TECNOLOGÍA QUE CONECTA

GUÍA PARA LA ALTA DIRECCIÓN · 2026

10 preguntas que tu junta debería hacerle a TI

La ciberseguridad ya no es solo un tema técnico: es un riesgo del negocio. Estas preguntas ayudan a la alta dirección a entender qué tan protegida está la empresa, sin necesidad de ser expertos.

Cómo usar esta guía

1. **Lleva las preguntas a la próxima reunión**
   Con TI y con tu proveedor de seguridad.
2. **Compara cada respuesta**
   Con la "buena respuesta" y la "señal de alerta".
3. **Pide indicadores cada trimestre**
   Al final encontrarás cuáles revisar.

01 ¿Cuáles son nuestros activos más críticos y quién los protege?

Por qué importa: Sin saber qué es lo más valioso, no se puede priorizar la protección ni el presupuesto.

BUENA RESPUESTA
Un inventario actualizado de sistemas y datos críticos, con un responsable para cada uno.

SEÑAL DE ALERTA
"Lo protegemos todo por igual" o no hay un inventario.

02 Si mañana un ransomware cifrara nuestros sistemas, ¿en cuánto tiempo volveríamos a operar?

Por qué importa: Es el escenario de mayor impacto para la mayoría de las empresas.

BUENA RESPUESTA
Un tiempo de recuperación estimado y probado, con un plan documentado.

SEÑAL DE ALERTA
"Depende" o "nunca lo hemos calculado".

03 ¿Tenemos respaldos aislados y cuándo fue la última prueba de restauración?

Por qué importa: Los atacantes buscan cifrar o borrar también los respaldos.

BUENA RESPUESTA
Copias fuera de la red o inmutables, y una prueba de restauración reciente con resultados.

SEÑAL DE ALERTA
Respaldos en la misma red o "nunca hemos restaurado una copia".

04 ¿Quién vigila nuestra seguridad fuera del horario de oficina?

Por qué importa: Muchos ataques se ejecutan de noche o en fines de semana.

BUENA RESPUESTA
Monitoreo 24/7, propio o gestionado, con tiempos de respuesta definidos.

SEÑAL DE ALERTA
"Lo revisamos cuando llegamos el lunes".

05 ¿Usamos autenticación multifactor en todos los accesos críticos?

Por qué importa: Una contraseña robada es la puerta de entrada más común.

BUENA RESPUESTA
MFA en el correo, los accesos remotos y las cuentas de administrador, con un porcentaje de cobertura medido.

SEÑAL DE ALERTA
"Solo en algunos casos" o "los usuarios se quejaron y lo quitamos".

06 ¿Cuánto tardamos en aplicar los parches críticos?

Por qué importa: Las vulnerabilidades conocidas son explotadas rápidamente.

BUENA RESPUESTA
Un plazo definido, priorizado por riesgo, con reportes de cumplimiento.

SEÑAL DE ALERTA
No hay un plazo, o los parches se aplican "cuando hay tiempo".

07 ¿Tenemos un plan de respuesta a incidentes probado? ¿Quién decide durante una crisis?

Por qué importa: Improvisar en medio de un incidente multiplica el daño.

BUENA RESPUESTA
Un plan escrito, con roles claros, contactos y al menos un simulacro al año.

SEÑAL DE ALERTA
"TI se encarga" sin plan escrito ni roles definidos.

08 ¿Cómo capacitamos a los colaboradores contra el phishing y cómo lo medimos?

Por qué importa: Las personas son la primera línea de defensa.

BUENA RESPUESTA
Capacitación periódica con simulaciones y métricas de mejora.

SEÑAL DE ALERTA
Una charla al año sin medición, o ninguna capacitación.

09 ¿Qué terceros tienen acceso a nuestros sistemas y cómo lo controlamos?

Por qué importa: Proveedores y contratistas pueden ser una vía de entrada.

BUENA RESPUESTA
Una lista de accesos de terceros, con permisos mínimos, MFA y revisión periódica.

SEÑAL DE ALERTA
Nadie sabe con certeza quién tiene acceso.

10 ¿Cumplimos con la Ley 81 de 2019 y la regulación de nuestro sector? ¿Cómo lo demostraríamos?

Por qué importa: El incumplimiento puede traer sanciones y daño reputacional.

BUENA RESPUESTA
Responsables definidos, controles documentados y evidencias disponibles ante una auditoría.

SEÑAL DE ALERTA
"Creemos que sí", sin evidencias.

PARA CADA TRIMESTRE

Indicadores que la junta debería revisar

Pide estos indicadores de forma periódica. Lo importante no es un número aislado, sino ver cómo evolucionan.

Cobertura de MFA
Porcentaje de cuentas críticas con autenticación multifactor.

Tiempo de parcheo
Días promedio para aplicar los parches críticos.

Incidentes
Cantidad, gravedad y tiempo de respuesta de los incidentes del periodo.

Phishing
Porcentaje de colaboradores que caen en las simulaciones, y su tendencia.

Respaldos
Fecha y resultado de la última prueba de restauración.

Accesos de terceros
Cantidad de accesos activos y fecha de su última revisión.

VIVA SOLUTIONS · CISO AS A SERVICE

¿Necesitas ayuda para responder estas preguntas?

Con Vi-CISO acompañamos a la alta dirección a definir prioridades, medir indicadores y presentar el estado de la seguridad en un lenguaje de negocio.

Habla con un ingeniero: vivaconecta.com/#contacto
(507) 216-9004 · webforms@vivaconecta.com

Guía orientativa. No sustituye una evaluación profesional ni la asesoría legal.