www.mexis.net

CIBERSEGURIDAD Y GOBERNANZA CORPORATIVA: HACIA UNA CULTURA DE PREVENCIÓN

mexis aggity

La globalización, la digitalización y la interconectividad sin precedentes han transformado el entorno empresarial, haciendo de la protección digital un elemento clave para la supervivencia corporativa.

En la última década, la ciberseguridad ha dejado de ser un tema exclusivo del departamento de TI para convertirse en un pilar fundamental dentro de la gobernanza corporativa.

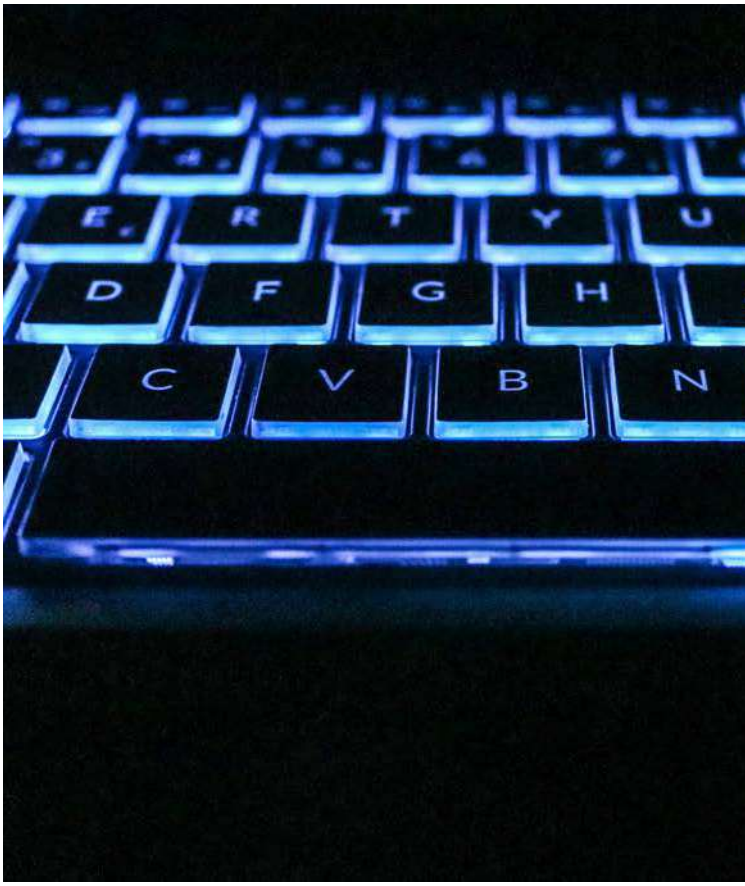
Las crecientes amenazas cibernéticas, que van desde el robo de datos hasta ataques de ransomware, exigen una visión estratégica que vaya más allá de la simple protección de datos. **Hoy, la ciberseguridad debe ser vista no sólo como un conjunto de prácticas técnicas, sino como un asunto estratégico que afecta el núcleo de las organizaciones.**

La globalización, la digitalización y la interconectividad sin precedentes han transformado el entorno empresarial, haciendo de la protección digital un elemento clave para la supervivencia corporativa. Sin embargo, aún persiste una mentalidad reactiva: **muchas organizaciones se limitan a implementar herramientas de seguridad tecnológica sin considerar los riesgos sistémicos que enfrentan** o la importancia de educar a sus colaboradores para lograr un cambio de comportamiento a largo plazo.

