DELL Technologies

Impulse la madurez en ciberseguridad y la confianza cero.

No permita que los riesgos de seguridad obstaculicen su capacidad de innovación

Sepa en qué punto se encuentra su ciberseguridad

Sepa dónde tiene que llegar

El panorama de las amenazas actual es complejo y evoluciona rápidamente; ante él, las organizaciones suelen contar con recursos y conocimientos limitados a la hora de mantener unas prácticas de ciberseguridad sólidas. Conseguir madurar los protocolos de ciberseguridad y confianza cero es esencial para combatir las ciberamenazas en evolución y mantener un entorno seguro sin mermar la innovación.

Utilice estas listas de control para evaluar el estado actual de su madurez en materia de ciberseguridad. Conocer los puntos fuertes y las vulnerabilidades de su organización le permite tomar las medidas correctas para mejorar la madurez de su ciberseguridad.

Índice

Más información

Obtenga más información sobre cómo avanzar en la madurez de sus protocolos de ciberseguridad y confianza cero

Lista de verificación:

Reducción de la superficie de ataque

La superficie de ataque son todos los puntos o áreas de un entorno que pueden ser atacados o explotados por un ciberatacante. Estos puntos pueden incluir vulnerabilidades de software, configuraciones incorrectas, mecanismos de autenticación débiles, sistemas sin parches, privilegios de usuario excesivos, puertos de red abiertos, seguridad física deficiente y mucho más. Estas preguntas pueden ayudar a determinar cómo minimizar las vulnerabilidades y los puntos de entrada que un actor malicioso puede poner en peligro.

Sí	No	
☐	☐	¿Su organización realiza evaluaciones, pruebas de penetración o simulaciones de vulneraciones y ataques con regularidad para identificar las debilidades de los sistemas y redes, lo que permite realizar correcciones y mejoras oportunas?
☐	☐	¿Su organización lleva a cabo formación periódica sobre seguridad para sus empleados?
☐	☐	¿Su organización utiliza la autenticación multifactor (MFA) y los controles de acceso basados en roles (RBAC)?
☐	☐	¿Su organización ha implementado la segmentación de la red para aislar los activos críticos y limitar el acceso entre diferentes partes de su red?
☐	☐	Implemente prácticas de cifrado seguras, lleve a cabo pruebas de seguridad y revisiones de código con regularidad, y utilice un firewall de aplicaciones web (WAF) para protegerse frente a ataques comunes a nivel de aplicaciones y reduzca la superficie de ataques a aplicaciones web.
☐	☐	¿Su organización elige proveedores de TI que puedan dar fe de los procesos y procedimientos para proteger su cadena de suministro?
☐	☐	¿Su organización implementa principios de confianza cero para sustituir la seguridad tradicional basada en el perímetro?
☐	☐	¿Su organización aprovecha el principio de privilegios mínimos para limitar a los usuarios y las cuentas del sistema a fin de que solo tengan los derechos de acceso mínimos necesarios para realizar sus tareas?
☐	☐	¿Su organización aplica parches regularmente a sus sistemas y software?
☐	☐	¿Las herramientas de seguridad de su organización utilizan capacidades de IA/ML para ayudar a identificar vulnerabilidades de forma proactiva?

Lista de verificación:

Detección y respuesta ante ciberamenazas

Detectar las ciberamenazas y responder a ellas es un componente esencial de cualquier estrategia de seguridad. Implica monitorear y analizar el tráfico de red, los registros del sistema y otras áreas, así como los datos de seguridad para identificar signos de acceso no autorizado, intrusiones, infecciones de malware, violaciones de datos u otras amenazas cibernéticas. Estas preguntas pueden ayudar a determinar cómo su organización identifica de forma proactiva y aborda activamente posibles incidentes de seguridad y actividades malintencionadas dentro de una red informática, un sistema o una organización.

