Proyecto tercer parcial ISO 2701 Seguridad informática.

Edgar Omar Rodriguez Hernandez 177888

Ivan Ros Padilla 177573

Estefano Alessandro Rodriguez Morin 178584

Josué Emmanuel López López 182078

Mauricio Josafat Salinas Carrilo 177406

Aaron Efraím Mata Martínez 179419

Universidad Politécnica de San Luis Potosí

Mtro. Servando López Contreras

Contenido

Introducción y descripción de la empresa

Es una aplicación de mensajería enfocada en la velocidad y seguridad, es súper rápida, simple y gratuita. Puedes usar Telegram en todos tus dispositivos al mismo tiempo. Tus mensajes se sincronizan a la perfección a través de cualquiera de tus teléfonos, tablets o computadoras. Telegram es una de las 5 apps más descargadas del mundo con más de 1000 millones de usuarios activos.

Historia

Creada en 2013 por los hermanos Pável y Nikolái Dúrov como una plataforma de mensajería totalmente encriptada, Telegram actualmente supera los 500 millones de usuarios activos tras la migración masiva de usuarios de Whatsapp en enero del 2021 en busca de un nuevo canal de comunicación con políticas de protección de datos y seguridad más estrictas.

¿Quién está detrás de Telegram?

Telegram es apoyado por Pavel Duróv y su hermano Nikolai. Pavel apoya a Telegram financiera e ideológicamente, mientras el aporte de Nikolai es tecnológico. Para hacer Telegram posible, Nikolai desarrolló un protocolo de datos personalizado y único, que es abierto, seguro y optimizado para trabajar con múltiples centros de datos. Como resultado, Telegram combina seguridad, confiabilidad y velocidad en cualquier red.

Objetivos estratégicos

Misión y Visión

Garantizar el derecho a la privacidad y la libre comunicación global mediante tecnología de vanguardia, accesible y gratuita.

Convertirse en la infraestructura de comunicación más segura y eficiente del mundo, redefiniendo los estándares de libertad digital y autonomía del usuario.

SECCIÓN 1: ALCANCE

Organigrama

Estructura: Organización Horizontal (Flat Structure)

- **Nivel Estratégico:** Pável Dúrov (CEO/Product Manager) y Nikolái Dúrov (CTO/Lead Architect).
- **Nivel Operativo Especializado:** Vicepresidencia de Operaciones (Ilia Perekopsky).
- **Nivel de Ejecución Técnica:** Núcleo de Ingeniería (30 desarrolladores Senior con acceso total al despliegue).
- **Nivel de Soporte Externo:** Red de Voluntarios (TSF) y Moderadores distribuidos.

Organización

Telegram opera bajo una filosofía de minimalismo radical, funcionando más como una startup tecnológica de élite que como una corporación multinacional. Su estructura es extremadamente horizontal y carece de la burocracia tradicional; no existen mandos intermedios ni directores de producto, ya que el propio Pavel Durόv supervisa personalmente el desarrollo de las funciones. Este enfoque permite una toma de decisiones veloz, donde un grupo reducido de ingenieros de alto nivel implementa cambios que en otras empresas requerirían meses de validación por comités.

Núcleo de Ingeniería y Desarrollo: Un grupo de aproximadamente 30 desarrolladores seleccionados mediante concursos globales, encargados del código base, la infraestructura de servidores y la seguridad del protocolo.

Liderazgo Estratégico y de Producto: Encabezado por los hermanos Durov; mientras Pavel define la visión y el diseño, Nikolai se encarga de la arquitectura técnica y el cifrado.

Operaciones y Relaciones Comerciales: Un equipo mínimo liderado por la vicepresidencia que gestiona la monetización (Telegram Premium), las asociaciones y la administración financiera.

Fuerza de Soporte de Telegram (TSF): Una red global de voluntarios que gestiona la atención al usuario y la moderación, permitiendo que la empresa mantenga una nómina oficial muy pequeña.

El modelo económico refuerza esta organización compacta al evitar la entrada de capital de riesgo tradicional. Al financiarse mediante la fortuna personal de su fundador y la emisión de bonos de deuda, la empresa no tiene una junta directiva externa a la que rendir cuentas. Esto garantiza que la estructura organizativa permanezca cerrada y centrada únicamente en la ejecución técnica y la privacidad, sin las distracciones operativas que suelen acompañar a las empresas que cotizan en bolsa.

