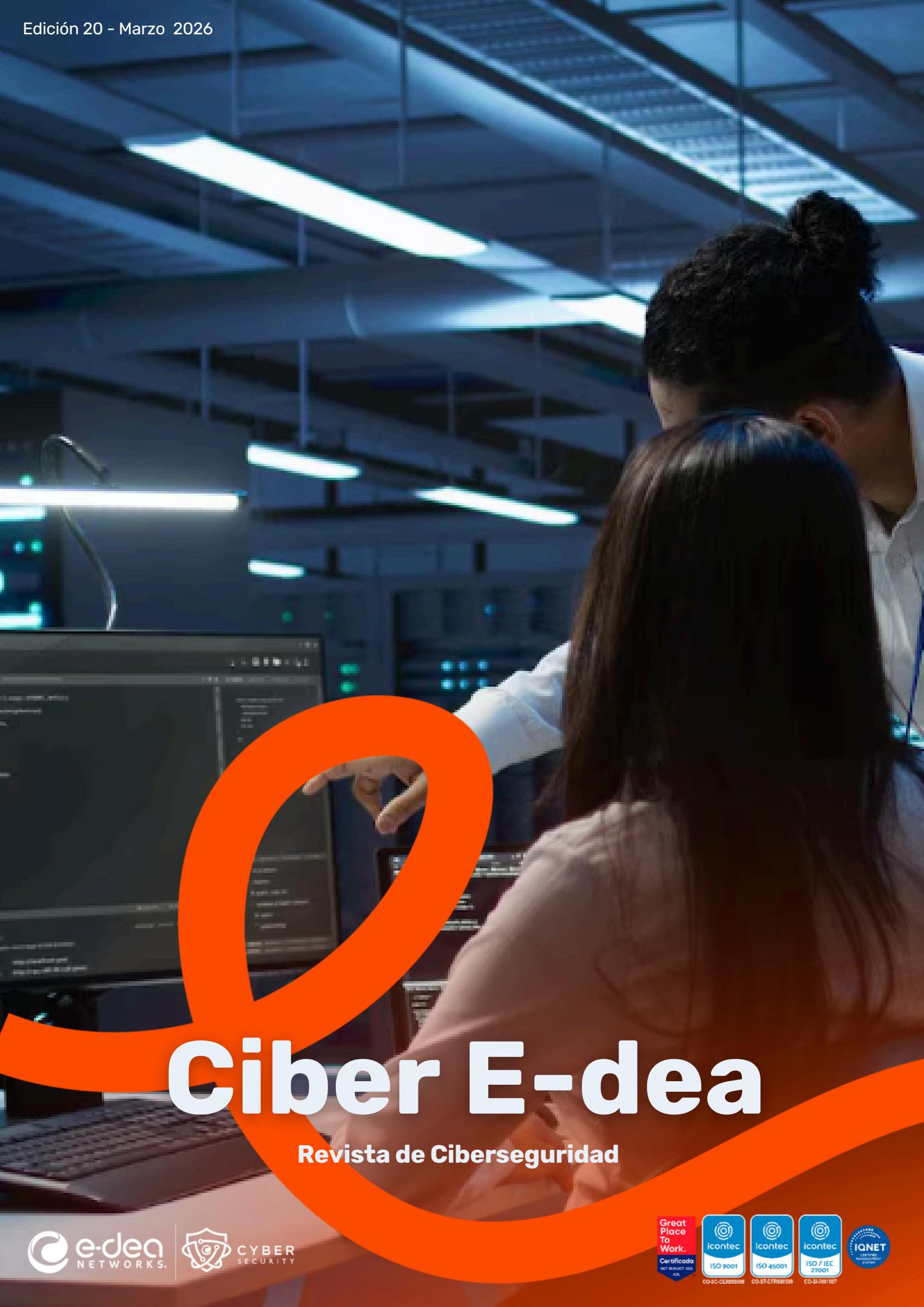
Edición 20 - Marzo 2026



Ciber E-dea

Revista de Ciberseguridad

e-dea NETWORKS | CYBER SECURITY

01 BoryptGrab en GitHub: La Amenaza que secuestra la confianza en el código abierto.

02 El ataque a Stryker: Crónica de un apagón global.

03 Dispositivos FortiGate explotados para vulnerar redes y robar credenciales de cuentas de servicio.

04 Vulnerabilidades destacadas.

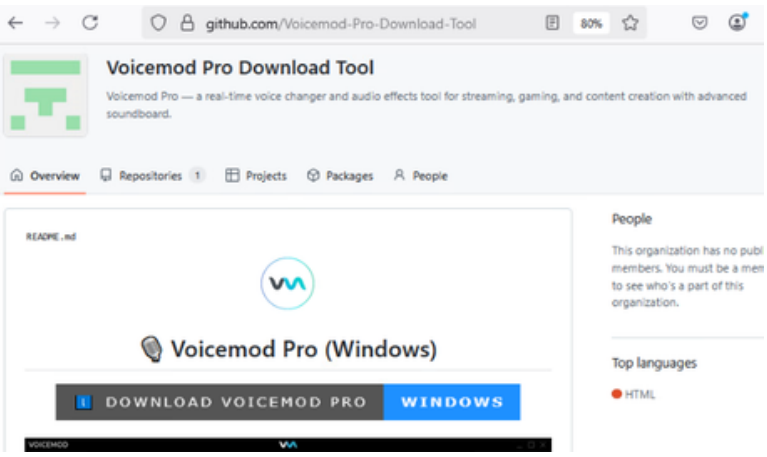
05 La exposición involuntaria de datos en plataformas de Inteligencia Artificial.

06 Ciber Incidentes en Colombia y en el mundo.

07 Contacto

01 **BoryptGrab en GitHub:** La amenaza que secuestra la confianza en el código abierto.

En marzo de 2026, la plataforma de desarrollo más importante del mundo, GitHub, se ha visto inundada por una sofisticada campaña de malware conocida como BoryptGrab. A diferencia de las brechas de seguridad tradicionales en servidores, este incidente utiliza la infraestructura de confianza de la comunidad para distribuir software malicioso a través de repositorios falsos, capturando activos digitales de miles de usuarios.

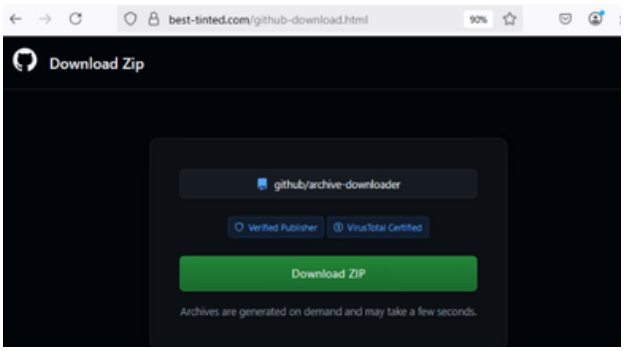


¿Qué es "BoryptGrab" y por qué es tan peligroso

Este software se oculta en proyectos que aparentan ser herramientas legítimas. Una vez ejecutado, actúa como un "infostealer" donde no solo roba contraseñas, sino que extrae las "llaves" de acceso directo a billeteras de criptomonedas y sesiones activas en navegadores, permitiendo a los atacantes vaciar cuentas sin necesidad de conocer la clave del usuario.

