recomendación No R(2000)13 sobre una política europea relativa al acceso a los archivos* (2000); Antonio González Quintana, CIA, *Políticas archivísticas para la defensa de los Derechos Humanos: versión actualizada y más completa del informe preparado por la Unesco y el Consejo Internacional de Archivos (1995), acerca de la gestión de archivos de los servicios de seguridad estatales de antiguos regímenes represivos* (2009).

y conservación ciertos documentos e información en los casos en que esto sea autorizado por ley.

(b) La información se debe conservar en forma adecuada. Los sistemas de archivos deben ser congruentes, transparentes (sin revelar información clasificada de forma legítima) y exhaustivos, de forma tal que cuando se efectúen solicitudes de acceso específicas sea posible localizar toda la información relevante, aun cuando ésta no pueda ser divulgada.

(c) Cada organismo público debería crear y publicar, y periódicamente revisar y actualizar, una lista detallada y precisa de los archivos clasificados que posee, exceptuando aquellos documentos excepcionales, si los hubiere, cuya existencia pueda clasificarse de forma legítima de acuerdo con el Principio 19.

Nota: La actualización de dichas listas anualmente supone una buena práctica.

Principio 16: Limitación temporal al período de clasificación

(a) Se podrá clasificar información por razones de seguridad nacional únicamente durante el período que sea necesario para proteger un interés legítimo de seguridad nacional. La decisión de no divulgar cierta información debe revisarse periódicamente para asegurar que se cumpla este Principio.

Nota: la revisión exigida por ley al menos cada cinco años supone una buena práctica. Varios países requieren que se revisen en un período menor de tiempo.

(b) La persona que determina la clasificación deberá indicar la fecha y las condiciones o el acontecimiento por virtud de los cuales cesará la clasificación.

Nota: La revisión periódica de esta limitación temporal o especificación de las condiciones o evento por virtud del cual cesará la clasificación, supone una buena práctica.

(c) Ningún tipo de información podrá tener carácter clasificado en forma indefinida. El período máximo de clasificación por razones de seguridad nacional deberá estar fijado por ley.

(d) La información podrá ser clasificada por un período superior al plazo estimado sólo en circunstancias excepcionales de conformidad con una nueva decisión de clasificación, considerada por otro responsable, y se deberá fijar un nuevo plazo máximo.

Principio 17: Procedimientos de desclasificación

(a) Se debería identificar, en la legislación nacional, la responsabilidad gubernamental de coordinar, monitorear e implementar actividades de desclasificación gubernamentales, incluyendo la consolidación y la actualización periódica de directrices de relativas a la desclasificación.

(b) Se deben establecer procedimientos que permitan identificar la información clasificada que revista interés público, a fin de disponer su desclasificación con carácter prioritario. Si se ha clasificado información de interés público, incluida aquella comprendida en las categorías enumeradas en el Principio 10, debido a su carácter extremadamente sensible, deberá ser desclasificada tan pronto como sea posible.

(c) Se deben establecer en la legislación nacional procedimientos específicos para disponer la desclasificación en bloque (en lotes y/o muestras).

(d) Se deben identificar en la legislación nacional períodos preestablecidos para la desclasificación automática de distintas categorías de información clasificada. A fin de reducir al mínimo la carga que supone la desclasificación, cuando sea posible los registros deben ser desclasificados automáticamente sin previa revisión.

(e) Se debe establecer en la legislación nacional un procedimiento público y accesible para solicitar la desclasificación de documentos.

(f) Los documentos desclasificados, incluyendo aquellos desclasificados por jueces, tribunales u otros organismos de supervisión, defensoría del pueblo y apelación, deberían divulgarse en forma proactiva o bien ser puestos a disposición del público (por ejemplo, a través de la armonización con la legislación sobre archivos nacionales, acceso a la información, o ambas).

Notas: Este principio se entiende sin perjuicio de las disposiciones que tengan que ver con otros motivos para la clasificación, tal y cómo se expone en el párrafo preambular 15.

Entre otras buenas prácticas, se pueden mencionar:

- *la evaluación periódica del uso de nuevas tecnologías en los procesos de desclasificación y*
- *la consulta periódica a personas con experiencia profesional respecto al proceso para establecer las prioridades en materia de desclasificación, incluidas la desclasificación automática y en bloque.*

Parte III.B: Normas sobre gestión de solicitudes de información

Principio 18: Obligación de considerar las solicitudes incluso si la información tiene carácter clasificado

Que la información haya sido clasificada no es un factor decisivo al determinar cómo se debe responder a una solicitud de información. Por el contrario, la autoridad pública en cuyo poder se encuentra la información debe considerar la solicitud teniendo en cuenta los presentes Principios.

Principio 19: Obligación de confirmar o negar

(a) Al recibir una solicitud de información, la autoridad pública debe confirmar o negar que esta se encuentre en su poder.

(b) Si la jurisdicción permite la posibilidad de que, en circunstancias extraordinarias, la existencia o no de información específica pueda clasificarse de acuerdo con el Principio 3, entonces, cualquier renuencia a confirmar o negar la existencia de información en respuesta a una solicitud específica debe estar basada en la evidencia de que una mera confirmación o negación de la existencia de dicha información podría suponer un riesgo de perjuicio a una categoría de información distinta establecida en una ley o reglamentación nacional, en la cual se requiera ese trato excepcional.

Principio 20: Obligación de expresar los motivos de la negativa por escrito

(a) Si una autoridad pública niega una solicitud de información, en todo o en parte, debe hacer constar por escrito los motivos concretos de esta decisión, de acuerdo con los Principios 3 y 9, dentro del período de tiempo especificado por ley para la respuesta a las solicitudes de información.

Nota: Véase el Principio 25 sobre el requisito de establecer en ley el tiempo límite en que se debe dar contestación a una solicitud de información.

