GUÍA DE SEGURIDAD ICC PARA LOS NEGOCIOS

CÁMARA DE COMERCIO INTERNACIONAL

La organización empresarial mundial

“Traducido y editado en español
con la colaboración de Telefónica”.

GUÍA DE SEGURIDAD ICC PARA LOS NEGOCIOS

Agradecimientos

La guía de seguridad cibernética de la ICC para los negocios se inspiró en la guía de seguridad cibernética belga, una iniciativa de la ICC Bélgica y VBO-FEB, EY Bélgica y Microsoft Bélgica, con el B-CCENTRE e ISACA Bélgica. Bien apreciada en Bélgica, la Guía se ofreció a la Comisión de Economía Digital de la ICC como un modelo que podría adaptarse para servir como un recurso global con el permiso de las empresas y organizaciones involucradas.

La ICC reconoce la amable contribución de los implicados en la preparación y producción de la guía belga, así como a los miembros del Grupo de Trabajo de la ICC sobre Seguridad Cibernética que desarrollaron esta guía global.

ICC Publication No. 450/1081-5
ISBN: 978-92-842-0336-9

TABLA DE CONTENIDOS

INTRODUCCIÓN

Secretario General de la ICC, John Danilovich

La Cámara de Comercio Internacional (ICC) tiene el orgullo de contar con casi cien años de historia a lo largo de los cuales viene proporcionando a las empresas tanto las herramientas como la orientación en autorregulación para promover la buena práctica empresarial. Como organización empresarial mundial, compuesta por miembros empresariales de todos los sectores y regiones, ICC se complace especialmente en proporcionar esta guía sencilla y clara a empresas de todos los tamaños para ayudarles a desempeñar su papel afrontando el reto cada vez más serio de la Ciberseguridad.

ICC es una organización dedicada a facilitar el comercio y la inversión, lo que incluye el fomento de la confianza en la economía digital y el aumento de las considerables oportunidades que esta conlleva para los negocios, los consumidores, los gobiernos y la sociedad. La interconectividad no solo ha transformado el mercado, sino que ha cambiado la estructura de la sociedad. Los beneficios que se derivan de un mayor acceso al conocimiento, la información, bienes y servicios son posibles gracias a una Internet global y abierta. Debe de ser confiable y segura. Por lo tanto, cualquier estrategia de ciberseguridad debería ser apropiada, justificada y proporcionada, con el fin de preservar estos beneficios.

Dado que la seguridad –al igual que la perfección- es un objetivo difícil de alcanzar, con múltiples compromisos, también puede resultar desalentador. El miedo o el desconocimiento pueden ser una barrera para que las empresas evalúen los riesgos y tomen las medidas adecuadas. Esta guía sensibiliza acerca de una sencilla serie de pasos capaces de derribar esa barrera intimidatoria. La ICC ha producido la *Cybersecurity guide for business* (guía de ciberseguridad para los negocios) con el fin de llegar a un público más amplio, teniendo en mente a sus más de seis millones de miembros. Se pretende que sea accesible a los propietarios de los negocios, sus ejecutivos o al personal, y que no se limite solo a los equipos de tecnologías de la información, y debería compartirse también con los proveedores de la cadena de suministro de bienes y servicios, además del sector público, con el fin de mejorar la capacidad de recuperación en un sentido amplio.

La guía se distribuirá a través de la red global de comités nacionales de la ICC, sus miembros, asociaciones empresariales y cámaras de comercio, a través de la Federación Mundial de Cámaras ICC, que abarca más de 130 países. ICC cree que la acción colectiva global de su red y colaboradores pueden hacer una contribución esencial a la reducción de ciberriesgos para las empresas y la sociedad en general.

LA CIBERSEGURIDAD EMPIEZA POR USTED

Las modernas tecnologías de la información y las comunicaciones están permitiendo a las empresas de todos los tamaños innovar, alcanzar nuevos mercados e impulsar las eficiencias que benefician a los clientes y la sociedad. Sin embargo, cada vez más, las prácticas empresariales y políticas están siendo retadas al tener que adaptarse a los impactos directos e indirectos producidos por una generalización de entornos de comunicación y flujos de información a través de internet que son requeridos en la entrega de bienes y servicios. Muchas empresas adoptan modernas tecnologías de información y comunicaciones sin ser plenamente conscientes de que, como consecuencia, deben también gestionarse los nuevos tipos de riesgos. Esta guía aborda esta carencia y describe cómo las empresas de todos los tamaños pueden identificar y gestionar los riesgos de ciberseguridad.

Los fallos en ciberseguridad aparecen constantemente en la prensa informando sobre criminales que atacan a empresas grandes y pequeñas – aparentemente a discreción y con suma facilidad. Las empresas están ahora expuestas a una creciente fuente de riesgos[1] como criminales, hackers, agentes estatales y competidores desleales cada vez más sofisticados en el aprovechamiento de las debilidades de las modernas tecnologías de la información y las comunicaciones. La combinación de los sistemas de información conectados con diversos dispositivos[2] externos aumenta el nivel de complejidad y amenaza a dichos sistemas de información empresariales. Las empresas no sólo se enfrentan a amenazas externas, sino que deben gestionar también los riesgos que para sus sistemas de información suponen las amenazas internas como aquellas personas dentro de la organización que podrían ser capaces de corromper datos o abusar de los recursos de la empresa desde la comodidad de su residencia o desde una cafetería próxima. Desde una perspectiva empresarial, es vital que la empresa – grande o pequeña – sea capaz de identificar sus riesgos para la ciberseguridad y gestionar eficazmente las amenazas a sus sistemas de información. Al mismo tiempo, todos los gerentes de negocios, incluyendo ejecutivos y directores deben reconocer que la gestión del ciberriesgo es un proceso continuo, donde no hay, ni nunca la habrá, una seguridad absoluta.

A diferencia de otros retos empresariales, la gestión de riesgos de ciberseguridad continúa siendo un problema sin fácil solución. Se requiere una consistente aplicación de atención por parte de la administración, con tolerancia para las malas noticias y disciplina para una comunicación clara. Existen muchos y excelentes recursos disponibles, que proporcionan explicaciones completas sobre las amenazas informáticas más importantes, y sin embargo continua siendo escaso el material adecuado para ayudar a la gestión empresarial de la ciberseguridad. Este documento ayudará a los gestores empresariales de pequeñas y

1 Algunos ejemplos de amenazas externas a la ciberseguridad que están aumentando son el software malicioso (como el software para intrusiones, la inyección de código, herramientas de explotación, gusanos, troyanos, etc.) la denegación de servicios, las violaciones de datos de carácter personal y otros. Para una actualización de los más relevantes véase, por ejemplo el informe de ENISA “Escenario de Amenazas 2014”, EL 2014 https://www.enisa.europa.eu

2 Tales como teléfonos móviles, módems, terminales de pago, actualizaciones de software automáticas, sistemas de control industrial, así como Internet de las Cosas.

grandes organizaciones a interactuar con sus administradores de tecnología de información y les guiará en el desarrollo de prácticas de gestión de riesgos de ciberseguridad.

Mejorar la ciberseguridad de una organización es posible a través de un proceso de gestión de riesgos – con énfasis en la gestión. Debido al constante cambio de la tecnología y de los vectores de amenaza, los sistemas de información de la empresa nunca estarán completos, y nunca estarán completamente seguros. Operar de manera efectiva en un entorno tan cambiante requiere un compromiso con un enfoque de gestión de riesgos a largo plazo y sin un final estático. Los gerentes del negocio acabarán frustrados con las iniciativas de ciberseguridad si no enfocan el trabajo con unas expectativas adecuadas para esta tarea. Y sin unas limitaciones adecuadas, las empresas podrían consumir rápidamente todos los recursos disponibles en un intento de mitigar los ciberriesgos. Es esencial enfocar la gestión de riesgos de ciberseguridad a través de un proceso que permita a una empresa entender y dar prioridad a lo que es importante para la organización (activos físicos y de información).

Es fundamental tener en cuenta que, sin adoptar las precauciones adecuadas, Internet, las redes y los dispositivos de información de la empresa no son seguras. Los modernos sistemas de información empresariales son el objetivo de una serie de agentes maliciosos. Un concepto útil para establecer las expectativas de quienes se dedican a la gestión de riesgos de ciberseguridad es esta simple afirmación: “Si algo de valor está en línea, está en riesgo, y es probable que ya esté comprometido.” Afortunadamente, lo que es valioso para un actor malicioso no siempre está alineado con los activos (tales como dinero, secretos comerciales e información de los clientes) que la empresa considera valiosos. Si bien existen técnicas y procesos que pueden ayudar a reducir los riesgos de compromiso, determinados agentes maliciosos se benefician del eslabón más débil en los sistemas interconectados. Existen numerosas vulnerabilidades potenciales (organizativas, humanas, además de las tecnológicas) presentes en toda la empresa. A pesar de los mejores esfuerzos de proveedores de tecnología, proveedores de servicios y de los empleados de su organización, no se alcanzará una seguridad absoluta. Por lo tanto, los procesos de gestión de riesgos de ciberseguridad deben evaluar las amenazas y debilidades que resulten singulares para su empresa y alinear éstas con los bienes prioritarios para la organización.

