DELL Technologies

5 Recomendaciones para un entorno seguro para la innovación

1	2	3	4	5
Comuníquese con prontitud y frecuencia	**Racionalice y simplifique la pila de seguridad**	**Establezca límites de ciberseguridad**	**Mantenga la flexibilidad, utilice la creatividad**	**Fomente una cultura de seguridad sólida**
Involucre a ejecutivos y partes interesadas clave	Reduzca la complejidad	Defina las políticas	Adopte nuevos métodos de seguridad	Facilite una amplia participación
Comprenda los planes de innovación	Elimine las redundancias	Implemente controles de acceso	Céntrese en métodos de seguridad que se adapten a la innovación	Promueva la transparencia
Capacite al equipo de seguridad para fomentar la conversación	Cree un único panel	Realice integraciones en sistemas lógicos y físicos	Tenga en cuenta que la innovación puede producirse en el departamento de seguridad	Impulse la colaboración
	Desarrolle un proceso sólido de evaluación de adquisiciones			

Cree un entorno seguro para la innovación.

Para maximizar la innovación en nuestro mundo tecnológico y basado en los datos, la ciberseguridad debe diseñarse para respaldar la innovación. Pero, ¿cómo puede una organización crear un entorno que potencie el crecimiento, la creatividad y la innovación sin poner en riesgo la seguridad?

Para investigar un ejemplo real de este tipo de entorno, Sameer Shah, del equipo de ciberseguridad y marketing de Dell, se reunió con el Dr. Tony Bryson, director de seguridad de la información (CISO) de la ciudad de Gilbert, Arizona, para hablar sobre la innovadora iniciativa City of the Future y el papel que desempeña la seguridad en su desarrollo.

Siga leyendo para obtener un resumen de las recomendaciones del Dr. Bryson y para ver la conversación completa, visite **dell.com/cybersecuritymonth**.

> "Asegúrese de saber a dónde quieren ir [las partes interesadas] y cómo pueden aprovechar la tecnología y la innovación para beneficiar a la empresa y al cliente".
>
> ***Dr. Tony Bryson**, Director de seguridad de la información (CISO) en la ciudad de Gilbert*

The City of the Future

La iniciativa City of the Future de la ciudad de Gilbert se diseñó para crear una infraestructura sostenible y resiliente que utilice datos para enriquecer la vida de sus ciudadanos. La tecnología está muy involucrada en la prestación de servicios, desde el pago de las facturas por parte de los residentes hasta las gestiones de tráfico, pasando por la disponibilidad y calidad del agua. También implica la recopilación de datos para predecir el uso y las necesidades futuras del servicio. La iniciativa no tiene un punto final concreto, sino que es un proceso iterativo que impulsa el progreso continuo.

Como primer CISO, el compromiso del Dr. Bryson era adoptar un enfoque más estratégico de la ciberseguridad. La prestación de servicios urbanos modernos y basados en la tecnología requeriría sólidas funciones de protección, clasificación y control de datos diseñadas para respaldar los ambiciosos objetivos de la ciudad.

A medida que ese proceso ha continuado y ha dado sus frutos, el Dr. Bryson ha identificado algunas recomendaciones clave que facilitaron el éxito y crearon el entorno adecuado para crecer e innovar de manera segura.

Comuníquese con prontitud y frecuencia

El Dr. Bryson hizo hincapié en la necesidad de involucrar a los ejecutivos y otras partes interesadas clave en las primeras etapas del proceso de innovación. "Asegúrese de saber a dónde quieren ir y cómo pueden aprovechar la tecnología y la innovación para beneficiar a la empresa y al cliente", dijo.

Una extensión natural de la comunicación en las fases tempranas es mantener la conversación sobre ciberseguridad al inicio del ciclo de innovación y, como socio clave, el equipo de ciberseguridad puede ser el catalizador de estos debates.

El uso de la IA en la ciudad de Gilbert ofrece un buen ejemplo. El departamento de seguridad comenzó estas conversaciones hace dos años y asumió un papel de liderazgo en la formulación de preguntas críticas: cómo confiar en los datos generados por IA, cómo almacenarlos y cómo garantizar que los residentes comprendan correctamente el uso de la IA. Esto llevó a la creación de un comité multifuncional, que luego condujo a la contratación del director de inteligencia artificial a tiempo completo de la ciudad de Gilbert, también un puesto pionero en el oeste de los EE. UU.

"Nada de esto habría sucedido si hubiéramos trazado una valla de seguridad que impidiera que se produjera esa innovación en particular", dice el Dr. Bryson. "Cuando se trata de intentar innovar y hacer las cosas de la manera correcta, lo primero que hay que hacer es conversar".

Racionalice y simplifique la pila de seguridad

Una de las primeras tareas del Dr. Bryson fue hacer inventario de la pila de seguridad para comprender el uso de cada producto y servicio. Ese esfuerzo descubrió una redundancia significativa. Reducir y racionalizar ahorraría dinero, pero lo que es más importante, le daría al pequeño equipo de seguridad un único panel y una fuente única de información mediante la cual gestionar las capacidades de ciberseguridad y abordar los problemas.

El Dr. Bryson se hizo eco del anticuado dicho de que la complejidad es el enemigo de la ciberseguridad cuando dijo: "No quiero ver a la gente teniendo que saltar de un sistema a otro tratando de averiguar qué está pasando".

Establezca las barreras de ciberseguridad adecuadas

Los innovadores de la organización deben comprender y respetar las guías de seguridad que protegen los sistemas y los datos. Esas reglas pueden ser políticas, controles de acceso u otros principios que ayuden a los innovadores a comprender el campo de juego. Estas condiciones representan un entorno seguro para la innovación, creado a través de una colaboración eficaz entre la seguridad y los innovadores.

Mantenga la flexibilidad, utilice la creatividad

El Dr. Bryson señaló que, si bien es importante contar con estándares de ciberseguridad y aplicarlos, la innovación requerirá fluidez y creatividad en ciertas ocasiones. Y señaló: "La innovación no solo se da en la unidad de negocio. La innovación muchas veces ocurre dentro de la tecnología de la información e incluso en el departamento de seguridad de la información. Es posible que deba encontrar formas nuevas y creativas de proteger sus sistemas y datos a medida que su empresa innova a su alrededor. Así que prepárese para ello".

DELL Technologies

Fomente una cultura de ciberseguridad sólida

El Dr. Bryson destacó la importancia de desarrollar una cultura de seguridad sólida. "La cultura lo es todo... cuando hablamos de ciberseguridad. Si no se crea una cultura en la que las personas sean conscientes de la ciberseguridad, reconozca la superficie de la amenaza".

La base de una cultura de ciberseguridad sólida se fundamenta en muchos de los elementos ya mencionados: diálogo abierto y transparente, amplia participación, estándares claramente articulados y un espíritu de colaboración entre el equipo de seguridad y sus clientes, tanto internos como externos.

A medida que el crecimiento se acelera, la ciberseguridad debe evolucionar de una postura reactiva centrada en la defensa a un enfoque proactivo que priorice la obtención de resultados positivos.

Las organizaciones deben adoptar un enfoque de seguridad moderno que no solo proteja, sino que también potencie la innovación.

Esto se puede lograr a través de la comunicación y la colaboración que integra las medidas de seguridad en el proceso de desarrollo. El objetivo es un entorno en el que la creatividad prospere sin comprometer la seguridad.

Descubra cómo afrontar algunos de los principales retos de ciberseguridad actuales en **dell.com/cybersecuritymonth**