(b) La autoridad debe asimismo proporcionar al solicitante información suficiente acerca de la identidad del funcionario o funcionarios públicos que dispuso o dispusieron que la información tendría carácter clasificado, y el proceso de dicha disposición, a menos que esa identificación constituya por sí misma una divulgación de información clasificada, e indicar los medios de impugnación disponibles para permitir una evaluación del cumplimiento de la ley por parte de la autoridad.

Principio 21: Obligación de recuperar o reconstruir la información faltante

(a) Cuando una autoridad pública no pueda localizar la información necesaria para responder una solicitud, y los registros de dicha información deberían haber sido preservados, recopilados o elaborados la autoridad debe adoptar medidas razonables para recuperar o reconstruir la información faltante a fin de permitir su eventual entrega al solicitante.

Nota: este principio se aplica a la información que no puede ser localizada por cualquier razón, por ejemplo, porque nunca fue recolectada, fue destruida o no se puede rastrear.

(b) Debería solicitarse el que un representante de la autoridad pública indique, bajo juramento, y en un tiempo razonable y establecido por ley, todos los procedimientos llevados a cabo para la recuperación o reconstrucción de la información de manera que dichos procedimientos puedan ser judicialmente revisados.

Nota: Cuando no se pueda localizar un documento o información que, por ley, debería haber sido conservado, la cuestión deberá remitirse a las autoridades policiales o administrativas para que investiguen lo sucedido. El resultado de la investigación debe tener carácter público.

(c) La obligación de recuperar o reconstruir información es particularmente imperiosa (i) cuando ésta se vincula con presuntas violaciones graves o sistemáticas de los derechos humanos y/o (ii) durante una transición a una forma de gobierno democrática de un gobierno caracterizado por la violación generalizada de los derechos humanos.

Principio 22: Obligación de divulgar partes de documentos

Las excepciones a la divulgación se aplican únicamente a información específica y no a la totalidad de documentos u otros registros. Solamente podrá impedirse la divulgación de información específica cuando se haya demostrado la validez de la restricción ("información exenta"). Cuando un registro contenga a la vez información exenta y no exenta, las autoridades públicas tienen la obligación de separar y divulgar la información no exenta.

Principio 23: Obligación de identificar la información reservada

La autoridad pública que tenga en su poder información que se niegue a difundir, debe identificar dicha información con la mayor precisión posible. Como mínimo, la autoridad debe divulgar el volumen de información que se niegue a difundir, por ejemplo, ofreciendo una estimación del número de páginas.

Principio 24: Obligación de proporcionar información en formatos disponibles

Las autoridades públicas deben proporcionar la información en el formato que sea de preferencia del solicitante en la medida de lo posible.

Nota: Esto incluye, por ejemplo, la obligación de las autoridades públicas de tomar las medidas apropiadas para proporcionar información a personas con discapacidad en formatos y tecnologías accesibles de forma oportuna y sin un costo adicional, de acuerdo con la Convención de las Naciones Unidas para las Personas con Discapacidad.

Principio 25: Plazo para responder solicitudes de información

(a) Los plazos para responder a solicitudes, incluida la respuesta sobre aspectos de fondo, el control interno, las decisiones de organismos independientes cuando corresponda y la revisión judicial, deben ser establecidos en la legislación y deben ser tan breves como sea posible.

Nota: se considera como una buena práctica, conforme a los requisitos establecidos en la mayor parte de las leyes de acceso a la información, establecer veinte días laborales o menos como el período de tiempo en el que ha de darse una respuesta sustantiva. Cuando el plazo para responder a una solicitud no se establezca en ley, éste no debería ser mayor a 30 días para una solicitud estándar. Las leyes podrán establecer diferentes plazos para tomar en cuenta el volumen de documentos y su nivel de complejidad y sensibilidad.

(b) Deben aplicarse plazos abreviados cuando se demuestre que existe una necesidad urgente de acceder a la información, como por ejemplo, si se trata de información necesaria para preservar la vida o la libertad de una persona.

Principio 26: Derecho a recurrir las decisiones relativas a la clasificación de información

(a) El solicitante tiene derecho a interponer un recurso rápido y a bajo costo para que la negativa de proporcionar determinada información, o asuntos relacionados con la solicitud, sea revisada por una autoridad independiente.

Nota: Dicha negativa podría incluir un rechazo implícito o silencioso, y los asuntos sujetos a la revisión por parte de una autoridad independiente podrían incluir tarifas, plazos y formato.

(b) La autoridad independiente debe tener la competencia y recursos necesarios para garantizar una revisión efectiva, incluyendo pleno acceso a toda la información relevante, incluso si se trata de información clasificada.

(c) Cualquier persona debería tener derecho a obtener una revisión independiente y efectiva de todas las cuestiones relevantes por parte de un tribunal competente.

(d) Si un tribunal se pronuncia a favor de la clasificación de la información, debería publicar las razones, basadas en hechos, y su análisis legal por escrito, excepto en circunstancias extraordinarias y congruentes con el Principio 3.

Parte IV: Aspectos judiciales relativos a la seguridad nacional y al derecho a la información

Principio 27: Principio general de control judicial

(a) Nadie podrá invocar argumentos relativos a la seguridad nacional para menoscabar el derecho fundamental a un juicio justo por parte de un tribunal competente, independiente e imparcial establecido por ley.

(b) Cuando una autoridad pública pretenda clasificar información por razones de seguridad nacional en el marco de un procedimiento legal, los tribunales tendrán la potestad de revisar la información para determinar si debería tener carácter clasificado. Por norma general, un tribunal no podrá desestimar un caso sin revisar la información.

Nota: En consonancia con el Principio 4(d), el tribunal no adoptará su decisión sobre la base de resúmenes o declaraciones juradas donde simplemente se afirme la necesidad de confidencialidad sin que se proporcione una base probatoria para dicha afirmación.

