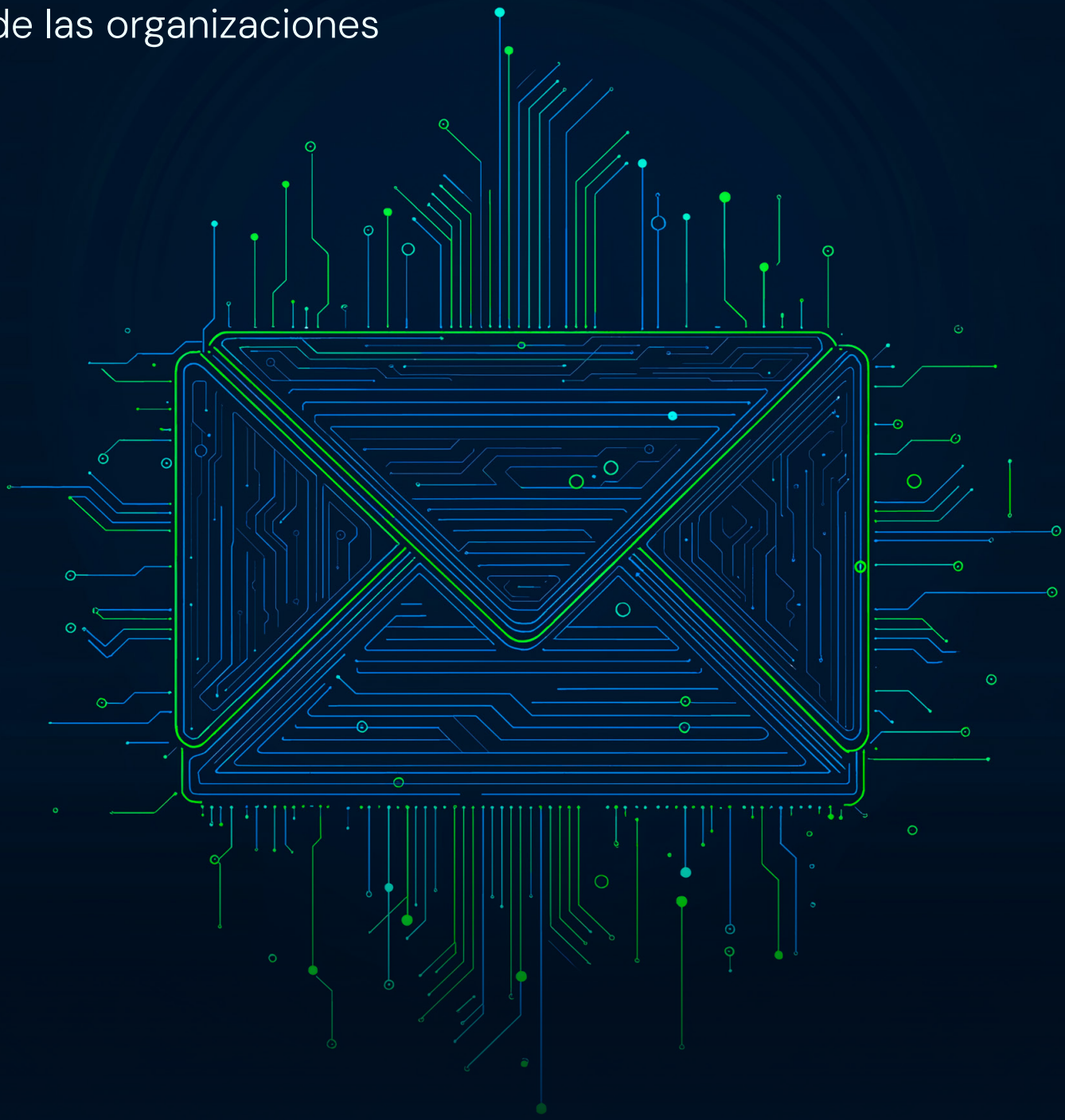
DELTA PROTECT®

Abnormal

EMAIL SECURITY

Cómo proteger el principal vector de ataque de las organizaciones



Tendencias, riesgos y mejores prácticas en la era de la inteligencia artificial

WHITEPAPER

Tabla de Contenidos

El Correo Electrónico: el vector de ataque favorito

En un mundo donde las organizaciones invierten cada vez más en firewalls, EDR y sistemas de detección de intrusos, los atacantes han encontrado una puerta que casi siempre está abierta: la bandeja de entrada.

El correo electrónico sigue siendo el canal de comunicación central en las empresas, y precisamente por eso es también el vector de ataque número uno a nivel mundial. No requiere vulnerabilidades técnicas sofisticadas; basta con que un empleado haga clic en el lugar equivocado.

3.04B

pérdidas por BEC en 2025
FBI IC3 2025 Annual Report
(+26% vs. 2024)

20.8B

pérdidas totales por cibercrimen en 2025
Récord histórico FBI IC3 2025

c/19s

1 email malicioso evade los filtros cada 19 seg. en 2025
2x más rápido que 2024
(Cofense, feb. 2026)

191K

quejas de phishing en 2025, el ciberdelito #1 en volumen
FBI IC3 2025

1.1 Por qué el email es tan vulnerable

A diferencia de otros canales digitales, el correo electrónico fue diseñado para ser abierto y accesible, no para ser seguro. Sus protocolos base (SMTP, POP3, IMAP) datan de los años 80 y no contemplaban el ecosistema de amenazas actual.

Además, el email es un canal de confianza: las personas están condicionadas a responder mensajes de colegas, directivos, proveedores y clientes. Los atacantes explotan exactamente esa confianza.

Lo que hace que el panorama actual sea especialmente urgente: así como las empresas adoptan inteligencia artificial para ser más eficientes, los atacantes también la están usando y con resultados alarmantes.

Los correos de phishing y BEC generados con IA son hoy indistinguibles de los legítimos, se producen a escala industrial y en 2025 se detectó un email malicioso evadiendo los filtros cada 19 segundos. La amenaza no solo persiste, se está acelerando.

