Engineer

Incidente

Suceso que pone en riesgo datos o servicios de un sistema

Qué es

Un incidente es un problema en un sistema activo que ha alcanzado la gravedad suficiente para dejar el trabajo previsto y atenderlo de inmediato: un servicio que no responde, registros alterados, una máquina sin memoria, una cuenta usada por otra persona. Los equipos de seguridad dicen «incidente de seguridad»; los de operaciones, «incidente de producción» o simplemente «caída». La mayoría de las organizaciones los clasifican por gravedad.

La guía de respuesta a incidentes del NIST traza la separación en tres pasos, también útiles fuera de seguridad. Un evento es cualquier suceso observable que involucre activos informáticos: un intento de inicio de sesión, una actualización de software, una aplicación respondiendo a una petición. Un evento adverso tiene una consecuencia negativa, con independencia de su causa; la guía incluye desastres naturales y fallos eléctricos junto a los ataques. Un incidente es un evento adverso que alguien ha juzgado que cumple los criterios de la organización: el verbo de la guía para ese juicio es *declarar*. La definición que utiliza, tomada de la legislación federal estadounidense, cubre un suceso que pone, o amenaza de forma inminente con poner, información o un sistema en riesgo de perder confidencialidad, integridad o disponibilidad, o que infringe la política de seguridad.

Seguridad y operaciones usan el término con énfasis distintos. En seguridad suele implicar un adversario, una infracción de políticas o datos que pueden haber salido de la organización. En operaciones significa cualquier interrupción imprevista o degradación grave de un servicio, sin atacante. Ambos usos se solapan más de lo que sugiere el vocabulario: un ataque de denegación de servicio y un pico normal de tráfico pueden parecerse al principio en un gráfico; un disco lleno puede perder datos tan completamente como un intruso.

Conviene distinguir los términos vecinos. Un defecto es una imperfección del producto: puede permanecer inadvertido durante años y solo forma parte de un incidente cuando causa daño. Una alerta es un mensaje que avisa de un posible problema; muchas nunca se convierten en incidentes y muchos incidentes los comunica primero un cliente. La gestión de servicios registra por separado la causa de uno o más incidentes, como problema.

Utilice el concepto en una decisión

Aplique «¿Qué es un incidente?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Monitorización y alertas que avisan cuando un fallo aún es pequeño, y cifras que muestran con qué frecuencia se mantiene así.

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. Primer panel de observabilidad de la empresa — la primera visión de la empresa sobre sus propios sistemas

Primer panel de observabilidad de la empresa Póngase en contacto →

Por qué importa

La decisión implícita es un umbral. ¿Cuándo una página lenta, un inicio de sesión extraño o una cola creciente dejan de ser el ticket de un ingeniero y pasan a ser la primera prioridad del equipo? Si el umbral es demasiado alto, alguien que no ve cómo se extiende una intrusión la tratará como trabajo rutinario. Si es demasiado bajo, se interrumpe tan a menudo el trabajo que declarar ya no significa nada. El NIST propone acordar los criterios antes de necesitarlos: se declaran incidentes cuando los eventos adversos cumplen criterios previamente definidos, teniendo en cuenta los falsos positivos conocidos. Unos criterios escritos con ejemplos cuestan mucho menos que una discusión a las dos de la mañana.

La declaración cambia quién hace qué. Una persona dirige y coordina en lugar de depurar, otras dejan sus tareas normales, un canal reúne los hechos y empieza un registro con marcas temporales. Sin ello, las mismas personas duplican trabajo en paralelo y la primera explicación clara del problema la escribe un cliente.

Para algunas empresas también se activa un plazo legal. La Directiva NIS2 de la UE, Directiva (UE) 2022/2555, exige a las organizaciones incluidas en su ámbito comunicar un incidente significativo a la autoridad nacional: alerta temprana en las 24 horas siguientes a tener conocimiento del incidente, notificación del incidente en las 72 horas siguientes a ese conocimiento e informe final en el plazo de un mes desde esa notificación. Su definición no se limita a ataques: abarca cualquier evento que comprometa disponibilidad, autenticidad,

integridad o confidencialidad de los datos o de los servicios de un sistema de redes e información, por lo que una interrupción grave puede contar. Un equipo que empieza a preguntar «¿es un incidente?» el segundo día ya ha consumido la primera ventana.

El coste continuo es el tiempo de las personas y es mayor que antes. La revisión de 2025 de la guía del NIST señala que los incidentes son frecuentes y que recuperarse suele llevar semanas o meses; su predecesora de 2012 los consideraba poco frecuentes y resueltos en uno o dos días. Presupuestar incidentes implica incluir el trabajo posterior, además de la propia noche.

