Engineer

seguridad de la información

Proteger datos y sistemas frente al uso indebido y los daños

Qué es

La seguridad de la información es la disciplina que mantiene la información y los sistemas que la almacenan y transmiten en el estado previsto por sus propietarios: que solo la lean las personas autorizadas, que solo se modifique de las maneras previstas y que esté disponible cuando haga falta. En el habla cotidiana y en la mayoría de los nombres de puestos se abrevia a seguridad. La definición del glosario de NIST procede de la legislación federal estadounidense, 44 U.S.C. 3552, y nombra tres propiedades. La confidencialidad conserva las restricciones autorizadas sobre el acceso y la divulgación. La integridad protege frente a la modificación o destrucción indebidas e incluye poder demostrar que la información es auténtica y que su remitente no puede negar de manera verosímil haberla enviado. La disponibilidad significa poder acceder a la información y utilizarla de forma oportuna y fiable.

Las tres tiran en direcciones distintas, y esa tensión explica la mayor parte de la dificultad del trabajo. Una base de datos a la que nadie puede acceder es perfectamente confidencial y no sirve a nadie. Una copia de seguridad guardada en tres lugares mejora la disponibilidad y ofrece a un ladrón tres sitios donde buscar. La mayoría de las decisiones del ámbito consisten en encontrar un equilibrio entre esas fuerzas para un tipo concreto de información, y la respuesta para una lista pública de precios es muy distinta de la de un historial clínico.

El trabajo se realiza mediante controles, cada uno una salvaguarda concreta con un propósito definido. Algunos son técnicos: cifrado, autenticación, cortafuegos o control de acceso. Otros son de procedimiento: revisar un cambio antes de publicarlo, retirar el acceso al personal que se marcha en su último día o disponer de un plan de incidentes por escrito. Otros son físicos, como una sala cerrada con llave. NIST SP 800-53 es un catálogo de estos controles, agrupados en familias y redactados para que una organización pueda escoger los que se ajusten a sus riesgos. El Marco de Ciberseguridad de NIST 2.0 trabaja un nivel por encima.

Describe resultados bajo seis funciones —Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar— y declara que no prescribe cómo deben lograrse.

Utilice el concepto en una decisión

Aplique «¿Qué es la seguridad de la información?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Cuentas, contraseñas y permisos organizados para que cada persona tenga exactamente el acceso que necesita y lo pierda el mismo día que deja la empresa.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 1.000 reglas RBAC para servidores Linux — 1,000 reglas de acceso escritas para cerrar una brecha de seguridad

1.000 reglas RBAC para servidores Linux Póngase en contacto →

Por qué importa

El daño a la información es difícil de deshacer. Los datos filtrados siguen filtrados, se corrija lo que se corrija después. Un registro alterado sin que nadie lo advierta pone en duda toda decisión posterior que se apoye en él. Una interrupción el día en que se procesan las nóminas o vence una licitación cuesta más que las horas que dura. Normalmente pagan primero las personas a las que pertenecían los datos y después la empresa que los custodiaba.

Para quien contrata un servicio, lo difícil es que la seguridad resulta invisible mientras funciona. Dos proveedores pueden enumerar las mismas herramientas con las mismas palabras, y quizá solo uno haya comprobado que hacen lo que dice la lista. Las preguntas útiles versan, por tanto, sobre las pruebas: qué controles están implantados, cómo se sabe que funcionan hoy y no solo el día de su instalación, y qué ocurre cuando uno informa de un problema. Un proveedor que responde con un informe generado a partir del sistema en funcionamiento está en una situación distinta de otro que responde con un documento de políticas.

Las contrapartidas son reales y tienen que ver principalmente con el tiempo y las fricciones. Todo analizador produce hallazgos y cada hallazgo necesita a alguien que decida si importa. Cada paso adicional para iniciar sesión es un paso que las personas intentarán eludir. Todo control añadido requiere mantenimiento o acaba convertido, sin que nadie lo note, en un control que solo existe sobre el

papel. La función Gobernar abre el marco porque estas decisiones son tanto de gestión como técnicas: alguien debe decidir cuánto riesgo es aceptable, qué datos merecen más cuidado y cuánto cuesta el resto de la protección.