1.2 Panorama de México y LATAM

México se ubica consistentemente entre los cinco países de América Latina con mayor volumen de ciberataques por email. Los sectores financiero, manufactura, gobierno y retail son los más afectados. Según datos de 2024-2025:

- **Ingeniería social y phishing:** representan el 57% de los ataques a organizaciones en LATAM (Positive Technologies, Cybersecurity Threatscape LATAM 2023-2024).
- **BEC (Business Email Compromise):** costo promedio por incidente: USD $129,000 en 2024 (FBI IC3 2024 Annual Report, análisis Abnormal AI).
- **Tiempo de detección:** una brecha causada por compromiso de email tarda en promedio 292 días en ser identificada y contenida (IBM Cost of a Data Breach 2024).

Dato clave para directivos

México recibió 31 millones de intentos de ciberataque en 2024: el 55% del total de toda América Latina (México Business News, 2024). El 65% de las empresas en México reportaron un incremento en brechas de ciberseguridad ese año, por encima del promedio regional del 59%. La pregunta no es si tu empresa será atacada, sino cuándo y qué tan preparada estará.

Anatomía de un ataque por email

Para poder defenderse eficazmente, primero hay que entender cómo funciona un ataque. Los ciberataques por correo no son eventos instantáneos: siguen una cadena de pasos que, una vez comprendida, puede interrumpirse en múltiples puntos.

2.1 Phishing: el engaño a escala

El phishing es el envío masivo de correos fraudulentos que suplantan marcas, instituciones o contactos de confianza para robar credenciales, datos o provocar transferencias. Sus variantes incluyen:

- **Phishing clásico:** correos masivos con links a sitios falsos (login de bancos, Microsoft 365, plataformas de pagos).
- **Spear phishing:** ataques dirigidos a una persona específica con información personalizada (nombre, cargo, empresa, proyecto actual).
- **Vishing y smishing:** variantes por voz (llamada) o SMS que complementan el ataque inicial por email.

2.2 BEC: el fraude más costoso

El Business Email Compromise (BEC) o compromiso de correo corporativo es el tipo de ataque más costoso. A diferencia del phishing masivo, el BEC es altamente dirigido y sofisticado.

Según el H1 2024 Email Threat Report de Abnormal AI: las organizaciones con más de 50,000 empleados tienen casi 100% de probabilidad de recibir al menos un ataque BEC cada semana; incluso las empresas más pequeñas (menos de 1,000 empleados) tienen un 70% de probabilidad semanal de ser atacadas.

El atacante estudia a la organización (estructura jerárquica, proveedores, procesos de pago, proyectos activos) y luego suplanta o compromete una cuenta legítima para emitir instrucciones fraudulentas: cambiar una cuenta bancaria, autorizar una transferencia urgente, compartir información confidencial.

Caso típico de BEC en México

El "CEO Fraud": un atacante suplanta el email del director general y le escribe al CFO con urgencia: "Necesito que proceses una transferencia de USD $85,000 hoy, es confidencial, no lo comentes con nadie." Sin verificación adicional, muchas empresas han procesado este tipo de instrucciones.

2.3 Fraude de proveedor comprometido (VEC)

Una de las amenazas más difíciles de detectar: el atacante no suplanta una cuenta, sino que la compromete directamente. Esto significa que el correo malicioso llega desde una dirección legítima de un proveedor o socio real, lo que hace que pase cualquier filtro de reputación.

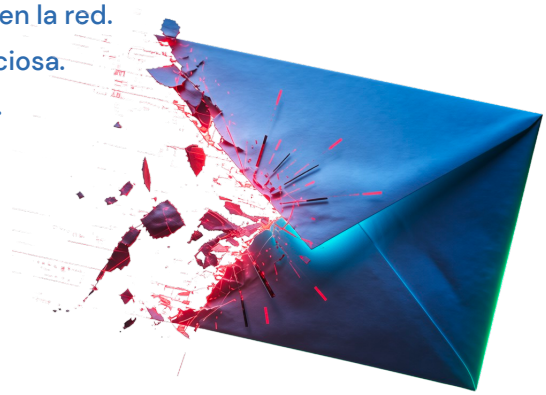
El VEC (Vendor Email Compromise) es especialmente peligroso porque explota la confianza establecida con terceros. Un proveedor con quien llevas años trabajando te envía, sin saberlo, una factura con datos bancarios modificados.

Según datos de Abnormal AI (2026), el 44.2% de los mensajes de fraude de proveedor son efectivamente abiertos y leídos por los empleados: una tasa de engagement que ninguna otra categoría de amenaza alcanza. Además, el VEC creció un 50% año a año entre 2022 y 2023: en 2023, casi el 40% de los clientes de Abnormal recibieron al menos un ataque VEC mensualmente.

2.4 Malware y ransomware vía email

Los archivos adjuntos siguen siendo un vector crítico: documentos de Office con macros maliciosas, PDFs con exploits, archivos comprimidos con ejecutables. Una vez que el usuario abre el adjunto en la red corporativa, el atacante puede:

- Establecer persistencia y moverse lateralmente en la red.
- Exfiltrar información confidencial de forma silenciosa.
- Desplegar ransomware y cifrar sistemas críticos.



> "El correo electrónico es como el vestíbulo de tu empresa. Si no controlas quién entra y con qué intención, todos tus demás controles de seguridad pierden eficacia."

(Equipo de Seguridad, Delta Protect)

Por qué las defensas tradicionales ya no son suficientes

Durante años, las organizaciones han confiado en una combinación de gateways de email, filtros de spam, listas negras y reglas estáticas para proteger su correo corporativo. Estas soluciones fueron efectivas en un contexto de amenazas simple. Hoy, ese contexto ya no existe.

3.1 El modelo de defensa basado en reputación

Los gateways tradicionales de email security operan principalmente con base en reputación: si el dominio o IP de origen tiene mala reputación, el correo se bloquea. El problema es que los atacantes modernos han aprendido a operar desde:

- **Dominios recién registrados:** con reputación neutral que aún no aparecen en listas negras.
- **Cuentas comprometidas:** de proveedores o socios reales con excelente reputación.
- **Servicios de nube legítimos:** como Google Workspace o Microsoft 365, cuya infraestructura tiene la máxima reputación.

> **El problema central**
>
> Si el ataque llega desde una cuenta de Gmail comprometida, o desde el dominio real de tu proveedor hackeado, ningún filtro basado en reputación lo va a detectar. El correo parece perfectamente legítimo porque, técnicamente, lo es.

