Diligent

El papel de los CIO en el gobierno corporativo moderno

Septiembre de 2020 | Diligent.com/es

Diligent

El papel de los CIO en el gobierno corporativo moderno

El buen gobierno corporativo también depende del director de sistemas, del CIO y de los expertos en TI

La pandemia del coronavirus ha conllevado un cambio forzado y rápido cambio al trabajo remoto y este será seguramente uno de los legados más duraderos que nos deje. Las nuevas oportunidades de colaboración a distancia generadas por esta transición y el renovado foco sobre los riesgos inherentes a un entorno digital externo han concienciado de la importancia del CIO en el gobierno corporativo moderno. Debido al papel destacado del CIO en el gobierno corporativo, este año Diligent creó un programa especial para CIO, directores de sistemas y expertos de TI en el evento Modern Governance Summit 2020. Durante este evento, se presentaron ideas clave para que los profesionales de la tecnología puedan guiar a sus empresas a realizar dicha transformación digital.

"En el siglo XXI, no hay decisión empresarial importante que no incluya consideraciones en cuanto a ciberseguridad. La ciberseguridad debe estar integrada en todo los procesos, desde la fase de I+D hasta la fabricación y las relaciones públicas. Ese es el mensaje sobre ciberseguridad: todos estamos juntos en esto".

Larry Clinton
Presidente
Internet Security Alliance

La tecnología, los procesos y las habilidades que necesitan las empresas de hoy en día cambian tan rápidamente como el paisaje empresarial. Las organizaciones deben estar más informadas, ser más seguras y colaboradoras, y tener propósitos más definidos. El gobierno corporativo moderno proporciona a las organizaciones las herramientas necesarias para proteger los datos más confidenciales, optimizar la colaboración de los órganos de gobierno y, en última instancia, impulsar una mejor toma de decisiones.

En el Modern Governance Summit 2020 de Diligent, los líderes tecnológicos se reunieron virtualmente para compartir recomendaciones destinadas a impulsar la transformación digital y mitigar el riesgo operativo. A partir de sus discusiones sobre la colaboración segura, se creó un plan de acción para directores de sistemas y de seguridad en una era altamente dinámica.

Esta guía recopila tres conclusiones clave de la conferencia virtual. Mientras trabajamos en esta nueva normalidad, Diligent espera convertirse en su socio de confianza.

Brian Stafford
Presidente y director ejecutivo,
Diligent Corporation

1. Alinear los departamentos legales y de tecnología de la información y seguridad

Acciones recomendadas

- ☐ Comparta regularmente información sobre las responsabilidades y los próximos plazos de seguridad y cumplimiento.
- ☐ Creen políticas y procedimientos con roles claramente definidos para cada equipo y realice pruebas de seguridad periódicas.
- ☐ Implemente una plataforma de colaboración totalmente cifrada que ayude a prevenir la pérdida de datos sensibles.

Las empresas con demasiada frecuencia mantienen separados los departamentos legales y de seguridad y tecnología de la información. Sin embargo, como analizaron Henry Jiang, CISO de Diligent, y el vicepresidente sénior y asesor general, Jack Van Arsdale, este es un enfoque que dista mucho de ser óptimo para el complejo tema de la seguridad.

En el mundo virtual de hoy, los equipos legales y tecnológicos deben estar más alineados para proteger a la empresa de los riesgos cibernéticos. En caso de que se produzca un ciberdelito, la existencia de una sólida colaboración entre estos equipos garantiza una respuesta más efectiva y rápida. Sin embargo, esto requiere construir los cimientos adecuados antes de que se produzca la crisis.

"Estar bien preparados es lo más importante. Es imprescindible contar con una buena organización, tener un plan definido. De manera que, cuando haya un problema, no sea necesario abordar cuestiones básicas. Hay que dedicar el tiempo a las cosas importantes".

Jack Van Arsdale
Vicepresidente sénior y asesor general, Diligent

Para estar bien preparados, los equipos de tecnología y jurídicos deben comprender cómo difieren sus funciones y, al mismo tiempo, cómo encajan entre sí. En los entornos más colaborativos:

- Los equipos jurídicos, y de seguridad de la información y tecnología se tratan como asesores de confianza.
- Los equipos deben colaborar en la redacción, negociación e implementación de las políticas y los procedimientos de seguridad; cada equipo invita a los demás a participar en los talleres de diseño de políticas.
- Cada equipo debe tener roles y responsabilidades claramente definidos respecto de esas políticas y procedimientos.
- Los equipos construyen "memoria muscular" colectiva participando conjuntamente en ejercicios de ataques cibernéticos.
- Los equipos están alineados cuando presentan los planes y procedimientos al Consejo de Administración.
- Las vulneraciones de la seguridad se deben resolver mediante herramientas predefinidas y cada equipo opera en consonancia, según sus funciones y responsabilidades definidas en los planes de acción.