A pesar del sombrío panorama esbozado anteriormente, las empresas de todos los tamaños pueden desarrollar y fomentar capacidades organizativas clave para tener éxito en la gestión de riesgos de ciberseguridad.

- En primer lugar, la gerencia del negocio debe realizar un análisis de riesgos para su organización y priorizar los activos que requieran una mayor protección.
- En segundo lugar, es necesario el liderazgo para tomar las medidas adecuadas y garantizar que la empresa adopta las mejores prácticas de seguridad de la informació.
- En tercer lugar, las organizaciones deben estar preparadas para detectar y responder – interna y externamente- a cibereventos a través de procesos organizativos formalizados.

Las actividades de respuesta requerirán de la comunicación entre compañeros, con representantes relevantes del gobierno, con clientes e incluso competidores. La preparación por adelantado de cualquier ciberincidente asegurará que el problema inicial no se verá agravado por errores evitables que se pudieran cometer durante la respuesta. Por último, los mecanismos para aprender de los ciberincidentes y modificar prácticas de respuesta son esenciales para impulsar el cambio institucional necesario que promulgue las mejores prácticas de gestión de riesgos de ciberseguridad en toda la empresa.

UTILIZANDO ESTA GUÍA

Durante la última década, los gobiernos, organizaciones e individuos han desarrollado numerosos libros sobre cómo abordar el desafío de la seguridad de la información en el ciberespacio. Disponemos de tantos documentos y guías que puede resultar difícil de identificar por dónde empezar la lectura y qué tipo de documento será el apropiado para su organización. La gama de material disponible es considerable (y creciendo en su especificidad):

- **Directrices** – Declaraciones de alto nivel que muestran preocupación por la seguridad cibernética y proporcionan una carta constituyente para organizaciones e individuos. Ejemplos: Directrices de Seguridad de la OCDE, etc.
- **Estrategias Nacionales** – A menudo basadas en directrices, estos documentos articulan un acercamiento a la ciberseguridad adaptado a un contexto nacional o jurídico determinado. Ejemplos: International Strategy to Secure Cyberspace, las estrategias nacionales de países europeos y de otros estados[4], etc.
- **Marcos** – Llevando las estrategias nacionales un paso más allá, los marcos de referencia reúnen un catálogo de recursos priorizados o evaluados que ayudan a las organizaciones a comparar su madurez y el progreso alcanzado en el tratamiento de los riesgos de seguridad cibernética. Ejemplos: National Institute of Standards and Technology (NIST) Cybersecurity Framework[5], etc.
- **Códigos de buenas prácticas** – Documentos que guían o gobiernan los procesos de organización para garantizar un funcionamiento robusto y coherente de las mejores prácticas de seguridad cibernética. Ejemplos: Estándares ISO 27001, 27002, 27032, Estándar de Seguridad PCI, etc.
- **Normativas técnicas** – Especificaciones detalladas para la implementación de interfaces que cumplimenten determinados tipos de requisitos de interoperabilidad. Ejemplos: HTTPS, AES, EMV, estándares de pago PCI, etc.

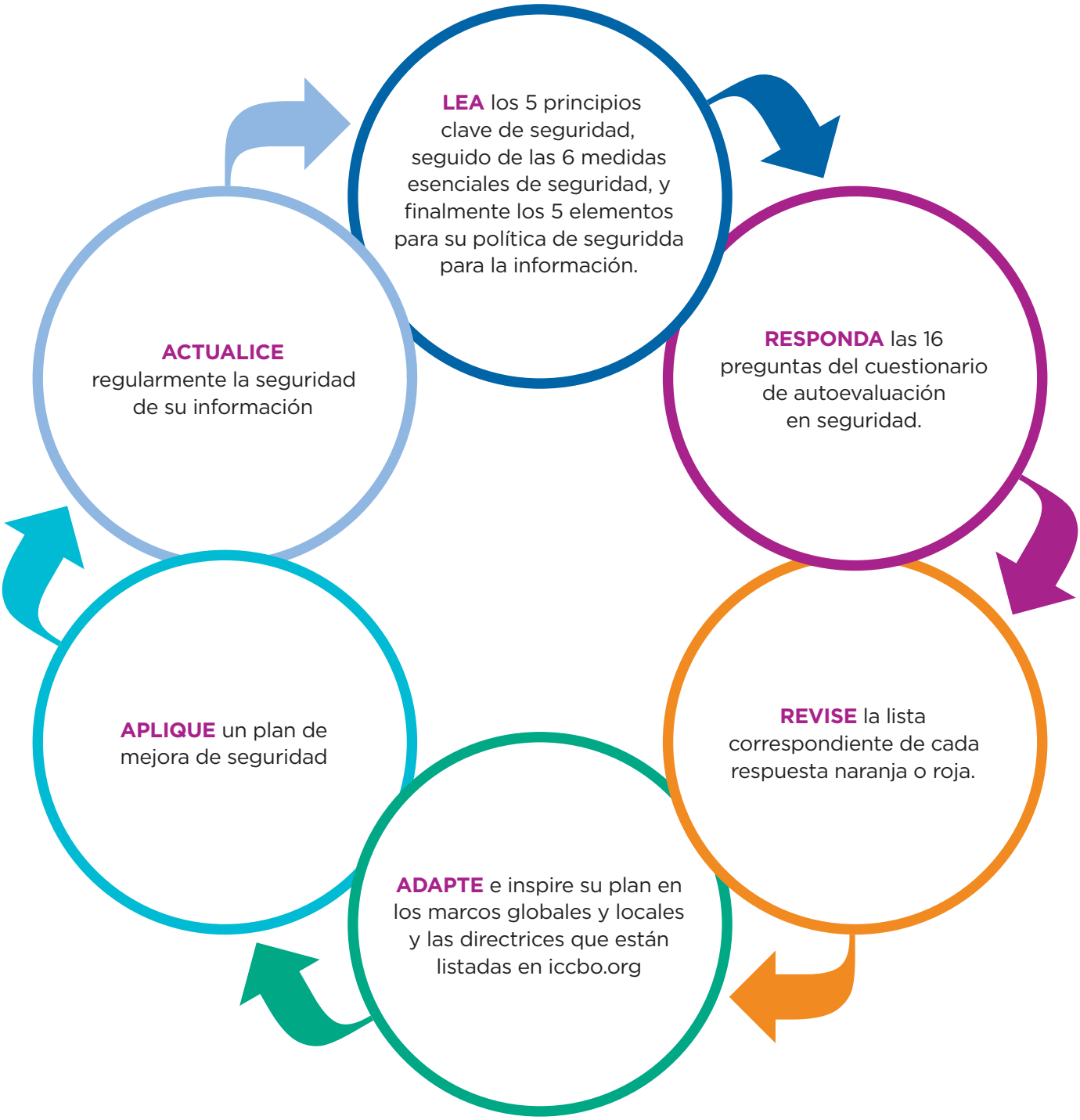
En primer lugar, esta guía directa, fruto de directrices globales de ciberseguridad y de estrategias nacionales ofrece a las empresas un marco para examinar el problema de la seguridad en línea – comenzando por un conjunto de cinco principios para las empresas de cualquier tamaño cuando deciden abordar los riesgos de ciberseguridad. En segundo lugar, esta guía identifica seis acciones clave que las empresas deberían tomar, a partir de materiales y mejores prácticas procedentes de diversas fuentes. A continuación, la guía explica cómo aplicar los cinco principios iniciales en políticas que guíen el desarrollo de las actividades de gestión de riesgos de ciberseguridad en la organización. Un apéndice digital en evolución servirá como recurso vivo y compendio de otros recursos que complementan a esta guía, proporcionando un asesoramiento más específico según se vayan desarrollan estas políticas – desde los procedimientos hasta normas técnicas y mucho más. Si bien no se puede alcanzar una seguridad absoluta, los conceptos de gestión de riesgos de ciberseguridad que se acaban de describir ayudarán a las empresas a estar a la altura del desafío de seguridad de la información en este entorno cambiante. No es sólo una guía de valor para empresas individualmente consideradas, sino para compartirla con aquellos que participan en la cadena de relaciones de su organización, y de este modo asegurar mejor los puntos de entrada y el intercambio con sus sistemas y procesos.