Datos clave

Destaca por su capacidad de manipular la percepción de seguridad de los desarrolladores y usuarios técnicos.
Se han detectado más de 100 repositorios maliciosos que utilizan técnicas de SEO Hijacking y manipulación de métricas (estrellas y commits falsos) para aparecer en los primeros resultados de búsqueda de GitHub.



¿Cómo protegerse de este ataque?

La recuperación ante una infección por BoryptGrab es extremadamente delicada. Al tratarse de un robo de identidad, no basta con eliminar el malware; el usuario debe asumir que todas sus cuentas han sido comprometidas.
Los expertos en seguridad recomiendan actualmente un protocolo de confianza cero.

¡Conoce más aquí!

02 **El ataque a Stryker:** Crónica de un apagón global.

El pasado 11 de marzo de 2026, Stryker Corporation, uno de los mayores gigantes de tecnología médica a nivel mundial, se convirtió en el blanco de un devastador ciberataque que ha paralizado sus operaciones en más de 60 países. A diferencia de los ataques habituales de "secuestro de datos" (ransomware), este incidente involucra un software mucho más agresivo conocido como wiper malware.

¿Qué es el "Wiper Malware" y por qué es tan peligroso?

Para entender la gravedad de lo ocurrido en Stryker, es fundamental diferenciar entre el malware tradicional y el wiper.
Mientras que el ransomware cifra los archivos y pide un rescate económico para devolver el acceso, el objetivo del wiper malware es la destrucción total y permanente. Este software borra o corrompe los archivos de tal manera que no pueden ser recuperados.

