PLAYBOOK OPERATIVO

Ciberhigiene y respuesta rápida ante ataques cibernéticos

Guía práctica para empresas, pymes e instituciones en Panamá

Uso recomendado

Este documento puede usarse como comunicado ejecutivo, checklist de autoevaluación y guía de ejecución para los primeros 7 y 30 días. Debe personalizarse con responsables, contactos, sistemas críticos y proveedores de cada organización.

Campo	Información
Organización	
Responsable principal	
Fecha de aprobación	
Versión	2.0 - Operativa
Clasificación sugerida	Uso interno / público según ajuste de la organización

Índice

1. Resumen ejecutivo para dirección

Contexto. En Panamá, muchas organizaciones están expuestas a ataques que aprovechan fallas prevenibles: sistemas sin parches, accesos remotos mal protegidos, contraseñas débiles, cuentas de exempleados activas, respaldos no probados y configuraciones inseguras. La inteligencia artificial debe considerarse una hipótesis de riesgo que puede acelerar phishing, reconocimiento y explotación, pero no debe usarse como explicación automática sin evidencia técnica.

Objetivo. Convertir la preocupación en acciones concretas, medibles y asignables. Este documento indica qué hacer, cómo empezar, quién debe hacerlo y qué evidencia guardar para demostrar avance.

Prioridad ejecutiva. No todas las empresas necesitan iniciar con un SOC avanzado. Todas sí necesitan: MFA, parches, backups probados, revisión de accesos, monitoreo básico y un contacto definido para incidentes.

Decisiones que debe tomar la dirección

- Nombrar un responsable interno de ciberseguridad o continuidad tecnológica.
- Aprobar una ventana de mantenimiento para parches críticos.
- Exigir evidencia mensual de backups, MFA, parches y revisión de accesos.
- Definir proveedor de soporte o respuesta ante incidentes antes de que ocurra una emergencia.
- Asignar presupuesto inicial a controles básicos antes de invertir en herramientas complejas.

2. Cómo usar este playbook

1. Completar la portada con el nombre de la organización, responsable y fecha.
2. Seleccionar el nivel de madurez aplicable: Nivel 1, Nivel 2 o Nivel 3.
3. Ejecutar el plan de 7 días para reducir riesgos inmediatos.
4. Continuar con el plan de 30 días para ordenar procesos, evidencias y responsables.
5. Usar la autoevaluación al final de cada mes para medir progreso.
6. Guardar evidencias: capturas, reportes, bitácoras, actas de reunión, tickets y correos de aprobación.

Regla de evidencia. Si una actividad no tiene evidencia, para efectos de gestión se considera no ejecutada. La evidencia no tiene que ser sofisticada: puede ser un reporte, captura, ticket, acta o bitácora firmada.

3. Niveles de madurez y ruta recomendada

Nivel	Aplica a	Prioridad
Nivel 1 - Básico	Pymes, comercios, clínicas, escuelas, despachos o empresas sin seguridad dedicada.	MFA, parches, backups, antivirus activo, cierre de accesos expuestos y contacto externo de emergencia.
Nivel 2 - Intermedio	Empresas con TI interno o proveedor administrado.	Inventario, gestión mensual de parches, revisión de accesos, pruebas de backup, logs de firewall/VPN/correo y procedimiento de respuesta.
Nivel 3 - Regulado o crítico	Banca, gobierno, salud, logística, energía, telecomunicaciones o servicios esenciales.	SIEM o monitoreo centralizado, EDR administrado, gestión continua de vulnerabilidades, segmentación, simulacros y reportes ejecutivos.

Ruta recomendada

- Si la empresa está en Nivel 1, completar primero el plan de 7 días y la autoevaluación.
- Si la empresa está en Nivel 2, formalizar la matriz de ejecución y los indicadores mensuales.
- Si la empresa está en Nivel 3, conectar este playbook con NIST CSF 2.0, gestión de riesgos y respuesta formal a incidentes.

4. Matriz de ejecución: control, responsable, frecuencia y evidencia

Control	Qué hacer	Responsable	Frecuencia	Evidencia esperada
MFA	Activar doble factor en correo, VPN, cuentas administrativas y nube.	TI / Proveedor	Una vez; revisar mensual	Reporte de usuarios con MFA o capturas de configuración.
Parches	Aplicar actualizaciones críticas en servidores, estaciones, firewall, VPN y aplicaciones expuestas.	TI	Semanal para críticos; mensual para estándar	Reporte de parches, ticket de cambio o bitácora.