3 http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

4 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

5 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

UTILIZANDO ESTA GUÍA



Mientras los enfoques de seguridad de la información pueden diferir de una empresa a otra en función de diversos factores[6] existe una serie de principios de alto nivel que engloban sólidas prácticas de seguridad de la Información para cualquier empresa, independientemente de su tamaño o sector. Esta guía presenta cinco principios clave divididos en dos categorías:

A. Visión y Mentalidad

B. Organización y procesos

Estos principios se complementan con un conjunto de seis medidas de seguridad críticas y a continuación cinco elementos iniciales para aplicar estos principios y reforzar así las políticas de seguridad de la información de una empresa.

En conjunto, los principios y las acciones sugeridas en esta guía mejorarán la capacidad de recuperación de la empresa contra las ciberamenazas y limitarán las interrupciones asociadas con brechas de seguridad.

A. VISIÓN Y MENTALIDAD

Principio 1: Centrarse en la información, no en la tecnología

Usted es la primera línea de defensa contra las amenazas informáticas de la organización y ayudará a establecer el tono para el enfoque de su organización respecto de la seguridad de la información. Por lo tanto, piense en la seguridad de la información en un sentido más amplio, no sólo en términos de tecnología de la información.

La seguridad de la información es una combinación de personas, procesos y tecnología que implica a toda la empresa, no sólo a los asuntos de tecnología de la información (IT). La implementación de medidas de seguridad no debe limitarse al departamento de IT, sino más bien reflejarse en toda la empresa y en cada proyecto. El alcance y la visión de la seguridad de la información, por lo tanto incluye tanto a personas como productos, instalaciones, procesos, políticas, procedimientos, sistemas, tecnologías, dispositivos, redes y, por supuesto, la información.

Las personas son clave. La identificación y la gestión de vulnerabilidades y amenazas de los activos de información[7] pueden ser una tarea inabarcable. Sin embargo, basándonos en la experiencia, sabemos que el 35% de los incidentes de seguridad son producto de errores humanos en lugar de ataques deliberados. Más de la mitad de los incidentes de seguridad restantes fueron el resultado de ataques deliberados que podrían haberse evitado si el personal hubiera manejado la información de una manera más segura.

Enfoque los esfuerzos de seguridad específicamente en la protección de su información más valiosa y los sistemas en los que la pérdida de confidencialidad, integridad o disponibilidad perjudicaría seriamente la empresa. Esto no quiere decir que otros activos de información puedan ignorarse en términos de seguridad. Implica que un enfoque basado en el riesgo con foco en las “joyas de la corona” de la organización es en la práctica un enfoque eficaz y eficiente de seguridad de la información. Al mismo tiempo, admite que un 100% de eliminación de riesgos, además de imposible no es ni siquiera necesario, si lo ponemos en contexto con los costes asociados.

6 Incluyendo la naturaleza del negocio, el nivel de riesgo, factores ambientales, nivel de interconexión, requisitos regulatorios y tamaño de la compañía, entre muchos otros.

7 EY – 2012 Global Information Security Survey – Fighting to close the gap

Principio 2: Hacer de la resiliencia una mentalidad

El objetivo debe ser la resiliencia de la empresa a los riesgos de pérdida o daños en la información. Las empresas están sujetas a muchas leyes y reglamentos, muchos de los cuales requieren la implementación de controles de seguridad apropiados. El cumplimiento de estas leyes, reglamentos y normas puede conducir a la mejora de la seguridad de la información; sin embargo, también puede conducir a la complacencia, una vez que se han alcanzado estos objetivos de cumplimiento. Las amenazas de seguridad cambian mucho más rápido que las leyes y reglamentos, creando un objetivo en movimiento para las actividades de gestión de riesgos. Como resultado de ello, las políticas y procedimientos pueden quedar obsoletos o simplemente resultar ineficaces en la práctica.

La evaluación periódica de la resistencia de una empresa frente a las ciberamenazas y vulnerabilidades es esencial para medir el progreso hacia nuestra meta de adecuación en la gestión de riesgos y en las actividades de ciberseguridad. Las actividades de evaluación se pueden realizar a través de análisis y auditorías internas y/o independientes, incluyendo medidas como pruebas de intrusión y detección de intrusiones. La responsabilidad de la ciberseguridad debe ir más allá del departamento de IT, los órganos de decisión del negocio deben participar no solo en la identificación del problema, sino además en la implementación de un ecosistema saludable a largo plazo. Más aún, el verdadero valor de la revisión periódica por parte del negocio se materializa cuando se utiliza este proceso de revisión para la mejora de la cultura de la empresa y la mentalidad de los empleados hacia las prácticas de gestión de riesgos de ciberseguridad.

Una mentalidad de sistemas de información resilientes es más crítica en el momento en que nuevas soluciones y dispositivos son adoptados por el negocio. Es entonces, durante el periodo de adopción, cuando deben ser consideradas tan pronto como sea posible las adecuadas medidas de seguridad, idealmente durante la identificación de los requisitos del negocio. Tal “seguridad por diseño” puede resaltar el papel de los empleados, que son los que hacen posible la innovación en una empresa, al centrarse en la gestión de riesgos de seguridad información.

B. ORGANIZACIÓN Y PROCESOS

Principio 3: Prepárese para responder

Incluso la empresa mejor protegida experimentará en algún momento una violación de seguridad de la información. Vivimos en un mundo donde la pregunta no es si nos sucederá, sino **cuándo sucederá**. Por lo tanto, la forma en cómo una empresa responde a una brecha será la forma en cómo **usted** será evaluado.

Con el fin de minimizar el impacto en el negocio debido a incidentes de ciberseguridad, las empresas deben desarrollar planes de respuesta organizativos, además de las medidas de respuesta técnicas. Un plan de respuesta debe establecer hitos que ayuden a los gerentes de la empresa a entender cuándo deben participar terceros especializados para ayudar a contener y remediar un incidente de seguridad, y cuándo es conveniente ponerse en contacto con terceras partes externas (incluyendo la policía o los organismos de supervisión del gobierno). Tenga en cuenta que el reporte a las autoridades competentes es una forma de mejorar el escenario general de la seguridad y en algunos casos puede ser obligatorio para evitar incumplimientos regulatorios y sanciones. Una gestión de respuesta a incidentes exitosa incluye una estrategia (interna y externa) de comunicación, lo que puede marcar la diferencia entre terminar con un titular embarazoso en la portada de un periódico, o como un exitoso “estudio del caso” de una escuela de negocios.

Si bien las actividades de gestión de riesgos internos son esenciales, recuerde también dedicar tiempo para participar con sus colegas y socios de la industria, la comunidad empresarial en general y con la policía en particular, para ayudar a comprender las amenazas actuales y las emergentes, así como para construir relaciones personales que más adelante puedan servirle durante la gestión de un incidente.

Principio 4: Demostrar un compromiso de liderazgo

Con el fin de gestionar la seguridad de la información con eficacia y eficiencia, los líderes empresariales deben entender y apoyar las actividades de gestión de riesgos como un elemento esencial para el éxito de su organización. Usted y su equipo directivo debe participar visiblemente en la gestión y supervisión de las políticas de gestión de riesgos de ciberseguridad de su empresa.

Deben asegurarse de que se asignan los recursos adecuados – tanto humanos como financieros- a la protección de los activos de la empresa. Pero no es suficiente con dotar recursos; debe facultarse una función de seguridad de la información en la empresa, sea ésta grande o pequeña, para permitir una respuesta de toda la compañía a ciberamenazas y vulnerabilidades.

La eficacia y adecuación de las medidas de seguridad de la información de la empresa deberían ser comunicada formalmente al máximo responsable de su empresa, y por lo menos una vez al año al equipo directivo, los auditores, y al consejo de administración. Regularmente estos informes – sobre la base de varios indicadores y métricas de seguridad – deberían ser una ayuda para la toma de decisiones en la política y las inversiones en seguridad, y dar una idea de lo bien que su empresa está protegiendo sus activos.

Aunque a menudo nos referimos a él como el eslabón más débil cuando se trata de seguridad de la información – eduque a su gente a ser el mayor activo para una buena seguridad mediante la creación de conciencia individual y colectiva sobre la seguridad de información que dé como resultado empleados con perfiles efectivos.

Principio 5: Actuar según su visión

Sólo la lectura de esta guía no resulta suficiente – debe llevar a la práctica su visión singular para la gestión de riesgos de ciberseguridad de la empresa mediante la creación (o revisión) de diversas políticas de seguridad de la información. Las políticas de seguridad de la información corporativa proporcionan una línea base estándar para guiar las actividades de seguridad en toda la empresa, a través de todas las unidades de negocio y del personal, al tiempo que aumentan la conciencia de seguridad en toda la empresa.

