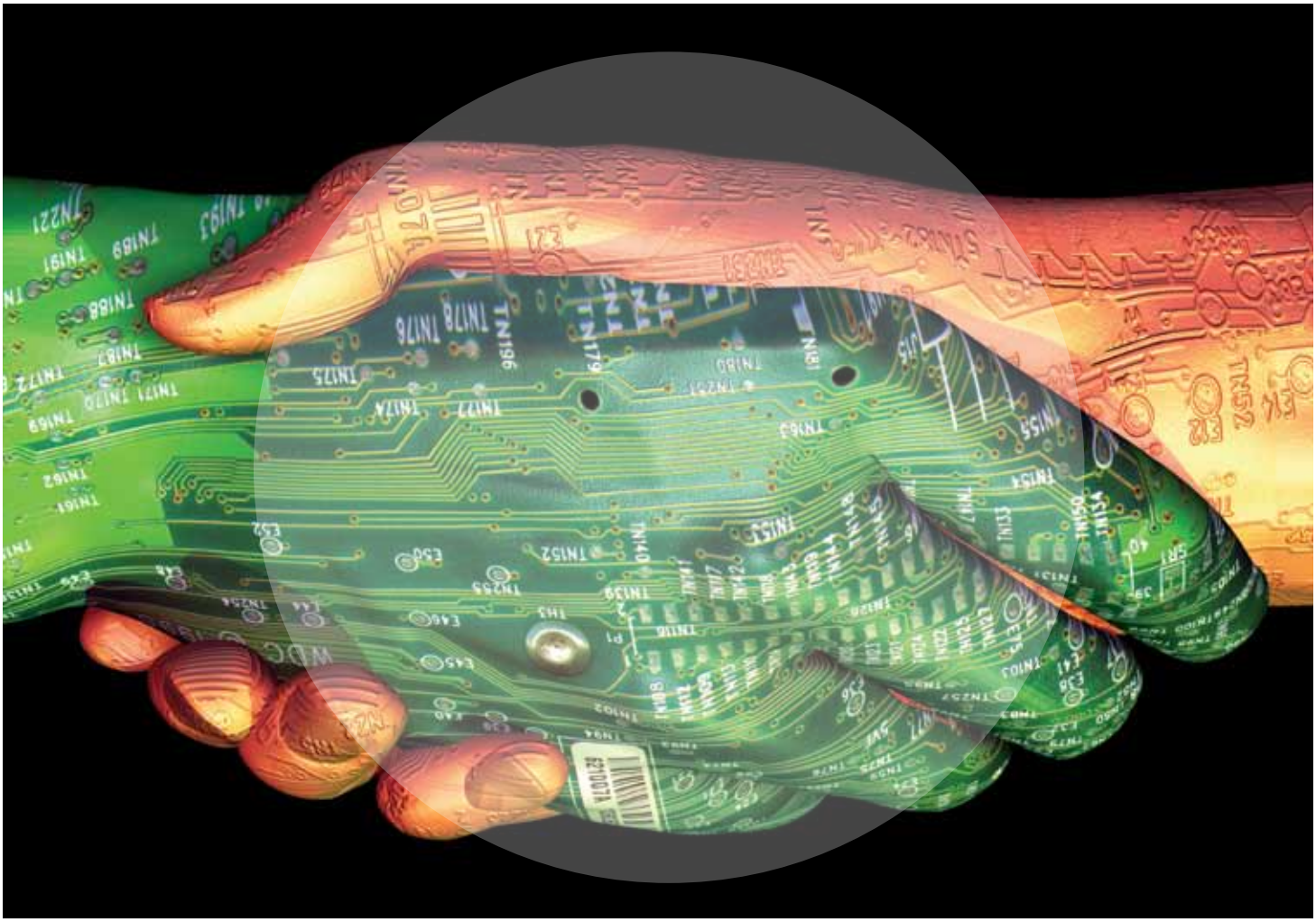
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Asociación por la resiliencia cibernética

Riesgo y responsabilidad en un mundo hiperconectado: principios y directrices

Marzo de 2012



Este documento se ha elaborado en colaboración con múltiples asociados. Los autores agradecen especialmente la participación de los asesores de proyecto de Deloitte.

REF.: 230312

Índice

Introducción

El Foro Económico Mundial es consciente de que los riesgos, las recompensas y la gobernanza de la economía interconectada constituyen cuestiones esenciales de la agenda global, fundamentales para el crecimiento sustentable y la estabilidad. Asimismo, es consciente de que el único modo de garantizar el pleno aprovechamiento de las nuevas oportunidades de crecimiento, así como la gestión de los riesgos, es adoptar un enfoque coordinado.

Durante 2011, el Foro Económico Mundial elaboró un proyecto multilateral destinado a identificar y abordar los riesgos sistémicos globales derivados de la conectividad, cada vez mayor, entre las personas, los procesos y los objetos. Unas sencillas observaciones sobre este entorno, que evoluciona a un ritmo acelerado, pueden ayudarnos a formular una respuesta apropiada.

