EDICIÓN CONSEJEROS
JUNIO 2017

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Ciberseguridad

10 preguntas que un Consejero debe plantearse

Los ciberataques se han multiplicado en los últimos años, y cada vez son más complejos y más difíciles de prevenir y detectar, lo que hace que los órganos de gobierno de las organizaciones deban incrementar la supervisión de la gestión del riesgo de ciberseguridad incluyendo, además de los conceptos clásicos asociados a la seguridad de los sistemas de información, los de prevención de la ciberseguridad y la resiliencia.

Las amenazas pueden incluir el fraude dinerario, el robo de información o el sabotaje de infraestructuras, entre otros, que pueden acarrear consecuencias económicas, legales y reputacionales muy importantes.

Este documento aborda 10 cuestiones clave que un consejero debe plantear sobre el gobierno de la ciberseguridad en su organización, que le ayuden a cumplir con las obligaciones derivadas de la Ley de Sociedades de Capital en materia de gestión de riesgos.

The Institute of Internal Auditors

Instituto de Auditores Internos de España

PRÓLOGO DEL PATROCINADOR

La ciberseguridad es una de las principales preocupaciones de empresas e instituciones. Las Tecnologías de la Información y las Comunicaciones (TIC) propician el desarrollo económico, pero con su expansión surgen nuevos retos y desafíos como la proliferación de delitos en el ciberespacio.

Los riesgos cibernéticos provienen de amenazas continuas a escala industrial sobre los activos digitales, las operaciones y la información corporativa, que se exponen a riesgos como el fraude, la indisponibilidad de servicios o los sabotajes de infraestructuras. También a robos de información, por lo que deben protegerse especialmente la información personal o documentos clasificados para evitar la pérdida de reputación, objetivo de gran parte de los ciberataques.

Como responsables de la toma de decisiones, los Consejos de Administración deben predicar con el ejemplo a la hora de gestionar y compartir la información más estratégica y confidencial. Pero el simple hecho de que el Consejo se situé "por encima" de la organización, hace que muchas veces éste quede fuera de las políticas y procedimientos de seguridad.

Como líderes en soluciones seguras de gobierno corporativo y colaboración para Consejos de Administración, en Diligent creemos imprescindible entender los riesgos asociados a la ciberseguridad, y estamos convencidos de que esta publicación le ayudará a supervisar el control de estos riesgos y a tomar mejores decisiones.

Laura Espinosa. DILIGENT

10 Preguntas que un Consejero debe plantearse

Estas preguntas ayudarán a que los miembros del Consejo de Administración puedan cuestionarse y supervisar a alto nivel acerca del control y madurez existentes en la organización sobre estos riesgos.

1 ¿Dispone la entidad de una estrategia para la gestión de los riesgos de ciberseguridad?

Para asegurar una adecuada gestión de los riesgos de ciberseguridad de una organización, el punto de partida fundamental es definir y establecer una estrategia global en ciberseguridad que contenga, al menos:

- **Modelo o marco de gestión de ciberriesgos,** que incluya las premisas y principios básicos por los que debe regirse la gestión de la ciberseguridad en la compañía.
- **Definición de roles y responsabilidades en materia de seguridad** CISO (Chief Information Security Officer), CDO (Chief Data Officer) y CRO (Chief Risk Officer), para cada uno de los departamentos involucrados en la gestión, control y supervisión de este riesgo, incluyendo el papel a desempeñar por cada una de las 3 Líneas de Defensa.
- **Comités y órganos de gobierno de ciberseguridad** que realizarán el seguimiento, escalado y *reporting* de las actividades relevantes llevadas a cabo en la gestión de la seguridad.
- **Metodología de evaluación de riesgos de seguridad** (Cyber Risk Assessment), para medir el nivel de exposición de la entidad a estos riesgos, identificando las principales carencias y *gaps* en esta materia.

2 ¿Cuenta la organización con normativa, políticas y procedimientos de seguridad de la información y ciberseguridad?