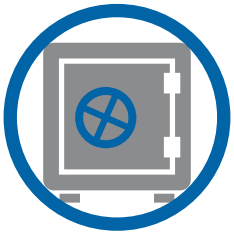
Por lo general, el documento de política de seguridad, sus directrices y normas de apoyo, están enmarcados en una estructura normativa de seguridad de la información que se traduce posteriormente en procedimientos operativos habituales. Sin embargo, con el aumento de la adopción y la integración de proveedores de servicios de terceros en las cadenas de valor del negocio, las organizaciones deben comprender cómo fluyen sus activos de información entre, y son interdependientes de, diversas partes externas. Si un tercero no está protegiendo adecuadamente su información (o sus sistemas de información, en los que usted confía), un incidente de seguridad que les ocurra a ellos puede llegar a convertirse en una responsabilidad grave para las operaciones de negocio de usted, la reputación y el valor de marca de la empresa. Anime a los proveedores a adoptar al menos los principios de seguridad de la información que usted aplica dentro de su empresa. Allí donde resulte apropiado dirija auditorías o exija a los proveedores de servicios que le detallen sus prácticas de seguridad de la información para obtener así, al menos, una garantía adicional acerca de sus prácticas de negocio.

Los terceros no son sólo fuentes de riesgo – de hecho algunos pueden ayudar a reducir el riesgo y le permitirán cumplir con los objetivos críticos de la gestión de riesgos de ciberseguridad. Los proveedores de servicios de tecnología de la información pueden ayudar a mejorar su infraestructura de administración de riesgos de ciberseguridad, incluso a través de las evaluaciones y auditorías de seguridad así como mediante el uso de dispositivos de seguridad de la información y soluciones o servicios, ya sea en el lugar, gestionadas externamente o basadas en la nube[8].

8 Los servicios en la nube son soluciones mediante las cual se utiliza un proveedor de servicios externo para almacenar, procesar o gestionar datos a través de una red como Internet con un muy alto grado de flexibilidad y monitoreo en tiempo real.

Esta lista de acciones es un conjunto de medidas prácticas que las empresas de todos los tamaños pueden tomar para reducir el riesgo asociado con los incidentes de ciberseguridad. Si bien no es completa ni exhaustiva, asegurar que su negocio está comprometido con estas actividades le ayudará a establecer un rumbo apropiado hacia la excelencia en seguridad de información.

Usted debe recordar que la gestión de riesgos de seguridad cibernética es un proceso continuo. Una vez que esté satisfecho de que estas actividades iniciales están en marcha, consulte el portal web asociado a esta guía e identifique normas y recursos que le ayudarán a tomar nuevas medidas para aumentar la fortaleza de su programa de seguridad de la información.



Acción 1: Copia de seguridad de la información del negocio y validación del proceso de restauración

Asegúrese de que su información del negocio está protegida haciendo una copia de seguridad – antes de que su negocio sufra un fallo de seguridad que ocasione que la información sea robada, alterada, borrada o perdida. Pero sólo hacer una copia de seguridad no es suficiente[9]. Una correcta gestión de los procesos de copia de seguridad debe incluir la validación del contenido de los datos de negocio y de la información contenida en los archivos de copia de seguridad, así como de los procesos de prueba de restauración. Si se utilizan terceros para el almacenamiento de información (por ejemplo de servicios en la nube), asegúrese que también se hacen back-ups de respaldo de esa información.

Tenga en cuenta que los medios físicos, como un disco, una cinta o unidad de almacenamiento utilizada para almacenar datos de copias de seguridad, también son vulnerables a ciertos riesgos. El material de respaldo debe disfrutar al menos del mismo nivel de protección que los datos en origen, sobre todo en materia de seguridad física, dada la facilidad con la que se mueven esos elementos de almacenamiento.

Acción 2: Actualización de los sistemas de tecnología de la información

Los sistemas y software de todo tipo, incluidos los equipos y dispositivos de red, deben actualizarse a través de los parches y las actualizaciones de firmware disponibles. Estas actualizaciones y parches de seguridad solucionan las vulnerabilidades del sistema de

9 Un procedimiento de copia de seguridad es un proceso técnico que debe gestionarse adecuadamente. Por ejemplo, solo el uso de varios repositorios de almacenamiento conectados al mismo tiempo en el mismo sitio es insuficiente como procedimiento de respaldo. Una política de respaldo eficaz debe tener en cuenta varios tipos de riesgo, incluyendo la pérdida de datos debido a una pérdida de lugar de operación, entre otras cuestiones, lo que requiere normalmente que las copias de respaldo se encuentran físicamente fuera de las instalaciones.

las que podrían abusar los atacantes. Muchos incidentes de seguridad hoy son resultado de las vulnerabilidades que cuentan con actualizaciones disponibles, a menudo, incluso más de un año antes de producirse el incidente.

Cuando sea posible, utilice servicios automatizado de actualización, especialmente para los sistemas de seguridad como las aplicaciones anti-malware, herramientas de filtrado web y sistemas de detección de intrusos. La automatización de estos procesos de actualización puede ayudar a asegurar que los usuarios realicen las actualizaciones de software de seguridad genuinas directamente facilitadas por el vendedor original.

Acción 3: Invertir en la formación

Es esencial establecer, y repetir continuamente, una concienciación básica acerca de las ciber amenazas más importantes así como sobre otros temas de seguridad, en todo el personal de su empresa. El entrenamiento[10] garantiza que el personal con acceso a la información y los sistemas de información, entiende sus responsabilidades diarias a la hora de manejar, proteger y apoyar las actividades de seguridad de la información de la empresa. Sin una formación adecuada, los empleados pueden convertirse rápidamente en fuentes de riesgo dentro de la empresa, creando incidentes de seguridad o vulnerabilidades que los adversarios puedan utilizar para violar las medidas de seguridad de la información.

Usted puede establecer una cultura de gestión del riesgo de seguridad de la información en su negocio. Con el paso del tiempo, la inversión en formación reforzará en el personal los mensajes de seguridad de información empresarial, y desarrollará las habilidades y atributos de seguridad deseados.

Acción 4: Controle su entorno de información

Las empresas deben implementar sistemas y procesos para asegurarse de que son alertadas en caso de que suceda un incidente de seguridad de información. Con demasiada frecuencia, las empresas no son conscientes de que están sufriendo una brecha de seguridad; experimentan violaciones o infecciones durante meses o años antes de que alguien detecte la intrusión[11]. Existen varias soluciones tecnológicas para ayudar en esta tarea, incluyendo los sistemas de prevención

10 Información general y advertencias sobre ciberseguridad para los usuarios finales pueden encontrarse en www.staysafeonline.org. http://www.enisa.europa.eu/media/multimedia/material, una iniciativa de ENISA. Usted está autorizado a utilizar toda esta información, videos, infografías y con fines educativos, dentro de su empresa.

11 http://www.verizonenterprise.com/DBIR/2013/ – Verizon 2013 Data Breach Investigations Report

y detección de intrusiones y de gestión de incidentes de seguridad; sin embargo, la simple instalación de estas soluciones es insuficiente. Es necesaria la monitorización continua y el análisis de las salidas de estos sistemas para obtener todo el beneficio de estas tecnologías. Las empresas deben implementar sistemas y procesos para asegurarse de que son alertados en caso de un incidente de seguridad de información que está sucediendo dentro de su organización. Con demasiada frecuencia, las empresas son conscientes de una brecha de seguridad; algunas empresas experimentan violaciones o infecciones durante meses o años antes de que alguien detecta la intrusión. Existen varias soluciones tecnológicas para ayudar con esta tarea, que incluyen sistemas de detección y prevención de intrusiones y de gestión de incidentes de seguridad; sin embargo, la simple instalación de estas soluciones es insuficiente. Es necesaria una monitorización continua y el análisis de la información recogida en estos sistemas para beneficiarse de dichas tecnologías.

Muchas empresas pueden no tener expertos propios ni los recursos necesarios para controlar los sistemas y procesos vitales. Existen servicios disponibles tanto para ser desplegados “in-situ” en sus instalaciones como para ser gestionados remotamente, que son ofrecidos por varios proveedores bajo diferentes modelos de negocio, y que incluyen tecnologías y servicios basados en la nube. Encuentre el sistema más adecuado para su organización, busque ayuda externa con experiencia para su asesoramiento, y apoye la inclusión del clausulado apropiado en las condiciones contractuales.

Si su empresa está experimentando un ciberincidente, considere informar sobre esta circunstancia a las agencias gubernamentales apropiadas[12] y a las asociaciones de la industria – la comunicación con los demás puede ayudarle a determinar si su negocio está experimentando un hecho aislado o forma parte de un ciberincidente a mayor escala. A menudo, esta clase de divulgación puede dar lugar a información y asesoramiento que ayudan a la empresa a tomar medidas eficaces.

Acción 5: defensa en capas para reducir el riesgo

Los perímetros de seguridad en la red y el control de acceso tradicionales ya no son suficientes, sobre todo cuando el sistema de información de la empresa se conecta a Internet, proveedores de servicios de Internet, servicios de *outsourcing* y de la nube, proveedores y socios, así como con dispositivos portátiles que están fuera del alcance y control de las compañías. La protección efectiva contra virus, software malicioso o dispositivos y *hackers* requiere varias capas de medidas defensivas para reducir el riesgo de un incidente de seguridad de información. La combinación de múltiples técnicas[14] para hacer frente a los riesgos de ciberseguridad puede reducir significativamente la posibilidad de que una pequeña brecha se termine convirtiendo en un incidente en toda regla.