- La dependencia cada vez mayor de la conectividad para el funcionamiento normal de la sociedad hace que la protección de la conectividad sea una cuestión crítica para todos; al tratarse de un recurso compartido como lo son el aire limpio o el agua, el reto se define como un reto de interdependencia.
  - Ninguna organización puede resolver esta cuestión por sí sola, y debe adoptarse un enfoque multilateral de colaboración; incluso los competidores de un mismo sector deben convertirse en asociados en un intento por garantizar un entorno estable y de confianza.

- El panorama del riesgo cibernético evoluciona a un ritmo acelerado: las estrategias defensivas nos llevan siempre a librar la última batalla, y existen numerosas "incógnitas desconocidas".
  - Las soluciones que se centran en aspectos específicos pronto quedarán obsoletas; es necesario un enfoque basado en principios.

- La libre circulación de información debe seguir impulsando el valor económico; una economía aislada es una economía congelada.
  - El objetivo es la resiliencia, no la intensificación del aislamiento; sabiendo que se van a producir fallos, el objetivo consiste en restablecer las operaciones habituales y garantizar la protección de los activos y de la reputación.

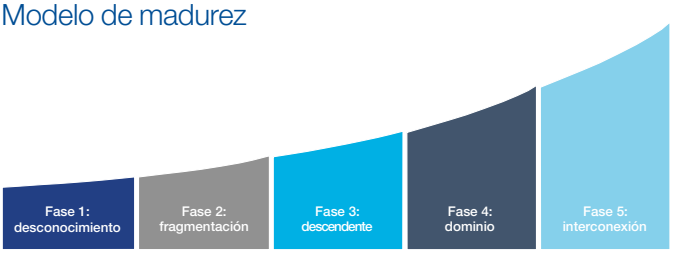
- La principal vulnerabilidad de numerosas organizaciones es de carácter humano: concienciación, liderazgo y ejecución.
  - La función de los líderes consiste en fijar la estructura y marcar la pauta; el perfil de riesgo de una organización puede mejorar sustancialmente mediante la aplicación de prácticas sencillas.

Así, el objetivo de esta iniciativa consiste en alcanzar un compromiso con respecto a un conjunto común de principios compartidos en materia de liderazgo: cambiar la mentalidad para dejar de limitarse a asegurar las fronteras e incluir también la atención a la interdependencia y a la resiliencia.

Estos principios están dirigidos a todas las organizaciones, independientemente de su industria, sector, jurisdicción, geografía o nivel de experiencia actual. No se pretende que sean prescriptivos, pues existirán diferencias de contexto. Están basados en buenas prácticas organizativas sencillas y en el reconocimiento del carácter repartido del reto.

Los principios se sustentan en un conjunto de directrices que pueden consultar las organizaciones para formular sus propias respuestas. Asimismo, se ofrece un sencillo modelo de madurez y una definición de términos a modo de referencia común.

Figura 1: modelo de madurez para la resiliencia cibernética organizativa



1. Compromiso con la resiliencia cibernética

Los abajo firmantes apoyamos la iniciativa y los principios multisectoriales, multinacionales y multilaterales para mejorar la resiliencia sistémica ante los riesgos cibernéticos.

Con la adopción generalizada de estos principios se pretende ayudar a elevar las normas empresariales asociadas a los sistemas de información hiperconectados de todo el mundo y contribuir a los objetivos compartidos de prosperidad y estabilidad económica.

Reconocemos colectivamente la interdependencia de las organizaciones del sector público y el sector privado en el entorno global hiperconectado. Así, reconocemos que contribuimos a los niveles globales de mitigación del riesgo cibernético a escala nacional y global.

Apoyamos los principios para la resiliencia cibernética (en lo sucesivo, los "Principios"), que se derivan del diálogo multilateral celebrado ente múltiples regiones y sectores. Los Principios (que se detallan ut infra) son los siguientes:

1. Reconocimiento de la interdependencia: todas las partes han de contribuir al fomento de un espacio digital compartido resiliente.

2. Función de los líderes: promover la concienciación a nivel ejecutivo y el liderazgo en materia de gestión del riesgo cibernético.

3. Gestión integrada del riesgo: elaborar un programa de ejecución práctico y eficaz.

4. Promoción de la aceptación: cuando proceda, instar a los proveedores y a los clientes a que adquieran un nivel de concienciación y compromiso similar.

Con la firma del presente documento nos comprometemos con estos Principios en apoyo de la creación y el mantenimiento de un entorno en línea resiliente y una red de entidades que confían entre sí.

En fe de lo cual apoyamos esta iniciativa e instamos al apoyo generalizado de la misma.

Nombre (en letras mayúsculas):

Cargo:

Empresa:

Fecha:

Firma:

2. Principios de la resiliencia cibernética

2.1. La organización es consciente del carácter interdependiente de nuestro mundo hiperconectado y de la función que ella misma ha de desempeñar para contribuir a la consecución de un entorno digital compartido seguro.

Nuestra fuerza está supeditada a la fuerza del eslabón más débil de las cadenas de las que todos dependemos; todos contribuimos a la seguridad de nuestro mundo hiperconectado. Un espacio en línea abierto, seguro y resiliente es un bien público; todos los agentes comparten la responsabilidad de crear y respaldar este recurso.