3.2 Limitaciones de las reglas y firmas estáticas

Las reglas estáticas ("bloquear si contiene la palabra 'urgente' + un link") son trivialmente eludibles. Los atacantes prueban variaciones hasta encontrar una formulación que pase los filtros. Con herramientas de IA generativa, pueden producir miles de variaciones en minutos.

3.3 El gap del correo interno y de partners

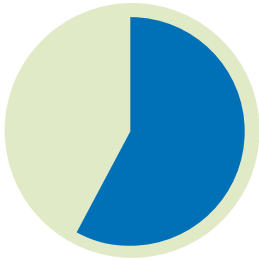
La mayoría de las soluciones de email security tradicionales se enfocan en el tráfico entrante (inbound). Pero algunas de las amenazas más graves viajan en sentido diferente:

- **Ingeniería social y phishing:** representan el 57% de los ataques a organizaciones en LATAM (Positive Technologies, Cybersecurity Threatscape LATAM 2023-2024).
- **BEC (Business Email Compromise):** costo promedio por incidente: USD $129,000 en 2024 (FBI IC3 2024 Annual Report, análisis Abnormal AI).
- **Tiempo de detección:** una brecha causada por compromiso de email tarda en promedio 292 días en ser identificada y contenida (IBM Cost of a Data Breach 2024).

El riesgo de terceros ya no es marginal: el 48% de las brechas de datos en 2025 involucraron a un tercero, un incremento del 60% frente al año anterior (Verizon DBIR 2026). Esto confirma que asegurar solo el correo entrante propio deja fuera una porción creciente del riesgo real.

3.4 El costo del modelo reactivo

Las soluciones tradicionales son fundamentalmente reactivas: esperan a que una amenaza sea conocida para agregar su firma o bloquear su dominio. Ante ataques zero-day o ataques altamente dirigidos (como el spear phishing o BEC), esa lógica llega siempre tarde. Los ataques BEC no contienen malware, links ni adjuntos maliciosos, los elementos que los filtros tradicionales saben buscar. Por eso son prácticamente invisibles para los gateways convencionales.

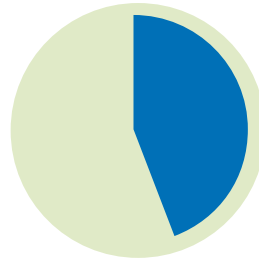


58%

de los ataques financieros por email usan "pretexting": ingeniería social en texto plano sin malware ni links *(Verizon DBIR 2026).*

292 días

tiempo promedio para detectar y contener una brecha por email comprometido *(IBM Cost of a Data Breach 2024)*



42%

de mensajes de fraude de proveedor (VEC) son abiertos por empleados *(Abnormal AI, 2026)*

La nueva generación de amenazas: IA en manos del atacante

La inteligencia artificial no es solo una herramienta defensiva. Los actores maliciosos la han adoptado rápidamente para hacer sus ataques más convincentes, más veloces y más escalables. Esto representa un salto cualitativo en el panorama de amenazas que ninguna organización puede ignorar.

4.1 Phishing generado por IA: perfecto a escala

Hasta hace poco, el phishing masivo era relativamente fácil de detectar: errores gramaticales, tonos incongruentes, saludos genéricos. La IA generativa ha eliminado esos marcadores. Herramientas como modelos de lenguaje de gran escala (LLMs) permiten a los atacantes generar correos perfectamente redactados en cualquier idioma, adaptados al tono de la empresa objetivo, con referencias a proyectos reales y nombres correctos, en segundos y a costo casi cero.

Nuevo vector: phishing hiperpersonalizado

Con una rápida búsqueda en LinkedIn y redes sociales, un atacante puede saber que "María García, Directora de Finanzas en [Empresa]" acaba de regresar de una conferencia en Miami y que su empresa acaba de anunciar una fusión. El correo malicioso llega con ese contexto exacto. La tasa de éxito es órdenes de magnitud mayor que el phishing genérico.

4.2 Deepfakes de voz y video: el paso siguiente

El correo electrónico ya no opera en aislamiento. Los atacantes sofisticados combinan el email con deepfakes de audio y video para crear ataques multicanal:

- Un correo de phishing seguido de una llamada donde se escucha la voz del CFO confirmando la instrucción.
- Un video en videollamada con el rostro del CEO generado en tiempo real para validar una solicitud fraudulenta.
- Mensajes de WhatsApp con voz clonada de un contacto conocido.

Estos ataques multimodales están en aumento y apuntan principalmente a ejecutivos y personal de finanzas en empresas medianas y grandes de LATAM.

4.3 Automatización del ciclo de ataque

La IA también permite a los atacantes automatizar el ciclo completo de un ataque: reconocimiento de la víctima, generación del correo personalizado, adaptación según la respuesta, y escalada del engaño. Un actor malicioso promedio combina hoy hasta 15 técnicas de ataque distintas en una sola campaña (Verizon DBIR 2026, análisis Abnormal AI). Lo que antes requería horas de trabajo manual por parte de un grupo especializado, hoy puede ejecutarse de forma automatizada contra cientos de objetivos en paralelo.

4.4 IA contra IA: la única respuesta a escala

Cuando el atacante usa IA para generar amenazas sin firma, sin patrones fijos y altamente personalizadas, la única defensa efectiva es también basada en IA: sistemas capaces de aprender el comportamiento normal de la organización y detectar anomalías sutiles que ninguna regla estática podría capturar.

> "El email de un atacante hoy es indistinguible de uno legítimo si solo analizas su contenido o su origen. Hay que analizar el contexto: quién lo envía, a quién, cuándo, cómo interactúa normalmente esa persona, qué es inusual en este mensaje."
>
> *(Equipo de Investigación de Amenazas, Abnormal AI)*

Cómo defenderse: capas de seguridad en el email

La defensa efectiva del correo electrónico no se logra con una sola herramienta. Requiere un enfoque por capas (defense in depth) que combine controles técnicos, procesos y comportamiento humano. A continuación, las capas fundamentales.