12 Las víctimas de un (ciber) delito también deben presentar una denuncia ante las autoridades policiales correspondientes. Aunque la policía local es a menudo el mejor punto de contacto para la delincuencia tradicional, sin embargo podrá encontrar cuerpos policiales especializados en ciberdelincuencia (piratería, sabotaje, espionaje).

13 Un ataque puede ser horizontal (se dirige a empresas de un mismo sector) o vertical (dirigidos a subcontratistas) o puede ser una amenaza a la seguridad de un elemento específico de software o hardware en particular.

14 Incluyendo filtrado web, antivirus, protección contra malware proactiva, cortafuegos, políticas de seguridad sólidas y formación de los usuarios, por nombrar sólo algunos.

Las capas de defensa de seguridad de la información trabajan para limitar los grados de libertad disponibles para adversarios y aumentar las oportunidades para su detección por parte de los sistemas de vigilancia de la empresa.

El seguro de ciberriesgo puede ser no solo una manera para que las empresas mitiguen las consecuencias financieras de un incidente, sino también para gestionar proactivamente las exposiciones, y fortalecer la gestión del riesgo interno de una empresa.

Acción 6: Prepararse para cuando la brecha ocurra

La gestión del riesgo no trata solo de disminuir la probabilidad, sino también de minimizar el daño potencial en el caso de que ocurra un evento. Esto significa que hemos de prepararnos para investigar rápidamente un incidente – asegurándonos de que estarán a mano los recursos adecuados y los sistemas y procesos estarán atentos para capturar la información crítica. Si la brecha consiste en la entrada de un programa malicioso, este deberá ser eliminado. La preparación también significa tener un plan organizativo para adoptar buenas decisiones rápidamente y coordinar las acciones necesarias para tomar el control de un incidente. ¿Quién va a responder y cómo? Su equipo puede influir en el resultado a través de acciones bien diseñadas y una comunicación eficaz.

Por último, una preparación anticipada puede minimizar algunos de los elementos más dañinos de una brecha – pérdida de operatividad, falta de acceso a los datos, imposibilidad de reanudar las actividades. La continuidad del negocio y la planificación de recuperación minimizan esta pérdida, ya que se centran en las prioridades y la anticipación.

ELEMENTOS PARA SU POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Una tarea frecuente en la gestión empresarial es traducir los principios de documentos como éste en políticas y prácticas que tengan sentido para su organización. Hacer esa tarea más fácil es el objetivo de esta sección. Organizados según los cinco principios clave de seguridad que se han descrito en esta guía, los siguientes elementos ofrecen puntos de partida para el desarrollo de las políticas y prácticas de gestión de riesgos de seguridad cibernética de su organización.

Centrarse en la información, y no en la tecnología

- Crear una función y nombrar a una persona que dirija y facilite iniciativas de seguridad de la información, sin olvidar que la responsabilidad sobre la seguridad sigue estando compartida en toda la compañía.
- Al planificar cómo alcanzar sus objetivos de seguridad de la información, una organización debe determinar lo siguiente:
  - Qué va a hacer;
  - Qué recursos se requerirán;
  - Quién sera el responsable;
  - Cuándo se completará;
  - Cómo serán evaluados los resultados.[15]
- n el caso de que una empresa no tenga suficiente experiencia en seguridad interna, busque información y expertos en ciberseguridad en el exterior para ayudar a integrar la seguridad de la información en el diseño de los procesos de negocio y los sistemas de información.

Establecer una mentalidad resiliente

- Las actividades de seguridad de la información deben estar alineadas – y en lo posible integradas – con otras tareas de cumplimiento y esfuerzos de mitigación de riesgos con el fin de reducir solapamientos de iniciativas y responsabilidades.
- La aversión al riesgo no debe bloquear la introducción de nuevas tecnologías. Un buen enfoque en seguridad de la información puede posicionar a la empresa para la introducción de tecnologías nuevas e innovadoras, al tiempo que se alcanzan los objetivos de gestión de riesgos de ciberseguridad.
- Compruebe que la seguridad se tiene en cuenta en cada proyecto que la empresa esté llevando a cabo, sobre todo en los nuevos proyectos. Cuando se incluye desde el principio, con una adecuada participación del área de negocio correspondiente, la seguridad no aumenta significativamente el coste ni la duración de los proyectos. Sin embargo, cuando se añade la seguridad al final, o –en el peor de los casos- después de haberse producido un incidente, entonces los sobrecostes, retrasos y otros impactos son de una magnitud bastante mayor.

15 ISO/IEC 27001:2013

- Determine qué dispositivos – con un enfoque en los dispositivos móviles, tales como los de su personal o de sus colaboradores- pueden acceder a la red y/o información de la compañía[16], y considere la forma en cómo se gestiona el software y la configuración de seguridad de los equipos de la empresa.
- Evalúe el acceso a los datos para garantizar que los controles están en vigor de manera que preserven la confidencialidad, integridad y disponibilidad de la información.
- La dirección debe recibir, revisar y validar los usuarios (internos y externos) que tienen acceso a las aplicaciones y datos en su departamento – el acceso es una responsabilidad y un riesgo de modo que resulta aconsejable ejercer el control sobre el acceso de los empleados a los datos y los sistemas de información.
- Desarrolle procedimientos de reporte de equipos perdidos o robados y, cuando sea posible, las funciones de borrado remoto de la información de la empresa que pueda encontrarse en en esos dispositivos perdidos o robados.

Prepárese para la respuesta

- Todos cometemos errores, pero las compañías que convierten los percances de seguridad de la información en una oportunidad para realizar un examen abierto acerca del incidente pueden crear una cultura donde los empleados no tendrán miedo de reportar este tipo de situaciones cuando se produzcan.
- Autorice al personal seleccionado a compartir información apropiada con sus colegas y otras partes interesadas de la industria, tanto para ayudar a construir prácticas innovadoras como para advertir de posibles ataques futuros.
- Designe un órgano responsable para garantizar una custodia adecuada de las evidencias desde el inicio de las investigaciones acerca de los incidentes de seguridad y, en particular, en aquellos casos de ciberdelito.[17]
- Determine cómo y cuándo reportar incidentes de seguridad de la información a los equipos de respuesta a ciberemergencias (también conocidos como los CERT), agencias gubernamentales o funcionarios policiales.

16 Exija a los usuarios que configuren los ajustes de seguridad de dispositivos móviles de manera adecuada para impedir que los delincuentes roben información a través del dispositivo.

17 Directrices para la adquisición de datos en los incidentes de seguridad para fines de investigación por parte del personal de las TIC o en caso de infección por malware, están disponibles en línea en: http://cert.europa.eu/cert/plainedition/en/cert_about.html

Cuestiones de Liderazgo

- El personal debe ser responsable de la información y de su protección y deben tener la autoridad necesaria, el acceso a la alta dirección, las herramientas y la capacitación que les prepare para asumir sus responsabilidades, así como para enfrentarse a las amenazas que puedan encontrarse.[18]
- Las pequeñas empresas deben tener a alguien, dentro o fuera de la empresa, que adquiera formalmente la responsabilidad de la seguridad de la información y compruebe periódicamente su adecuación. Aunque podría no ser un papel a tiempo completo, es alguien muy importante que puede resultar vital para la supervivencia de la empresa.
- En las grandes empresas, la asignación de funciones, roles y responsabilidades debe ser una mezcla deliberada de individuos y virtual de grupos de trabajo y comités. Cada miembro del equipo debe conocer claramente sus responsabilidades y jerarquía. Para esto resulta esencial una documentación apropiada y buena comunicación.

Actúe sobre su visión

- Controle el acceso a (y desde) su red interna, priorizando el acceso a los servicios y recursos esenciales para las necesidades del negocio y de los empleados.[19]
- Haga cumplir una política de contraseñas seguras y considere la implementación de métodos de autenticación fuertes[20] que requieren información adicional, más allá de una simple contraseña, para poder entrar en los sistemas.
- Utilice el cifrado para proteger los datos en almacenamiento y en tránsito,[21] con atención especial para conexiones de red pública y en dispositivos portátiles, tales como ordenadores portátiles, llaves USB y *smartphones* que son fáciles de perder o de robar.

18 Un empleados de amenazas importantes deben estar capacitados en adelante, es la ingeniería social. La ingeniería social es la técnica de la manipulación de las personas en la realización de acciones para divulgar información sensible o confidencial.