Alcance

Normas ISO/IEC 27000

La serie **ISO/IEC 27000** (conocida comúnmente como la "familia ISO 27000") es un conjunto de estándares internacionales orientados a la seguridad de la información. Fue desarrollada de manera conjunta por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).

A diferencia de otras normas que se enfocan en la seguridad puramente informática (firewalls, antivirus), la familia 27000 adopta un enfoque holístico basado en la gestión del riesgo. Su objetivo principal es proteger tres principios fundamentales de la información:

- **Confidencialidad:** Garantizar que solo las personas autorizadas tengan acceso a la información.
- **Integridad:** Asegurar que la información no sea alterada de manera no autorizada o fraudulenta.
- **Disponibilidad:** Garantizar que los usuarios autorizados tengan acceso a la información cuando la requieran.

Dentro de esta familia coexisten diversos documentos: **ISO 27000** (proporciona el vocabulario y las definiciones), **ISO 27002** (una guía de buenas prácticas para implementar los controles), **ISO 27005** (especializada en la gestión de riesgos de seguridad), entre otras. Sin embargo, solo una de ellas es certificable.

Norma Seleccionada: ISO/IEC 27001:2022

Esta es la norma central de la familia porque establece los requisitos formales para diseñar, implementar, mantener y mejorar continuamente un **Sistema de Gestión de Seguridad de la Información (SGSI)**.

Cláusulas 4 a 10

Establece los requisitos del sistema de gestión bajo la estructura de alto nivel de ISO, siguiendo el ciclo de mejora continua PHVA (Planificar, Hacer, Verificar, Actuar):

- **Cláusula 4. Contexto de la organización:** Entender los factores internos y externos (en el caso de Telegram, su naturaleza distribuida y sus desafíos geopolíticos).
- **Cláusula 5. Liderazgo:** El compromiso de la alta dirección (Pavel Durov y el equipo directivo) con la seguridad.
- **Cláusula 6. Planificación:** Identificación y evaluación de riesgos, y establecimiento de objetivos de seguridad.
- **Cláusula 7. Soporte:** Recursos, competencias y concientización del equipo.
- **Cláusula 8. Operación:** Ejecución de los procesos para cumplir con la seguridad de la información.
- **Cláusula 9. Evaluación del desempeño:** Auditorías internas y revisión por la dirección.
- **Cláusula 10. Mejora:** Gestión de no conformidades y acciones correctivas.

B. El Anexo A (Los Controles de Seguridad)

La versión 2022 de la norma reestructuró los antiguos 114 controles en **93 controles**, divididos en 4 grandes temáticas. Para tu enfoque en el **procesamiento de información**, estos son los dominios aplicables:

- **Controles Organizacionales (Cláusula 5 del Anexo A):** Políticas, gestión de identidades, uso de activos.
- **Controles de Personas (Cláusula 6 del Anexo A):** Seguridad antes, durante y después del empleo (vital para el reclutamiento hermético de Telegram).
- **Controles Físicos (Cláusula 7 del Anexo A):** Seguridad en centros de datos y perímetros.
- **Controles Tecnológicos (Cláusula 8 del Anexo A):** Cifrado, desarrollo seguro, gestión de vulnerabilidades y redes.

3. Áreas y Procesos Específicos a Proteger en Telegram

Dado que el enfoque está en el **procesamiento de información**, los datos fluyen a través de procesos críticos ejecutados por un equipo sumamente pequeño. Debemos centrar la aplicación de la norma en las siguientes áreas:

Proceso A: Ciclo de Vida de Desarrollo de Software (SDLC) Seguro

- **Descripción:** Telegram actualiza sus aplicaciones móviles y de escritorio de manera sumamente veloz. El procesamiento de información comienza desde que un desarrollador escribe una línea de código.
- **Controles ISO 27001 Aplicables:**
  - **A.8.25 (Desarrollo seguro de software):** Exige reglas para el desarrollo de software seguro.
  - **A.8.28 (Gestión de la configuración):** Evita que configuraciones erróneas en el código expongan datos de los usuarios.
- **Enfoque de análisis:** Comprobar si los 30 ingenieros de Telegram (O el equipo designado a pruebas) aplican pruebas estáticas (SAST) y dinámicas (DAST) automatizadas antes de liberar actualizaciones a las tiendas de aplicaciones, mitigando el riesgo de introducir vulnerabilidades críticas en el procesamiento de mensajes.