Control	Qué hacer	Responsable	Frecuencia	Evidencia esperada
Backups	Respaldar información crítica y probar restauración.	TI / Operaciones	Backup según criticidad; prueba mensual	Bitácora de respaldo y prueba de restauración.
Accesos	Revisar usuarios activos, exempleados, privilegios administrativos y cuentas compartidas.	RRHH + TI	Mensual	Listado de usuarios revisado y cuentas deshabilitadas.
Exposición	Revisar servicios publicados a Internet y cerrar accesos innecesarios.	TI / Proveedor	Mensual y ante cambios	Capturas de firewall, escaneo externo o reporte técnico.
Monitoreo	Revisar alertas de antivirus/EDR, correo, VPN, firewall y nube.	TI / Seguridad	Diario o semanal según nivel	Registro de alertas revisadas y acciones tomadas.
Capacitación	Entrenar al personal en phishing, fraude, contraseñas y reporte de incidentes.	Gerencia + TI	Trimestral	Registro de asistencia y material usado.
Respuesta	Mantener contactos, roles y pasos de contención ante incidentes.	Dirección + TI + Legal	Revisar trimestral	Plan aprobado, simulacro o acta de revisión.

5. Guía paso a paso por control crítico

5.1 Activar MFA

1. Identificar todos los servicios críticos: correo, VPN, nube, banca, sistemas administrativos y cuentas de administrador.
2. Activar MFA primero en administradores y usuarios con acceso a información sensible.
3. Extender MFA a todos los usuarios.
4. Revisar usuarios que aún no han completado el registro.

5. Definir procedimiento para pérdida de celular o cambio de equipo.

Evidencia mínima esperada: Reporte de adopción de MFA, capturas de política activa y listado de excepciones aprobadas.

5.2 Gestión de parches

1. Hacer lista de sistemas críticos y productos expuestos a Internet.
2. Revisar boletines de fabricantes y vulnerabilidades explotadas conocidas.
3. Aplicar primero parches críticos en firewall, VPN, correo, servidores y aplicaciones web.
4. Probar servicios después del parche.
5. Documentar fecha, responsable y resultado.

Evidencia mínima esperada: Ticket de mantenimiento, reporte de parches, capturas de versión antes/después y aprobación del cambio.

5.3 Revisar exposición a Internet

1. Listar IP públicas, dominios, servicios publicados y paneles administrativos.
2. Cerrar RDP público y cualquier acceso remoto sin MFA.
3. Restringir administración a VPN o direcciones autorizadas.
4. Validar reglas de firewall y NAT.
5. Repetir revisión después de cambios de infraestructura.

Evidencia mínima esperada: Reporte de exposición externa, reglas de firewall revisadas y listado de servicios autorizados.

5.4 Backups y restauración

1. Definir qué datos son críticos: facturación, contabilidad, correo, documentos, bases de datos y sistemas de operación.
2. Asegurar al menos una copia separada del ambiente principal.
3. Proteger credenciales de backup con MFA o controles equivalentes.
4. Probar restauración de un archivo y un sistema crítico.
5. Registrar tiempos de recuperación y errores encontrados.

Evidencia mínima esperada: Bitácora de backup, evidencia de restauración exitosa y responsable de custodia.

5.5 Revisión de usuarios y privilegios

1. Comparar lista de empleados activos con cuentas de correo, VPN, dominio, sistemas financieros y nube.
2. Deshabilitar cuentas de exempleados y proveedores sin contrato activo.

3. Eliminar cuentas compartidas o documentar excepción temporal.
4. Revisar administradores locales, de dominio, nube y aplicaciones.
5. Aplicar privilegio mínimo.

Evidencia mínima esperada: Acta de revisión, listado de cuentas deshabilitadas y aprobación de cuentas privilegiadas.

5.6 Monitoreo básico

1. Revisar alertas de antivirus/EDR.
2. Revisar inicios de sesión fallidos y exitosos desde ubicaciones inusuales.
3. Revisar cambios de privilegios y creación de usuarios.
4. Revisar reglas sospechosas de correo, reenvíos o buzones delegados.
5. Escalar hallazgos críticos al responsable del negocio.

Evidencia mínima esperada: Bitácora de revisión, alertas priorizadas y acciones correctivas.