(c) El tribunal debería asegurarse de que la persona que solicita acceder a la información pueda, en la mayor medida posible, conocer e impugnar el argumento invocado por el gobierno para no divulgar la información.

(d) El tribunal debe pronunciarse sobre la legalidad y procedencia del argumento invocado por la autoridad pública, , y podrá exigir que se difunda la información o que

se otorgue un resarcimiento adecuado en caso de que ésta no se divulgue en forma parcial o total, incluyendo la desestimación de cargos en procesos penales.

(e) El tribunal debe valorar en forma independiente si la autoridad pública ha invocado adecuadamente un motivo para no permitir la divulgación; la mera clasificación no podrá ser concluyente en cuanto a la solicitud de la no divulgación de una información. Asimismo, el tribunal debe evaluar la naturaleza del perjuicio referido por la autoridad pública, la probabilidad de que ocurra y el interés público en que se divulgue la información, de acuerdo con las normas definidas en el Principio 3.

Principio 28: Acceso público a procesos judiciales

(a) Nadie podrá invocar argumentos relativos a la seguridad nacional para menoscabar el derecho fundamental de acceso público a procesos judiciales.

(b) Las sentencias judiciales —en las cuales se establezcan todas las determinaciones de un tribunal y se incluyan las principales conclusiones, evidencias y fundamentos jurídicos— deben darse a conocer en forma pública, salvo cuando esto no sea conveniente para preservar el interés de niños menores de dieciocho años.

Notas: la legislación internacional no permite la derogación, por motivos de seguridad nacional, de la obligación de pronunciar sentencias públicamente.

Los registros de los procedimientos judiciales de menores no deberían publicarse. Los registros de otros procedimientos judiciales que involucren a niños deberían, normalmente, no divulgar los nombres y otra información que haga identificable a aquellos niños menores de dieciocho años.

(c) El derecho de la sociedad de acceso a la justicia debería incluir el acceso público inmediato a: (i) los fundamentos de las decisiones judiciales; (ii) información sobre la existencia y el progreso de los casos; (iii) argumentos escritos presentados ante el tribunal; (iv) audiencias y procedimientos judiciales; y (v) evidencias en procedimientos judiciales que constituyan el fundamento de una condena, a menos que se justifique una derogación de lo expuesto de conformidad con estos Principios.

Nota: El derecho internacional relativo a los requisitos de un juicio justo permite a los tribunales excluir a la totalidad o a parte del público de una audiencia por razones de seguridad nacional en una sociedad democrática, así como la moral, el orden público, el

interés de la vida privada de las partes o para evitar un perjuicio a los intereses de la justicia, siempre que dichas restricciones sean en todos los casos necesarias y proporcionadas.

(d) La sociedad debe tener la posibilidad de impugnar los argumentos invocados por la autoridad pública para justificar la estricta necesidad de restringir el acceso público a procesos judiciales por razones de seguridad nacional.

(e) Cuando un tribunal emita una decisión restringiendo el acceso público a procesos judiciales, debe informar públicamente y por escrito los hechos, razones y fundamentos legales en los que se base su decisión, excepto cuando se trate de circunstancias extraordinarias de acuerdo con el Principio 3.

Nota: Este Principio no pretende modificar la legislación vigente en un Estado sobre procedimientos preliminares a los cuales normalmente el público no tiene acceso. Su aplicación se prevé exclusivamente para casos en que el proceso judicial permitiría en general el acceso público y el intento por impedirlo se justifique invocando motivos de seguridad nacional.

El derecho de la sociedad de acceder a procedimientos y documentos judiciales surge de la importancia que reviste dicho acceso para fomentar (i) la imparcialidad real y percibida de los procedimientos judiciales; (ii) una actuación adecuada y más honesta de las partes; y (iii) una mayor precisión de los comentarios públicos.

Principio 29: Acceso de las partes a información en los procesos penales

(a) El tribunal no podrá prohibir que una persona acusada comparezca en su propio juicio por razones de seguridad nacional.

(b) En ningún caso la condena o privación de la libertad podrá dictarse sobre la base de pruebas que el acusado no ha tenido oportunidad de examinar e impugnar.

(c) En aras de la justicia, una autoridad pública deberá dar a conocer al acusado y a su defensa, los cargos contra una persona y cualquier información necesaria para garantizar un juicio justo, con independencia de si la información tiene carácter clasificado con arreglo a los Principios 3-6, 10, 27 y 28, incluyendo la consideración de los intereses públicos.

(d) Cuando la autoridad pública se niegue a difundir información necesaria para garantizar un juicio justo, el tribunal deberá suspender o desestimar la acusación.

Nota: Las autoridades públicas no deben usar información en provecho suyo cuando invoquen su carácter clasificado, no obstante podrán optar por que no se divulgue la información y afrontar las consecuencias.

Nota: Los principios 29 y 30 se incluyen en estos Principios en relación con el acceso público a la información a la luz del hecho de que, la revisión judicial y las divulgaciones relacionadas en el contexto de la supervisión judicial, son a menudo medios importantes para la divulgación pública de información.

Principio 30: Acceso de las partes a información en los procesos civiles

(a) Todas las impugnaciones relativas a la clasificación de información por parte de una autoridad pública en un caso civil habrán de revisarse de manera congruente con los Principios 3-6, 10, 27 y 28, incluyendo la consideración de los intereses públicos.

(b) Las víctimas de violaciones de los derechos humanos tienen derecho a un recurso y una reparación efectiva, incluida la difusión pública de los abusos sufridos. Las autoridades públicas no deben clasificar información que sea trascendental para las reclamaciones de las víctimas de un modo incompatible con este derecho.

(c) Además, la sociedad tiene también derecho a la información que tenga que ver con violaciones graves de los derechos humanos y violaciones graves del derecho internacional humanitario.