Proceso B: Gestión de la Infraestructura y Servidores Distribuidos

- **Descripción:** El procesamiento y almacenamiento de los chats en la nube (que no son los chats secretos) se realiza en servidores repartidos por múltiples jurisdicciones.
- **Controles ISO 27001 Aplicables:**
  - **A.8.22 (Segregación de redes):** Asegura que las redes de producción estén separadas de las redes de prueba.

    - **A.8.14 (Seguridad de la información durante interrupciones):** Continuidad del procesamiento de datos en caso de caída de un nodo de red.
- **Enfoque de análisis:** Evaluar cómo Telegram fragmenta y distribuye las claves de descifrado en diferentes jurisdicciones para que ningún gobierno pueda forzar el procesamiento o entrega de datos completos.

Proceso C: Criptografía y Gestión de Claves

- **Descripción:** Telegram utiliza su protocolo propio (*MTProto*). El procesamiento seguro de la información depende enteramente de la fortaleza de sus algoritmos y del manejo de las llaves.
- **Controles ISO 27001 Aplicables:**
    - **A.8.24 (Uso de criptografía):** Exige políticas estrictas sobre el uso de controles criptográficos y gestión de llaves.
- **Enfoque de análisis:** Analizar la gobernanza sobre la generación, almacenamiento y destrucción de las claves criptográficas que protegen la información de los usuarios tanto en tránsito como en reposo.

4. Justificación de por qué se utiliza esta norma (ISO 27001) en Telegram

La elección de la **ISO/IEC 27001** como la normativa para auditar o estructurar la seguridad en Telegram es la más adecuada por las siguientes razones justificadas:

1. Proporcionalidad y Adaptabilidad al Tamaño del Equipo

- **Justificación:** Otras normas o marcos de trabajo (como COBIT o ITIL a gran escala) requieren pesadas estructuras burocráticas, comités de aprobación y múltiples niveles de auditoría que destruirían la agilidad de los 30 ingenieros de Telegram. ISO 27001 no te dice *cómo* debes hacer las cosas obligatoriamente, sino *qué objetivos* debes cumplir. Esto permite a Telegram mantener su estructura plana y ágil, pero bajo un marco auditable y estandarizado internacionalmente.

2. Blindaje contra la Ingeniería Social y la Amenaza Interna

- **Justificación:** En una empresa pequeña con acceso masivo a infraestructura, el eslabón más débil no es el código, sino el factor humano. Si un ingeniero es coaccionado por un gobierno o sobornado, la integridad de toda la red cae. El bloque de **Controles de Personas** y **Gestión de Accesos** de la ISO 27001 obliga a implementar el principio de mínimo privilegio y la revisión de antecedentes, limitando el radio de impacto si uno de los pocos empleados se ve comprometido.

3. Armonización Legal Internacional (Compliance)

- **Justificación:** Al procesar información de ciudadanos de la Unión Europea, América Latina, Asia y Medio Oriente, Telegram está sujeto a marcos legales contradictorios (GDPR, leyes locales de retención de datos, etc.). Adoptar ISO 27001 como estándar base dota a la empresa de una "presunción de cumplimiento". Al estar certificada o alineada con esta norma internacional, la empresa puede demostrar a reguladores externos que sus procesos de información cumplen con las mejores prácticas globales, independientemente de dónde estén ubicados físicamente sus servidores.

4. Enfoque Basado en Riesgos para la Autonomía Financiera

- **Justificación:** Dado que Telegram no rinde cuentas a una junta directiva tradicional ni a accionistas públicos, sus decisiones de seguridad podrían volverse unilaterales o impulsivas bajo el mando de Pavel Durov. La implementación de la Cláusula 6 (Planificación y Gestión de Riesgos) de la ISO 27001 obliga a la organización a justificar las inversiones y decisiones técnicas basándose en análisis de riesgos matemáticos y lógicos, y no en meras intuiciones de producto.

Referencias normativas

Activo en Cuestión

En el marco de la ISO 27001, un activo no es solo un servidor; es "algo que tiene valor para la organización". Por lo que el activo principal para esta investigación es:

- **Activo Primario:** El **Dato del Usuario** (Mensajería, Metadatos de contacto y archivos multimedia).
- **Activos de Soporte:**
  - **Código Fuente:** El protocolo **MTProto 2.0** y las aplicaciones cliente.
  - **Infraestructura:** Servidores distribuidos y el sistema de almacenamiento fragmentado.
  - **Talento Humano:** El conocimiento crítico de los **30 ingenieros** (especialmente Nikolai Durov).