2.2. El equipo de dirección ejecutiva es consciente de su función de liderazgo a la hora de marcar la pauta y fijar la estructura de la resiliencia cibernética.

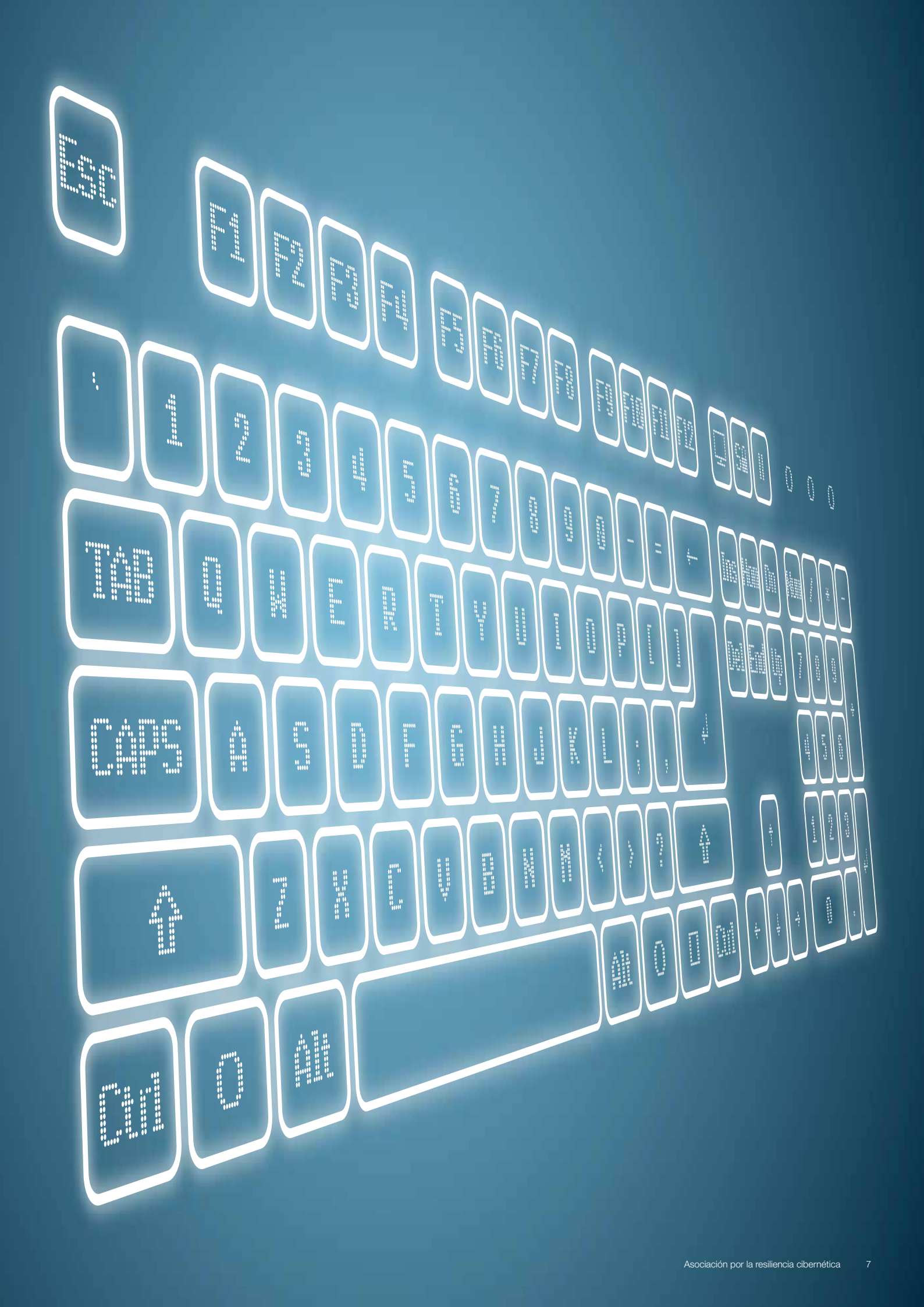
En consonancia con sus obligaciones fiduciarias y demás obligaciones en materia de liderazgo, la directiva ejecutiva reconoce la importancia de mitigar los riesgos relacionados con el mundo cibernético como elemento esencial para la continuidad de la viabilidad y el éxito de su institución, salvaguardando su propiedad intelectual y protegiendo la información que posee con el fin de proporcionar productos o servicios a su base de grupos constitutivos y clientes, de conformidad con la legislación sectorial y jurisdiccional pertinente.

2.3 La organización es consciente de la importancia de integrar la gestión del riesgo cibernético en sus prácticas más generalizadas de gestión del riesgo y en consonancia con estos Principios y directrices.

En consonancia con las buenas y homogéneas prácticas de información sectoriales o jurisdiccionales actualmente o próximamente en vigor, la entidad deberá aplicar constantemente un programa específico dirigido a la gestión de los riesgos cibernéticos conocidos que pueda tomar en consideración la orientación y los estándares relevantes para los sectores y regiones en los que opere. De este modo, reduce el riesgo de sufrir daños, contribuye positivamente a la resiliencia de los entornos de información conectados en los que opera y demuestra su civismo (corporativo).