Parte V: Organismos que supervisan el sector de seguridad

Principio 31: Establecimiento de organismos de supervisión independientes

Los Estados deben establecer, cuando aún no lo hayan hecho, organismos de supervisión independientes encargados de supervisar a las entidades del sector de seguridad, incluyendo sus operaciones, normas, políticas, finanzas y administración. Estos organismos de supervisión deben ser institucional, operacional y financieramente independientes de las instituciones a las que han de supervisar.

Principio 32: Acceso irrestricto a información necesaria para el desempeño de la función

(a) Los organismos de supervisión independientes deben contar con acceso legalmente garantizado a toda la información necesaria para el desempeño de su función. No deben aplicarse restricciones a este acceso, con independencia del nivel de reserva o confidencialidad de la información, una vez cumplidos los requisitos razonables sobre seguridad de la consulta.

(b) La información a la cual deben tener acceso los organismos de supervisión incluye, sin carácter restrictivo:

(i) todos los registros, tecnologías y sistemas en poder de autoridades del sector de seguridad, con independencia de la forma o medio, y de si han sido o no creados por dicha autoridad;

(ii) sitios, objetos e instalaciones; e

(iii) información en posesión de personas a quienes los supervisores consideren relevantes para sus funciones de supervisión.

(c) Cualquier obligación que tenga el personal del sector de seguridad de preservar el carácter reservado o confidencial de información, no debería impedir que proporcionen información a las instituciones de supervisión. Proveer tal información no debería considerarse como un incumplimiento de la ley o del contrato aplicable donde se establezcan esas obligaciones.

Principio 33: Facultades, recursos y procedimientos necesarios para asegurar el acceso a información

(a) Los organismos de supervisión independientes deben contar con facultades jurídicas suficientes para poder consultar e interpretar información relevante que consideran necesaria para desempeñar sus funciones.

(i) Como mínimo, estas facultades deben incluir el derecho a interpelar a miembros actuales y anteriores del poder ejecutivo y empleados y contratistas de autoridades públicas, solicitar e inspeccionar los registros correspondientes e inspeccionar sitios e instalaciones.

(ii) Los organismos de supervisión independientes también deberían tener la potestad de citar a personas, requerir registros y recibir el testimonio, bajo juramento u otro tipo de declaración solemne, de personas que se considere que tienen en su poder información relevante para el desempeño de sus funciones, con la plena cooperación de organismos de aplicación de la ley, cuando resulte necesario.

(b) Los organismos de supervisión independientes, al gestionar la información y recibir testimonios, deben tener en cuenta, entre otras cosas, la leyes relevantes sobre privacidad, así como las garantías contra la autoincriminación y otros requisitos del debido proceso.

(c) Los organismos de supervisión independientes deben tener acceso a los recursos financieros, tecnológicos y humanos necesarios para que puedan identificar, consultar y analizar información relevante para el efectivo desempeño de sus funciones.

(d) Se debe exigir por ley a las instituciones del sector de seguridad que presten a los organismos de supervisión independientes la cooperación que éstos necesitan para consultar e interpretar la información indispensable para el desempeño de su función.

(e) Se debe exigir por ley a las instituciones del sector de seguridad que, en forma oportuna y proactiva, divulguen a los organismos de supervisión independientes categorías concretas de información que los supervisores hayan determinado como necesarias para desempeñar su función. Tal información deberá incluir, sin carácter restrictivo, posibles transgresiones de la ley y de los estándares de los derechos humanos.

Principio 34: Transparencia de los organismos de supervisión independientes

A. Aplicabilidad de las leyes sobre acceso a la información

Las leyes que regulan el ejercicio del derecho de la sociedad de acceso a la información en poder de autoridades públicas deben aplicarse a los organismos de supervisión del sector de seguridad.

B. Elaboración de informes

(1) Los órganos de supervisión deben estar legalmente obligados a elaborar informes periódicos y a hacerlos públicos. Dichos informes deben incluir, como mínimo, información sobre el propio órgano supervisor, incluidas sus funciones, integración, presupuesto, desempeño y actividades.

Nota: Estos informes deberían, además, incluir información acerca de las funciones, estructura, presupuesto y actividades generales de cualquier institución del sector de la seguridad que no divulgue por sí misma dicha información al público.

(2) Los organismos de supervisión independientes también deben proporcionar versiones públicas sobre sus investigaciones y estudios temáticos y casuísticos, y deben proporcionar la mayor cantidad de información posible sobre cuestiones de interés público, incluidas las áreas enumeradas en el Principio 10.

(3) Los organismos de supervisión independientes deberían, siempre que elaboren informes públicos, respetar los derechos de todas las personas implicadas, incluyendo su derecho a la privacidad.

(4) Los organismos de supervisión independientes deberían ofrecer a las instituciones supervisadas, la posibilidad de examinar, en forma oportuna, los informes que tengan previsto difundir, a fin de que puedan plantear inquietudes sobre la inclusión de contenidos que puedan ser clasificados. La decisión definitiva sobre qué contenidos serán difundidos corresponderá al propio organismo de supervisión.

C. Difusión y accesibilidad

(1) La normativa que da origen a los organismos de supervisión, incluidas sus funciones y facultades, debe estar a disposición del público y ser de fácil consulta.

(2) Los organismos de supervisión independientes deberían establecer mecanismos y medios para personas analfabetas, que hablen lenguas minoritarias o tengan alguna discapacidad visual o auditiva para que puedan acceder a información relativa a su labor.

(3) Los organismos de supervisión independientes deberían establecer una serie de mecanismos de libre acceso a través de los cuales el público, incluidas personas en sitios geográficos remotos, pueda ponerse en contacto con tales organismos y, en el caso de las entidades que gestionan denuncias, presentar denuncias o inquietudes.