Revisión de Términos y Condiciones (T&C) vs ISO 27001

Análisis de como los T&C de Telegram se alinean con la norma:

- **Punto de T&C:** *"No utilizamos tus datos para mostrarte anuncios"* (Alineado con el control de ISO 27001 sobre **Clasificación de la Información**).
- **Punto de T&C:** *"Almacenamos los datos necesarios para que el servicio funcione"* (Alineado con el principio de **Minimización de Datos** y **Retención de Información** de la norma).
- **Conflicto Potencial:** Telegram declara que solo entrega datos bajo órdenes judiciales de alta sospecha de terrorismo. Bajo ISO 27001, esto debe estar procedimentado en el control de **Relación con las Autoridades**.

Activos Internos

- **Código fuente del protocolo MTProto:** El núcleo criptográfico propietario que define cómo se cifra y transfiere la información entre los clientes y los servidores.
  Política funcional: **Control de Versiones y Auditoría:** Todo cambio en las librerías del núcleo criptográfico debe someterse a una revisión por pares (Peer Review) y a pruebas de estrés criptográfico antes de su despliegue.

- **Claves criptográficas privadas:** Las llaves maestras de descifrado distribuidas y fragmentadas en servidores de distintas jurisdicciones.
  Política funcional: **Fragmentación Jurisdiccional:** Ninguna clave de descifrado maestra podrá ser almacenada íntegramente en un solo centro de datos o país. La reconstrucción de una clave requiere la autorización técnica de múltiples nodos en distintas jurisdicciones.

- **Bases de datos de metadatos:** Registros que contienen la información de contactos, nombres de usuario y grafos de conexión social de la plataforma.
  Política funcional: **Minimización de Datos:** Solo se almacenarán los metadatos estrictamente necesarios para la funcionalidad del servicio (ej. sincronización de contactos); los registros efímeros deben ser purgados tras 24 horas.

- **Infraestructura de servidores en la nube (Nodos de almacenamiento):** Los servidores lógicos configurados y administrados por el equipo de ingeniería para el almacenamiento de los "Cloud Chats".
  Política funcional: **Aislamiento de Nodos:** Cada clúster de almacenamiento debe operar de forma estanca. Un compromiso en un nodo de almacenamiento no debe permitir el escalamiento lateral hacia otros nodos de la red.

- **Código fuente de las aplicaciones cliente:** Los repositorios de código correspondientes a las versiones de iOS, Android, Desktop y Web de la plataforma.
  Política funcional: **Publicación y Reproducibilidad:** Se mantendrá un repositorio público actualizado para cada plataforma (iOS, Android, Desktop), permitiendo que terceros verifiquen que el código publicado coincide exactamente con los binarios disponibles en las tiendas de aplicaciones (Reproducible Builds).

- **Talento humano especializado (Núcleo de Ingeniería):** El conocimiento técnico crítico residente en los aproximadamente 30 desarrolladores y arquitectos de software.
  Política funcional: **Dispersión Geográfica y Redundancia:** El equipo de ingeniería no debe concentrarse en una sola ubicación física. Se implementará un programa de "Conocimiento Compartido" donde al menos tres ingenieros dominen cada módulo crítico para evitar puntos únicos de falla (Bus Factor).

- **Documentación técnica y arquitectura de red:** Los diagramas, topologías y procedimientos internos que describen el funcionamiento y la recuperación ante desastres de la red descentralizada.
  Política funcional: **Cifrado de Documentación Sensible:** Los diagramas de topología y manuales de recuperación ante desastres (DRP) se almacenarán en contenedores cifrados con acceso restringido bajo el principio de "necesidad de saber".

- **Registros de auditoría y logs de sistemas:** Los historiales de acceso, modificaciones de configuración y alertas de seguridad generados por los servidores internos.
  Política funcional: **Logs Inalterables (Write-Once):** Los registros de auditoría deben ser enviados en tiempo real a un servidor de logs centralizado y protegido contra escritura, de modo que ningún administrador pueda modificar o borrar sus propias huellas de acceso.

