Los primeros 100 días de un CISO (P100D)

Período crítico: una oportunidad para no perderla.

El beneficio de un buen comienzo. “Hay una sola oportunidad de crear una buena impresión”
Una ventana limitada para tomar decisiones y crear imagen

En los P100D hay que formular planes, hacer las conexiones y mostrar el estilo gerencial.

Muchos CISOs fracasan, no por razones técnicas u operativas, sino porque no satisfacen los requerimientos y expectativas del “negocio”; o, en todo caso, porque fallan en comunicar como han cumplido con las expectativas.

Recordar: un CISO es principalmente un líder, un gerente y un comunicador, antes que un tecnólogo.

2

Tareas a encarar

- ✓ Inventario de recursos (gente, tecnología, métricas, reportes, presupuesto, proyectos en curso, incidentes, …).
- ✓ Contacto con superiores y pares: presentación (corta) y entrevista (larga).
- ✓ ¿Comité de SI *(Steering Committee*)?
- ✓ Evaluar del estado de la situación actual.
- ✓ Escribir y difundir una misión/visión.
- ✓ Redactar (o revisar) la política de SI.
- ✓ Analizar los proyectos de SI en marcha.
- ✓ Analizar cuidadosamente la gente a su cargo.
- ✓ Analizar y evaluar el presupuesto del área.
- ✓ Identificar y conversar con proveedores de hard, soft y servicios (¿SLA?)
- ✓ Nivel de madurez
- ✓ ¿PESI? (poco tiempo)

3

Entrevistas iniciales

A superiores, pares, gente de TI/SI, proveedores, consultores, para detectar y conocer:

- Cómo es el negocio
- Problemas
- Expectativas para el área y para el nuevo CISO
- Recursos
- Cultura de la organización y, en particular, respecto de la SI.
- Dinámica (cómo funciona)
- Proyectos en proceso
- Descubrir "quick wins" "quick hits"
- Prioridades, desafíos,
- Transmitir una visión (SI al servicio del negocio / Cómo la SI agrega valor al negocio)
- Estado general de la seguridad
- *Petit* FODA de cómo es percibida el área de SI

4

Personal del área SI

- ✓ Reunir a la gente del área.
- ✓ Reuniones individuales con subordinados inmediatos.
- ✓ ¿Qué hace cada uno? (independientemente del cargo que ocupa)
- ✓ Conocimiento técnico, habilidades sociales, actitud.
- ✓ Prestar atención a la moral del grupo

5

Recomendaciones I

- ✓ Identifique rápidamente las demandas del negocio y los recursos con que cuenta.
- ✓ Trabaje “codo a codo” con el cuerpo ejecutivo para ser visto como un líder.
- ✓ Evite criticar las acciones de su predecesor ante los otros.
- ✓ Planifique con detalle las acciones de los P100D.
- ✓ Focalícese en las relaciones de la SI con el negocio.
- ✓ Escribir algo (corto, interesante, pertinente): “el valor de la SI como herramienta del negocio”.

6

Recomendaciones II

- ✓ Crear confianza y credibilidad
- ✓ Identificar aliados. Encontrar un sponsor.
- ✓ Construir relaciones personales.
- ✓ Fijar prioridades
- ✓ Conocer la “historia” de TI/SI en la organización.
- ✓ ¿Qué ha pasado antes de que yo llegara?
- ✓ Evitar crear sobre expectativas.
- ✓ Escuchar atentamente y leer entre líneas.

7

Establezca el alcance

¿Seguridad informática?

¿Seguridad de la información?

¿Privacidad?

¿Continuidad del negocio?

¿Gestión del riesgo?

¿Cumplimiento?

8

La mayoría de los CISOs pasan el primer, segundo y tercer mes trabajando tres caminos paralelos simultáneamente:

- atendiendo a los problemas de "solución fácil" de manera correcta,
- reuniéndose con los ejecutivos y aprendiendo el negocio, y
- evaluando a sus propios equipos.

Pero si lo desglosamos en cómo se acercan cada mes individualmente, diríamos que:

- el primer mes es escuchar y aprender,
- el segundo mes es planificar, y
- el tercer mes es cumplir con alguna parte de ese plan.