Es imprescindible contar con un conjunto de políticas, normas y procedimientos, que contemplen al menos los siguientes aspectos:

- Ámbito de aplicación y alcance de las políticas de seguridad.
- Normativa regulatoria y legislación vigente aplicable.
- Inventario y clasificación de activos e información crítica.
- Uso responsable de la información, Internet y correo electrónico.
- Gestión de usuarios, control de accesos y políticas de contraseñas.
- Procedimientos de gestión de incidentes de seguridad.
- Configuración de seguridad de sistemas, dispositivos y redes de comunicaciones.
- Controles de seguridad en el desarrollo de aplicaciones.

Es recomendable que el cuerpo normativo esté alineado con alguno de los principales estándares de buenas prácticas de seguridad (por ejemplo, ISO 27001, SOGP, ISM3) estableciéndose además revisiones, al menos con periodicidad anual.

Para la protección de la marca, reputación y propiedad industrial de la organización, así como para prevenir posibles sanciones o multas por parte de reguladores u organismos oficiales, son aspectos fundamentales a tener en cuenta la identificación, conocimiento y cumplimiento de la normativa y regulación en esta materia.

3 ¿Se realizan actividades e iniciativas en materia de formación y concienciación en ciberseguridad?

Estas actividades deben **incluir a todos los empleados**, ya que cualquiera puede ser objeto y víctima de un ciberataque, **incluyendo a la alta dirección y consejo de administración,** dada la criticidad de este colectivo debido al nivel de confidencialidad de la información que manejan; **y también a clientes,** puesto que un incidente de ciberseguridad sobre ellos puede provocar en nuestra organización pérdidas económicas, impacto reputacional, sanciones regulatorias o reclamaciones de terceros.

Es necesario concienciar y formar a todos ellos acerca de la criticidad e importancia de la ciberseguridad y de las medidas básicas para identificar y prevenir posibles ataques, mediante cursos de formación, comunicados internos, políticas y buenas prácticas, simulacros de ataques, ejercicios de prueba (por ejemplo, campañas falsas de *phishing*), etc.

La entidad deberá a su vez establecer los mecanismos necesarios para medir el nivel de cumplimiento de los empleados con las medidas propuestas, y para evaluar el grado de utilidad, beneficio y calado de estas medidas.

4 ¿Cuenta la organización con personal dedicado a la monitorización, vigilancia y gestión proactiva de la seguridad?

Es necesario contar con personal dedicado íntegramente a las tareas de monitorización, detección, análisis y tratamiento de los eventos y posibles ataques de seguridad sobre los sistemas de la compañía.

Las organizaciones de cierto tamaño comienzan a necesitar herramientas de correlación automática de eventos que proporcionen información en tiempo real de alertas de seguridad en los sistemas –para identificar posibles incidentes de seguridad o intrusiones– así como personal suficiente dedicado al análisis y tratamiento de estos eventos.

Para asegurar la correcta gestión de estas tareas de prevención y detección temprana en seguridad es fundamental contar con adecuados procesos de ciberinteligencia, que, basándose en la obtención de información de fuentes públicas, proporcionan conocimiento relevante sobre las amenazas y ataques en el ciberespacio que pueden resultar de gran utilidad en los procesos de toma de decisiones y acciones a realizar.

5 ¿Dispone la compañía de procedimientos y protocolos de gestión, respuesta y recuperación ante incidentes de seguridad?

Dada la alta probabilidad e impacto de los ciberataques, además de estar protegidos ante ellos o ser capaz de detectarlos es igualmente fundamental la capacidad de reacción, tratamiento y respuesta ante los mismos.