6. Plan de acción de los primeros 7 días

Día	Objetivo	Acciones mínimas	Evidencia
Día 1	Identificar lo crítico	Correo, archivos importantes, facturación, banca, sistemas de clientes, servidores, nube, VPN y responsables.	Mapa simple de activos críticos.
Día 2	Proteger accesos	Activar MFA, cambiar contraseñas débiles, revisar administradores y deshabilitar exempleados.	Reporte de MFA y cuentas revisadas.
Día 3	Revisar exposición	Verificar RDP, VPN, firewall, paneles web y accesos publicados.	Listado de servicios expuestos y acciones.
Día 4	Aplicar parches críticos	Actualizar servidores, estaciones, firewall, VPN y aplicaciones expuestas.	Bitácora de parches.
Día 5	Validar backups	Confirmar existencia, ubicación, frecuencia y prueba de restauración.	Evidencia de restauración exitosa.
Día 6	Monitoreo básico	Revisar alertas de antivirus, correo, VPN, firewall y accesos inusuales.	Bitácora de alertas revisadas.

Día	Objetivo	Acciones mínimas	Evidencia
Día 7	Preparar respuesta	Definir contactos, roles, proveedor externo y pasos de contención.	Lista de contactos y plan aprobado.

Consejo práctico. El plan de 7 días no busca perfección. Busca reducir riesgos inmediatos y crear evidencia mínima de control.

7. Plan de mejora de los primeros 30 días

Semana	Foco	Acciones	Resultado esperado
Semana 1	Cierre de brechas urgentes	MFA, parches críticos, backups, cierre de accesos innecesarios, cuentas de exempleados.	Riesgo inmediato reducido.
Semana 2	Orden y visibilidad	Inventario de activos, usuarios, aplicaciones, IP públicas, proveedores y sistemas críticos.	Inventario base y responsables.
Semana 3	Procesos repetibles	Calendario de parches, revisión de accesos, pruebas de backup, monitoreo semanal y capacitación.	Rutinas de control documentadas.
Semana 4	Validación y mejora	Autoevaluación, revisión ejecutiva, reporte de brechas, plan de inversión y simulacro de incidente.	Plan de mejora aprobado.

Indicadores mensuales recomendados

- Porcentaje de usuarios con MFA activo.
- Porcentaje de sistemas críticos parchados.
- Cantidad de servicios expuestos a Internet.
- Fecha de la última restauración de backup probada.
- Número de cuentas administrativas.
- Tiempo promedio para corregir vulnerabilidades críticas.
- Cantidad de incidentes o intentos reportados por usuarios.
- Tiempo de contención ante incidentes.

8. Playbook de respuesta ante incidente

Regla clave. Ante un incidente, no improvisar y no borrar evidencia. Contener rápido, documentar cada acción y preservar logs.

8.1 Activación

- Registrar fecha y hora.
- Identificar quién reporta.
- Describir qué ocurrió.
- Clasificar severidad: amarillo, naranja o rojo.
- Notificar a TI, seguridad, dirección y legal si aplica.
- Abrir bitácora del incidente.

8.2 Contención inicial

- Aislar equipos sospechosos de la red sin formatear.
- Deshabilitar cuentas comprometidas.
- Revocar sesiones activas en correo, VPN y nube.
- Cambiar contraseñas afectadas.
- Bloquear indicadores confirmados si existen.
- Preservar logs de firewall, VPN, correo, EDR, servidores y nube.

8.3 Análisis rápido

- Determinar usuario o sistema afectado.
- Estimar inicio de la actividad sospechosa.
- Confirmar si hubo acceso exitoso o solo intento.
- Revisar si se usaron credenciales válidas.
- Buscar evidencia de movimiento lateral, exfiltración, cifrado o borrado.
- Definir sistemas críticos en riesgo.

8.4 Erradicación

- Eliminar malware o herramientas no autorizadas.
- Revocar credenciales comprometidas.
- Aplicar parches pendientes.
- Corregir configuraciones inseguras.
- Eliminar reglas maliciosas de correo o nube.
- Validar que no queden cuentas o accesos no autorizados.

8.5 Recuperación

- Restaurar desde respaldos limpios.
- Validar integridad de datos.

- Monitorear actividad posterior.
- Confirmar MFA y parches críticos.
- Confirmar que no existan cuentas sospechosas.
- Documentar lecciones aprendidas.

8.6 Comunicación

- Preparar mensaje interno para empleados.
- Preparar mensaje para clientes o proveedores si aplica.
- Coordinar con legal antes de comunicaciones públicas.
- Reportar a autoridades o regulador cuando corresponda.
- Mantener un único vocero autorizado.