- **Entornos de integración y despliegue continuo (CI/CD):** Las herramientas y servidores utilizados internamente para probar, compilar y liberar actualizaciones de software.
  Política funcional: **Aislamiento del Entorno de Construcción:** Los servidores de compilación deben operar en entornos efímeros y limpios, sin conexión directa a internet, para evitar la inyección de dependencias maliciosas durante el proceso de empaquetado.

- **Redes de administración interna:** Las VPNs, canales encriptados y credenciales de acceso utilizadas por el equipo de desarrollo para gestionar la infraestructura global.
  Política funcional: **Autenticación Multifactor de Hardware (MFA):** El acceso a las VPNs y canales de administración interna requerirá obligatoriamente el uso de llaves físicas de seguridad (tokens de hardware), eliminando la dependencia exclusiva de contraseñas.

- **Red Blockchain**: La red blockchain desarrollada por telegram para la transferencia de criptomonedas bajo su propio protocolo.
  Política funcional: **Gobernanza y Consenso Distribuido:** Se implementará un protocolo de consenso que impida la concentración de poder de cómputo o de participación (Staking) en una sola jurisdicción geográfica o entidad legal, asegurando que la red permanezca operativa incluso si nodos críticos son desconectados.

Activos Externos:

- **Infraestructura física de centros de datos de terceros:** Los proveedores que suministran el espacio físico, enfriamiento y energía eléctrica para alojar los servidores de Telegram en diversas regiones.
  Política funcional: **Aislamiento de Hardware (Bare Metal):** Se priorizará el uso de servidores físicos dedicados sobre instancias virtuales para evitar ataques de canal lateral. Los discos duros deben contar con cifrado de hardware total (SED) que impida la lectura de datos si el disco es extraído físicamente.

- **Plataformas de distribución de software:** Las tiendas de aplicaciones (Apple App Store, Google Play Store, Microsoft Store) necesarias para la entrega de actualizaciones a los usuarios finales.
  Política funcional: **Diversificación de Canales:** Además de las tiendas oficiales, se mantendrán versiones de instalación directa (APKs) y versiones web independientes para garantizar el acceso en caso de retiro arbitrario de las tiendas de Apple o Google.

- **Dispositivos finales de los usuarios (Endpoints):** Los teléfonos inteligentes, tabletas y computadoras personales donde reside temporalmente o permanentemente la información descifrada (ej. Secret Chats).
  Política funcional: **Higiene de Datos Local:** La aplicación implementará por defecto el borrado de caché sensible y la opción de "Autodestrucción de mensajes" para reducir la huella forense en el almacenamiento físico del dispositivo.

- **Proveedores de pasarelas de SMS (OTP):** Las empresas de telecomunicaciones de terceros contratadas para el envío masivo de códigos de verificación durante el registro o inicio de sesión.
  Política funcional: **Transición a Verificación Interna:** Se priorizará el envío de códigos de acceso a través de dispositivos ya vinculados. El SMS se considerará un método de última instancia con caducidad ultra-corta (menor a 2 minutos).

- **Redes de proveedores de servicios de internet (ISPs):** La infraestructura global de telecomunicaciones que permite el enrutamiento del tráfico entre los usuarios y los servidores de la aplicación.
  Política funcional: **Resiliencia de Red (Domain Fronting/Proxies):** La infraestructura debe soportar el uso de protocolos de ofuscación de tráfico y sistemas de proxies inteligentes (MTProto Proxy) para evadir la censura por parte de los ISPs.

- **Pasarelas de pago de terceros:** Los procesadores financieros (como Stripe, Google Pay o Apple Pay) utilizados para gestionar las suscripciones de Telegram Premium y la compra de activos digitales.
  Política funcional: **Tokenización de Pagos:** La plataforma no almacenará números de tarjetas de crédito; toda transacción se manejará mediante tokens proporcionados por el procesador, asegurando que un compromiso en la base de datos de Telegram no exponga datos financieros.

- **Servicios de mitigación de ataques DDoS:** Los proveedores externos de filtrado de tráfico utilizados para absorber y repeler ataques de denegación de servicio a gran escala.
  Política funcional: **Filtrado de Capa de Transporte (Capa 4):** La mitigación se limitará preferentemente a las capas de red y transporte para bloquear tráfico malicioso basado en volumen, evitando la inspección de la capa de aplicación (Capa 7) siempre que sea técnicamente viable.