Por eso las organizaciones deben contar con adecuados **procedimientos para gestionar ciberincidentes,** que incluyan al menos:

- Su correcta **identificación y clasificación,** así como una estimación de su posible impacto (financiero, regulatorio, reputacional).
- **Protocolos para su tratamiento** (comités de crisis, cascada de llamadas) **y análisis** (investigaciones forenses, activación de la póliza de un ciberseguro o de fraude).
- **Notificación y escalado de los incidentes:** incluyendo posibles comunicaciones a clientes, medios de comunicación, organismos reguladores y alta dirección (Consejo de Administración y Comisión de Auditoría).
- **Mecanismos, medidas y procedimientos para su mitigación,** como activación de Planes de Continuidad de Negocio (PCN) y de Contingencia Tecnológica (PCT), o aislamiento parcial y/o total de los sistemas expuestos a Internet.

6 ¿Se realizan periódicamente ejercicios de intrusión *(hacking* ético) en los sistemas de la entidad?

Es recomendable realizar periódicamente ejercicios de intrusión/*hacking* ético sobre su plataforma tecnológica; al menos una vez al año sobre los sistemas más críticos, y con especial atención en aquellos que sean directamente accesibles desde Internet.

Estos ejercicios recrean un escenario similar a un ataque real, utilizando las técnicas, herramientas y conocimientos que un ciberdelincuente emplearía, por lo que resultan de gran utilidad para identificar vulnerabilidades de seguridad en la organización y facilitar su corrección y mitigación.

Es recomendable que estos ejercicios se realicen desde el exterior y el interior de la organización (conexión a los sistemas como lo estaría un empleado).

7 ¿Existen controles de seguridad con los proveedores externos que prestan servicios críticos a la entidad?

Gran parte de los incidentes de seguridad relevantes sufridos en los últimos años tienen su origen o están relacionados directamente con proveedores o terceros prestadores de servicios.

La externalización de servicios en diferentes modalidades –de servicios de Tecnologías de la Información o de cualquier otra naturaleza– representa un reto para mantener un nivel adecuado de ciberseguridad en cualquier organización.

Para prevenir, evitar y minimizar el impacto de un ataque e incidente de seguridad sobre o a través de los proveedores de una entidad, los procesos de selección y homologación de terceros deben incluir una evaluación de estos riesgos (Cyber-Security Risk Assessment), obteniendo el nivel de riesgo de ciberseguridad del proveedor y el servicio, que pasará a ser una variable más a tener en cuenta para su contratación.

8 ¿Cuenta la organización con revisiones periódicas de la configuración de seguridad de sus sistemas y dispositivos?

Los accesos no autorizados e intrusiones en los sistemas de nuestra organización se pueden prevenir realizando revisiones periódicas de la configuración de seguridad *(hardening)* de los sistemas de la entidad; incluyendo servidores, aplicaciones de bases de datos, dispositivos móviles, ordenadores personales y dispositivos de comunicaciones y seguridad.

Para ello se debe contar con guías o procedimientos de bastionado actualizados y completos basados en estándares y marcos de seguridad de referencia, y en las recomendaciones de los fabricantes.

El Consejo de Administración deberá conocer el plan y resultados de las auditorías internas y revisiones de seguridad realizadas por la **Tercera Línea de Defensa** (Auditoría Interna), puesto que constituyen un mecanismo de control fundamental para la compañía, para alcanzar los objetivos y niveles de protección adecuados en materia de seguridad.

9 ¿Cuenta La entidad con controles, mecanismos y herramientas para la detección y prevención de fugas y robos de información?

En la era de la digitalización, la información es el principal y más valioso activo de las empresas, con lo que su protección y seguridad son una prioridad. A su vez, **el robo de información confidencial se ha convertido junto al fraude económico en el principal objetivo de *hackers* y otras organizaciones de ciberdelincuentes.**

La aparición y sofisticación de los ataques y amenazas actuales ha provocado que los sistemas para la protección de los datos, y en concreto para la detección y prevención de robos / fugas de información (DLP: Data Loss / Leak Prevention) hayan evolucionado a gran velocidad durante los últimos años.

Actualmente existen a través de Internet y en puestos de trabajo sofisticados sistemas y herramientas de DLP dedicados a la detección y prevención de fugas de información que permiten obtener alertas en tiempo real y bloquear automáticamente este tipo de eventos y situaciones.