(4) Los organismos de supervisión independientes deben contar con mecanismos que permitan mantener de manera efectiva la confidencialidad de las denuncias y el carácter anónimo del denunciante.

Principio 35: Medidas para la protección de información manejada por organismos de supervisión del sector de seguridad

(a) La ley debería exigir a los organismos de supervisión independientes que implementen todas las medidas necesarias para proteger la información que tengan en su poder.

(b) El poder legislativo debería tener la potestad de decidir si (i) los miembros de comisiones de supervisión legislativas, y (ii) los máximos responsables y los miembros de organismos de supervisión independientes de carácter extraparlamentario deben ser objeto de un control de seguridad antes de su nombramiento.

(c) Si se requiere un control de seguridad, debería realizarse (i) de forma oportuna, (ii) de acuerdo con los principios establecidos, (iii) sin sesgos políticos ni motivaciones, y (iv) siempre que sea posible, por parte de una institución que no esté sujeta a la supervisión por parte del organismo cuyo personal está siendo examinada.

(d) Con arreglo a lo dispuesto en los Principios enumerados en las Partes VI y VII, los miembros o el personal de los organismos de supervisión que difundan información reservada o confidencial por medios distintos a los mecanismos de presentación de informes habituales y establecidos legalmente para estos organismos, deberán cumplir los correspondientes procedimientos administrativos, civiles o penales.

Principio 36: Potestad del poder legislativo de difundir información

El poder legislativo debería tener la potestad de difundir cualquier información al público, incluso si se trata de información que el poder ejecutivo reclama clasificada por motivos de seguridad nacional, cuando lo considere pertinente en virtud de los procedimientos que establezca para ese fin.

Parte VI: Divulgaciones de interés público por parte del personal de organismos públicos

Principio 37: Tipos de irregularidades

Si un funcionario público divulga una información, independientemente de su clasificación, que dé cuenta de una irregularidad que corresponda a alguna de las siguientes categorías, se considerará como una "divulgación protegida" si cumple con las condiciones establecidas en los Principios 38-40. Una "divulgación protegida" puede referirse a irregularidades que hayan ocurrido, estén teniendo lugar o sea probable que ocurran.

(a) acciones criminales;

(b) violaciones de los derechos humanos;

(c) violaciones del derecho internacional humanitario;

(d) corrupción;

(e) riesgos para la salud y la seguridad pública;

(f) riesgos para el medioambiente;

(g) abuso de la función pública;

(h) errores judiciales;

(i) manejo indebido o desperdicio de recursos;

(j) represalias por la difusión de las anteriores categorías de irregularidades; y

(k) ocultamiento deliberado de asuntos comprendidos en alguna de las categorías anteriores.

Principio 38: Aspectos, motivación y pruebas para la difusión de información que evidencia una irregularidad

(a) La ley debería proteger de posibles represalias, tal y cómo se define en el Principio 41, al personal de organismos públicos que divulgue información que evidencia una irregularidad, con independencia de que ésta tenga carácter reservado o confidencial, siempre que, al momento de la divulgación:

(i) la persona que difunde la información haya tenido motivos razonables para suponer que ésta estaba relacionada con una de las categorías de irregularidades establecidas en el Principio 37; y

(ii) La divulgación cumpla con las condiciones establecidas en los Principios 38–40.

(b) La motivación para efectuar una divulgación protegida es irrelevante, salvo cuando se demuestre que la divulgación haya sido falsa a sabiendas.

(c) No se podrá exigir a una persona que efectúe una divulgación protegida que presente evidencias para sustentar su denuncia ni se le impondrá tampoco la carga de la prueba.

Principio 39: Procedimientos para efectuar y responder divulgaciones protegidas en el ámbito interno o a organismos de supervisión

A. Divulgaciones internas

Se debe exigir por ley a las autoridades públicas que establezcan procedimientos internos y designen a personas para recibir divulgaciones protegidas.

B. Divulgaciones a organismos de supervisión independientes

(1) Los Estados deberían también establecer o identificar organismos independientes que se encarguen de recibir e investigar divulgaciones protegidas. Estos organismos deben ser independientes en términos institucionales y operativos respecto del

sector de seguridad en su totalidad y de otras autoridades desde las cuales pudieran hacerse divulgaciones de información, incluido el poder ejecutivo.

(2) El personal público debería estar autorizado para llevar a cabo divulgaciones protegidas en forma directa a organismos de supervisión independientes o cualquier otra autoridad competente para que investiguen el caso, sin antes tener que efectuar la divulgación internamente.

(3) La ley debería garantizar que los organismos de supervisión independientes puedan acceder a toda la información relevante y brindarles todas las facultades de investigación necesarias para garantizar tal acceso. Tales facultades deberían incluir la facultad de citar a personas y exigir que se rinda testimonio bajo juramento u otro tipo de declaración solemne.

C. Obligaciones de los órganos internos y los organismos de supervisión independientes que reciben divulgaciones

Si una persona realiza una divulgación protegida, tal y cómo se define en el Principio 37, en el ámbito interno o a un organismo de supervisión independiente, el organismo que reciba la divulgación estará obligado a:

(1) investigar la supuesta irregularidad y tomar medidas oportunas para resolver el asunto en un período de tiempo especificado por ley, o, tras haber consultado con la persona que realizó la divulgación, referirla a un organismo autorizado y competente para llevar a cabo una investigación;
(2) proteger la identidad del personal público que desee proporcionar información de manera confidencial; la información proporcionada de forma anónima debería ser considerada con base en sus méritos;
(3) proteger la información divulgada y el hecho de que se ha realizado una divulgación excepto si una divulgación adicional fuera necesaria para remediar la irregularidad; y
(4) notificar a la persona que ha realizado la divulgación del progreso y la finalización de una investigación y, siempre que sea posible, los pasos que se han dado o las recomendaciones efectuadas.

