CEGA SECURITY ■ EBOOK

DEL PUNTO CIEGO AL CONTROL

Cómo gestionar certificados digitales
cuando los ciclos se acortan

PARTE 2 · EL CONTROL

CEGA SECURITY

LO QUE DEJÓ LA PARTE 1

Dime qué certificados tienes y dónde están.

> **Es la pregunta más simple. Y la que más trabajo cuesta responder.**

04

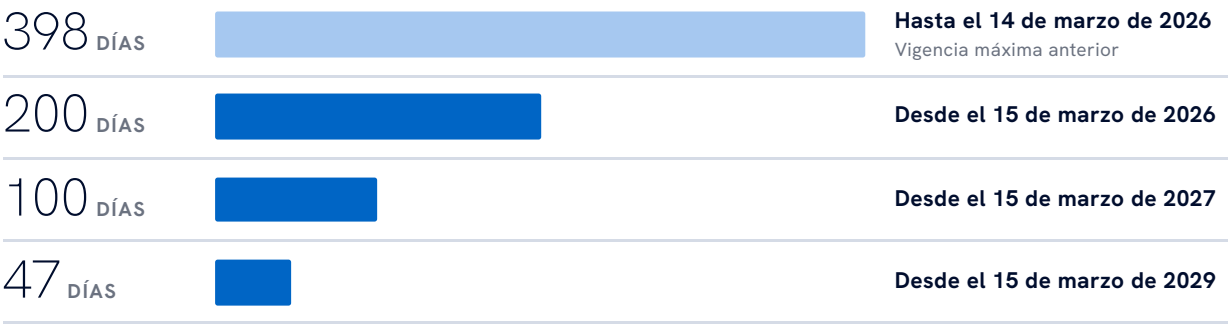
CAPÍTULO 04

EL NUEVO RITMO DE LOS CERTIFICADOS

Desde el 15 de marzo de 2026, ningún certificado TLS público puede emitirse con más de 200 días de vigencia. Desde el 15 de marzo de 2027, con más de 100. Y a partir del 15 de marzo de 2029, el máximo será de 47 días.

Lo decidió el CA/Browser Forum, el foro donde las autoridades certificadoras y los fabricantes de navegadores acuerdan las reglas que hacen que un certificado sea confiable en internet. La lógica es de seguridad y es sólida, porque un certificado que vive menos tiempo expone menos si algo sale mal con él. Desde la operación, la misma decisión se lee distinto.

Misma base instalada. Otro ritmo operativo.



A quién aplica. Certificados TLS de servidor emitidos por autoridades públicas, los que un navegador acepta sin preguntar. **A quién no.** PKI interna, certificados de firma, fiscales e integraciones entre sistemas propios.

CA/Browser Forum · TLS Baseline Requirements §6.3.2 · balota SC-081v3

Qué cambia

No vas a tener más certificados. Vas a reemplazarlos más veces.

Un parque que con 398 días de vigencia exigía cierto número de renovaciones al año exige el doble con 200, y el cuádruple con 100. Cada renovación es un evento operativo: alguien tiene que enterarse, alguien tiene que actuar, algo tiene que desplegarse. Y cada uno de los mecanismos de falla del capítulo 01 (la hoja que dejó de actualizarse, la alerta que llegó a quien no era) ocurre por evento.