19 Considere la posibilidad de filtrar servicios y sitios web que aumentan los riesgos de seguridad para los recursos de la empresa, por ejemplo el intercambio peer-to-peer de archivos o sitios web de pornografía. Las reglas de filtrado deben ser transparentes para todos los usuarios de la organización e incluir un proceso para desbloquear sitios web de negocios que pueden ser negados inadvertidamente.

20 Autenticación de múltiples factores utiliza una combinación de elementos, como las cosas que conozco (por ejemplo, contraseñas o PIN), cosas que tengo (por ejemplo, una tarjeta inteligente o SMS) y que yo soy (por ejemplo, huellas dactilares o el iris scan).

21 Por ejemplo, como el correo electrónico enviado a través de Internet es a menudo en las empresas de texto claras deben considerar métodos para cifrar correo electrónico cuando se transmite información sensible.

ELEMENTOS PARA SU POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Cree una detallada política de copia de seguridad de archivos en línea cumpliendo con los requisitos legales y reglamentarios para la retención de la información, donde se detalle:
  - De qué datos se hace copia de seguridad y cómo se hace dicha copia;
  - Con qué frecuencia se copian los datos;
  - Quién es el responsable de la creación de copias de seguridad y de validar el contenido;
  - Dónde y cómo se almacenan las copias de seguridad;
  - Quién tiene acceso a esas copias de seguridad;
  - Cómo funciona el proceso de restauración (y se ponen a prueba los datos restaurados).
- Desarrolle programas de capacitación en concienciación de seguridad de la información, incluyendo temas tales como:
  - Comunicar de forma segura y responsable;
  - El buen uso de los medios sociales;
  - Transferencia de archivos digitales de forma segura;
  - El uso apropiado de contraseñas;
  - Evitar la pérdida de información importante;
  - Asegurarse de que sólo las personas adecuadas puede acceder a su información;
  - Mantenerse a salvo de virus y otros programas maliciosos;
  - A quién avisar cuando usted detecte un potencial incidente de seguridad;
  - Cómo no ser engañados para que facilitemos información inconscientemente.

CUESTIONARIO DE AUTOEVALUACIÓN EN SEGURIDAD

La siguiente sección presenta una sencilla lista como herramienta de gestión para ayudar a guiar su revisión interna de las capacidades de resiliencia cibernéticas de su empresa, y con el objetivo de hacer las preguntas correctas a los equipos que participan en dichas iniciativas. Las preguntas formuladas en la herramienta le pueden ayudar a identificar las fortalezas y debilidades específicas – y los caminos hacia la mejora dentro de su empresa.

Al mismo tiempo, este cuestionario de autoevaluación se puede utilizar como una lista de tareas por las empresas que están empezando en sus iniciativas de seguridad de la información, y quieren usar la información como base para la planificación de sus capacidades de resiliencia cibernética.

Para cada una de las siguientes preguntas, las empresas deben identificar, de entre las opciones propuestas, la que le parezca el reflejo más exacto de las prácticas actuales de su empresa. A cada una de las opciones le ha sido dado un color, donde:

- ✖ Esta es la respuesta menos deseable; Claramente debe considerarse una mejora.
- ! Es posible una mejora adicional para proteger mejor la empresa.
- ✔ Es el mejor reflejo de capacidad de recuperación frente a las ciberamenazas.

Las respuestas al cuestionario representan la respuesta única de cada evaluador, la presencia de una lista *más específica bajo cada pregunta* tiene por objeto ayudar a identificar y documentar el estado de un conjunto de controles básicos de seguridad de la información para su empresa. La información recogida en este proceso de preguntas le ayudará a poner de relieve brechas o vulnerabilidades de modo que las empresas que utilizan esta guía sabrán dónde tienen que actuar con mayor urgencia.

1

¿Evalúa cómo de sensible es la información que se maneja dentro de su empresa?

✖ No, pero tenemos un firewall para protegernos del robo de información.

! Sí, entendemos la importancia de nuestra información y de implementar las medidas de seguridad generales.

✔ Sí, y tenemos un modelo de clasificación de la información y sabemos dónde se almacena y se procesa nuestra información sensible. Ponemos en práctica medidas de seguridad en función de la sensibilidad de dicha información.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Están sus datos sensibles identificados y clasificados?		
¿Es usted consciente de su responsabilidad con respecto a los datos identificados como sensibles?		
¿Los datos más sensibles están altamente protegidos o cifrados?		
¿ La gestión de la información privada del personal queda cubierta por los procedimientos?		
¿Son todos los empleados capaces de identificar y proteger correctamente los datos sensibles y no sensibles?		

2

¿Realiza evaluaciones de riesgos relacionados con la seguridad de la información?

- ✖ Nosotros no realizamos evaluaciones de riesgo.
- ! Evaluamos riesgos, pero no sobre ningún tema relacionado específicamente con la seguridad de la información.
- ✔ Llevamos a cabo las evaluaciones de riesgos sobre asuntos específicos de seguridad de la información.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Organiza los resultados del análisis de vulnerabilidades desde alto riesgo a bajo riesgo?		
¿Son identificados los eventos que podrían causar interrupciones en los procesos de negocio y está evaluado el impacto que potencialmente producirían dichas interrupciones?		
¿Tiene un plan de continuidad de negocio que se prueba y se actualiza de forma regular?		
¿Realiza una evaluación periódica de riesgos para actualizar el nivel de protección que necesitan los datos y la información?		
¿Están las áreas de riesgo identificadas a lo largo de sus procesos de negocio para evitar la corrupción en el tratamiento de la información o su mal uso deliberado?		

3

¿A qué nivel está implementado el gobierno de seguridad de la información?

- ✖ No se ha implantado un gobierno de seguridad de la información.
- ! La gobernanza de la seguridad de información se hace en el departamento de TI ya que es donde hace falta que la información esté protegida.
- ✔ La gobernanza de la seguridad de información se instala a nivel corporativo para asegurar su impacto en toda la empresa.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Los miembros del comité de dirección y el CEO destinan un presupuesto a seguridad de la información?		
¿La seguridad de la información forma parte de la gestión de riesgos que hacen los directores?		
¿La dirección aprueba la política de seguridad de la información de la empresa y la comunica a los empleados por un medio adecuado?		
¿Están regularmente informados los miembros del comité de dirección yd el equipo gestor de la empresa acerca de los últimos avances en políticas, normas, procedimientos y directrices seguridad de la información?		
¿Hay por lo menos un oficial perteneciente al equipo gestor que esté a cargo de la protección de los datos de carácter personal y la privacidad?		

4

¿Dispone de un equipo de seguridad de la información o una función dedicada dentro de su empresa?

✖ No tenemos un equipo de seguridad de la información ni funciones o responsabilidades específicas sobre seguridad de la información.

! No tenemos un equipo de seguridad de la información, pero hemos definido las funciones y responsabilidades específicas de seguridad de información dentro de la empresa.

✔ Tenemos un equipo de seguridad de la información o una función dedicada a la seguridad de la información.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Tiene identificado un especialista en seguridad de la información o un equipo que coordine internamente el conocimiento y proporcione ayuda al equipo gestor en la toma de decisiones?		
¿El especialista identificado o equipo de seguridad de la información, es responsable de revisar y actualizar sistemáticamente la política de seguridad de la información basada en cambios significativos o incidentes?		
¿Tiene el especialista identificado o equipo de seguridad de la suficiente visibilidad y apoyo para intervenir en cualquier iniciativa relacionada con la información en la empresa?		
¿Existen diferentes gestores responsables para distintos tipos de datos?		
¿Se revisan regularmente, por parte de un organismo independiente o de un auditor, la viabilidad y la eficacia de la política de seguridad de la información, así como la eficacia del equipo de seguridad de la información?		

5

¿De qué manera trata su empresa los riesgos de seguridad de información relacionados con proveedores que pueden acceder a su información confidencial?

- ✖ Tenemos una relación basada en la confianza mutua con nuestros proveedores.
- ! Para algunos contratos se incluyen cláusulas relacionadas con la seguridad de la información.
- ✔ Tenemos procesos que validan el acceso de los proveedores y pautas específicas de seguridad que se comunican y son firmados por nuestros proveedores.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Están los contratistas y proveedores identificados por una tarjeta de identificación con una foto reciente?		
¿Tiene usted las políticas que abordan la verificación de antecedentes para los contratistas y proveedores?		
¿El acceso a las instalaciones y los sistemas de información se cierra automáticamente cuando un contratista o proveedor termina su misión?		
¿Saben los proveedores cómo y a quién informar de inmediato en su empresa sobre la pérdida o robo de información?		
¿Se asegura su empresa de que los proveedores tienen su software y aplicaciones actualizadas con los parches de seguridad?		
¿Los requerimientos de seguridad están claramente definidos dentro de acuerdos contractuales con contratistas/proveedores?		

6

¿Evalúa su compañía de forma regular la seguridad de los equipos informáticos y de la red?