Datos clave del incidente:

Alcance: El grupo de hackers Handala, que se atribuyó la responsabilidad, afirma haber comprometido más de 200,000 dispositivos, incluyendo servidores y sistemas móviles.
Pérdida de datos: Se estima que se extrajeron o destruyeron cerca de 50 terabytes de información.
Motivación política: El grupo Handala declaró que el ataque fue una represalia por una acción militar de Estados Unidos en una escuela en Minab, Irán. Según los atacantes, esto marca una "nueva fase" en la guerra cibernética.

Impacto en la salud y la cadena de suministro

Stryker no es una empresa cualquiera; emplea a 56,000 personas y fabrica desde implantes ortopédicos y equipo quirúrgico hasta camas de hospital y dispositivos neurotecnológicos.
La interrupción de su red global tiene un efecto dominó en los hospitales de todo el mundo. El retraso en la entrega de suministros médicos críticos puede afectar directamente cirugías y tratamientos de emergencia, convirtiendo un problema digital en una crisis de salud pública.

¡Conoce más aquí!

03 **Ciberdelincuentes usan vulnerabilidades** en FortiGate para vaciar credenciales corporativas.

Los investigadores de ciberseguridad están llamando la atención sobre una nueva campaña en la que los actores de amenazas están abusando de los dispositivos FortiGate Next-Generation Firewall (NGFW) como puntos de entrada para violar las redes de las víctimas.

La actividad implica la explotación de vulnerabilidades de seguridad recientemente descubiertas o credenciales débiles para extraer archivos de configuración que contienen credenciales de cuentas de servicio e información de topología de red, según informó **SentinelOne.**

La empresa de seguridad indicó que la campaña ha identificado entornos vinculados a la atención médica, el gobierno y proveedores de servicios gestionados.

Análisis de la amenaza

- **Vectores de ataque:** La explotación se basa en vulnerabilidades recientemente descubiertas o credenciales débiles que permiten la extracción de archivos de configuración y topologías de red.
- **El rol de los IABs (Intermediarios de acceso):** En incidentes registrados desde noviembre de 2025, los atacantes crearon cuentas falsas (como "soporte") para garantizarse el acceso y posteriormente venderlo a otros criminales para obtener beneficio económico.
- **Robo de credenciales LDAP:** Las evidencias muestran que en febrero de 2026 los atacantes lograron descifrar archivos de configuración de **FortiGate** para extraer contraseñas en texto plano de cuentas de servicio, logrando registrar estaciones de trabajo no autorizadas.

¡Conoce más aquí!

Vulnerabilidades **destacadas**

Microsoft

CVE-2026-21316

Un atacante podría explotar esta vulnerabilidad para provocar que la aplicación se bloquee o deje de responder. La explotación de este problema requiere la interacción del usuario, ya que la víctima debe abrir un archivo malicioso.

SQL server

CVE-2026-21262

Un control de acceso inadecuado en SQL Server permite que un atacante autorizado eleve sus privilegios en una red.

GitHub

CVE-2026-23654

La dependencia de un componente vulnerable de terceros en el repositorio de GitHub: zero-shot-scfoundation permite que un atacante no autorizado ejecute código a través de una red.

¡Conoce más aquí!

05 La exposición involuntaria de datos en plataformas de Inteligencia Artificial.

La Inteligencia Artificial se ha consolidado como una herramienta indispensable para optimizar nuestra productividad. Hoy en día, es común utilizar asistentes virtuales para resumir contratos, redactar correos estratégicos o analizar reportes.

Sin embargo, esta adopción masiva ha traído consigo un nuevo reto de ciberseguridad: la sobreexposición de información confidencial.

El riesgo oculto en la productividad

Recientes incidentes corporativos han revelado un nuevo tipo de fuga de datos: la sobreexposición por IA. Profesionales están copiando y pegando contratos confidenciales, listas de clientes, códigos fuente o incluso sus propias declaraciones de impuestos en asistentes de IA públicos para que se los resuman. El problema es que, en muchas de las versiones gratuitas o estándar, esa información puede ser utilizada para "entrenar" al modelo de la IA.

Cómo evitar la exposición de datos corporativos.

- Antes de subir un documento o texto a una herramienta de IA pública, elimina o cambia nombres e información sensible.
- En la mayoría de los asistentes de IA, existe una opción en los ajustes llamada "Controles de datos" o "Historial del chat". Apaga la opción que permite que tus conversaciones se usen para entrenar sus modelos.
- Si tu empresa proporciona una versión corporativa o privada de una IA, úsala siempre en lugar de tu cuenta personal gratuita. Las versiones empresariales garantizan que tus datos no se comparten con el mundo.

La Inteligencia Artificial es un acelerador de resultados, pero no es un repositorio seguro. Trata cada instrucción que ingreses en un chat de IA como si la estuvieras publicando en un foro abierto de internet.