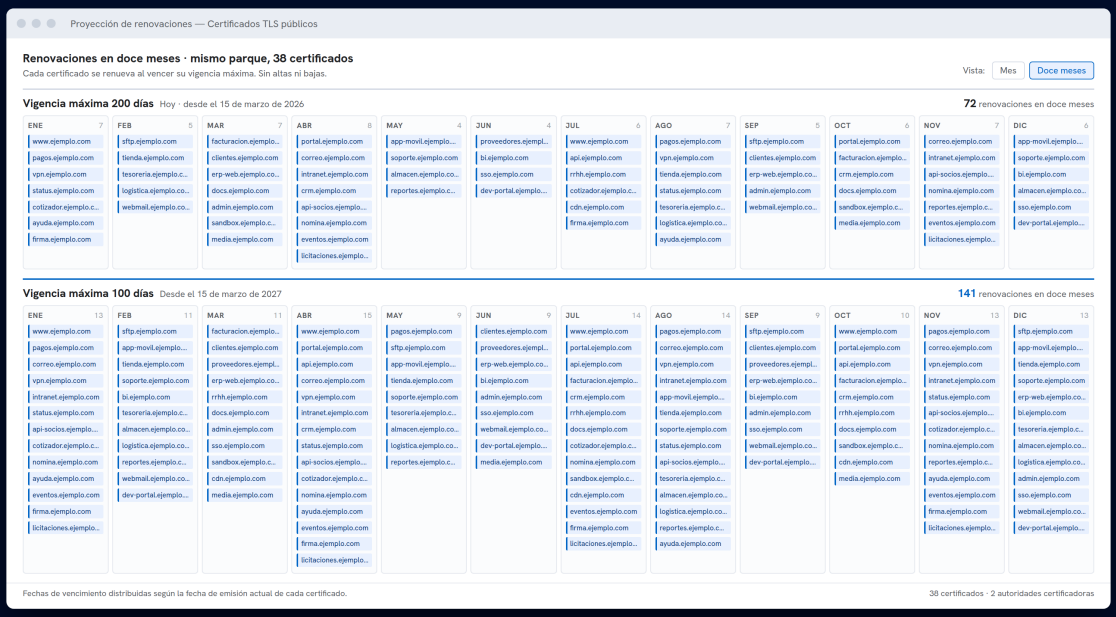
El argumento no es que menos días signifique más fallas, sino que más eventos exigen mejores bases: saber qué se tiene, quién responde y con cuánto margen. Lo que se sostiene a base de memoria y buena voluntad tiene el doble de ocasiones para fallar, y luego el cuádruple.

Qué no cambia

La regla aplica a una categoría precisa: certificados TLS de servidor emitidos por autoridades públicas, los que un navegador acepta sin preguntar. No aplica a la PKI interna, ni a los certificados de firma, ni a los fiscales, ni a los que sostienen integraciones entre sistemas propios.

Eso importa por dos razones. La primera es obvia: no hay que entrar en pánico por todo el parque. La segunda es que desde marzo de 2026 tu parque corre a dos ritmos distintos, y saber qué certificado corre a cuál, y qué parte de lo que tienes está de cada lado, es una pregunta de visibilidad antes que de calendario. Contestarla exige el inventario completo, y el inventario completo, como vimos, es justo lo que suele faltar.

EL MISMO PARQUE, EL DOBLE DE EVENTOS



Lo que todavía no se sabe

Conviene ser precisos sobre lo que sí se puede afirmar. La vigencia de 200 días entró en vigor en marzo de 2026, y en los entornos reales el efecto todavía no se siente con fuerza: las organizaciones apenas empiezan a notar el trabajo extra. Nadie puede decir todavía qué se rompe primero cuando la frecuencia sube, si el proceso de compra, la disponibilidad de la gente, la coordinación con el área dueña del servicio o el despliegue. Es un cambio demasiado reciente, y afirmarlo sería inventar.

Lo que sí se puede afirmar es más simple. Marzo de 2027 está en el calendario, el cuádruple de eventos está en la aritmética, y cada evento pasa por las mismas manos, las mismas listas y los mismos avisos que ya fallan al ritmo actual.

El calendario ya está decidido. Con qué visibilidad lo recibes, todavía no.

05

CAPÍTULO 05

VISIBILIDAD, GOBIERNO Y AUTOMATIZACIÓN

Tres palabras que en las conversaciones sobre certificados se usan como si fueran intercambiables, y no lo son. Cada una responde a una pregunta distinta, y confundirlas es la forma más común de resolver muy bien un problema que no era el tuyo.

CONOCER

VISIBILIDAD Y CONTEXTO

Qué existe, dónde está, quién responde y qué servicios dependen de ello.