- ✖ No realizamos auditorías o pruebas o de intrusión para evaluar nuestra seguridad en ordenadores y redes.
- ! No tenemos un enfoque sistemático para la realización de auditorías de seguridad y / o pruebas de intrusión, pero ejecutamos alguna "ad-hoc" cuando resulta necesario.
- ✔ Las auditorías regulares de seguridad y/o pruebas de intrusión son parte sistemática de nuestro enfoque para evaluar la seguridad de ordenadores y de la red.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Realiza pruebas de forma regular y mantiene un registro de las amenazas identificadas?		
¿Tiene procedimientos para evaluar las amenazas humanas a sus sistemas de información, incluyendo la falta de honradez, la ingeniería social y el abuso de confianza?		
¿Solicita su empresa los informes de auditoría de seguridad de la información a sus proveedores de servicios?		
¿Se evalúa también durante las auditorías de seguridad la utilidad de cada tipo de dato almacenado?		
¿Audita usted sus procesos y procedimientos de cumplimiento de las demás políticas y normas establecidas dentro de la empresa?		

7

Cuando se introducen nuevas tecnologías, ¿evalúa su empresa los riesgos potenciales para la seguridad de la información?

- ✖ La seguridad de la información no se tiene en cuenta en el proceso de implantación de nuevas tecnologías.
- ! La seguridad de la información se implementa "ad-hoc" en el proceso de adopción de nuevas tecnologías, sólo cuando resulta necesario.
- ✔ La seguridad de la información está incluida en el proceso de implementación de las nuevas tecnologías.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
Al considerar la aplicación de nuevas tecnologías, ¿evalúa usted su impacto potencial en la política de seguridad de la información que tiene establecida su empresa?		
¿Existen medidas de protección para reducir el riesgo en la aplicación de nuevas tecnologías?		
¿Están documentados los procesos para aplicar nuevas tecnologías?		
En la aplicación de nuevas tecnologías, ¿puede su empresa confiar en suministradores que permitan esfuerzos de colaboración y el intercambio de información crítica de seguridad?		
¿Se considera a menudo la política de seguridad de la información de su empresa como una barrera a las oportunidades tecnológicas?		
¿Gestiona la empresa las nuevas tecnologías utilizando metodología de seguridad en el desarrollo de sistemas dentro del ciclo de vida de los sistemas?		

8

¿Proporciona su empresa entrenamiento en seguridad de información?

✖ Confiamos en nuestros empleados y no consideramos que las orientaciones sobre seguridad de la información sean un valor añadido.

! Sólo nuestro personal de TI reciben capacitación específica para proteger nuestra TI.

✔ Regularmente se organizan sesiones de sensibilización de seguridad de información para todos los empleados.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Se adaptan algunas de las sesiones de concienciación sobre seguridad de información al ámbito de actividad de los empleados?		
¿Se enseña a los empleados a estar atentos ante posibles brechas de seguridad de información?		
¿Dispone su empresa de una guía para que los usuarios reporten debilidades de seguridad en, o amenazas hacia, sistemas o servicios?		
¿Saben los empleados manejar correctamente los datos de tarjetas de crédito y datos de carácter personal privados?		
¿El personal ajeno y otros usuarios (en su caso) reciben también apropiada capacitación en seguridad de información y actualizaciones periódicas en las políticas y procedimientos de la organización?		

9

¿Cómo se usan las contraseñas en su empresa?

✖ Compartimos las contraseñas con otros colegas y/o no existe una política para el uso seguro de las contraseñas o para el cambio periódico de contraseñas.

! Todos los empleados, incluyendo al equipo gestor, tienen contraseñas únicas pero no se obliga a elegirlas según reglas de mínima complejidad. El cambio de contraseñas es opcional, no es obligatorio.

✔ Todos los empleados, incluyendo al equipo gestor, tienen una clave personal que debe cumplir con unos requisitos específicos y debe ser cambiada regularmente.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Su empresa ha establecido y obligado el cumplimiento de una política de contraseñas aceptada globalmente para todos los activos de la empresa?		
¿Puede usted asegurar lo siguiente acerca de todas las contraseñas en su empresa? • No se almacenan en archivos de fácil acceso; • No son débiles o en blanco o se dejan con la configuración por defecto; • Se cambian, especialmente en los dispositivos móviles.		
¿Se siente bien protegido contra el acceso físico no autorizado a los sistemas?		
¿Son los usuarios y los suministradores conscientes de su responsabilidad para proteger equipos desatendidos (por ejemplo, cerrando las sesiones cuando se marchan al finalizar su trabajo)?		
¿Se ha enseñado a los empleados cómo reconocer los trucos de ingeniería social que se utilizan para engañar a la gente para que divulguen detalles de seguridad y cómo deben reaccionar ante esta amenaza?		

10

¿Existe una política de empresa para un uso aceptable de Internet y de las redes sociales?

- ✖ No, no existe una política para el uso aceptable de Internet.
- ! Sí, existe y está disponible en una ubicación centralizada accesible a todos los empleados, pero no ha sido firmado por los empleados.
- ✔ Sí, una política para el uso apropiado Internet es parte del contrato laboral / todos los empleados han firmado la política de uso aceptable.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Existen directrices y procesos generales de comunicación para los empleados en la empresa, que incluyen la relación con la prensa y los medios de comunicación?		
¿Hay un proceso disciplinario para los empleados que violen las pautas de comunicación de la empresa?		
¿Monitoriza Internet un determinado gerente de comunicación o su equipo con el fin evaluar los riesgos a la reputación y la posición de su empresa?		
¿Ha evaluado su empresa la responsabilidad por los actos de los empleados u otros usuarios internos o atacantes de los sistemas que puedan utilizarlos para perpetrar actos ilícitos?		
¿Ha tomado medidas su empresa para evitar que un empleado u otro usuario interno ataque a otros sitios?		

11

¿Su empresa mide, reporta y hace seguimiento de asuntos relacionados con Seguridad de la Información?

✖ Nosotros no controlamos, ni informamos o hacemos seguimiento sobre la eficacia y la adecuación de las medidas de seguridad implementadas.

! Nuestra empresa ha implementado herramientas y métodos para monitorizar, reportar y hacer seguimiento de la eficacia y la adecuación de una selección de medidas de seguridad implementadas.

✔ Nuestra empresa ha puesto en marcha las herramientas y los métodos necesarios para monitorizar, reportar y hacer seguimiento de la eficacia y la adecuación de todas nuestras medidas de seguridad implementadas.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Se conservan las trazas de auditoría y registros relativos a los incidentes y se desarrollan acciones proactivas para que el incidente no vuelva a ocurrir?		
¿Verifica su empresa el cumplimiento de los requisitos legales y regulatorios (por ejemplo los de privacidad de datos)?		
¿Ha desarrollado su empresa alguna herramienta propia para ayudar al equipo gestor en la evaluación de la postura en seguridad y que permita a la compañía acelerar su capacidad para mitigar riesgos potenciales?		
¿Existe en su empresa una hoja de ruta o plan de seguridad de información que incluya objetivos, evaluación de los avances y posibles oportunidades de colaboración?		
¿Se reportan los informes sobre incidentes a las autoridades y otros grupos de interés como asociaciones de empresas del sector?		

12

¿Cómo se mantienen actualizados los sistemas de su empresa?

✖ Contamos con gestión automática de parches, proporcionada por el vendedor, para la mayoría de nuestras soluciones.

! Las actualizaciones de seguridad se aplican cada mes de forma sistemática.

✔ Tenemos un proceso de gestión de vulnerabilidades continuamente busca información sobre las posibles vulnerabilidades (por ejemplo a través de una suscripción a un servicio que envía automáticamente avisos de nuevas vulnerabilidades) y aplicamos parches basados en los riesgos que mitigan.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Es el análisis de vulnerabilidades una tarea de mantenimiento programada regularmente en la empresa?		
¿Se revisan y prueban las aplicaciones después de cualquier cambio en el sistema operativo?		
¿Pueden los usuarios comprobar por sí mismos si existen aplicaciones sin parches?		
¿Son los usuarios conscientes de que también tienen que mantener el sistema operativo y las aplicaciones actualizadas incluyendo el software de seguridad de sus dispositivos móviles?		
Están los usuarios entrenados para reconocer un mensaje auténtico de advertencia como la solicitud de permiso para actualizar (por ejemplo distinguiéndolo de solicitudes de falsos antivirus), y a notificarlo adecuadamente al equipo de seguridad si sucede algo malo o cuestionable?		

13

¿Se revisan y gestionan de forma regular los derechos de acceso de los usuarios a las aplicaciones y los sistemas?

✖ Los derechos de acceso a las aplicaciones y los sistemas no revisan ni se retiran consecuentemente.

! Los derechos de acceso a las aplicaciones y los sistemas sólo se eliminan cuando un empleado deja la compañía.