2. El Consejo de Administración debe comprender los riesgos cibernéticos empresariales

Acciones recomendadas

- ☐ El CIO debe asegurarse de que los riesgos cibernéticos se entienden como un riesgo estratégico para toda la empresa.
- ☐ Ayudar a los consejos de administración a comprender las obligaciones legales de su organización.
- ☐ Proporcionar a los consejos de administración información adecuada sobre ciberseguridad.

La ciberseguridad ha sido tradicionalmente tratada con un enfoque general, algo que un departamento de TI debía resolver por su cuenta. Sin embargo, como Larry Clinton, presidente de la Internet Security Alliance, analizó con Henry Jiang, CISO de Diligent, la ciberseguridad requiere un enfoque descendente que comience con la colaboración del Consejo de Administración y el equipo de liderazgo.

"La ciberseguridad no es un asunto del departamento de TI, sino de toda la empresa. Necesitamos la supervisión del Consejo de Administración a fin de crear el entorno adecuado para una correcta cultura de ciberseguridad y luego establecer parámetros para el apoyo cultural, incluido el soporte económico, de manera que toda la organización ponga en práctica la ciberseguridad y siga las recomendaciones".

Larry Clinton
Presidente de la Internet Security Alliance

En los últimos cinco años, se ha producido un cambio significativo de la atención del Consejo de Administración hacia la ciberseguridad. El riesgo cibernético ya no es un elemento único en la agenda del Consejo de Administración, sino una perspectiva que se aplica a cada una de las decisiones que adopta.

"Tradicionalmente, la ciberseguridad se consideraba un problema anexo que se agregaba a una reunión del Consejo de Administración durante 15 minutos al final", dijo Clinton, explicando que ahora la ciberseguridad debe tratarse de la misma manera que las decisiones legales y financieras. "No hay ni una sola decisión empresarial importante [hoy] que no incluya consideraciones de ciberseguridad. La ciberseguridad debe formar parte de todo el proceso".

Según Clinton, el equipo de dirección, liderado por el CISO, debe presentar al Consejo de Administración:

1. Un marco de seguridad cibernética que detalle dónde están los datos y cómo funcionan.
2. Una estrategia de gestión cibernética liderada por alguien con responsabilidad en varios departamentos de la organización.

Los Consejos de Administración también deberían esperar una evaluación de riesgos económica y empírica por parte del equipo directivo. Con esta información, los Consejos de Administración y los puestos de liderazgo pueden colaborar para determinar la propensión al riesgo y gestionar el riesgo a ese nivel.

3. Garantizar una colaboración segura en un mundo virtual

El correo electrónico, los mensajes de texto y otras herramientas obsoletas siguen siendo los elementos más utilizados para la comunicación y la colaboración en las empresas. De hecho, una reciente encuesta realizada por Forrester/Diligent reveló que más del 50 % de los consejeros y altos directivos utilizan a menudo el correo electrónico personal para comunicarse sobre los temas más confidenciales de la empresa. Sin embargo, el cambio hacia el trabajo remoto motivado por la pandemia ha incrementado exponencialmente la amenaza de una brecha iniciada desde dentro, ya sea por un error humano involuntario o por un abuso malicioso de privilegios.

"En su mayoría, los equipos de tecnología corporativa actúan siempre conforme a los intereses de sus organizaciones. Sin embargo, dada la naturaleza de su papel como guardianes de datos, estos empleados se consideran usuarios privilegiados cuando pueden ver en qué está trabajando el equipo directivo o qué está debatiendo, decidiendo o planificando , de modo que exponen a su organización a riesgos adicionales. Los actores maliciosos se orientan a menudo a este tipo de usuarios a través de métodos de ingeniería social u otros mecanismos de ataque para obtener acceso completo al sistema".

Henry Jiang
CISO de Diligent

Los CIO y los CISO se están percatando rápidamente de la necesidad de contar con soluciones mejoradas que permitan a los consejos de administración y al equipo directivo llevar a cabo funciones y colaborar con flujos de trabajo empresariales, al tiempo que mantienen protegida la información más sensible. Confiar la información más confidencial de una empresa a herramientas digitales requiere una evaluación seria de la infraestructura de colaboración virtual.

Evalúe la solución actual que se utiliza para la colaboración del equipo de liderazgo