→

DECIDIR

GOBIERNO

Qué política aplica, qué prioridad tiene, quién debe actuar y qué evidencia debe quedar.

→

EJECUTAR

AUTOMATIZACIÓN

Cómo emitir, reemplazar, desplegar, revocar y orquestar procesos repetibles.

Por qué gobierno va en medio

Porque ver no equivale a gobernar. Un inventario perfecto, con contexto completo, sigue siendo información. Alguien tiene que convertirla en responsables, prioridades, políticas, excepciones y una acción definida, y ese paso no lo da ninguna herramienta: lo da alguien con autoridad para decidir.

De los tres, en la práctica es el que más seguido falta. Lo primero que no aparece cuando se pregunta por un certificado sin dueño no es el inventario ni la alerta, sino la política que diría quién es el dueño. Sin ella, el responsable se asigna por defecto, a seguridad casi siempre, y el resto del contexto se hereda de una decisión que nadie tomó.

La automatización, por su parte, gana valor exactamente en proporción a lo bien que se entiende el proceso que va a ejecutar. Automatizar un proceso que nadie ha decidido no es eficiencia, es acelerar la improvisación.

No es una elección

La pregunta que más se escucha es "¿visibilidad o automatización?", como si hubiera que quedarse con una. No hay que quedarse con una. Las tres hacen falta y ninguna sustituye a la otra. Lo único que está en discusión es el orden, y el orden no es una preferencia sino una consecuencia: no puedes decidir sobre lo que no ves, y no deberías ejecutar lo que no has decidido.

Hay una forma rápida de comprobarlo. Imagina que automatizas mañana exactamente lo que ves hoy: todo lo que está en tu inventario se renueva solo, a tiempo, sin que nadie intervenga. ¿Qué pasa con lo que no está en el inventario? Exactamente lo mismo que pasaba antes. La automatización cubrió lo que ya conocías y el punto ciego siguió donde estaba, con una diferencia: ahora tienes la sensación de que el problema está resuelto.

La automatización no resuelve lo que todavía no puedes ver.

Por eso lo que sigue no discute si automatizar. Discute qué tiene que ser verdad antes.

06

CAPÍTULO 06

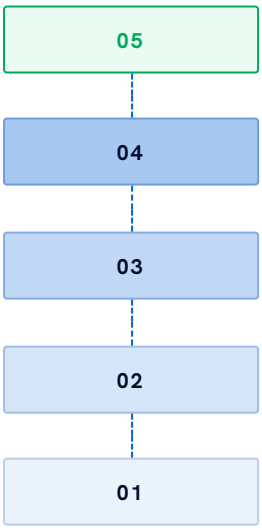
EL CERTIFICADO NO VIVE SOLO

Un certificado, visto de cerca, es un archivo. Lo que lo vuelve importante no está en el archivo sino encima de él.

Encima hay un componente —un balanceador, un servidor, un equipo de red, un contenedor— que lo usa para identificarse o para cifrar. Sobre el componente corre una aplicación; la aplicación sostiene un servicio que alguien dentro o fuera de la organización consume; y el servicio existe para un proceso de negocio con nombre propio: facturar, autenticar, integrar, firmar.

Cuando el certificado falla, la falla sube por esa cadena. Cuando alguien intenta entender por qué falló, tiene que bajarla. Eso es exactamente lo que hizo el equipo del capítulo 01 durante esas dos a cuatro horas: recorrer la cadena de arriba abajo, sin mapa, a oscuras.

Lo que sigue es el mapa.



PROCESO DE NEGOCIO
Facturar, autenticar, integrar, firmar. Es lo que se cae.

SERVICIO
Dueño: negocio. Lo que alguien consume dentro o fuera de la organización.

APLICACIÓN
Dueño: desarrollo, o un proveedor. Lo que corre sobre el componente.

COMPONENTE
Dueño: infraestructura. Balanceador, servidor, equipo de red, contenedor.