✔ Se ha establecido una política de control de acceso con revisiones periódicas de los derechos de acceso asignados a los usuarios para todas las aplicaciones relevantes del negocio y los sistemas de que las soportan.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Están los accesos a sistemas de información y recursos limitados por política y procedimientos?		
¿Su empresa dispone de una política de privacidad donde se declara el tipo de datos personales que se recogen (por ejemplo, en el caso de sus clientes: direcciones postales, direcciones de correo electrónico, historial de navegación, etc.), y las finalidades para la que se aplican los tratamientos de dichos datos?		
¿Las políticas y procedimientos especifican los métodos utilizados para controlar el acceso físico a zonas seguras tales como cerraduras de puertas, sistemas de control de acceso físico o videovigilancia?		
¿Se le retira automáticamente la autorización de acceso a las instalaciones y los sistemas de información cuando causa baja un empleado?		
¿Están clasificados los datos por razón de su sensibilidad (por ejemplo, altamente confidencial, sensible uso interno.) y sus usuarios figuran en una lista de control de acceso?		
¿Está regulado el acceso remoto a los sistemas de información de la empresa?		

14

En su empresa, ¿pueden los empleados usar sus propios dispositivos personales, como teléfonos móviles y tabletas, para almacenar o transferir información de la empresa?

✖ Sí, podemos almacenar o transferir información de la empresa en los dispositivos personales sin aplicar medidas de seguridad adicionales.

! Existe una política que prohíbe el uso de dispositivos personales para almacenar o transferir información de la compañía, pero técnicamente es posible hacerlo sin que tengamos que aplicar medidas de seguridad adicionales.

✔ Los dispositivos personales sólo pueden almacenar o transferir información de la empresa después de aplicar medidas de seguridad en el dispositivo personal y / o cuando se nos ha proporcionado una solución profesional.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Su empresa confía en la política ampliamente aceptada de “traiga usted su propio dispositivo (Bring Your Own Device)”?		
¿Están los dispositivos móviles protegidos contra usuarios no autorizados?		
¿Están todos los dispositivos y conexiones permanentemente identificados en la red?		
¿Se han instalado el cifrado en cada dispositivo móvil para proteger la confidencialidad e integridad de los datos?		
¿Es consciente el nivel corporativo de que mientras el empleado puede ser responsable de un dispositivo, sin embargo la compañía sigue siendo responsable de los datos?		

15

¿Su empresa ha tomado medidas para prevenir la pérdida de información almacenada?

- ✖ No tenemos ningún proceso de copia/restauración de seguridad.
- ! Tenemos un proceso de copia/restauración de seguridad, pero no se realizan pruebas de restauración.
- ✔ Tenemos un proceso de copia/restauración de seguridad, que incluye pruebas de restauración/ resiliencia. Tenemos copias de respaldo almacenadas en otro lugar seguro o utilizamos otras soluciones de alta disponibilidad.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Entre sus empleados existe personal suficiente que sea capaz de crear copias de seguridad y archivar ficheros?		
¿Están protegidos los equipo contra fallos de energía mediante el uso de fuentes de alimentación permanente como alimentación múltiple, fuentes de alimentación ininterrumpida (UPS), generadores de emergencia, etc.?		
¿Se prueban con regularidad los medios de copia de seguridad para asegurarse de que podrán ser restaurados dentro del plazo de tiempo fijado en el procedimiento de recuperación?		
¿Se aplican en su empresa procedimientos de reporte de equipos móviles perdidos o robados?		
¿Están los empleados capacitados sobre qué hacer si se borra accidentalmente la información y cómo recuperar la información en caso de desastre?		
¿Se han implementado medidas para proteger tanto la confidencialidad como la integridad de las copias de seguridad en su lugar de almacenamiento?		

16

¿Está su empresa preparada para manejar un incidente de seguridad de información?

✖ No tendremos ningún incidente. En caso de que lo tengamos, nuestros empleados son lo suficientemente competentes para hacerles frente.

! Tenemos procedimientos de gestión de incidentes, sin embargo, no están adaptados para manejar incidentes de seguridad de la información.

✔ Tenemos un proceso dedicado para manejar incidentes de seguridad de la información, con los mecanismos necesarios de comunicación y escalado. Nos esforzamos para manejar incidentes tan eficientemente como nos es posible, de modo que aprendemos cómo protegernos mejor a nosotros mismos en el futuro.

Las siguientes preguntas se ofrecen como una lista de verificación de seguridad de información básica para para ayudar a evaluar dónde se encuentra su empresa en este proceso.	SÍ	NO
¿Tienen en cuenta sus procesos los diferentes tipos de incidentes que van desde una denegación de servicio a la violación de la confidencialidad, etc., y las forma de manejarlos?		
¿Su empresa tiene un plan de comunicación en la gestión de incidentes?		
¿Sabe usted a qué autoridades tiene que notificar y cómo hacerlo en el caso de un incidente?		
¿Su empresa dispone de información de contactos identificados y ordenados según cada tipo de incidente?		
¿Usted confía en un gestor de comunicación interna para contactar con los empleados y sus familias durante la gestión de incidentes?		
¿Existe un proceso de lecciones aprendidas con el fin de hacer mejoras en la gestión de incidentes después de que haya ocurrido un incidente de seguridad de información?		

RECURSOS Y MARCOS MUNDIALES Y LOCALES

Junto con esta guía se ofrece un apéndice en formato electrónico con material adicional, desde códigos de buenas práctica hasta normas técnicas. Catalogados en la web www.iccwbo.org/cybersecurity, en este sitio se incluye una lista de los correspondientes marcos globales, recursos y contactos y, con el tiempo, los marcos locales que vayan proporcionando los miembros y comités nacionales de la CCI. Es una fotografía de los recursos proporcionados en el momento de publicarse este documento, pero este será un recurso que se actualizará y ampliará con el tiempo.

www.iccwbo.org/cybersecurity

The ICC Cyber security guide is also online with a one-stop resource portal offering globally relevant and localized standards, practices and advice on matters relating to technical as well as functional aspects of information security.

The portal features:

- Downloads of the ICC Cyber security guide for business
- Translated and/or locally adapted versions of the guide
- Links to globally recognized good practices, standards and frameworks
- List of public bodies and organizations with a global reach that are active in the domain of cyber and information security
- Links to country-specific resources developed by companies, government agencies and other entities.

LA CÁMARA DE COMERCIO INTERNACIONAL (ICC)

La ICC es la organización empresarial mundial, es un organismo de representación que habla con autoridad en nombre de las empresas de todos los sectores en cualquier rincón del mundo.

La misión de la ICC es fomentar la apertura del comercio internacional e inversión, así como ayudar a las empresas a enfrentarse a los retos y las oportunidades que surgen con la globalización. La convicción de la ICC data desde sus orígenes al inicio del siglo XX, en la cual el comercio es una poderosa fuerza de paz y prosperidad para el mundo. El pequeño grupo de sagaces líderes empresariales que fundaron la ICC se denominaron a sí mismos "los mercaderes de la paz".

La ICC cuenta con tres actividades principales: la elaboración de normas, la resolución de controversias y la formulación de políticas. Puesto que las empresas y asociaciones miembros están involucradas en el comercio internacional, la ICC posee una autoridad sin igual en la creación de reglas que rigen la conducta de las dichas empresas a través de las fronteras. A pesar de ser voluntarias, día a día estas reglas se aplican en innumerables operaciones y se han convertido en parte integral del comercio internacional.

La ICC también presta otros servicios esenciales, entre los que destaca la Corte Internacional de Arbitraje de la ICC, la institución arbitral líder en el mundo, Así como el servicio de la Federación Mundial de Cámaras, la red internacional de cámaras de comercio de la ICC que fomenta la interacción y el intercambio de las mejores prácticas camerales. La ICC también ofrece entrenamientos, conferencias y una amplia lista de publicaciones y herramientas especializadas en comercio internacional, banca y arbitraje internacional.

Líderes empresariales y expertos procedentes de las empresas miembros de la ICC determinan la perspectiva empresarial sobre cuestiones de gran importancia relacionadas con las políticas del comercio y la inversión, así como temas técnicos esenciales como la anti-corrupción, la banca, la economía digital, las telecomunicaciones, la ética en la mercadotecnia, el medioambiente y la energía, la legislación sobre la competencia y la propiedad intelectual, entre otros.

La ICC mantiene una estrecha colaboración con las Naciones Unidas, la Organización Mundial del Comercio y organismos intergubernamentales, entre los que figura el G20.

La ICC fue creada en 1919. Hoy en día agrupa a cientos de miles de empresas y asociaciones miembros provenientes de más de 130 países. Los comités nacionales trabajan con los miembros de la ICC en sus propios países para abordar sus preocupaciones e sus intereses y haciéndole llegar a sus respectivos gobiernos los puntos de vista formulados por la ICC.

La organización empresarial mundial

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 **F** +33 (0)1 49 53 28 59
E icc@iccwbo.org www.iccwbo.org