2.4 La organización insta a sus proveedores a adoptar estos Principios y directrices.

Consciente de que la adopción generalizada de estos Principios contribuye a la continuidad y al aumento de las posibilidades de que todas las partes interesadas puedan beneficiarse de la hiperconectividad, así como a asegurar con mayor eficacia las cadenas de suministro y a gestionar la interdependencia y la vulnerabilidad inherentes a dicha conectividad, la organización deberá aprovechar sus relaciones para instar a otros a que adopten los Principios.



3. Directrices de la resiliencia cibernética: elaboración del Programa

En esta sección se define un conjunto de capacidades que todas las empresas deberían aspirar a poseer, como mínimo, cuando apliquen su propio programa de gestión del riesgo cibernético (en lo sucesivo, el "Programa"). Los elementos que se enumeran a continuación se ofrecen a modo de orientación no prescriptiva con respecto a las capacidades que debería incluir este Programas para ser eficaz, y pueden, asimismo, describir prácticas que ya se apliquen. Los estándares, procesos y requisitos legales concretos variarán en función de la industria y la jurisdicción y pueden sufrir modificaciones con el paso del tiempo. Los ejemplos específicos de un Programa relevante estarán informados por dicho contexto.

3.1 Supuestos de partida

3.1.1 La interdependencia de todas las organizaciones del entorno en línea ofrece un supuesto de base para la totalidad de la gestión del riesgo cibernético.

3.1.2 La mejora de las prácticas de gestión del riesgo cibernético en el seno de una organización contribuye a la resiliencia cibernética global.

3.1.3 Un enfoque basado en el riesgo constituye un enfoque eficaz para abordar las amenazas cibernéticas.

3.1.4 Reconociéndose que ningún sistema complejo permite una mitigación completa (100%) del riesgo, el objetivo global de un enfoque basado en el riesgo con respecto a la seguridad cibernética es la resiliencia del sistema: su supervivencia y rápida recuperación tras un ataque o accidente.

3.2 Gobernanza: liderazgo y pauta

3.2.1 El equipo de dirección ejecutiva es el encargado de supervisar la elaboración y la ejecución de un programa eficaz de mejores prácticas para la gestión del riesgo cibernético en el marco de sus actividades más generalizadas de gestión del riesgo.

3.2.1.1 El Programa deberá basarse en los Principios y demás prioridades relevantes de la compañía, y el equipo de dirección ejecutiva deberá proporcionar el liderazgo, los recursos y el apoyo activo necesarios para la ejecución del Programa.

3.2.1.2 El equipo de dirección ejecutiva se asegura de que se realice una revisión interna de la eficacia del Programa y de que, si se identifican carencias, se adopten medidas correctivas.

3.2.2 El Director General (o equivalente) y el equipo de dirección ejecutiva demuestran un compromiso visible y activo con respecto a la aplicación de los Principios.

3.2.3 El Director General (o equivalente) es responsable, en última instancia, de que el Programa se ejecute de forma coherente con unas líneas claras de autoridad, rendición de cuentas, delegación y responsabilidad.

3.2.4 A los ejecutivos y los directores se les otorgan las herramientas y la autoridad necesarias para fomentar la resiliencia y mitigar los riesgos cibernéticos susceptibles de incidir y/u originarse en sus respectivas líneas de negocio y, en cualquier caso, para ejercer sus responsabilidades con respecto a la organización de forma coherente con los Principios.

3.2.5 El Director General (o equivalente) posee un plan y una trayectoria decisoria claros en materia de actuación y comunicación en caso de que se produzca un fallo significativo de los sistemas de información interconectados proporcionados o utilizados por la organización.

3.3 Ejecución del Programa: componentes operativos críticos

3.3.1 Los conceptos y los elementos del Programa están integrados en el programa global de gestión de riesgos de la empresa cuando procede.

3.3.2 El Programa incluye un mecanismo para evaluar y hacer un seguimiento del riesgo cibernético.

3.3.2.1 El Programa forma parte de las prácticas vigentes de gestión de riesgos de la organización e incluye políticas destinadas a identificar, evaluar, medir, establecer prioridades entre, hacer un seguimiento de, mitigar y transferir el riesgo cibernético, mediante la aplicación, en la medida de lo posible, de mejores prácticas o directrices.

3.3.2.2 El Programa incluye evaluaciones internas del impacto sobre las operaciones, los activos y la reputación tanto en términos cualitativos como cuantitativos (financieros).

3.3.2.3 El Programa incluye estrategias específicas con las que se pretende reducir el promedio de tiempo necesario para la recuperación (es decir, mejorar la resiliencia) en caso de grandes ataques o fallos.

3.3.2.4 La organización hace un seguimiento de la eficacia de la mejora de la resiliencia cibernética y de la reducción del riesgo cibernético.

3.3.2.5 Cada cierto tiempo, la organización evalúa y asegura la asignación de los recursos para que sean adecuados a su estrategia de gestión de riesgos.

3.3.3 La organización verifica interna y periódicamente su cumplimiento con las reglas y reglamentos pertinentes y relevantes para su exposición al riesgo cibernético.