Cómo se aplica en la práctica

Uno de los incidentes documentados en este sitio afectó a una aplicación de escritorio macOS. Sus informes de diagnóstico registraron 111 GB de páginas comprimidas en una máquina de 36 GB el 2026-09-01; una muestra separada de la huella de memoria registró un crecimiento de unos 41 MB por segundo durante un bucle de reintentos de conexión que emitía eventos del núcleo de la aplicación. Durante la intervención se encontraron eventos de registro retenidos en un flujo principal sin límite y copiados a suscriptores que no los usaban. Se limitaron los búferes, se filtraron suscripciones por tipo de evento y se asignó un presupuesto de frecuencia al registro. Una comparación de ejecuciones completas de pruebas registró una caída de 610.996 líneas del registro del núcleo de la aplicación a 1.411. Esas mediciones corresponden a la ejecución de pruebas, no al tráfico de producción ni a la memoria después de la corrección. Las comprobaciones de arquitectura y las pruebas de presupuestos de la aplicación protegen el diseño acotado. Su política de desbordamiento puede descartar diagnósticos repetitivos y actualizar el estado afectado; los tiempos de espera de apagado requirieron una corrección aparte.

Otros incidentes son recurrentes. Ocho túneles WireGuard e IPsec entre Google Cloud y sistemas Linux eran frágiles y lentos de diagnosticar; un túnel caído podía cortar la comunicación entre entornos. El trabajo estandarizó su configuración, vigiló su estado y atacó de raíz los problemas recurrentes de enrutamiento e intercambio de claves, en vez de reiniciar los túneles, y cesaron los incidentes recurrentes de conectividad. Cuando lo mismo ocurre por tercera vez, la causa es el incidente.

Algunos incidentes empiezan con alguien que quiere ayudar. En una plataforma sin herramienta administrativa, aprobar una solicitud de titularidad, ocultar una reseña o vaciar una caché recae en un ingeniero con consola de base de datos: la página lo describe como lento, sin registro y a una errata de un incidente. La herramienta interna para operadores, con unas 40 rutas administrativas construidas con 128 componentes, somete ese trabajo a la misma autorización y el mismo rastro de auditoría que el resto del producto, a cambio de mantener probada y accesible una amplia superficie interna.

Dónde surgen los problemas

Cinco personas trabajan y nadie dirige. El chat se llena de teorías, dos ingenieros revierten cosas distintas y los clientes pasan una hora sin noticias porque nadie declaró el incidente y nadie recibió la coordinación. Permita que cualquiera del equipo lo declare y haga que el primer acto sea nombrar a una persona responsable de conservar la visión de conjunto y el registro.

El mismo incidente vuelve cada pocas semanas. La respuesta termina cuando se recupera el servicio y un reinicio cuenta como solución. Trate restablecer el servicio y eliminar la causa como dos tareas: cierre la primera esa noche y asigne responsable y fecha a la segunda antes de volver a dormir.

Las herramientas agrandan el incidente. Registrar una línea por evento produce un registro tan grande como el fallo y las reglas de alerta envían cientos de avisos por una sola causa. Dé de antemano un presupuesto a registros y alertas, agrupe repeticiones y pruebe la vía de notificación bajo la carga del fallo que comunica.

La reparación causa el siguiente incidente. Un cambio apresurado escrito a mano en producción corrige un síntoma, origina otro problema y deja un hueco en la cronología que la revisión necesitará. Mantenga una lista breve de acciones de recuperación preaprobadas que dejen rastro y registre cada cambio realizado durante el incidente.

Las lecciones llegan meses tarde o como reproches. Una revisión tras semanas de recuperación recuerda poco; preguntar quién cometió el error enseña a ocultar el siguiente. La guía revisada del NIST dice que las lecciones deberían compartirse a menudo en cuanto se identifiquen; sus recomendaciones de recuperación terminan con un informe posterior sobre el incidente, las medidas y lo aprendido. Anote qué hizo fácil equivocarse y cámbielo.

Lecturas adicionales

- Incidente — Definiciones usadas por las publicaciones del NIST, cada una con su ley o norma de origen.
- SP 800-61 Rev. 3 — Recomendaciones de respuesta del NIST de 2025, organizadas por las funciones del CSF 2.0, no por un único ciclo de respuesta.
- Marco de ciberseguridad — Marco cuyas funciones Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar sirven para organizar la guía de incidentes.
- RFC 2350: expectativas para la respuesta a incidentes de seguridad informática — Buenas prácticas vigentes del IETF sobre lo que un equipo de respuesta debe publicar acerca de sí mismo.

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 un incidente?» 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/incident/