Cómo se aplica en la práctica

En una plataforma de aplicaciones, la seguridad pasó a ser un resultado de la compilación en lugar de una opinión mediante un programa continuo de seguridad para una plataforma de aplicaciones. CodeQL realiza el análisis estático, ZAP las pruebas dinámicas y govulncheck comprueba las dependencias de Go. En cada compilación se genera un inventario de componentes de software con Anchore y Syft, y Gitleaks examina el historial en busca de credenciales. También se cubre la propia cadena de suministro de la compilación: las Actions externas que invocan sus flujos de trabajo se fijan a commits exactos, nunca a etiquetas que alguien pueda mover. Dependabot vigila 6 ecosistemas. Junto a la automatización hay 21 auditorías de seguridad por escrito, entre ellas un modelo de amenazas y una evaluación frente a la guía de pruebas de OWASP. Una vulnerabilidad reconocida por las comprobaciones configuradas puede hacer fallar la compilación. El coste es el volumen de hallazgos y la evaluación y priorización continuas necesarias para mantener útil la señal.

El servidor propio de la empresa tiene 464 MB de memoria, insuficientes para un conjunto de herramientas de métricas, por lo que su seguridad se describe mediante siete roles de solo lectura que convierten el estado del servidor en funcionamiento en Markdown. El informe de acceso cubre cuentas, alcance de sudo, huellas de claves, usuarios de la forja y roles de bases de datos. El informe de seguridad responde si el endurecimiento se aplica de verdad, no solo si está configurado: imprime las reglas del cortafuegos en su orden de coincidencia y el conjunto de reglas de bloqueo vigente, sin mostrar ninguna cifra que la ejecución no haya medido. Entre otros hallazgos, los informes descubrieron dos controles de seguridad inoperantes y un puerto a la escucha no declarado.

La distancia entre lo configurado y lo aplicado ya se había manifestado en ese mismo servidor. Un límite de frecuencia pasó un año debajo de una regla de cortafuegos más amplia que coincidía primero, por lo que ningún paquete llegaba a él. Las comprobaciones leen ahora la lista numerada de reglas y la cadena de filtrado activa, y verifican su orden. Cada puerto tiene exactamente una regla, siempre con un protocolo; el puerto SSH lleva un límite de frecuencia y nunca una regla de permiso a su lado, y la superficie pública declarada de cinco puertos se comprueba como un conjunto.

Dónde surgen los problemas

Un control está configurado, pero nunca se aplica. Un ajuste en un archivo, una regla en una lista o una política en una wiki deja constancia de una intención. Solo una comprobación del sistema en funcionamiento muestra la realidad. Un programa que cuenta controles en vez de probarlos informa de una cobertura completa mientras las brechas siguen abiertas, y la primera prueba real la hace alguien ajeno.

Todo depende de una sola capa. Un perímetro sólido con acceso sin restricciones detrás implica que un único error puede exponerlo todo. La defensa en profundidad supone que cada capa fallará en algún momento y coloca otra detrás, de modo que una contraseña robada todavía se encuentre con un segundo factor y un servicio comprometido con un rol de base de datos limitado.

Los hallazgos llegan más deprisa de lo que se leen. Un analizador que presenta todos los problemas posibles con la misma urgencia enseña a dejar de leerlo. Responsables claros, umbrales de gravedad y una regla escrita que determine cuándo un hallazgo bloquea una publicación mantienen útil la salida.

La disponibilidad solo se recuerda durante la interrupción. La confidencialidad recibe la mayor parte de la atención porque las filtraciones son noticia. Las copias de seguridad que nunca se han restaurado, un servidor único sin plan de sustitución y los certificados que caducan sin que nadie lo advierta fallan en la tercera propiedad, y suelen hacerlo el peor día posible.

Las personas externas no tienen un lugar evidente donde comunicar un problema. Quien descubre una debilidad en un servicio público necesita saber dónde avisar. La RFC 9116 define un archivo security.txt, servido desde /.well-known/security.txt, con un campo Contact obligatorio que indica adónde enviar los informes y un campo Expires obligatorio que indica hasta cuándo puede confiarse en el archivo. Sin él, los avisos acaban en un buzón general o en manos de quien responda primero.

Lecturas adicionales

- Seguridad de la información en el glosario CSRC de NIST — la definición de FIPS 200 y 44 U.S.C. 3552, con sus tres propiedades.
- 44 U.S.C. 3552 — la disposición legal que define confidencialidad, integridad y disponibilidad.

- NIST SP 800-53, revisión 5 — el catálogo de controles de seguridad y privacidad, agrupados en familias.
- Marco de Ciberseguridad de NIST 2.0 — seis funciones que describen resultados de seguridad, de Gobernar a Recuperar.
- RFC 9116 — el formato security.txt que indica a los investigadores dónde comunicar una vulnerabilidad.

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es la seguridad de la información?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/security/