3.3.4 Las prácticas y las políticas de la organización incorporan y reflejan su compromiso con respecto a la mejora de la resiliencia cibernética y la reducción del riesgo.

3.4. Proveedores y terceros

3.4.1 La organización se asegura de que las partes que no estén directamente sujetas a las políticas internas de la compañía —pero cuya conducta fidedigna, incluida la de sus proveedores y terceras partes relevantes, se pueda establecer por contrato— respetan las normas específicas de gestión del riesgo cibernético o las mejores prácticas del sector en consonancia con los Principios, y formalizan este requisito mediante las citadas obligaciones contractuales.

3.4.2 Cuando proceda, los contratistas y los proveedores deberán recibir formación sobre el Programa.

4. Lista de comprobación para los puestos de dirección ejecutiva

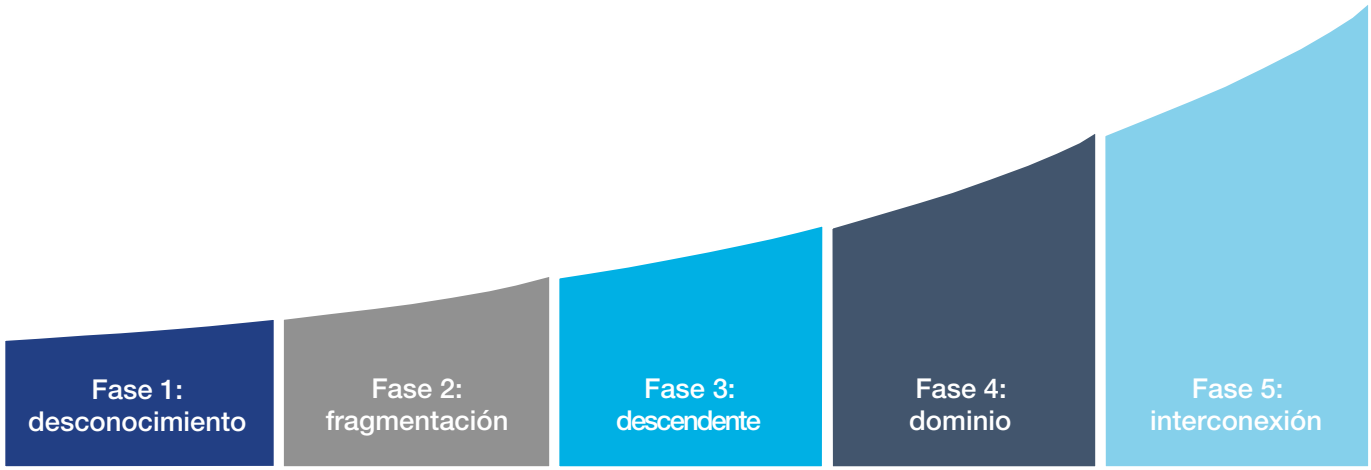
En esta sección se ofrece una sencilla herramienta de comprobación para que los directores generales y otros miembros de la dirección ejecutiva ayuden a orientar la revisión interna de las capacidades de resiliencia cibernética de su organización.

Con esta herramienta se pretende ofrecer a los ejecutivos información de carácter general y específico que les ayudará a informar sus acciones para la organización. Ofrece una puntuación compuesta aproximada para situar a la organización en una "curva de preparación para la hiperconexión" tal y como se indica a continuación. Las preguntas formuladas en la herramienta también pueden ayudar a los ejecutivos a identificar los puntos fuertes y los puntos débiles específicos, así como vías de mejora en el seno de su respectiva organización.

Nota: debido a la subjetividad de la evaluación entre las distintas entidades, y a que actualmente no existe ninguna métrica para ninguna de las variables mencionadas ut infra, la comparación no se ha diseñado para detectar las diferencias existentes entre el Programa de una y otra entidad, ni la conformidad de un Programa concreto con respecto a unas normas o reglas externas.