9

Promoción interna

Los candidatos que son promovidos internamente necesitan pasar sus primeros 100 días diferenciándose del papel que solían jugar.

Necesitan pasar los primeros 100 días marcando un delicado equilibrio entre honrar la estrategia de SI establecida por su predecesor y hacer su propia nueva marca en la dirección futura de SI.

Deben reunirse con otros ejecutivos para tener discusiones francas sobre lo que funcionó - y lo que no funcionó – en el régimen anterior, y trabajar con su nuevo equipo de liderazgo de SI para establecerse como el nuevo CISO.

10

Los primeros cien días Según Forrester Research

Para comenzar su viaje hacia la construcción de una organización de seguridad de clase mundial, Forrester recomienda que siga los siguientes cinco pasos, muchos de los cuales puede completar en sus primeros 100 días.

11

1. Documente formalmente roles e interacciones.

Esto suena como una tarea aburrida y mundana, pero es absolutamente esencial asegurarse de hacer que todos sean conscientes de sus responsabilidades formalmente, ya sea que formen parte de la organización de seguridad o no.

Esto también aclara el alcance y la amplitud de las responsabilidades de la organización de seguridad con las áreas de administración y negocios.

Algunas empresas crean una matriz de responsabilidades de seguridad basadas en un modelo como ISO 27001.

12

2. Construir relaciones informales.

La seguridad se trata de generar confianza, por lo que cuanto más pueda construir relaciones informales, mejor.

El CISO debe pasar su primer mes simplemente conociendo y entendiendo las necesidades de los gerentes de negocios.

Estas reuniones son típicamente informales, durante el café o el almuerzo, y rara vez se menciona la seguridad.

La atención se centra en el negocio y lo que hace que ese ejecutivo haga mejor su trabajo.

13

3. Comprender la seguridad de TI versus el riesgo de información.

Muchas organizaciones de seguridad no reciben la atención de la gerencia porque siempre se centran en las actividades de seguridad de TI, lo que la empresa no comprende.

Por otro lado, el negocio entiende bien el riesgo, y si articula esos mismos problemas en el contexto del riesgo, es mucho más probable que el negocio reaccione y responda a ellos.

14

4. Desarrollar un consejo de seguridad interfuncional.

Concéntrese en "quién" no "cómo".

Forrester ha profesado durante mucho tiempo los beneficios de un consejo de seguridad, pero una cosa que es absolutamente esencial para el éxito de este consejo es su composición.

El truco no es apuntar al hombre de negocios de alto rango, sino al más interesado en cuestiones de seguridad y riesgo que tiene un nivel razonable de visibilidad en el negocio.

Cuando tenga un equipo apasionado trabajando en los problemas de seguridad, será fácil determinar el "cómo".