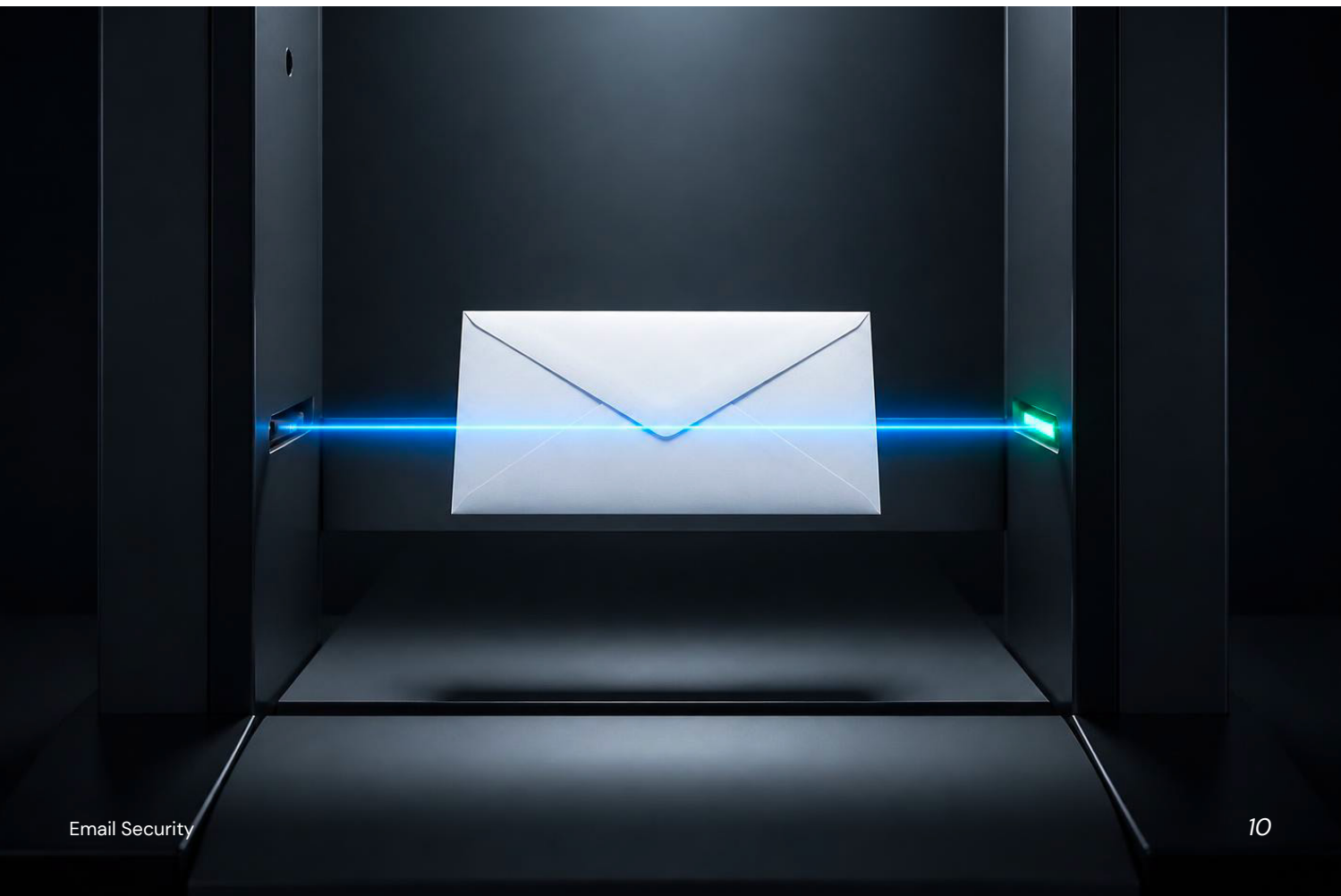
5.1 Autenticación del dominio: SPF, DKIM y DMARC

Antes de evaluar el contenido de un correo, hay que garantizar que quien dice enviarlo realmente lo envió. Los tres protocolos de autenticación de email son la base de cualquier estrategia:

- **SPF (Sender Policy Framework):** define qué servidores están autorizados a enviar correo en nombre de tu dominio.
- **DKIM (DomainKeys Identified Mail):** añade una firma digital criptográfica al correo que el receptor puede verificar.
- **DMARC:** define qué hacer cuando un correo falla SPF o DKIM (reject, quarantine o none) y envía reportes al propietario del dominio.

El problema global con DMARC

Solo el 47.7% de los principales dominios a nivel global tienen DMARC configurado, y apenas el 19.5% con política de rechazo activo (EasyDMARC Global DMARC Adoption Report 2025). Más revelador aún: de todos los dominios que tienen DMARC, solo el 10.2% ha alcanzado p=reject, la única configuración que bloquea activamente correos no autorizados. El tiempo promedio de la industria para llegar a esa configuración es de 195 días (Sendmarc Cyberthreat Report 2025). Configurar DMARC en modo 'reject' es uno de los pasos de mayor impacto y menor costo que puede tomar tu organización hoy.