		1: No describe en absoluto a mi organización				5: Describe con precisión mi organización
Gobernanza						
1.	El Director General y el equipo de dirección ejecutiva son responsables de supervisar la elaboración de un programa de mejores prácticas para la gestión del riesgo cibernético, y de confirmar la ejecución del mismo.	1	2	3	4	5
2.	El Director General y el equipo de dirección ejecutiva se aseguran de que se revise la eficacia del programa y de que, si se identifican carencias, se apliquen medidas correctivas.	1	2	3	4	5
3.	El Director General y el equipo de dirección ejecutiva demuestran un compromiso visible y activo con respecto a la aplicación de los Principios.	1	2	3	4	5
4.	Los ejecutivos y los directores son responsables de comprender, en el nivel adecuado, cuál puede ser el impacto de los riesgos cibernéticos y cómo pueden generarse en su línea de negocio.	1	2	3	4	5
5.	La alta dirección comprende quién es responsable de gestionar el riesgo cibernético cuando se gestionan los incidentes de seguridad.	1	2	3	4	5
6.	La organización tiene acceso a expertos en materia cibernética en sus más altos niveles de gestión.	1	2	3	4	5
7.	La organización se compromete con la mejora continua de la integración de su gestión del riesgo cibernético con el resto de sus iniciativas de gestión de riesgos.	1	2	3	4	5
8.	El Director General (o equivalente) tiene una trayectoria decisoria clara en materia de actuación y comunicación en respuesta a un accidente o fallo de seguridad significativos.	1	2	3	4	5
Programa						
9.	La organización realiza evaluaciones exhaustivas de sus vulnerabilidades con respecto a riesgos cibernéticos internos y externos acordes con su industria y sector.	1	2	3	4	5
10.	La organización hace un seguimiento de la eficacia de su estrategia de gestión del riesgo cibernético.	1	2	3	4	5
11.	La organización verifica periódica e internamente su cumplimiento con las reglas y los reglamentos.	1	2	3	4	5
12.	El compromiso de la organización con el Programa se refleja en sus políticas y prácticas.	1	2	3	4	5
13.	Los directores, los empleados y los agentes reciben formación específica sobre el Programa, adaptada a las necesidades y circunstancias pertinentes.	1	2	3	4	5
14.	La organización ha identificado sus datos y su información como activos esenciales y organiza su Programa en torno al reconocimiento de que los datos y la información poseen un valor que puede reconocerse y protegerse de forma independiente.	1	2	3	4	5
15.	El Programa de gestión del riesgo incluye todas las relaciones materiales con terceros y los flujos de información.	1	2	3	4	5
16.	La organización realiza evaluaciones internas y exhaustivas sobre el impacto de los riesgos cibernéticos a corto y largo plazo.	1	2	3	4	5
Red						
17.	La organización busca garantizar que sus proveedores y terceras partes relevantes cumplan las normas de gestión del riesgo cibernético específicas de la organización o las mejores prácticas de la industria, en consonancia con los Principios, y formaliza este requisito mediante obligaciones contractuales.	1	2	3	4	5
18.	La organización ha forjado relaciones con sus homólogos y sus socios para gestionar conjuntamente el riesgo cibernético y abordar con mayor eficacia los incidentes cibernéticos.	1	2	3	4	5
19.	El Programa de gestión del riesgo incluye todas las relaciones materiales con terceros y los flujos de información.	1	2	3	4	5
Promedio (indica la fase de madurez)						

Modelo de madurez



Para la organización, el riesgo cibernético es muy poco relevante y no forma parte de su proceso de gestión del riesgo. La organización no conoce su nivel de interconexión.

La organización reconoce la hiperconectividad como un foco potencial de riesgo y posee una percepción limitada de sus prácticas de gestión del riesgo cibernético. La organización aplica un enfoque independiente con respecto al riesgo cibernético, con una presentación de información fragmentada y casual.

El Director General ha marcado las pautas con respecto a la gestión del riesgo cibernético y ha iniciado un programa de carácter descendente de amenaza-riesgo-respuesta, pero no considera la gestión del riesgo cibernético una ventaja competitiva.

La dirección de la organización asume la plena rendición de cuentas con respecto a la gestión del riesgo cibernético, ha formulado políticas y marcos y ha definido responsabilidades y mecanismos para la presentación de información. Comprende las vulnerabilidades de la organización, sus controles y sus interdependencias con terceras partes.

Las organizaciones están altamente conectadas con sus homólogas y sus socios, comparten información y mitigan conjuntamente el riesgo cibernético como parte de sus operaciones rutinarias. Sus empleados demuestran una conciencia cibernética excepcional y la organización es un líder industrial en términos de gestión del riesgo cibernético.

5. Elaboración del Programa: alcance y definiciones

Esta iniciativa adopta un enfoque del tipo "actuación local, mentalidad global". Se centra en la mejora de la resiliencia cibernética local de organizaciones independientes. Mediante la coordinación de unos principios comunes, estas acciones locales generan beneficios globales. Los principios comunes impulsan la eficacia de las acciones de cada organización en pos de la creación de una comunidad unida de resiliencia cibernética.

Las diferencias en cuanto a la interpretación del alcance y los términos que definen el problema constituyen un obstáculo crítico para la interpretación común y para resolver cualquier reto. En esta sección se ofrecen una serie de definiciones y se describen algunos de los términos utilizados a lo largo de este documento, relevantes a la hora de diseñar, formular y aplicar soluciones para abordar el riesgo cibernético en consonancia con los Principios.

5.1 Cibernético

5.1.1 "Cibernético" hace referencia a la red interdependiente de infraestructuras de tecnología de la información e incluye "herramientas" tecnológicas tales como Internet, redes de telecomunicaciones, sistemas informáticos y procesadores integrados y controladores de industrias críticas.

5.2 Seguridad cibernética

5.2.1 "Seguridad cibernética" hace referencia a los análisis, advertencias, intercambio de información, reducción de la vulnerabilidad, mitigación del riesgo y esfuerzos de recuperación dirigidos a los sistemas de información interconectados.

5.3 Riesgos cibernéticos

5.3.1 Los "riesgos cibernéticos" se definen como la combinación de la probabilidad de que se produzca un evento en el ámbito de los sistemas de información interconectados y las consecuencias del mismo para los activos y la reputación.