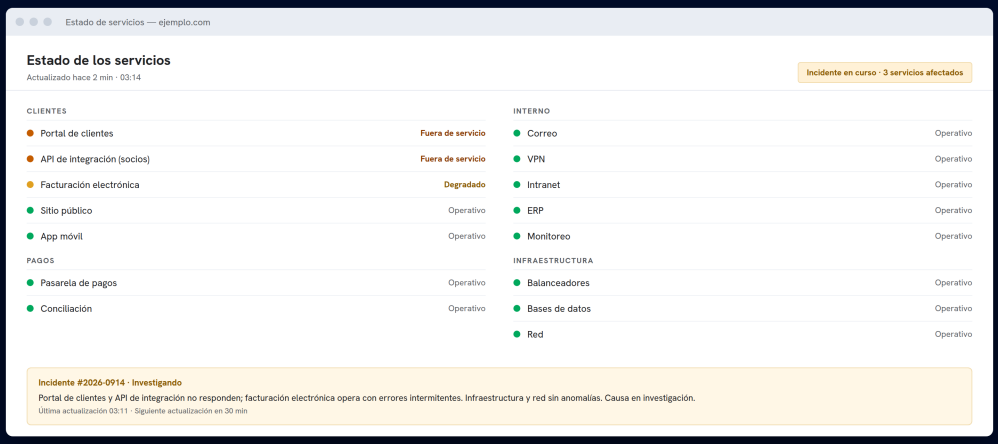
CERTIFICADO
Dueño: seguridad. El archivo. Lo que expira.

Cuatro eslabones, cuatro dueños

La cadena tiene una propiedad incómoda: casi nunca pertenece a un solo equipo. El certificado lo emitió seguridad; el componente lo administra infraestructura; la aplicación es de desarrollo, o de un proveedor; y el servicio tiene un dueño de negocio que probablemente no sabe qué es un certificado. Cuatro eslabones, cuatro dueños, y ninguno ve la cadena completa.

Por eso “quién responde” es una pregunta tan difícil, y por eso el capítulo 02 encontró el certificado asignado a seguridad y no a quien depende de él. No es por descuido, sino porque la cadena cruza fronteras que el organigrama no cruza. Contextualizar un certificado es, en el fondo, escribir esta cadena para cada uno y ponerle nombre a cada eslabón.

UN CERTIFICADO FALLA. TRES SERVICIOS SE CAEN.



No todos pesan lo mismo

Dos certificados técnicamente idénticos (mismo emisor, misma vigencia, mismo algoritmo) pueden tener criticidades opuestas, porque la criticidad no está en el certificado sino en lo que sostiene. El que protege un ambiente de pruebas y el que protege la facturación se ven iguales en cualquier lista. No se ven iguales a las 3:00 a.m.

Tratarlos igual es el error por defecto y el más caro: reparte la atención en partes iguales entre lo que no puede fallar y lo que puede esperar al lunes, y agota al equipo sin reducir el riesgo donde importa.

Y los certificados dependen de otros certificados

Hay una dependencia más, y es la que menos se ve porque es interna a la propia PKI. Un certificado no es confiable por sí solo; lo es porque lo firmó otro, que a su vez fue firmado por otro, hasta llegar a una raíz. Esa cadena de confianza también vence. Si

el certificado intermedio expira o se revoca, todos los que cuelgan de él dejan de ser válidos al mismo tiempo, aunque cada uno, por separado, esté vigente.

Es el escenario en que una sola fecha tumba decenas de servicios a la vez, y en que la alerta individual de cada certificado no sirve de nada, porque cada uno de ellos está bien. Por eso el diagnóstico del capítulo 07 lo pregunta de forma explícita.

La pregunta que la cadena responde es una sola: ¿qué se cae?

Si puedes contestarla para cada certificado sin preguntarle a nadie, tienes contexto. Si no, tienes una lista.

07

CAPÍTULO 07

¿EN QUÉ PARTE DEL CAMINO ESTÁS?

En la práctica, esta pregunta suele responderse con el nombre de una herramienta: “tenemos EJBCA”, “estamos con una autoridad pública”, “ya tenemos un inventario”.