Principio 40: Protección de las divulgaciones públicas

La legislación debe proteger de represalias, tal y cómo se define en el Principio 41, las divulgaciones al público de información que tenga que ver con irregularidades, tal y cómo se define en el Principio 37, si la divulgación cumple con los siguientes criterios:

(a) (1) la persona divulgó la misma, o prácticamente la misma información en el ámbito interno y al organismo de supervisión independiente y:

(i) el organismo al que se difundió la información se negó a investigar o no investigó eficazmente la divulgación, de conformidad con la normativa internacional aplicable; o

(ii) la persona no recibió un resultado razonable y apropiado dentro de un plazo razonable legalmente establecido.

O

(2) la persona consideró de forma razonable que la divulgación de forma interna o a un organismo de supervisión independiente implicaba un riesgo significativo de destrucción u ocultamiento de evidencia, interferencia con un testigo o toma de represalias en contra de la persona o un tercero;

O

(3) no existía un organismo interno ni un organismo de supervisión independiente establecido a quien divulgar la información;

O

(4) la divulgación estaba relacionada con un acto u omisión que constituía una amenaza seria e inminente a la vida, la salud y la seguridad de las personas, o del medio ambiente.

Y

(b) La persona que realizó la divulgación sólo divulgó la cantidad de información que era razonablemente necesaria para revelar una irregularidad;

Nota: Si en el proceso de divulgación de información que revele una irregularidad, la persona también da a conocer documentos que no son relevantes para demostrar la irregularidad, la persona deberá ser protegida de represalias en todo caso, a menos que el daño causado por la divulgación exceda cualquier interés público de la divulgación.

Y

(c) la persona que realizó la divulgación consideró de forma razonable que el interés público en conocer la información revelada compensaría cualquier perjuicio al interés público resultante de dicha divulgación.

Nota: La prueba que debería aplicarse al concepto "Considerar de forma razonable" es una prueba objetiva y subjetiva a la vez. La persona debe haber mantenido una creencia (subjetividad), y esa creencia debe haber sido razonable para él o para ella (objetividad). Si una impugnación tuviera lugar, la persona tendría que defender la racionalidad de su creencia, y, será en última instancia responsabilidad de un tribunal independiente la determinación de si esta prueba se ha satisfecho como para calificar la divulgación para su protección.

Principio 41: Protección frente a represalias por efectuar divulgaciones de información que evidencien irregularidades

A. Inmunidad contra responsabilidades civiles y penales por la realización de divulgaciones protegidas

De acuerdo con los principios 37–40, una persona que haya efectuado una divulgación no debería estar sujeto a:

(1) Procedimientos penales, incluidos, sin carácter restrictivo, las acciones penales por divulgación de información reservada o confidencial; o

(2) Procedimientos civiles relacionados con la divulgación de información reservada o confidencial, incluidos, sin carácter restrictivo, los recursos interpuestos para obtener una indemnización y causas por difamación;

B. Prohibición de otra clase de represalias

(1) La legislación debe prohibir las represalias tomadas contra una persona que haya efectuado, o se sospeche que haya efectuado, una divulgación de acuerdo con los Principios 37–40.

(2) Entre las medidas de represalia prohibidas se incluyen, sin carácter restrictivo:

(a) Medidas o sanciones administrativas incluidas, sin carácter restrictivo, cartas de amonestación, investigaciones en represalia, descenso de grado, transferencia, reasignación de funciones, negativa a otorgar ascensos, extinción de la relación laboral, acciones que pretendan dañar la reputación de una persona o suspensión o revocación de una autorización de seguridad;

(b) Daño o acoso físico o psicológico; o

(c) Amenazas de implementar alguna de las medidas anteriores.

(3) Las medidas contra personas distintas de quienes divulgaron la información podrían constituir represalias en determinadas circunstancias.

C. Investigación de las represalias por un organismo de supervisión independiente y autoridades judiciales

(1) Cualquier persona debería tener derecho a denunciar ante un organismo de supervisión independiente y/o ante una autoridad judicial cualquier represalia o amenaza de represalia en relación con una divulgación protegida.

(2) Los organismos de supervisión independientes deberían tener la obligación de investigar la denuncia de una represalia o amenaza de represalia. Dichos organismos deberían tener, además, la capacidad de iniciar investigaciones si no cuentan con una denuncia de represalias.

(3) Se debe dotar a los organismos de supervisión independientes de todas las facultades y recursos necesarios para investigar de forma efectiva cualquier represalia denunciada, incluyendo la facultad de citar a personas, consultar registros y escuchar testimonios bajo juramento u otro tipo de declaración solemne.

(4) Los organismos de supervisión independientes deberían esforzarse para garantizar que los procedimientos relativos a las represalias denunciadas son justos y de conformidad con los requisitos del debido proceso.

(5) Los organismos de supervisión independientes deberían tener la facultad para requerir a la autoridad pública de que se trate que tome medidas correctivas o

resarcitorias, incluidas, sin carácter restrictivo, la reincorporación; la reasignación; y/o el pago de los honorarios legales, otros costes razonables, cantidades pendientes y prestaciones relacionadas, gastos de desplazamiento, y/o indemnizaciones.

(6) Los organismos de supervisión independientes también deberían tener la facultad de prohibir que las autoridades públicas tomasen represalias.

(7) Dichos organismos deberían investigar las represalias denunciadas en un período de tiempo razonable y definido por ley.

(8) Dichos organismos deberían notificar a las personas relevantes al menos la finalización de la investigación, y siempre que sea posible, las medidas adoptadas o las recomendaciones realizadas.

(9) Las personas también deberían poder apelar una determinación de que las acciones en respuesta a la divulgación no constituyen una represalia, así como las medidas correctivas o resarcitorias de un organismo de supervisión independiente ante una autoridad judicial.