5.3.2 Los riesgos cibernéticos constituyen una cuestión empresarial que entraña aspectos técnicos. El riesgo cibernético afecta a todos los ámbitos de la organización y se ve afectado por ellos.

5.3.3 Las "amenazas cibernéticas" son eventos cibernéticos potenciales susceptibles de provocar resultados no deseados, causando daños a un sistema u organización. Las amenazas pueden originarse externa o internamente y pueden originarlas individuos u organizaciones.

5.3.4 Las "vulnerabilidades cibernéticas" son susceptibilidades o defensas insuficientes para la protección de un activo o grupo de activos y capacidades frente a las amenazas cibernéticas.

5.3.5 Los principales "valores en riesgo" de una entidad frente a las amenazas y vulnerabilidades cibernéticas son sus activos y su reputación.
A causa de las dependencias críticas, las consecuencias para estos activos podrían ser resultado de un acto en cascada y de mayor envergadura ajeno ala dirección o al control de la entidad.

5.4 Gestión del riesgo cibernético

5.4.1 Además de la aplicación de medidas técnicas, la gestión del riesgo cibernético tiene por objeto influir en la conducta humana y en las normas, así como en los controles técnicos y en las interacciones entre máquinas y se propone coordinar las actividades y los procesos con el fin de prevenir consecuencias no deseadas.

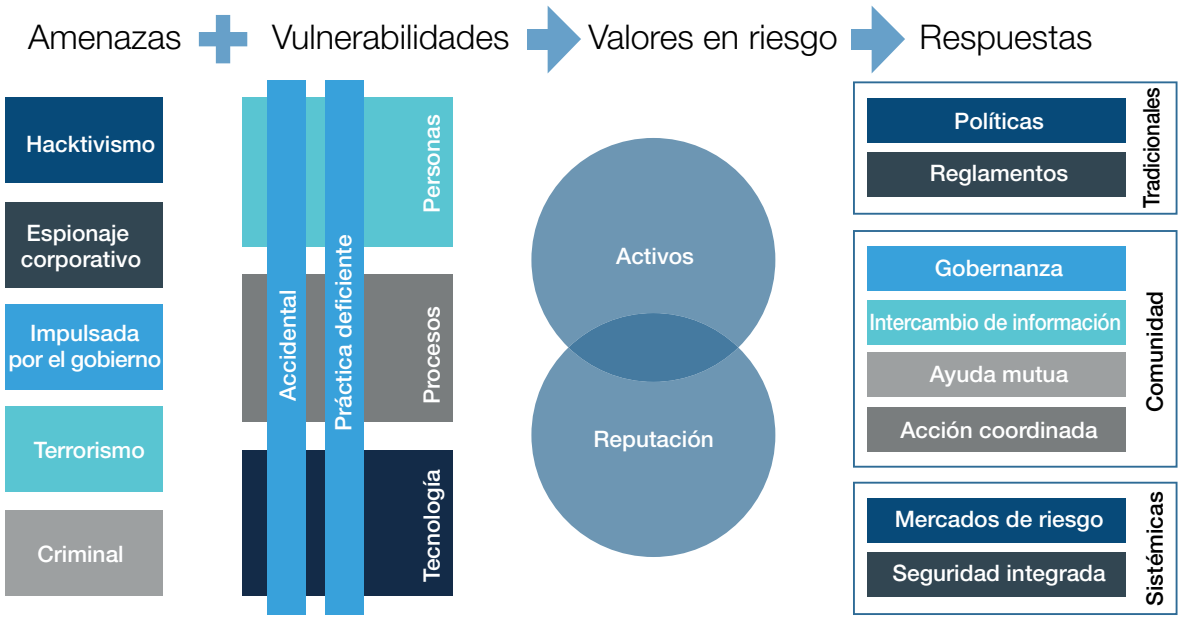
5.4.2 Una "evaluación de riesgos" es el proceso que emprende una organización con el fin de analizar, evaluar y comprender el espectro de riesgos, la probabilidad potencial de que se produzcan y su gravedad con el fin de poder actuar para mitigar los riesgos inaceptables para la organización.

5.4.3 "Estrategias para la transferencia del riesgo" (tales como la indemnización, el seguro y las soluciones de transferencia del riesgo estructuradas) son métodos a los que puede recurrir una organización para abordar el riesgo.

5.5 Resiliencia cibernética

5.5.1 Como dimensión adicional de la gestión del riesgo cibernético, la "resiliencia cibernética" se define como la capacidad de los sistemas y las organizaciones para resistir a los eventos cibernéticos, medida mediante la combinación del promedio de tiempo necesario para que se produzca un fallo y del promedio de tiempo necesario para la recuperación.