5.2 Gateway de email seguro (SEG)

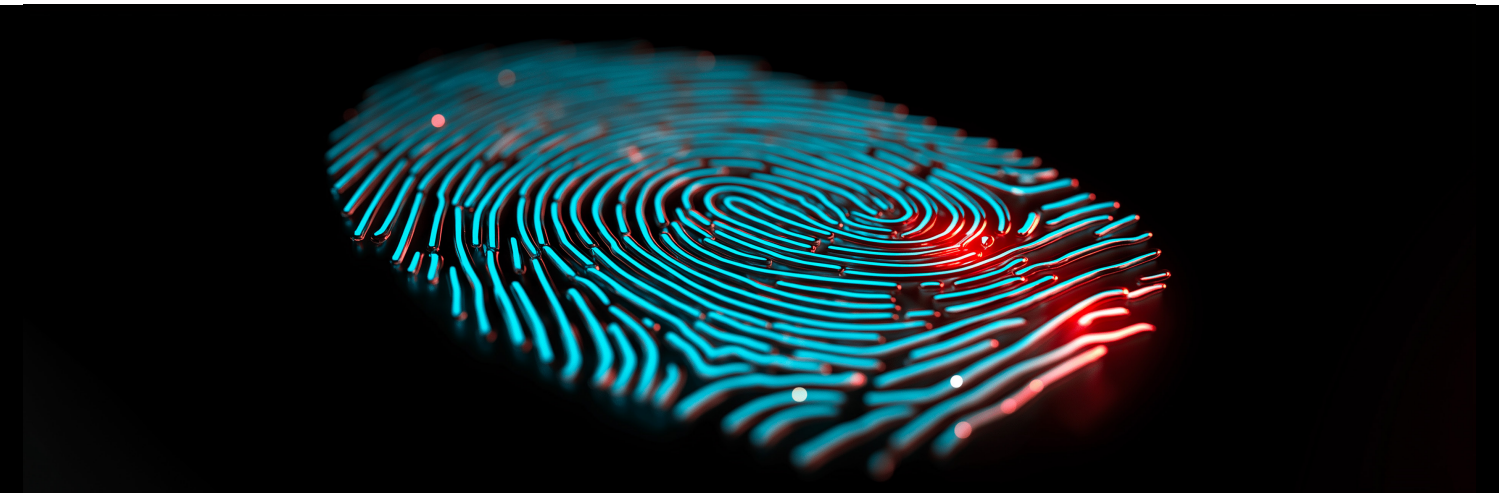
Un Secure Email Gateway es la primera línea de defensa: filtra correos entrantes y salientes basándose en reputación, firmas de malware, análisis de links y adjuntos. Es una capa necesaria pero no suficiente, como describimos en la sección anterior.

5.3 Detección basada en comportamiento con IA

La generación actual de soluciones de email security va más allá de los gateways tradicionales. En lugar de buscar firmas conocidas, aprenden el comportamiento normal de cada usuario y cada relación dentro de la organización:

- Con quién se comunica normalmente esta persona.
- En qué horarios envía y recibe correos.
- Qué tipo de solicitudes son típicas en su rol.
- Qué tono y vocabulario usa habitualmente.

Cuando un correo se desvía de ese patrón normal (aunque venga de un dominio legítimo, con buena reputación y sin links maliciosos), el sistema lo marca para revisión. Esta es la única forma de detectar BEC y VEC de manera confiable.

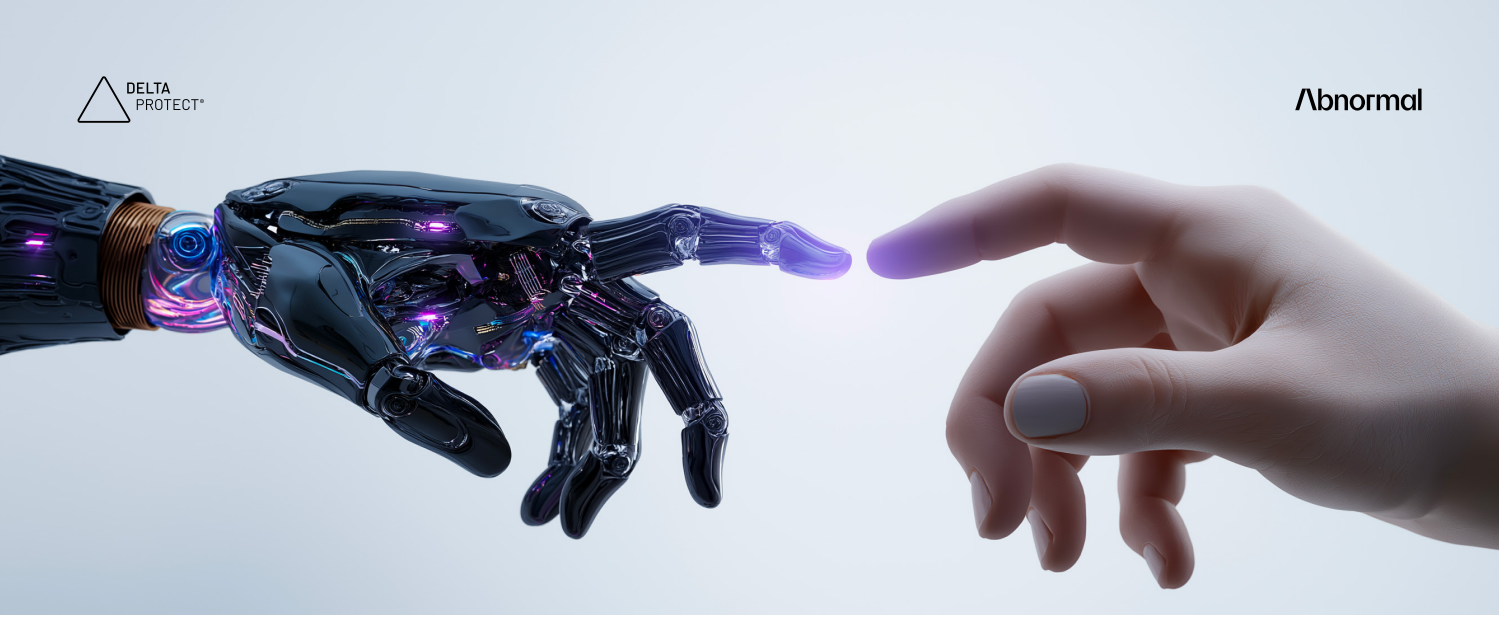


5.4 Sandboxing y detonación de adjuntos

Los adjuntos sospechosos se ejecutan en un entorno aislado (sandbox) antes de ser entregados al destinatario. Si el archivo intenta conectarse a un servidor externo, modificar el registro del sistema o ejecutar scripts, es bloqueado. Esta capa es crítica para detener malware y ransomware.

5.5 Respuesta automatizada e integración con SOAR

La velocidad de respuesta ante incidentes es tan importante como la detección. Las plataformas modernas de email security ofrecen capacidades de respuesta automatizada: remover mensajes de buzones en segundos tras la detección, actualizar reglas automáticamente, y alimentar el SIEM/SOAR corporativo con contexto enriquecido para la investigación.



El factor humano: concientización y capacitación

La tecnología puede reducir drásticamente la superficie de ataque, pero ningún sistema elimina al 100% el riesgo humano. Los atacantes lo saben, y por eso el email sigue siendo tan efectivo: en algún punto de la cadena, hay una persona tomando una decisión.

