Seguridad Corporativa

La vulnerabilidad corporativa: El error humano como principal detonante de filtración de datos en empresas costarricenses.

En Costa Rica, el crimen informático comúnmente ingresa por medio del recurso humano, es por ello que el riesgo empresarial ya no se mide únicamente en activos físicos o en pérdidas económicas visibles. Según datos recientes proporcionados por CAMTIC y la Unidad de Cibercrimen del Organismo de Investigación Judicial, el 85% de las filtraciones de datos en empresas se deben al error humano o a la falta de capacitación en ciberseguridad. Basta un clic, un archivo adjunto o una contraseña débil para comprometer información confidencial, afectar la reputación de una organización e incluso paralizar operaciones. El factor humano, más que la tecnología, se está convirtiendo en el talón de Aquiles empresarial.

Las empresas expuestas en silencio, tras la transformación digital que convirtió los sistemas de información en el corazón de las organizaciones. Sin embargo, muchas empresas continúan operando bajo la falsa premisa de que “tener antivirus” es suficiente para estar protegidas.

Las cifras demuestran lo contrario: la filtración de datos en empresas costarricenses es causada mayormente por decisiones humanas negligentes. Es decir, los incidentes no provienen de sofisticados hackers, sino de descuidos cotidianos: contraseñas compartidas, dispositivos sin bloqueo, enlaces abiertos sin verificación previa, entre otros.

La Criminología Corporativa plantea que el delito no surge solo por motivación, sino también por oportunidad (Felson & Clarke, 1998). Y en las empresas, las oportunidades se crean desde adentro.

Analizar el riesgo está en el recurso humano, por eso se han establecido recomendaciones clave como:

- **Implementar políticas de acceso:** solo personal autorizado debe acceder a información sensible.
- **Capacitar al personal en ciberseguridad:** identificar phishing, ingeniería social y uso seguro de dispositivos.
- **Establecer canales:** donde se puedan generar reporte de confidencial para incidentes.

Estas acciones se alinean con lineamientos internacionales como los del National Institute of Standards and Technology (NIST, 2022), que establece que la seguridad debe ser gestionada desde el comportamiento humano, no solamente desde la infraestructura. Asimismo, la IBM Security identificó que el costo promedio mundial de una brecha de datos supera los 4.45 millones de dólares y que el factor humano es responsable de la mayoría de incidentes (Ponemon Institute & IBM Security, 2024). Por eso la seguridad tecnológica es eficiente y la seguridad humana es indispensable.

Es así como la cultura de la seguridad y la reacción ante crisis se debe de evaluar desde el riesgo corporativo, para poder reducir drásticamente con cultura organizacional preventiva. No se trata solo de saber “qué hacer”, sino de construir la convicción de hacerlo. La evidencia criminológica indica que los delitos corporativos se reducen cuando existen tres factores:

Elemento	***Impacto en la prevención***
Capacitación continua	Reduce el error humano y las oportunidades del atacante
Protocolos claros de acceso	Disminuyen la exposición de datos sensibles
Sistemas para reportar incidentes	Facilitan detección temprana y respuesta

Fuente: Elaboración propia, 2025

Holt, Bossler y Seigfried-Spellar (2023) sostienen que la ingeniería social se basa en manipular comportamientos, no en vulnerar sistemas, por lo que las empresas deben invertir en fortalecer el criterio del personal, no solo en comprar tecnologías. Así la seguridad

corporativa no se logra únicamente instalando software, sino desarrollando un pensamiento crítico dentro del recurso humano, que cuando la protección de datos se convierte en cultura, la tecnología pasa de ser un escudo a un aliado.

"No hay firewall que proteja lo que un colaborador descuida"

"La seguridad no se instala, se construye."

"El verdadero valor de una empresa no es su información: es su capacidad de protegerla"

"La principal amenaza para las empresas no está afuera: está dentro y se llama descuido"

Fuentes Bibliográficas

CAMTIC & Organismo de Investigación Judicial. (2024). Informe sobre ciberseguridad y filtración de datos en empresas en Costa Rica. Unidad de Cibercrimen.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief. Home Office.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2023). Cybercrime and digital forensics: An introduction. Routledge.

National Institute of Standards and Technology. (2022). Digital Identity Guidelines (SP 800-63B). U.S. Department of Commerce.

Ponemon Institute & IBM Security. (2024). Cost of a Data Breach Report 2024.