15

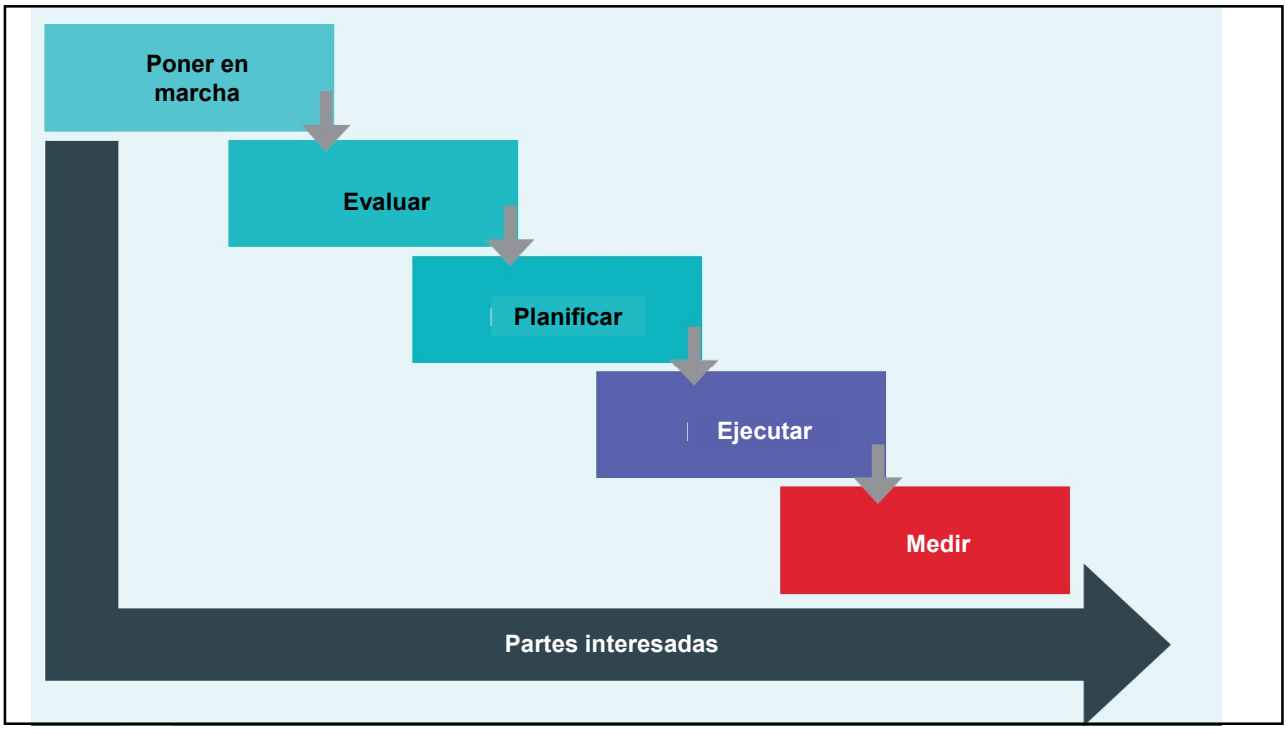
5. Equipar a la empresa para realizar evaluaciones de riesgos.

Para cumplir con las obligaciones de seguridad y riesgo de manera efectiva, debe delegar, y las evaluaciones de riesgos son ideales para esto.

Proporcione las listas de verificación y la capacitación básica a la empresa para realizar las tareas básicas de evaluación de riesgos de modo que alivie la presión de sus recursos.

Haga que sea fácil y sin problemas para la empresa incorporarlos en sus procesos existentes.

16



17

PONER EN MARCHA: antes de comenzar realice una investigación exhaustiva de la empresa, lea el informe anual de la empresa, quién es quién en el equipo ejecutivo, etc. Si es posible, reúnase con las partes interesadas clave antes de comenzar. Refine su plan.

EVALUAR: conozca primero a los interesados importantes, haga un mapa y aprenda sobre el negocio, cuáles son los problemas y las oportunidades para mejorar la situación. Recopile informes, evaluaciones, hallazgos de auditoría, documentos de estrategia existentes, políticas, métricas, informes de la Junta, etc.

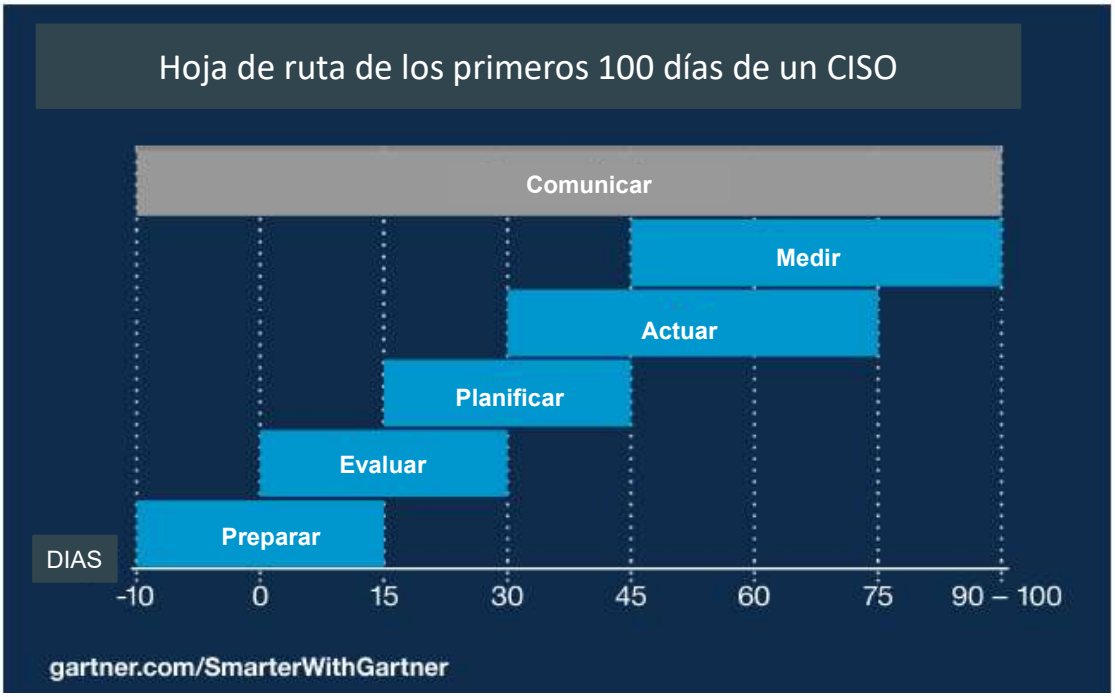
PLANIFICAR: conozca los “quick-wins”, comprenda qué problemas tardarán más en resolverse, qué procesos actuales funcionan bien y se deben seguir ejecutando. Desarrolle una visión y compártala con su gerente de línea, su equipo y sus principales interesados, obtenga comentarios y refine.