06 **CiberIncidentes en Colombia** y en el mundo

Filtración en la DIAN: Los datos de 18 millones de colombianos en riesgo.

A principios de marzo, foros especializados en la Dark Web revelaron la comercialización de un inmenso paquete de información confidencial presuntamente extraído tras vulnerar la plataforma de citas de la Dirección de Impuestos y Aduanas Nacionales (DIAN).

El impacto: Los ciberdelincuentes pusieron a la venta los registros por aproximadamente 2.000 dólares. El paquete no solo incluía información de ciudadanos, sino también un software diseñado para seguir explotando la falla en tiempo real.

SuperSalud bajo asedio: Más de 23 millones de ciberataques en un mes.

A finales de marzo, la Superintendencia Nacional de Salud (SuperSalud) confirmó que su infraestructura tecnológica fue blanco de una ofensiva sistemática y persistente. La entidad registró más de 23 millones de intentos de ataque diseñados para desestabilizar sus operaciones y procesos administrativos.

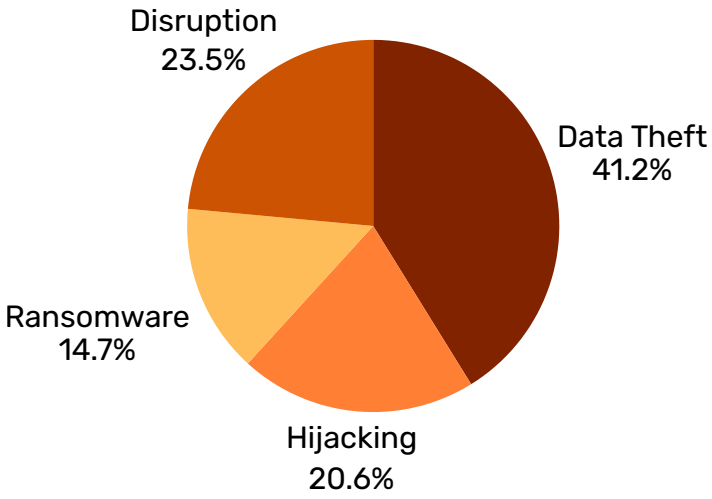
El impacto: Aunque la entidad activó protocolos de defensa tecnológica logrando mitigar el impacto en sus procesos esenciales, el volumen del ataque encendió las alarmas sobre posibles intentos de extorsión.

El mundo

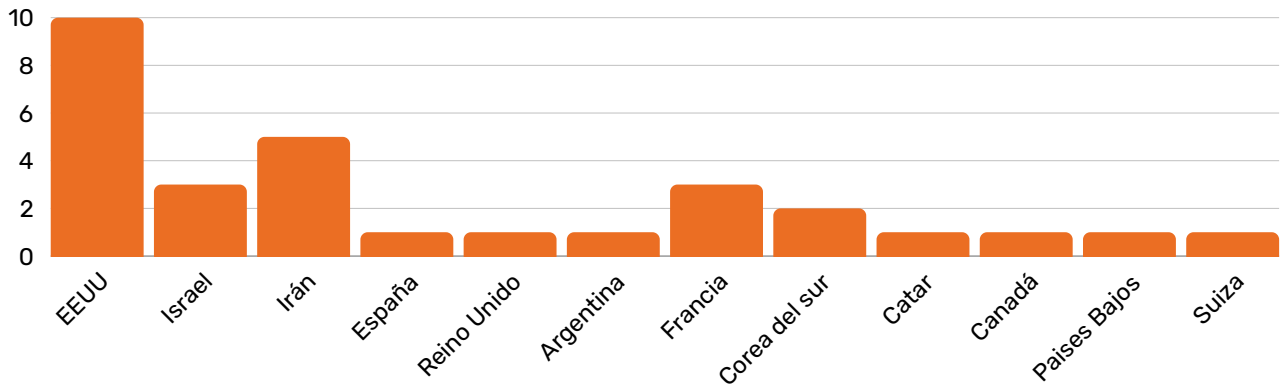
34
Ciber incidentes

Sectores afectados

Tipo de incidente



Países destacados



¡Conoce más aquí!

E-dea Networks

Para información adicional sobre cualquiera de nuestros productos o servicios, por favor contáctanos:

Email: contacto@e-dea.co
Teléfono: (601) 57 1 5188433 opción 2
Celular: (601) 57 3152231023

Visita nuestro sitio para más información: www.e-dea.co
Encuéntranos en: Carrera 7 # 156-10 Of. 1906-1801.
Torre Krystal - Centro Empresarial North Point