Ninguna de esas respuestas dice en qué parte del camino estás. Dicen qué compraste.

> **La madurez no se mide por lo que tienes instalado. Se mide por lo que puedes responder sin abrir una hoja de cálculo y sin llamarle a nadie.**

El modelo que sigue tiene cinco niveles y una sola regla: no se salta ninguno. Son los mismos escalones del capítulo 02, vistos desde la organización y no desde el certificado.

La regla suena obvia y en la práctica se respeta poco. Es común encontrar alertas configuradas sobre un inventario incompleto, o una política de certificados escrita sobre certificados cuyo responsable nadie puede nombrar. Eso no es un nivel cuatro con un pendiente. Es un nivel uno con herramientas caras.

Por eso el diagnóstico no se hace con un puntaje. Un promedio alto esconde exactamente el hueco que importa, y el hueco es donde ocurre el incidente.

Cómo se responde

Veinte afirmaciones en cuatro grupos, uno por cada nivel que se puede alcanzar. Tres respuestas posibles: sí, parcialmente, no.

“Parcialmente” cuenta como no. No es por severidad. Un inventario que cubre la mitad de tu parque te deja expuesto en la otra mitad, y la otra mitad es precisamente donde nadie está mirando.

Tu nivel es el más alto cuyo grupo respondiste completo, con "sí" en las cinco afirmaciones. Y los grupos no se saltan: si fallas una del nivel 3, te quedas en nivel 2 aunque tengas completos los del 4 y el 5. Responder por la organización real, no por la que está en el organigrama.

El nivel 1 no tiene grupo de preguntas. Es donde estás si no completas el primero. No es un resultado que haya que comprobar, sino el punto de partida de todos.

CAPÍTULO 07 · DIAGNÓSTICO

VEINTE AFIRMACIONES, CUATRO NIVELES

PARA EL NIVEL 2 · VISIBLE

Sabes qué tienes.

		SÍ	PARCIAL	NO
01	Puedo decir cuántos certificados tiene la organización hoy, con una cifra, sin pedirle el dato a nadie.	☐	☐	☐
02	Esa cifra incluye los emitidos por las CA internas, los comprados a autoridades públicas y los de uso fiscal o regulatorio.	☐	☐	☐
03	La lista se actualiza cuando se emite un certificado nuevo, sin que alguien tenga que acordarse de anotarlo.	☐	☐	☐
04	Sé cuándo fue la última vez que esa lista se verificó contra la realidad.	☐	☐	☐
05	Si me preguntan por un servicio específico, puedo decir qué certificados lo sostienen en menos de cinco minutos.	☐	☐	☐

PARA EL NIVEL 3 · CONTROLADA

Sabes de quién es y qué sostiene.

		SÍ	PARCIAL	NO
06	Cada certificado tiene una persona responsable con nombre, no un área.	☐	☐	☐
07	Sé en qué servicio o aplicación se usa cada certificado.	☐	☐	☐
08	Distingo los certificados críticos de los que no lo son, con un criterio escrito y no con la memoria del equipo.	☐	☐	☐
09	Sé qué certificados dependen de una cadena que también vence.	☐	☐	☐
10	Cuando alguien cambia de puesto o deja la organización, hay un paso definido para reasignar los certificados que tenía a su nombre.	☐	☐	☐

PARA EL NIVEL 4 · ANTICIPADA

Te enteras antes, y se entera quien puede actuar.

		SÍ	PARCIAL	NO
11	Recibo aviso de un vencimiento con anticipación suficiente para renovarlo dentro de un proceso normal, no de una emergencia.	☐	☐	☐
12	El aviso le llega a quien puede actuar, no a una lista de distribución general.	☐	☐	☐
13	Sé cuántos vencimientos vienen en los próximos noventa días, y ese dato lo veo, no lo pido.	☐	☐	☐
14	Además de vencimientos detecto cambios de estado: revocaciones, reemplazos y certificados que aparecieron sin pasar por el proceso.	☐	☐	☐
15	Sé qué ocurre si nadie atiende el aviso. Hay un escalamiento definido y alguien ya lo probó.	☐	☐	☐

PARA EL NIVEL 5 · GOBERNADA

Existe una respuesta organizacional, y se puede demostrar.