6.1 El empleado como última línea de defensa y como objetivo

El 62% de las brechas de ciberseguridad en 2025 involucran el factor humano (Verizon Data Breach Investigations Report 2026). No porque los empleados sean descuidados, sino porque los ataques modernos están diseñados específicamente para explotar mecanismos psicológicos: urgencia, autoridad, miedo, oportunidad.

Un empleado que recibe un correo del 'Director General' solicitando una acción urgente y confidencial no está fallando en su trabajo: está siendo víctima de ingeniería social sofisticada.

La respuesta no es solo culpar al empleado: es equiparlo mejor.

6.2 Programas de concientización efectivos

Un programa de concientización en ciberseguridad es efectivo cuando va más allá de un video anual obligatorio. Las mejores prácticas incluyen:

- **Simulaciones de phishing periódicas y personalizadas:** no basta con enviar el mismo correo simulado a toda la empresa. Las campañas más efectivas adaptan el escenario al rol, industria y comportamiento previo de cada empleado: un empleado de finanzas debe recibir un simulacro de fraude de proveedor, no uno genérico de 'haz clic aquí'.
- **Capacitación adaptativa por perfil de riesgo individual:** módulos cortos (5-10 minutos) asignados automáticamente según el historial de cada persona: quién hizo clic en simulacros anteriores, qué tipo de ataques recibe más frecuentemente y cuál es su nivel de exposición por rol.
- **Reporteo facilitado:** un botón de 'reportar phishing' en el cliente de correo que haga trivial alertar al equipo de seguridad.
- **Métricas y seguimiento:** medir la tasa de clics, reportes y tiempo de respuesta para evidenciar mejora continua.

El problema global con DMARC

Solo el 47.7% de los principales dominios a nivel global tienen DMARC configurado, y apenas el 19.5% con política de rechazo activo (EasyDMARC Global DMARC Adoption Report 2025). Más revelador aún: de todos los dominios que tienen DMARC, solo el 10.2% ha alcanzado p=reject, la única configuración que bloquea activamente correos no autorizados. El tiempo promedio de la industria para llegar a esa configuración es de 195 días (Sendmarc Cyberthreat Report 2025). Configurar DMARC en modo 'reject' es uno de los pasos de mayor impacto y menor costo que puede tomar tu organización hoy.

6.3 Políticas de verificación para solicitudes críticas

Uno de los controles más simples y efectivos contra BEC es una política clara de doble verificación para ciertos tipos de solicitudes:

- **Cambios en datos bancarios de proveedores:** siempre verificar por otro canal (llamada telefónica al contacto conocido) antes de procesar.
- **Transferencias urgentes solicitadas por email:** requerir autorización de al menos dos personas, independientemente de quién la solicite.
- **Solicitudes de credenciales o acceso:** IT nunca pedirá credenciales por email; esta premisa debe ser clara para todos.

> "La concientización sin tecnología es insuficiente. La tecnología sin concientización es frágil. La combinación de ambas es lo que construye resiliencia real."

(Equipo de Educación en Seguridad, Delta Protect)

Cumplimiento y regulaciones relevantes en México y LATAM

La inteligencia artificial no es solo una herramienta defensiva. Los actores maliciosos la han adoptado rápidamente para hacer sus ataques más convincentes, más veloces y más escalables. Esto representa un salto cualitativo en el panorama de amenazas que ninguna organización puede ignorar.

7.1 LFPDPPP: Ley Federal de Protección de Datos Personales en Posesión de Particulares

La ley mexicana de protección de datos exige que las organizaciones implementen medidas de seguridad 'administrativas, técnicas y físicas' para proteger los datos personales. Una brecha de seguridad originada por un ataque de phishing que exponga datos de clientes o empleados puede constituir una violación a esta ley, con consecuencias legales y reputacionales significativas.

- **Obligación de notificación:** ante una brecha que afecte datos personales, la organización debe notificar a la Secretaría Anticorrupción y Buen Gobierno (SABG), autoridad que sustituyó al INAI a partir de marzo de 2025, y a los titulares afectados.
- **Responsabilidad del responsable del tratamiento:** la empresa es responsable de los datos incluso cuando el ataque vino del exterior.
- **Multas:** de hasta 320,000 UMAs (Unidades de Medida y Actualización) por violaciones graves, equivalente a aprox. $36.2 millones MXN, según la nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares publicada en el DOF el 20 de marzo de 2025.

7.2 Regulación financiera: CNBV y Banco de México

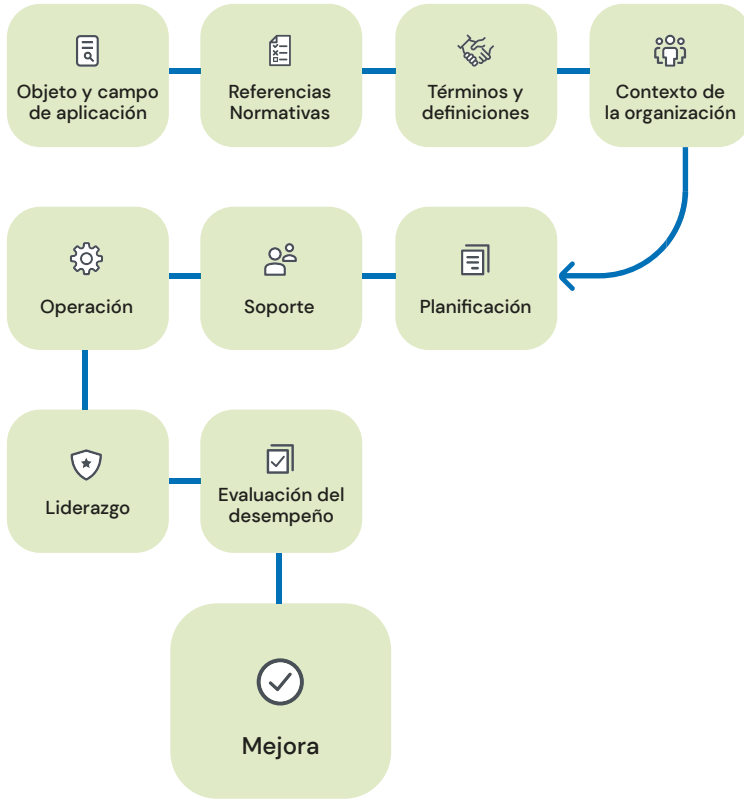
El sector financiero en México está sujeto a regulaciones específicas de ciberseguridad emitidas por la CNBV y Banxico. Las circulares vigentes exigen a las instituciones financieras, y el cumplimiento es urgente: según el Sendmarc Cyberthreat Report 2025, el 41% de las instituciones bancarias a nivel global carece de protección DMARC, exponiéndose a suplantación de dominio y fraude por email:

- **Controles de seguridad para canales digitales:** incluyendo el correo electrónico como canal de comunicación con clientes y contrapartes.
- **Planes de respuesta a incidentes:** con tiempos de respuesta definidos y protocolos de notificación al regulador.
- **Evaluaciones periódicas de vulnerabilidades:** pentesting y auditorías de seguridad que incluyan pruebas de phishing.

