¿Cuenta Cyber Crucible con un proceso de respuesta a incidentes y notificación de brechas?

Respuesta breve: Sí. Un proceso documentado de respuesta a brechas de datos define los roles y pasos para responder ante un presunto robo, brecha o exposición de datos protegidos, incluida la notificación al cliente. Se puede establecer contractualmente un plazo de notificación comprometido para clientes regulados.

El proceso de respuesta

Un presunto incidente se reporta de inmediato a través de canales internos supervisados por la función de Seguridad de la Información. Al identificarse, se elimina el acceso al recurso afectado y se convoca un equipo de respuesta a incidentes presidido por la alta dirección ejecutiva. Los investigadores y expertos forenses, proporcionados a través del seguro cibernético y tecnológico de Cyber Crucible, determinan cómo ocurrió el incidente, los datos involucrados, las partes afectadas y la causa raíz. Se desarrolla un plan de comunicación junto con los departamentos Legal, de Comunicaciones y de Recursos Humanos para notificar al personal, al público y a las partes afectadas según corresponda —incluida la notificación al cliente a través de un canal mutuamente acordado—, seguido de una revisión posterior al incidente.

Respuesta de soporte y notificación

Los incidentes orientados al cliente se rastrean conforme a los niveles de gravedad publicados en el SLA (SEV1 a SEV4), y se puede comprometer contractualmente un plazo de notificación de brechas o incidentes para clientes regulados.

Alineación con marcos de referencia y el límite honesto

El proceso se alinea con NIST SP 800-61 e ISO/IEC 27001:2022 A.5.24–A.5.26. No se reclama ninguna certificación. El procedimiento completo de respuesta a incidentes y notificación de brechas se proporciona a los revisores bajo NDA.

Revision #1
Created 2026-07-24 23:16:43 UTC by Dennis Underwood
Updated 2026-07-24 23:16:43 UTC by Dennis Underwood