		SÍ	PARCIAL	NO
16	Existe una política escrita de certificados y alguien responde por que se cumpla.	☐	☐	☐
17	Las excepciones a esa política están registradas, tienen dueño y tienen fecha de caducidad.	☐	☐	☐
18	Puedo entregar evidencia del estado de los certificados a una auditoría sin abrir un proyecto interno.	☐	☐	☐
19	Puedo demostrar, con registro, quién renovó qué y cuándo durante el último año.	☐	☐	☐
20	Cuando se decide un cambio —una CA nueva, una vigencia más corta, otro proveedor— sé a qué certificados y a qué servicios afecta antes de ejecutarlo.	☐	☐	☐

Qué significa tu resultado

Cada nivel trae la misma estructura: cómo se ve un día normal, cuál es el riesgo que domina y cuál debería ser la siguiente conversación interna. La siguiente conversación no es una compra. Es una decisión que alguien de tu organización tiene que tomar.

1 NIVEL 1 · REACTIVA

Ningún grupo completo. Te enteras de que un certificado existía cuando el servicio deja de responder. El inventario, si existe, es la hoja de cálculo de alguien. El riesgo dominante no es el vencimiento, sino no saber cuántos vencimientos tienes por delante.

La siguiente conversación: de dónde sale la lista completa. Mientras esa pregunta no tenga respuesta, cualquier inversión posterior cubre solo la parte que ya conocías.

2 NIVEL 2 · VISIBLE

Tienes la lista y confías en ella. Lo que la lista no te dice es a quién llamar, y averiguarlo cuando algo está por vencer sale del margen. El riesgo dominante es el envejecimiento: un inventario correcto se degrada solo si nadie es dueño de mantenerlo.

La siguiente conversación: quién responde por cada certificado, con nombre, y qué pasa con esos certificados cuando esa persona cambia de rol.

3 NIVEL 3 · CONTROLADA

Sabes qué tienes, de quién es y qué sostiene. Todavía reaccionas al calendario: la renovación empieza cuando alguien nota la fecha. Funciona mientras el volumen sea manejable. Vigencias más cortas significan más eventos al año, y el margen se acaba. El riesgo dominante es el margen, es decir, no la información sino el tiempo entre enterarte y tener que actuar.

La siguiente conversación: con cuánta anticipación necesitas enterarte para que la renovación ocurra en horario de oficina, y a quién específicamente tiene que llegarle ese aviso.

4 NIVEL 4 · ANTICIPADA

Nada te toma por sorpresa. Los avisos salen con margen y llegan a quien puede actuar. Pero cada renovación sigue siendo una decisión individual, y el proceso depende de que ciertas personas estén y se acuerden. Funciona hasta que alguien se va de vacaciones en la semana equivocada. El riesgo dominante ya no es técnico, sino que el control vive en personas y no en un proceso. Desde aquí ya tiene sentido automatizar de forma acotada, sobre lo que tiene responsable, criticidad y aviso resueltos. Lo que todavía no conviene es hacerlo la norma, porque la norma no existe.

La siguiente conversación: qué política escrita necesitas, qué excepciones vas a permitir y quién queda mal si no se cumple.

5 NIVEL 5 · GOBERNADA

El proceso existe sin ti. Hay política, hay excepciones con dueño y fecha, hay escalamiento probado y hay evidencia que se entrega sin abrir un proyecto. Aquí la automatización deja de ser caso por caso y puede volverse la norma: la política dice qué se automatiza, cada excepción tiene dueño y la evidencia queda sola. Es el nivel desde el que se orquesta el proceso completo, no certificados sueltos.

La siguiente conversación: qué parte del proceso conviene orquestar primero, medida por criticidad y no por facilidad técnica.