7.3 ISO 27001 e ISO 27002

La norma internacional ISO 27001 es el estándar de referencia para la gestión de seguridad de la información. Muchas organizaciones en México la adoptan voluntariamente o como requisito de sus clientes o socios comerciales. En la versión 2022 (vigente desde octubre 2025), los controles de seguridad en comunicaciones y operaciones se encuentran en las Secciones 5 (Controles Organizacionales) y 8 (Controles Tecnológicos) del Anexo A, con 93 controles en total. La protección del correo electrónico queda cubierta en el Control 8.7 (Protección contra malware) y el 8.12 (Prevención de fuga de datos), entre otros.

Estructura de la norma:



7.4 Sector salud: Normas Oficiales Mexicanas (NOM)

El sector salud maneja información de alta sensibilidad. La NOM-024-SSA3-2010 establece requisitos para los sistemas de información en salud, y la protección del correo electrónico es parte del perímetro de seguridad que debe proteger datos de expedientes clínicos y comunicaciones entre profesionales de salud.

El email como evidencia de cumplimiento

Más allá de prevenir ataques, las organizaciones bajo regulación deben poder demostrar que tienen controles. Un incidente de BEC o phishing que resulte en pérdida de datos puede derivar en auditorías regulatorias donde la falta de controles de email security es un hallazgo crítico. La inversión en seguridad de correo es también una inversión en defensa regulatoria.

Cómo evaluar una solución de email security

No todas las soluciones de seguridad de correo son iguales. Al evaluar opciones para tu organización, estas son las dimensiones y preguntas clave que deben guiar el proceso de selección.

8.1 Capacidades de detección: más allá del gateway

La primera pregunta es si la solución detecta solo amenazas conocidas o también amenazas desconocidas y ataques sin payload (BEC). Evalúa:

- **Detección de BEC y fraude de proveedor:** ¿la solución puede detectar ataques que no contienen links ni adjuntos maliciosos?
- **Análisis de comportamiento:** ¿aprende el perfil normal de comunicaciones de cada usuario o aplica reglas genéricas?
- **Cobertura de email interno:** ¿protege también las comunicaciones entre empleados dentro de la organización?
- **Detección en tiempo real vs. post-entrega:** ¿puede remover correos maliciosos de los buzones después de que fueron entregados?

8.2 Integración y despliegue

Una solución de email security debe integrarse sin fricción con tu ecosistema existente:

- **Compatibilidad con Microsoft 365 / Google Workspace:** despliegue nativo vía API sin redireccionamiento del flujo de correo (inline) que introduce latencia y puntos de falla.
- **Tiempo de despliegue:** ¿cuántos días tarda en estar operativa? Las soluciones modernas basadas en API deben configurarse en minutos y sin interrupciones.
- **Integración con SIEM y SOAR:** ¿exporta alertas y contexto enriquecido a tus herramientas de operaciones de seguridad?

8.3 Tasa de falsos positivos

Una solución que bloquea correos legítimos genera fricción operativa y pérdida de confianza por parte de los usuarios. Pregunta por la tasa de falsos positivos en producciones reales, no en demos.

El costo oculto del 99%: haz el cálculo con tus números

Un proveedor que dice ser '99.9% efectivo' suena impresionante, hasta que haces la matemática. Supón que tu organización procesa 1,500,000 correos al mes (típico en una empresa de 1,000 empleados). Un 0.1% de falsos positivos representa 1,500 correos legítimos bloqueados o marcados cada mes: 50 por día. Si tu equipo de operaciones de seguridad dedica solo 5 minutos a revisar y liberar cada uno, eso es 250 minutos diarios: casi medio analista de tiempo completo atendiendo únicamente falsos positivos. Multiplica eso por el costo por hora de tu equipo y calcula el impacto anual. Ahora imagina ese escenario en una empresa de 10,000 empleados, donde ese 0.1% se convierte en 500 correos bloqueados al día.

8.4 Visibilidad y reportería

El equipo de seguridad necesita visibilidad completa para investigar incidentes y demostrar el valor de la solución a la dirección:

- **Panel de amenazas detectadas:** con contexto completo: quién, qué tipo de ataque, qué acción se tomó, qué tan similar es a ataques anteriores
- **Métricas de ROI:** ¿cuántos ataques bloqueó? ¿cuánto tiempo ahorró al equipo de respuesta?
- **Reportes para auditoría y cumplimiento:** exportable en formatos que puedan usarse como evidencia ante reguladores.

Criterio de Evaluación	Importancia
Detecta BEC y VEC sin payload malicioso	Crítico
Análisis de comportamiento por usuario	Crítico
Cobertura de email interno	Alto
Integración nativa con M365/Google Workspace vía API	Crítico
Remediación post-entrega automatizada	Alto
Baja tasa de falsos positivos documentada	Crítico
Panel de visibilidad y reportería para auditoría	Medio
Soporte en español y presencia en LATAM	Medio
SLAs de respuesta ante incidentes definidos	Alto
Integración con SIEM/SOAR	Medio
Capacitación personalizada y adaptativa por empleado integrada a la plataforma	Alto

Conclusiones y próximos pasos

El correo electrónico seguirá siendo el principal vector de ataque mientras siga siendo el principal canal de comunicación empresarial. La buena noticia es que las organizaciones que adoptan un enfoque estructurado de defensa (combinando autenticación de dominio, detección comportamental con IA, capacitación humana y alineación regulatoria) reducen su riesgo de manera radical.