Figura 2: Marco del riesgo cibernético



Agradecimientos

Junta Directiva

Natarajan Chandrasekaran	Consejero Delegado y Director General	Tata Consultancy Services
Michael Chertoff	Cofundador y Director General	Chertoff Group
Ian Livingston	Director General	BT Group
William E. McCracken	Director General	CA Technologies
Robert Wainwright	Director	Europol (Oficina Europea de Policía)

Grupo de Trabajo

Mustaque Ahamad	Profesor y Director	Georgia Tech Information Security Center
Eric Allegakoen	Vicepresidente, Auditoría Global y Servicios de Seguros	Adobe
Mohd Amin	Presidente	Impact
Jolyon Barker	Director General, Tecnología Global, Medios de Comunicación y Telecomunicaciones	Deloitte (Asesor del proyecto)
Drew Bartkiewicz	Vicepresidente, Servicios Estratégicos	Mashery
Mark Bauhaus	Vicepresidente Ejecutivo y Director General	Juniper Networks
Jennifer Byrne	Vicepresidenta	Lockheed Martin
William Casazza	Vicepresidente Sénior y Consejero General	Aetna
Paloma Castro	Directora, Asuntos Corporativos Globales	LVMH
Steve Culp	Director General, Gestión de Riesgos	Accenture
Scott David	Asociado (Consejero Legal de OIX)	K&L Gates
Serge Dumont	Vicepresidente y Presidente del Grupo, Asia-Pacífico	Omnicom
John Evans	Vicepresidente, Innovación Empresarial	Lockheed Martin
Stacy Feuer	Directora Adjunta para la Protección Internacional de los Consumidores	Comisión Federal de Comercio
Allan Friedman	Director de Investigación, Centro para la Innovación Tecnológica	Brookings Institution
Marc Goodman	Profesor y Asesor en materia de Seguridad	Universidad de la Singularidad
Cristin Goodwin	Abogada Sénior	Microsoft Corporation
Meghan Hannes	Directora General	CloudInsure
Kevin Harried	Vicepresidente Sénior, Gestión de Riesgos	FIS/Capco
Phillip Harrington	Vicepresidente Ejecutivo, Riesgos y Director Administrativo	CA Technologies
Bret Hartman	Director Tecnológico, RSA	EMC
Anwarul Hasan	Director, Gestión de Riesgos	SwissRe
Ray Johnson	Vicepresidente Sénior y Director Tecnológico	Lockheed Martin
Yuecel Karabulut	Asesor Jefe de Seguridad	SAP
David Kirkpatrick	Fundador y Director General	Techonomy
Robert Kirkpatrick	Director	Iniciativa Global Pulse de las Naciones Unidas
Susan Kish	Directora de Plataformas Multisectoriales	Bloomberg
Tarkan Maner	Presidente y Director General	Dell Wyse
Christophe Nicolas	Vicepresidente Sénior y Director Tecnológico	Kudelski Group
JP Rangaswami	Científico Jefe	Salesforce.com
Paul Saffo	Autor y Analista	Discern Analytics
Alexis Samuel	Director de Riesgos	Wipro
Murat Sonmez	Vicepresidente Ejecutivo, Operaciones de Campo Globales	TIBCO Software
Deirdre Stanley	Consejera General	Thomson Reuters
Ray Stanton	Director Global de Continuidad Empresarial, Seguridad y Gobernanza	BT Group
Owen Tripp	Director de Operaciones	Reputation.com
Andrew Vitrano	Consejero General Adjunto y Subsecretario Corporativo	IntraLinks
Mark Walsh	Vicepresidente, Seguridad de la Información	BAE Systems
Jody Westby	Director General	Global Cyber Risk

Asesores adicionales

Colin Adams	Director de Comercialización, Facultad de Informática	Universidad de Edimburgo
Rod Beckstrom	Director General	ICANN
Michael Fertik	Fundador y Director General	Reputation.com
Lee Hibbard	Secretario, Comisión del Convenio sobre la Ciberdelincuencia y Director de Protección de Datos y Ciberdelincuencia, Dirección General de Derechos Humanos y Estado de Derecho	Consejo de Europa
Peter Hustinx	Supervisor	Europeo de Protección de Datos
Viktor Mayer-Schönberger	Profesor, Gobernanza y Regulación de Internet	Oxford Internet Institute
Jun Murai	Decano y Profesor, Facultad de Estudios de Medio Ambiente e Información	Universidad de Keio
Ken Senser	Vicepresidente Sénior de Seguridad Global, Aviación y Viajes	Wal-Mart
Hamadoun I. Touré	Secretario General	Unión Internacional de Telecomunicaciones (UIT)
Atsushi Umino	Director de Coordinación de Política Internacional, Oficina Mundial de Estrategias de TIC	Ministerio de Asuntos Interiores y Comunicaciones
Jonathan Zittrain	Profesor de Derecho y Profesor de Ciencias Informáticas	Universidad de Harvard

Contacto: Derek O'Halloran, Asociaciones de Tecnologías de la Información de Socios de Liderazgo Mundial, Foro Económico Mundial, derek.ohalloran@weforum.org
Alex de Leeuw, Asociaciones de Tecnologías de la Información, Foro Económico Mundial, alex.deleeuw@weforum.org
www.weforum.org/cyber

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

El Foro Económico Mundial es una organización internacional independiente que se compromete a mejorar la situación del mundo mediante la participación activa de líderes empresariales, políticos, académicos y otros líderes de la sociedad en la definición de la agenda global, regional y sectorial.

Constituido como fundación sin ánimo de lucro en 1971 y con sede en Ginebra (Suiza), el Foro no está ligado a ningún interés político, partidista o nacional.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Suiza

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org