1. **¿Está su plataforma actual totalmente integrada?**
   Esta plataforma debería evitar que las novedades, conversaciones, flujos de trabajo y documentos confidenciales circulen por canales no seguros como el correo electrónico. Los miembros del Consejo de Administración, los directivos y los equipos legales deben poder colaborar sin salir de los límites seguros del sistema.
2. **¿Ha habilitado el cifrado de extremo a extremo?**
   Proteger los materiales sensibles no sirve de mucho si los miembros del Consejo de Administración y los directivos siguen utilizando canales poco seguros (por ejemplo, el correo electrónico personal o los mensajes de texto) para comunicarse entre sí. Asegúrese de haber proporcionado una alternativa segura para el intercambio de mensajes y la colaboración de los órganos de gobierno.
3. **¿La solución propuesta es fácil de adoptar y usar?**
   Para garantizar la adopción, una plataforma debe reflejar la funcionalidad de las herramientas cotidianas con las que los consejos de administración y los equipos directivos ya están familiarizados. Asegúrese de que su solución sea tan fluida e intuitiva como el correo electrónico. También debe permitir que todos los grupos reciban actualizaciones y notificaciones en tiempo real.
4. **¿Se cumplen los estándares de seguridad de un mundo virtual?**
   ¿El proveedor invierte en mejorar la seguridad y realiza pruebas de intrusión? Busque la opción de garantizar permisos según los usuarios, la posibilidad de limpiar de forma remota dispositivos comprometidos y centros de datos redundantes.

4. Protección de los datos en un mundo digital remoto

Acciones recomendadas

- ☐ Centralizar los datos de la organización, las subsidiarias y terceros en una sola fuente de datos como **Diligent Entities**. Implementar protocolos de acceso para garantizar la seguridad y la precisión de los datos en todo momento.
- ☐ Automatizar los procesos de datos para identificar eficientemente las señales de alarma y proporcionar datos a los interesados.
- ☐ Implementar herramientas de colaboración y comunicación con cifrado integral para proteger los datos confidenciales mientras se trabaja en un entorno distribuido.

SOLICITAR UNA DEMOSTRACIÓN ›

La transformación digital, acelerada por la pandemia del coronavirus, ha puesto de relieve las complicaciones inherentes a una colaboración segura. En su panel de Modern Governance Summit 2020, Colleen Coda, directora ejecutiva de Technology & Innovations de The Blackstone Group, y Paolo Pelizzoli, vicepresidente ejecutivo y director de operaciones de International Realtime Payments, Mastercard, analizaron algunos de los componentes clave de un programa eficaz para garantizar la protección de los datos. Según ellos, el almacenamiento seguro de los datos, el control de acceso a la información y la prevención de filtraciones son clave.

Para las organizaciones dispersas en varias jurisdicciones o que gestionan sociedades de cartera, la centralización de los sistemas de datos y la implementación de protocolos de acceso son motores clave de un gobierno de datos eficaz.

"Hemos hecho grandes cambios para centralizar nuestros datos... ¿Cómo estar seguro de que los datos son correctos y de que la gente tiene el acceso y la visibilidad adecuados? Tenemos un equipo robusto de tecnología de la información que cuenta con un conjunto de procesos [automatizados] con los cuales se pueden realizar controles de calidad y detectar anomalías".

Colleen Coda
Directora ejecutiva, Technology & Innovations, The Blackstone Group

Además, la necesidad de optimizar y proteger las herramientas de colaboración y comunicación es mayor que nunca. A través de la implementación más amplia de técnicas y herramientas que han permitido optimizar y proteger las operaciones del Consejo de Administración, los líderes tecnológicos pueden lograr una colaboración más efectiva y segura en toda la organización.

"Lo que Diligent hace por el Consejo de Administración [se aplica al resto de la organización]. Va a parecer diferente; si observamos algunas de las decisiones que debe tomar el Consejo de Administración, estas son muy diferentes de las que se toman con un cliente o con los equipos de operaciones, seguridad, producto, finanzas, etc. Pero si pensamos en [la organización] como pequeños Consejos de Administración, las similitudes están claras".

Paolo Pelizzoli
Vicepresidente ejecutivo y director de operaciones, International Realtime Payments, Mastercard

Colaborar de forma segura y proteger a su organización de riesgos

Correo electrónico:
lespinosa@diligent.com

Teléfono: 34 91 781 70 48

Sitio web: diligent.com/es

SOLICITAR UNA DEMOSTRACIÓN ›

Las soluciones para la colaboración de la dirección y los órganos de gobierno de Diligent ayudan a los Consejos de Administración, ejecutivos y sus equipos a trabajar de forma eficaz y segura.

Los ejecutivos y los líderes empresariales necesitan una forma de colaborar en temas confidenciales a la velocidad del negocio, sin exponerse a filtraciones o ataques cibernéticos. Las soluciones de Diligent para la dirección y los órganos de gobierno permiten a los equipos directivos colaborar de forma segura, tomar decisiones con agilidad y mitigar los riesgos.

Gestión de reuniones confidenciales

- Órdenes del día seguros y distribución de materiales para las reuniones
- Gestión de tareas
- Celebración de reuniones virtuales
- Toma de decisiones, implementación de medidas y revisión de resultados

Mensajería segura

- Comunicaciones en tiempo real
- Conversaciones de grupo o privadas
- Confirmaciones de lectura
- Cifrado integral

Colaboración e intercambio de contenido confidencial

- Compartir archivos en formato nativo de forma segura
- Salas de datos con parámetros de seguridad
- Bóveda de almacenamiento
- Colaboración en directo basada en la web