Sí	No	
☐	☐	¿Su organización supervisa continuamente las actividades de los sistemas y las redes mediante herramientas y tecnologías de seguridad como Extended Detection and Response (XDR), intrusion detection systems (IDS), intrusion prevention systems (IPS), SIEM y análisis de registros?
☐	☐	¿Su organización analiza los datos recopilados para identificar patrones, anomalías e indicadores de riesgo (IoC) o indicadores de ataque (IOA) que puedan indicar una posible ciberamenaza?
☐	☐	¿Su organización ha implementado las últimas herramientas de visibilidad y supervisión para detectar y alertar rápidamente sobre posibles productos?
☐	☐	¿Su organización supervisa el tráfico de red en busca de patrones inusuales o actividades sospechosas que puedan indicar que se está produciendo un ciberataque?
☐	☐	¿Su organización ha implementado alguna herramienta de IA/ML para ayudar a detectar ciberamenazas mediante el análisis en tiempo real de patrones de datos o comportamientos inusuales?
☐	☐	¿Su organización ha considerado implementar una solución SIEM de última generación para gestionar mejor las alertas de seguridad y comenzar la correlación de los datos de eventos de seguridad de todo el ecosistema de TI?
☐	☐	¿Su organización pone en práctica las pruebas y la gestión de vulnerabilidades para priorizar y abordar las vulnerabilidades existentes, así como para responder de manera eficiente a las nuevas vulnerabilidades?
☐	☐	¿Su organización cuenta con un plan de respuesta ante incidentes para investigar y mitigar los incidentes de seguridad confirmados?
☐	☐	¿Su organización incorpora herramientas de coordinación, automatización y respuesta de seguridad (SOAR) para acelerar las acciones de respuesta ante incidentes que pueden ayudar a reducir la propagación de un ciberataque?
☐	☐	¿El plan de respuesta ante incidentes de su organización tiene en cuenta las políticas de contención, los planes de comunicación, los requisitos de cumplimiento normativo, el análisis forense y el proceso de recuperación?

Lista de verificación:

Recuperarse de un ciberataque

Lea acerca de la importancia de restaurar los sistemas, las redes y los datos afectados a un estado seguro y operativo tras un incidente de seguridad. Implica tomar medidas para mitigar el daño causado por el ataque, reconstruir servicios y dispositivos comprometidos o interrumpidos, analizar el incidente para evitar futuros ataques y devolver las operaciones de la organización a la normalidad. Estas preguntas pueden ayudar a determinar si su organización se está recuperando eficazmente de los ciberataques.

Sí	No	
☐	☐	¿Su organización ha implementado alguna medida de contención de incidentes para aislar y contener un ciberataque?
☐	☐	¿Su organización cuenta con procesos para la restauración de sistemas o dispositivos después de contener un incidente?
☐	☐	¿Su organización utiliza aislamiento de datos, inmutabilidad o un Cyber Vault para proteger sus datos?
☐	☐	¿Su organización ha establecido procedimientos para recuperar los datos de forma limpia en caso de que los datos se vean comprometidos, cifrados o eliminados?
☐	☐	¿Su organización utiliza tecnologías de IA/ML para ayudar a automatizar o acelerar la recuperación tras un ciberataque?
☐	☐	¿Su organización evalúa continuamente el incidente e identifica las áreas de mejora después de un ataque y se recupera?
☐	☐	¿Su organización ha llevado a cabo un análisis forense para comprender la metodología de ataque, determinar el alcance de la vulneración, identificar los sistemas y datos afectados y recopilar pruebas para aumentar su seguridad y emprender acciones legales o disciplinarias?
☐	☐	¿Sabe su organización que debe notificar a las partes relevantes, como clientes, socios y proveedores, acerca de un ciberataque y cualquier posible impacto en sus datos u operaciones?
☐	☐	¿Su organización pone en práctica sus estrategias de recuperación varias veces al año para ganar confianza en la restauración de su negocio y cumplir con sus SLA?
☐	☐	¿Colabora su organización con proveedores de servicios para ayudar con la recuperación de su organización?

Consiga un avance en la madurez de la ciberseguridad y la confianza cero

Es fundamental que las organizaciones de TI se planifiquen para el peor de los casos en lo que respecta a la ciberseguridad y que cuenten con varias capas de defensa. En el panorama de amenazas de ciberseguridad en constante evolución, es crucial avanzar continuamente en las prácticas de seguridad y adoptar los principios de confianza cero. Esto incluye:

Reducción de la superficie de ataque

Minimice las vulnerabilidades y los puntos de entrada que se pueden aprovechar para poner en riesgo el entorno.

Detecte ciberamenazas y responda ante ellas

Identifique y aborde activamente posibles incidentes de seguridad y actividades maliciosas.

Recuperarse de un ciberataque

Devuelva la organización a un estado anterior, conocido, seguro y operativo tras los incidentes de seguridad.

Gracias a los conocimientos de los servicios profesionales y a la colaboración con socios empresariales de confianza, Dell ayuda a las organizaciones a establecer un estado de seguridad integral que les proteja frente a ciberamenazas en constante evolución. A medida que la tecnología continúa avanzando, también debe hacerlo nuestro enfoque de ciberseguridad para salvaguardar nuestra infraestructura digital y mantener la confianza en el ámbito digital.

DELL Technologies

Acerca de Dell Technologies

Dell Technologies ayuda a las organizaciones y a las personas a crear su futuro digital y a transformar su forma de trabajar, vivir y jugar. La empresa proporciona a los clientes la cartera de tecnologías y servicios más amplia e innovadora del sector para la era de los datos.

Obtenga más información en
www.dell.com/securitysolutions