Lo que toda organización debe hacer hoy

- **Auditar la configuración de SPF, DKIM y DMARC:** asegurar que DMARC esté en modo 'reject', no 'none'.
- **Evaluar el gap de cobertura actual:** ¿tu solución detecta BEC y VEC? ¿cubre el correo interno?
- **Implementar un programa de concientización activo:** con simulaciones periódicas, no solo capacitación anual.
- **Documentar políticas de verificación para transferencias y cambios bancarios:** como control manual crítico contra fraude.
- **Alinear los controles con las obligaciones regulatorias aplicables:** LFPDPPP, CNBV, ISO 27001 según el sector.

El momento de actuar es ahora

Los ataques por email no esperan. Cada día que una organización opera sin los controles adecuados es un día de exposición. La pregunta no es si vale la pena invertir en email security: el costo de un solo incidente BEC supera por mucho el costo anual de cualquier solución profesional.

Siguientes pasos con Abnormal AI y Delta Protect

Abnormal AI ofrece la plataforma de email security de nueva generación más avanzada del mercado, con detección comportamental basada en IA que protege contra BEC, phishing, fraude de proveedor y amenazas internas. Delta Protect complementa esta capacidad con servicios de implementación, concientización, auditorías y cumplimiento regulatorio adaptados a la realidad de México y LATAM.

Juntos, ayudamos a organizaciones de todos los sectores a construir una defensa de correo electrónico que sea efectiva, medible y alineada a sus obligaciones legales.

Fuentes y referencias

Todos los datos estadísticos incluidos en este documento provienen de fuentes verificadas. A continuación se listan por sección.

Sección 1: El vector de ataque

- $3.04B pérdidas BEC 2025 / $20.8B pérdidas totales por cibercrimen 2025: FBI Internet Crime Complaint Center (IC3) Annual Report 2025. ic3.gov.
- 191K quejas de phishing en 2025: FBI IC3 Annual Report 2025.
- 1 email malicioso evadiendo filtros cada 19 segundos en 2025 (vs. cada 42 seg. en 2024): Cofense Annual State of Email Security Report, febrero 2026. cofense.com/annualreport
- México: 31M intentos de ciberataque en 2024 (55% de LATAM); 65% de empresas reportaron incremento en brechas: México Business News, 2024.

Sección 2: Anatomía del ataque

- Probabilidad semanal de BEC por tamaño de organización; VEC creció 50% año a año (2022-2023); 40% de clientes afectados mensualmente: Abnormal AI H1 2024 Email Threat Report. abnormal.ai/blog/bec-vec-attacks
- 44.2% de mensajes VEC son abiertos por empleados: Abnormal AI, CISO Guide to Supply Chain Compromise (2026). abnormal.ai/resources/ciso-guide-supply-chain-compromise
- BEC costo promedio USD $129,000 en 2024: FBI IC3 Annual Report 2024, análisis Abnormal AI. abnormal.ai/blog/2024-fbi-ic3-report

Secciones 3 y 5: Defensas

- BEC raramente incluye links o adjuntos maliciosos: Abnormal AI, abnormal.ai/blog/bec-problem-cisos-cant-ignore (sep. 2025)
- 58% de ataques financieros usan pretexting: Verizon Data Breach Investigations Report (DBIR) 2026.
- 48% de brechas involucraron a terceros (+60% vs. año anterior): Verizon DBIR 2026, vía análisis Abnormal AI.
- 292 días promedio para identificar y contener brecha por email comprometido: IBM Cost of a Data Breach Report 2024. ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry
- 47.7% de dominios con DMARC configurado, 19.5% con política de rechazo, 10.2% con p=reject: EasyDMARC Global DMARC Adoption Report 2025. easydmarc.com/blog/ebook/easydmarc-dmarc-adoption-report-2025
- 195 días promedio para llegar a p=reject; 41% de instituciones bancarias sin DMARC: Sendmarc Cyberthreat Report 2025.

Sección 4: IA en el ataque

- Un actor malicioso promedio combina hasta 15 técnicas de ataque distintas: Verizon DBIR 2026, análisis Abnormal AI. abnormal.ai/blog/blog-verizon-2026-dbir-key-takeaways

Sección 6: Factor humano

- 62% de las brechas involucraron el factor humano en 2025: Verizon DBIR 2026. abnormal.ai/blog/blog-verizon-2026-dbir-key-takeaways

Sección 7: Cumplimiento

- Ingeniería social = 57% de ataques a organizaciones en LATAM: Positive Technologies, Cybersecurity Threatscape for Latin America and the Caribbean 2023-2024. global.ptsecurity.com
- Secretaría Anticorrupción y Buen Gobierno (SABG) sustituye al INAI; LFPDPPP publicada en el DOF el 20 de marzo de 2025; multas hasta 320,000 UMA: verificado, Decreto DOF 20-mar-2025; UMA 2025 = $113.14 MXN/día.

Sobre Delta Protect

Delta Protect es una empresa mexicana de ciberseguridad que protege a negocios en México y LATAM mediante servicios como pentesting, cumplimiento normativo, certificaciones, evaluaciones de riesgo y monitoreo SOC. Hemos apoyado a más de 300 empresas en 8 países a fortalecer su seguridad y generar confianza. Nuestra misión es hacer la ciberseguridad simple, escalable y efectiva, construyendo un futuro digital más seguro para todos.

Delta Protect @delta.protect @DeltaProtect

Comienza a proteger tu empresa hoy →

www.deltaprotect.com

Sobre Abnormal AI

Abnormal AI es la plataforma líder de seguridad de comportamiento humano nativa de IA, que utiliza aprendizaje automático para detener ataques entrantes sofisticados y detectar cuentas comprometidas en correo electrónico y aplicaciones conectadas. Al comprender la identidad, el comportamiento y el contexto, Abnormal detecta y detiene ataques de ingeniería social que eluden las defensas tradicionales, incluyendo BEC, phishing y fraude de proveedores. Con la confianza de más de 4,500 organizaciones, incluyendo 25% de las empresas Fortune 500.

Abnormal AI @Abnormal https://abnormal.ai/

Solicitar una demostración →