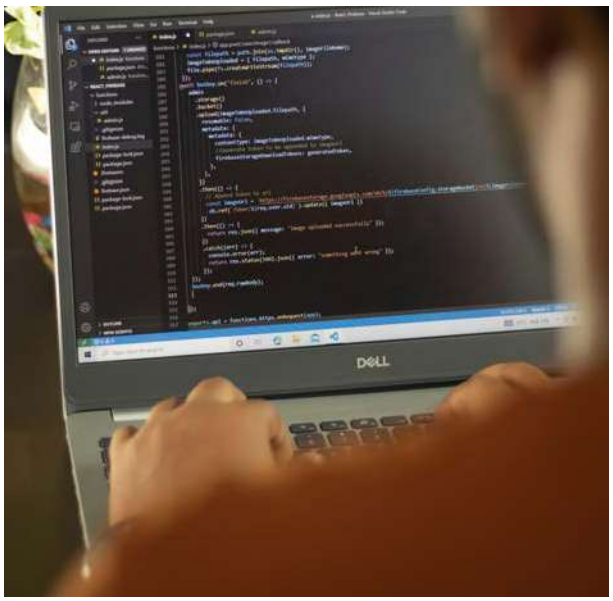
El ciberespacio es una arena de batalla donde las organizaciones deben protegerse tanto de actores maliciosos como de las vulnerabilidades internas, que pueden derivar en costosos errores de seguridad. En este sentido, la gobernanza corporativa no puede limitarse a cumplir con normas de protección de datos o adoptar tecnologías de vanguardia. **Es crucial que las empresas comprendan que la ciberseguridad debe estar integrada en todos los niveles de la organización,** desde el consejo de administración hasta los colaboradores de primera línea.

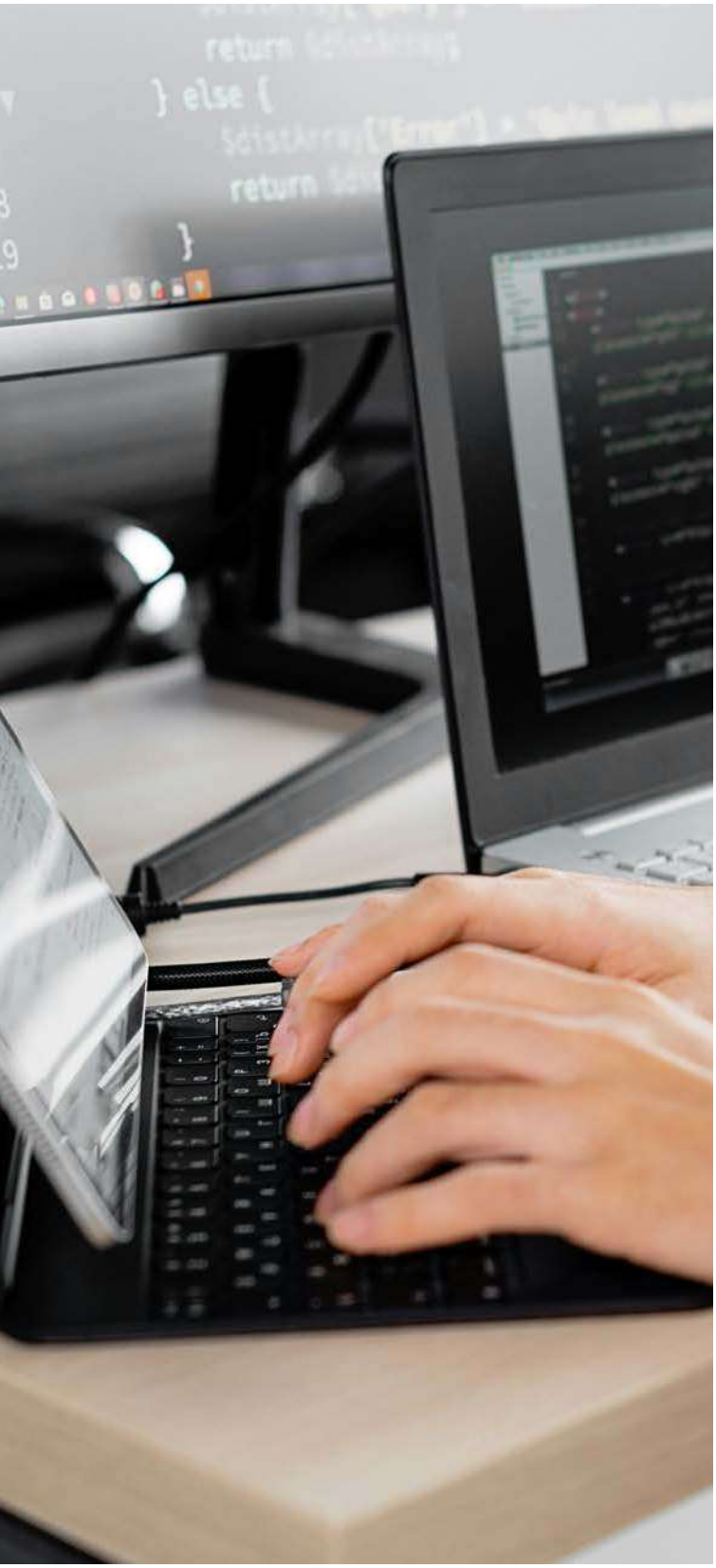
Los directivos tienen la responsabilidad de asegurar que la ciberseguridad sea parte de la estrategia general de la empresa, supervisando los riesgos asociados y asignando los recursos necesarios para mitigarlos. La integración de la ciberseguridad en la gobernanza corporativa también implica evaluar los riesgos de manera proactiva y constante, entendiendo que la dinámica de las amenazas cibernéticas cambia rápidamente.