UN APUNTE SOBRE EL RESULTADO

Conviene esperar quedar uno o dos niveles por debajo de donde creías estar. No es un problema del ejercicio.

08

CAPÍTULO 08

QUÉ HACER ANTES DE AUTOMATIZAR

Automatizar es la respuesta correcta a un problema de frecuencia, y la frecuencia ya subió: el doble de reemplazos desde marzo de 2026, el cuádruple desde marzo de 2027.

La automatización ejecuta; no elige. Cuál va primero, cuál se queda fuera y qué pasa con lo que ni sabes que tienes: eso se decide antes.

> **Un proceso automático sobre un parque que no conoces completo automatiza el parque que sí conoces. La parte que se cae sigue siendo la misma.**

Los ocho pasos que siguen son el orden que hace que el séptimo funcione. Cada uno trae un criterio de salida (cómo sabes que está hecho) y el error que más se repite. Los seis primeros no requieren cambiar tu infraestructura.

01

DESCUBRIR

Traer a la vista lo que ya existe: lo emitido por tus CA internas, lo comprado a autoridades públicas, lo fiscal y lo que vive en aplicaciones que nadie ha revisado en años.

Criterio de salida: la cifra de certificados no cambia cuando alguien la calcula por otro método.

Error frecuente: confundir “los que monitoreamos” con “los que tenemos”. El monitoreo de endpoints vigila lo que ya está en una lista; el incidente típico viene de lo que no está en esa lista.

02

CONSOLIDAR

Una sola vista, no cinco listas parciales que se contradicen entre sí.

Criterio de salida: existe un lugar donde se responde la pregunta, y las hojas paralelas se dieron de baja formalmente.

Error frecuente: dejar viva la hoja de cálculo “por si acaso”. El resultado ya se vio: dos listas, y en la primera discrepancia, ninguna.

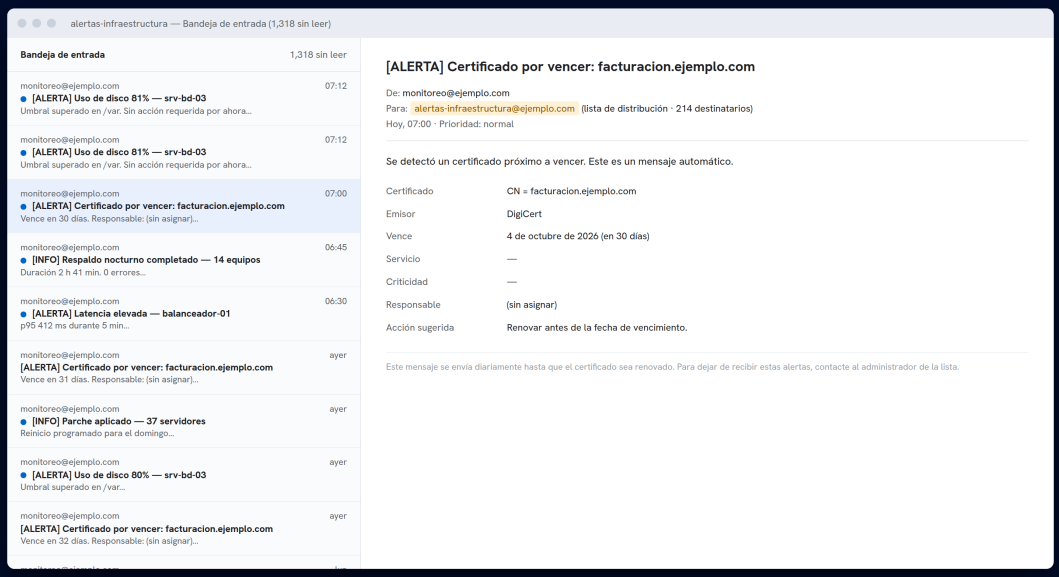
03 CONTEXTUALIZAR

Añadir lo que el certificado no trae dentro: responsable, servicio, ambiente, criticidad y dependencias.