10 ¿Disponen Los empleados únicamente de los accesos a los sistemas de información mínimos y necesarios para desempeñar su trabajo?

Para prevenir el fraude y accesos no autorizados a los sistemas y la información crítica por parte de personal interno y de un posible atacante, es indispensable que las organizaciones cuenten con adecuados procedimientos y políticas de segregación funcional.

Es necesario contar con un inventario actualizado de todas las aplicaciones y sistemas críticos, definiendo y estableciendo los perfiles de acceso correspondientes, y otorgando exclusivamente los permisos necesarios para la realización de su trabajo (principio de mínimo privilegio).

En el acceso a información especialmente crítica se deberán implantar mecanismos de seguridad adicionales, como el doble factor de autenticación, sistemas de doble firma (requieren la autorización por parte de un segundo usuario), diferentes niveles de autorización o atribución (como el establecimiento de límites) u otras restricciones similares.

El papel de Auditoría Interna

Auditoría Interna es una función clave de buen gobierno y apoyo fundamental de la Comisión de Auditoría y por ende del Consejo de Administración. Su independencia y la labor de aseguramiento que desarrolla hacen que sea un instrumento imprescindible para que los consejeros puedan supervisar la adecuada gestión y control de los riesgos de Tecnologías de la Información y específicamente de ciberseguridad. Auditoría Interna deberá contar con los medios y recursos adecuados para cumplir estos objetivos.

- La Dirección de Auditoría Interna proporciona aseguramiento en la evaluación de la eficacia del gobierno de las Tecnologías de la Información, la gestión de los riesgos, y de los controles internos de esta materia, incluyendo la valoración de cómo las dos primeras líneas de defensa alcanzan los objetivos establecidos en gestión y control de los riesgos.

- Mediante las auditorías sobre el universo de Tecnologías de la Información, Auditoría Interna evalúa el funcionamiento de los controles y emite su opinión en base a los riesgos asociados y los hallazgos detectados, estableciendo las recomendaciones necesarias para promover el cumplimiento de los objetivos de seguridad.

- Para elaborar y definir el plan de auditorías internas de ciberseguridad, que será aprobado por la Comisión de Auditoría, Auditoría Interna deberá incorporar la información de los procesos de análisis y evaluación (Risk Assessment) realizados por la Segunda Línea de Defensa, así como el resultado de sus propios procesos de análisis de los riesgos de ciberseguridad.

- La colaboración con la Segunda Línea de Defensa es muy importante para facilitar el alineamiento con el modelo de aseguramiento corporativo y poner en contexto y elevar tanto las bondades del mismo como las deficiencias encontradas en materia de ciberseguridad.

- Auditoría Interna también deberá estar informada puntualmente de las actividades de las áreas y responsables de seguridad de TI y ciberseguridad, asistiendo a sus comités, foros y órganos de decisión, y estableciendo entre ambas líneas un canal de comunicación y *reporting* adecuado.

Para más información sobre Ciberseguridad puede consultarse el ebook *Ciberseguridad. Manual de supervisión* en https://publicaciones.auditores internos.es y el documento *Ciberseguridad. Una guía de supervisión,* elaborado por LA FÁBRICA DE PENSAMIENTO del Instituto de Auditores Internos de España y disponible en https://auditoresinternos.es/la-fabrica-de-pensamiento /documentos.

La comisión técnica encargada de elaborar la guía y este resumen está coordinada por Israel Martínez (Grupo Santander), y formada por Josep Castells (Caixabank), José Antonio Castrillo (Mazars), Jordi Civit (Meliá Hoteles), Oliver Crespo (Sanitas), Sandra Fernández (Mapfre), Gregorio Hernández (Red Eléctrica de España), Juan José Huerta (BBVA), Eduardo Iglesias (Liberbank), Daniel Martínez (Cimpress), Raúl Mateos (BBVA), Marc Muntañá (Mutua Universal), Felipe Pastor (Ernst & Young), Fernando Picatoste (Deloitte) y Albert Sans (Inditex).