D. Carga de la prueba

Si una autoridad pública adopta medidas que sean adversas para cualquier persona, la autoridad tiene la carga de demostrar que tales medidas no estuvieron relacionadas con la divulgación.

E. Imposibilidad de renunciar a derechos y recursos

No se podrá limitar o renunciar a los derechos y recursos establecidos en los Principios 37–40, bajo ningún acuerdo, política, forma o condición laboral, ni por ningún acuerdo de arbitraje previo al conflicto. Cualquier intento de limitar o renunciar estos derechos y recursos se considerará nulo.

Principio 42: Fomentar y facilitar las divulgaciones protegidas

Los Estados deben alentar a los funcionarios públicos a efectuar divulgaciones protegidas. A fin de facilitar tales divulgaciones, los Estados deberían exigir que todas las autoridades públicas emitan lineamientos para la efectiva aplicación de los Principios 37 a 42.

Nota: Estos lineamientos deben proveer, como mínimo, (1) orientación respecto al derecho y/o la obligación de divulgar irregularidades, (2) los tipos de información que pueden o deben ser divulgados, (3) los procedimientos obligatorios para efectuar tales divulgaciones, y (4) las protecciones dispuestas por ley.

Principio 43: Defensa de interés público para el personal público

(a) Si el personal público fuere objeto de procedimientos penales o civiles, o sanciones administrativas en relación con la divulgación de una información no protegida bajo estos Principios, la ley le debería proporcionarle una defensa de interés público si el interés público en la divulgación de la información en cuestión supera el interés público en la no divulgación.

Nota: Este Principio se refiere a todas las divulgaciones de información que no están protegidas, ya sea porque el tipo de información no entra dentro de las categorías señaladas en el Principio 37, o bien porque la divulgación contiene información que entra dentro de las categorías señaladas en el Principio 37 pero no fue efectuada de acuerdo con los procedimientos señalados en los Principios 38-40.

(b) Al decidir si el interés público en la divulgación supera al interés público en la no divulgación, las autoridades fiscales y judiciales deberán considerar:

(i) si el alcance de la divulgación era razonablemente necesario para divulgar la información de interés público;

(ii) la extensión y riesgo de perjuicio al interés público causado por la divulgación;

(iii) si la persona tuvo motivos razonables para suponer que la divulgación redundaría en beneficio del interés público;

(iv) si la persona trató de efectuar la divulgación protegida a través de procedimientos internos y/o a un organismo de supervisión independiente, y/o al público con arreglo a los procedimientos estipulados en los Principios 38-40; y

(v) la existencia de circunstancias imperiosas que justifiquen la divulgación.

Nota: Cualquier ley que establezca sanciones penales para la divulgación no autorizada de información debería ser coherente con el Principio 46(b). Este Principio no pretende limitar los derechos de libertad de expresión que ya corresponden al personal público ni ninguna de las protecciones otorgadas bajo los Principios 37–42 o 46.

Parte VII: Límites a las medidas destinadas a sancionar o restringir la divulgación de información al público

Principio 44: Protección contra sanciones a divulgaciones razonables efectuadas de buena fe por funcionarios que manejan información

Las personas responsables de responder a solicitudes de información presentadas por el público no deberían ser sancionadas por divulgar información cuando hayan actuado de buena fe y creído razonablemente que la información podía ser difundida legalmente.

Principio 45: Sanciones para el supuesto de destrucción o negativa a difundir información

(a) El personal público será susceptible de sanciones cuando destruya o altere deliberadamente información con el propósito de impedir que pueda ser consultada por el público.

(b) Cuando un tribunal u organismo independiente haya dado instrucciones de que se divulgue cierta información y ésta no se difunda en un plazo razonable, el fun-

cionario y/o la autoridad pública responsable de que no se produzca la divulgación serán sujetos de las sanciones correspondientes, a menos que se interponga un recurso de apelación de conformidad con los procedimientos establecidos legalmente.

Principio 46: Limitaciones en las sanciones penales por la divulgación de información realizada por personal público

(a) La divulgación de información efectuada por personal público, incluso si dicha información no está protegida por la Parte VI, no debería ser objeto de sanciones penales, aunque sí podría serlo de sanciones administrativas tales como la revocación de una autorización de seguridad o incluso la extinción de la relación laboral.

(b) Si la ley, no obstante, impone sanciones penales por la divulgación no autorizada de información al público o a personas con la intención de que dicha información se haga pública, se aplicarán las siguientes condiciones:

(i) Se aplicarán sanciones penales sólo a la divulgación de categorías estrechas de información claramente establecidas por la ley.

Nota: si la legislación nacional establece categorías de información cuya divulgación puede ser objeto de sanciones penales, habrán de ser similares a las siguientes en cuanto a especificidad e impacto en la seguridad nacional: datos tecnológicos sobre armas nucleares; fuentes de inteligencia, códigos y métodos; códigos diplomáticos; identidades de agentes encubiertos; y propiedad intelectual en la que el gobierno tenga un interés de propiedad, además de conocimientos que pudieran perjudicar a la seguridad nacional.

(ii) La divulgación debería constituir un riesgo real e identificable de perjuicio significativo;

(iii) Cualquier sanción criminal, tal y como se establece en la legislación y se aplica, debería ser proporcional al perjuicio causado; y

(iv) La persona debería poder apelar a la defensa de interés público, tal y cómo se señala en el Principio 43.

Principio 47: Protección contra las sanciones por la posesión y diseminación de información clasificada por parte de personas que no trabajen en organismos públicos

(a) Una persona que no sea un funcionario público no puede ser sancionada por la recepción, posesión o divulgación de información clasificada.

(b) Una persona que no sea un funcionario público no puede ser objeto de cargos por conspiración u otros delitos basados en el hecho de que ha buscado y obtenido la información.