Criterio de salida: puedes explicar qué se cae si ese certificado falla, sin preguntarle a nadie.

Error frecuente: contextualizar todo el parque con el mismo esfuerzo. Es el camino más rápido a un proyecto que se abandona a la mitad. Empieza por lo crítico y acepta que la cola larga tarde meses.

UNA ALERTA SIN DESTINATARIO CORRECTO ES RUIDO



04 MONITOREAR

El objetivo no es detectar, sino detectar a tiempo y avisarle a quien puede hacer algo.

Criterio de salida: el aviso llega con margen suficiente para que la renovación ocurra dentro del proceso normal y en horario de oficina.

Error frecuente: configurar alertas antes de tener responsables. Una alerta sin destinatario correcto es ruido, y el ruido entrena al equipo a ignorar alertas, incluida la que sí importa.

05 GOBERNAR

Convertir información en respuesta organizacional: política, excepciones, escalamiento y evidencia. Es el paso que separa ver de gobernar.

Criterio de salida: alguien queda mal si no se cumple. Si nadie queda mal, no es una política: es un documento.

Error frecuente: escribir la política antes de conocer el parque. Sale una política que nadie puede cumplir, y eso le enseña al equipo que las políticas se ignoran.

06

PRIORIZAR

No todo merece el mismo esfuerzo, el mismo umbral de alerta ni el mismo nivel de escalamiento.

Criterio de salida: puedes nombrar los diez certificados que no pueden fallar y decir qué sostiene cada uno.

Error frecuente: priorizar por criterio técnico (el más viejo, el más expuesto) y no por lo que sostiene. El certificado de la facturación puede ser el más aburrido de la lista.

07

AUTOMATIZAR

Ahora sí. Y sobre un parque que ya conoces.

Criterio de entrada —no de salida: nivel 4 en el capítulo anterior para automatizar de forma acotada, sobre certificados con contexto y aviso resueltos; nivel 5 para hacerla la norma del proceso. Automatizar desde el nivel 2 es acelerar un proceso que todavía no entiendes.

Error frecuente: automatizar por cobertura en lugar de por criticidad: empezar por lo fácil de conectar y dejar para después lo que no puede fallar.

08

MEDIR

El paso que no termina. Cuatro indicadores bastan para empezar: cuántos vencimientos se atendieron con margen, cuántos escalaron, cuántos certificados aparecieron sin pasar por el proceso y cuánto tarda una auditoría.

Criterio de salida: no hay. Ese es el punto.

Error frecuente: medir cobertura de herramienta en lugar de comportamiento del proceso. Que el 90% del parque esté conectado no dice nada si los avisos siguen llegando tarde.

Seis de los ocho pasos no tocan tu infraestructura. Piden saber qué tienes, de quién es y qué se cae si falla. Eso no se compra: se decide.

El séptimo sigue siendo la respuesta correcta al problema de frecuencia. Pero es una respuesta que se gana. Cuando llegas ahí sabiendo exactamente qué vas a automatizar, la automatización deja de ser una apuesta y se vuelve lo que debía ser desde el principio: una decisión de eficiencia.

El octavo paso no termina nunca, porque el control no es un estado al que se llega. Es algo que se demuestra, o no se demuestra.

Y DESPUÉS DEL EBOOK

DEL PUNTO CIEGO AL CONTROL. Y AHORA, EN PILOTO AUTOMÁTICO.

Ya viste dónde se forma el punto ciego y qué hace falta para controlarlo. Lo que sigue es verlo funcionar: Keyfactor Command, la plataforma que encuentra, vigila y renueva tus certificados, de la mano de CEGA Security.

- **Keyfactor Command** encuentra tus certificados, avisa antes de que venzan y los renueva automáticamente.
- **Con quien sabe:** más de 13 años detrás de la confianza digital de empresas en toda Latinoamérica.
- **Sin compromiso:** conoce la plataforma y decide después.

¿Te quedaste con ganas de verlo funcionar?

Solicita una demo de Command

CEGA SECURITY