Niveles de alerta

Nivel	Estado	Señales	Acción
Verde	Operación normal	Sistemas actualizados, MFA activo, backups funcionando, sin alertas relevantes.	Mantener rutina mensual.
Amarillo	Riesgo elevado	Vulnerabilidad crítica nueva, phishing masivo, intentos fallidos inusuales o credenciales expuestas.	Revisión en 24 a 72 horas.
Naranja	Posible compromiso	Accesos exitosos inusuales, usuario desconocido, alerta de malware o actividad fuera de horario.	Activar equipo de respuesta y preservar evidencia.
Rojo	Incidente confirmado	Ransomware, exfiltración, cuenta administrativa comprometida o sistemas críticos fuera de servicio.	Contención inmediata, investigación y recuperación.

9. Autoevaluación rápida

Área	Pregunta	Sí	No
Accesos	¿Todos los correos y cuentas administrativas tienen MFA?	☐	☐
Parches	¿Los sistemas críticos están actualizados?	☐	☐
Backups	¿Se probó una restauración en los últimos 30 días?	☐	☐

Área	Pregunta	Sí	No
Exposición	¿La empresa sabe qué servicios están publicados en Internet?	☐	☐
Usuarios	¿Se desactivan cuentas de exempleados oportunamente?	☐	☐
Monitoreo	¿Alguien revisa alertas de seguridad de forma rutinaria?	☐	☐
Respuesta	¿Existe un contacto definido para incidentes?	☐	☐
Capacitación	¿El personal sabe reportar phishing o fraude?	☐	☐

Interpretación

0 a 3 respuestas Sí: riesgo alto. Requiere acción inmediata.

4 a 6 respuestas Sí: riesgo medio. Hay controles básicos, pero falta consistencia.

7 a 8 respuestas Sí: buen punto de partida. Debe mantenerse, probarse y documentarse.

10. Anexos operativos y plantillas

Anexo A - Registro de activos críticos

Activo / sistema	Responsable	Ubicación / nube	Criticidad	Observaciones

Anexo B - Bitácora de parches

Fecha	Sistema	Parche / versión	Responsable	Resultado	Evidencia

Fecha	Sistema	Parche / versión	Responsable	Resultado	Evidencia

Anexo C - Registro de prueba de backup

Fecha	Sistema / datos	Tipo de prueba	Resultado	Tiempo de restauración	Responsable

Anexo D - Bitácora de incidente

Campo	Detalle
Fecha y hora	
Reportado por	
Sistema afectado	
Descripción inicial	
Acciones de contención	
Evidencia preservada	
Responsables notificados	
Estado actual	

Anexo E - Contactos de emergencia

Rol / proveedor	Nombre	Teléfono / correo	Horario / observaciones

Anexo F - Mensaje interno ante phishing

Asunto: Alerta preventiva: correos o mensajes sospechosos

Mensaje sugerido: Se ha identificado una campaña de mensajes sospechosos que podría intentar obtener credenciales o inducir pagos no autorizados. No abra enlaces ni archivos adjuntos de mensajes inesperados. Si recibió un mensaje sospechoso, repórtelo al área de TI o al responsable designado. Ningún colaborador debe compartir contraseñas, códigos de verificación ni datos bancarios por correo, llamada o mensajería.

Anexo G - Qué pedirle al proveedor de TI

- Reporte de usuarios con MFA activo y usuarios pendientes.
- Reporte de parches instalados y pendientes en sistemas críticos.
- Listado de cuentas administrativas y cuentas de exempleados deshabilitadas.
- Evidencia de backup y prueba de restauración.
- Listado de servicios expuestos a Internet.
- Resumen de alertas de antivirus/EDR/firewall/correo revisadas.
- Recomendaciones priorizadas por riesgo: crítico, alto, medio y bajo.

11. Referencias y recursos de consulta

NIST Cybersecurity Framework 2.0: Marco de referencia para gobernar, identificar, proteger, detectar, responder y recuperar. https://www.nist.gov/cyberframework

CISA Known Exploited Vulnerabilities Catalog: Catálogo para priorizar vulnerabilidades que han sido explotadas activamente. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CISA StopRansomware Guide: Guía de mejores prácticas para reducir riesgo y responder a ransomware. https://www.cisa.gov/stopransomware

NCSC: Impact of AI on cyber threat: Evaluación sobre cómo la IA puede afectar amenazas cibernéticas, phishing y operaciones ofensivas. https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027

CSIRT Panamá: Equipo nacional de respuesta a incidentes de seguridad de la información de Panamá. https://cert.pa/

Nota de uso

Este documento es una guía de buenas prácticas y no sustituye asesoría técnica, legal, regulatoria o forense especializada. Debe adaptarse a la industria, tamaño, tecnología, obligaciones contractuales y nivel de riesgo de cada organización.