Notas: Este Principio trata de evitar el procesamiento criminal por la adquisición o reproducción de la información. Sin embargo, este Principio no pretende impedir el procesamiento de una persona por otros delitos cometidos, como robo o extorsión, cometidos con el objeto de obtener la información.

Las divulgaciones de terceras partes constituyen una importante medida correctiva para la clasificación excesiva generalizada.

Principio 48: Protección de las fuentes

Ninguna persona que no sea funcionario público debería ser obligada a revelar una fuente confidencial o materiales no publicados en el marco de una investigación sobre la divulgación no autorizada de información a la prensa o al público.

Nota: Este Principio hace referencia exclusivamente a investigaciones relativas a la divulgación no autorizada de información, y no a otros delitos.

Principio 49: Restricción previa

(a) Debe prohibirse la aplicación de restricciones previas a la publicación, efectuadas para proteger la seguridad nacional.

Nota: Las restricciones previas son órdenes dictadas por autoridades judiciales u otros organismos estatales en las cuales se prohíbe la publicación de determinados materiales que se encuentran en posesión de una personal que no es un funcionario público.

(b) Si la información se ha puesto ampliamente a disposición del público por cualquier medio, ya sea lícito o ilícito, se presumirá inválida cualquier medida destinada a impedir que continúe su difusión por el medio a través del cual ya ha tomado conocimiento público.

Nota: "Ampliamente a disposición" significa que la información ha sido difundida de manera suficiente y que no existe la posibilidad de tomar medidas prácticas para preservar su confidencialidad.

Parte VIII: Principio final

Principio 50: Relación de estos Principios con otras normas

No se interpretará que lo establecido en estos Principios restringe o limita algún derecho a la información reconocido por las leyes o estándares internacionales, regionales o nacionales, ni tampoco alguna de las disposiciones del derecho nacional o internacional que otorguen una protección más amplia a la divulgación de información efectuada por personal público u otras personas.

Anexo: Organizaciones asociadas

Las siguientes 22 organizaciones contribuyeron significativamente a la redacción de los Principios, y se encuentran comprometidas a trabajar en su diseminación y publicidad, además de ayudar en su implementación.[2] Tras el nombre de cada organización consta la ciudad en la que tiene su sede, si procede, y el país o región en la cual trabaja. Aquellas organizaciones que desarrollan trabajo sustancial en tres o más regiones han sido denominadas como "global."

- Africa Freedom of Information Centre (AFIC) (Kampala/África);
- African Policing Civilian Oversight Forum (APCOF) (Ciudad del Cabo/África);
- Alianza Regional por la Libre Expresión e Información (Américas);
- Amnistía Internacional (Londres/global);
- Artículo 19, Campaña Mundial para la Libertad de Expresión (Londres/global);
- Asian Forum for Human Rights and Development (Forum Asia) (Bangkok/Asia);
- Center for National Security Studies (CNSS) (Washington DC/Estados Unidos);
- Universidad Central Europea (Budapest/ Europa);
- Centre for Applied Legal Studies (CALS), Universidad de Witwatersrand (Johannesburgo/Sudáfrica);

2. Adicionalmente, Aidan Wills y Benjamin Buckland, del Centro de Ginebra para el Control de las Fuerzas Armadas, (DCAF) quienes no están afiliados con ninguna de las organizaciones mencionadas aquí, efectuaron contribuciones significativas a la Parte V: Organismos que supervisan el sector de seguridad, a la Parte VI: Divulgaciones de interés público, y a la creación de los Principios en su totalidad.

- Centre for European Constitutionalization and Security (CECS), Universidad de Copenhague (Copenhague/Europa);
- Centro de Derechos Humanos, Universidad de Pretoria (Pretoria/África);
- Centre for Law and Democracy (Halifax/global);
- Centre for Peace and Development Initiatives (CPDI) (Islamabad/Pakistán);
- Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Facultad de Derecho de Palermo (Buenos Aires/Argentina);
- Commonwealth Human Rights Initiative (CHRI) (Nueva Delhi/Commonwealth);
- Egyptian Initiative for Personal Rights (EIPR) (El Cairo/Egipto);
- Institute for Defence, Security and Peace Studies (Jakarta/Indonesia);
- Institute for Security Studies (ISS) (Pretoria/África);
- Comisión Internacional de Juristas (CIJ) (Ginebra/global);
- National Security Archive (Washington DC/global);
- Open Democracy Advice Centre (ODAC) (Ciudad del Cabo/África del Sur); y
- Open Society Justice Initiative (OSJI) (Nueva York/global).

"Los Principios representan una contribución importante al derecho de acceso a la información y al derecho a la verdad en relación con violaciones de los derechos humanos, y creo que deberían ser adoptados por el Consejo de Derechos Humanos. Todos los estados deberían reflejar estos Principios en sus interpretaciones de la ley de seguridad nacional."

***Frank La Rue**, Relator Especial de Naciones Unidas sobre libertad de opinión y expresión*

"La Relatoría acoge con satisfacción los Principios Tshwane ya que proponen un equilibrio correcto para asegurar la capacidad del estado de proteger la seguridad y las libertades personales."

***Catalina Botero**, Relatora Especial para la libertad de expresión de la Organización de los Estados Americanos*

"Estos Principios no podrían haber llegado en un momento más oportuno."

***Pansy Tlakula**, Relatora Especial sobre libertad de expresión y acceso a la información de la Comisión Africana de los Derechos Humanos y de los Pueblos*

"La Asamblea apoya los Principios Globales y apela a las autoridades competentes de todos los estados miembros del Consejo de Europa para que los tomen en cuenta en sus procesos de modernización de su legislación y prácticas de acceso a la información."

Resolución de la Asamblea Parlamentaria del Consejo de Europa, 2 octubre, 2013