Si bien las herramientas tecnológicas como los firewalls, los sistemas de detección de intrusos y el cifrado de datos son esenciales, no son suficientes para enfrentar el panorama de amenazas actual. **La ciberseguridad no es solo un problema técnico, también es humano.** Gran parte de las brechas de seguridad se deben a errores humanos, como el uso de contraseñas débiles, la falta de actualización de software o la vulnerabilidad ante ataques de phishing.



Por ello, un enfoque integral de la ciberseguridad debe incluir la concientización y la educación en todos los niveles de la organización. Las empresas deben adoptar una cultura de ciberseguridad en la que cada colaborador entienda su papel en la protección de los activos digitales de la organización. **Esto requiere la implementación de programas de capacitación continua que enseñen a identificar amenazas y promuevan una conducta cibersegura.**
Es vital que las empresas inviertan en formación y capacitación para que desarrollen una comprensión clara de los riesgos cibernéticos y las mejores prácticas para evitarlos. Un comportamiento responsable por parte de los empleados puede marcar la diferencia entre un ataque exitoso y uno frustrado. Además, la creación de políticas claras y el fomento de la comunicación interna sobre temas de seguridad pueden ayudar a prevenir errores y fortalecer la capacidad de respuesta ante incidentes.





Uno de los mayores retos para las organizaciones es lograr un cambio de comportamiento sostenible en sus colaboradores. La educación en ciberseguridad no debe verse como un proceso aislado o puntual, sino como parte de un esfuerzo continuo para crear una mentalidad de seguridad en toda la organización. **Esto requiere ir más allá de las capacitaciones tradicionales y adoptar enfoques innovadores que involucren activamente a los colaboradores.**

Además, es fundamental que los líderes de la organización promuevan el ejemplo. La seguridad debe estar alineada con la cultura organizacional, y los líderes deben asumir un papel activo en la promoción de buenas prácticas. **El liderazgo en ciberseguridad no debe recaer únicamente en el departamento de TI, sino que debe ser impulsado desde la alta dirección para generar un verdadero impacto.**

La creciente sofisticación de las amenazas cibernéticas demanda un enfoque estratégico, donde la gobernanza corporativa juegue un papel central en la identificación, gestión y mitigación de riesgos. **Más allá de la protección de datos, las empresas deben apostar por la concientización, la educación continua y un cambio de comportamiento en sus colaboradores.** Solo así será posible crear una cultura de ciberseguridad sostenible que proteja a las organizaciones de las amenazas del futuro.

Fuente de información: forbes.com.mx
Autor: Arlene Ramírez Uresti