18

EJECUTAR: ejecute los “quick-wins”, implemente planes acordados para abordar algunos de los problemas a más largo plazo. Organice su equipo, configure su sistema de gestión y asegúrese de que las estructuras de gobierno estén establecidas y sean efectivas.

MEDIR: vuelva a comprometerse con todas las partes interesadas clave, vuelva a confirmar las acciones clave que está tomando, cualquier progreso que haya realizado, en el que pueda necesitar su ayuda y comentarios en sus primeros 100 días. Prepare un informe de evaluación ejecutiva de riesgos y problemas clave.

19



20

Preparar

No espere hasta su primer día en el trabajo para prepararse.

Tome algunas medidas clave antes de comenzar a informarse, aprenda sobre colegas y personal, establezca reuniones con su equipo y los principales líderes empresariales y de TI.

No cometa el error de abordar su nuevo rol con comunicaciones y planes ad hoc.

Unas pocas horas de inversión en planificación antes de comenzar asegurarán que se completen los preparativos críticos. Demostrar que comprende "cómo funcionan las cosas por aquí" es crucial.

21

Evaluar

Obtenga una visión integral del estado actual del programa de seguridad de la organización; qué funciona y qué no; y los cinco desafíos principales que priorizará durante los primeros tres a seis meses.

Durante la primera semana, intente pasar la mayor parte de su tiempo creando un inventario de los recursos necesarios para administrar la organización de seguridad: personas, informes, métricas disponibles y parámetros fiinancieros. Utilice las reuniones cara a carapara desarrollar una sólida comprensión del negocio y establecer una buena relación con las partes interesadas clave.

22

Planificar

Convierta lo que ha aprendido en un plan de acción. Comparta la visión de su programa de seguridad con su equipo, gerentes de línea y partes interesadas del negocio. Esta es su oportunidad de diseñar y refiinar su nueva organización de seguridad.

A estas alturas, debe tener una imagen razonablemente precisa de su presupuesto mensual de operaciones de seguridad, así que planifiique su presupuesto para los próximos dos o tres meses.

23

Actuar

Esta es su oportunidad de entregar resultados visibles. Redefiina su equipo; involucrese en proyectos existentes; establezca presupuestos; establezca (o restablezcar) los procesos y foros de gobierno de seguridad; y garantice el compromiso de la alta gerencia para la carta de seguridad que desarrolló

24

Medir

Comience a proporcionar evidencia de su impacto.

Desarrolle un marco y proceso de informes ejecutivos; monitoree el progreso del programa y del proyecto; y resalte las primeras victorias, éxitos y desafíos.

Programe reuniones con su gerente de línea, líderes de equipo y partes interesadas clave para reunir sus opiniones sobre el progreso realizado y los desafíos encontrados durante los primeros 100 días de su mandato.

25