- **Proveedores de servicios de nombres de dominio (DNS):** Las entidades responsables de la resolución de los dominios oficiales de la empresa, vitales para que los clientes encuentren los servidores.
  Política funcional: **Implementación de DNSSEC y Bloqueo de Registro:** Todos los dominios críticos deben contar con extensiones de seguridad (DNSSEC) para prevenir el envenenamiento de caché y "Registry Lock" para evitar transferencias o cambios de DNS no autorizados mediante ingeniería social.

- **Red de voluntarios de soporte (Telegram Support Force - TSF):** El personal externo y descentralizado que asiste en la moderación y atención a usuarios, quienes manejan información de soporte sin ser empleados directos.
  Política funcional: **Acceso Compartimentado y Anonimizado:** Los voluntarios accederán a herramientas de soporte que oculten datos sensibles (como números de teléfono completos o direcciones IP) mediante máscaras de datos, mostrando solo lo estrictamente necesario para resolver la duda técnica.

- **Redes de entrega de contenido (CDN) descentralizadas:** Infraestructura externa utilizada de apoyo en regiones específicas para acelerar la descarga de archivos multimedia públicos y reducir la latencia.
  Política funcional: **Exclusión de Contenido Privado:** Solo se permitirá el almacenamiento en caché de archivos multimedia públicos (canales públicos, fotos de perfil públicas) en nodos de CDN externos; los mensajes de chats privados y grupos cerrados nunca deberán tocar servidores de CDN de terceros.

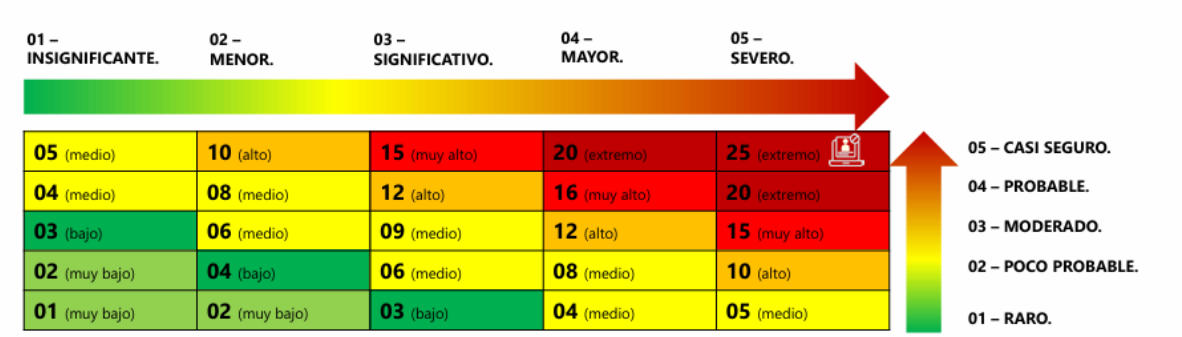
Términos y Definiciones de la ISO 27000 (Aplicables a Telegram)

De las ~81 definiciones, no necesitas todas. Para Telegram, estas son las más críticas que deberías incluir en tu reporte:

1. **Información (2.37):** Datos que tienen valor para la organización.
2. **Seguridad de la Información (2.28):** Preservación de la confidencialidad, integridad y disponibilidad.
3. **Sistema de Gestión de Seguridad de la Información (SGSI) (2.30):** Parte del sistema de gestión general basada en un enfoque de riesgo empresarial.
4. **Riesgo (2.61):** Efecto de la incertidumbre sobre los objetivos.
5. **Activo (2.4):** Algo que tiene valor para la organización.
6. **Confidencialidad (2.12):** Propiedad de que la información no se ponga a disposición de personas no autorizadas.
7. **Integridad (2.40):** Propiedad de exactitud y completitud.
8. **Disponibilidad (2.9):** Propiedad de ser accesible y utilizable a petición de una entidad autorizada.
9. **Control (2.16):** Medida que modifica el riesgo.
10. **Amenaza (2.77):** Causa potencial de un incidente no deseado.

SECCIÓN 6: PLANIFICACION

Matriz de riesgos



I. Riesgo Extremo (16 - 25)

Riesgos que requieren atención inmediata y controles estrictos.

1. **Claves Criptográficas Privadas**
    a. **Riesgo:** Pérdida de confidencialidad total de los datos.
    b. **Matriz:** Probabilidad (04) x Impacto (05) = **Extremo (20)**.
    c. **Política:** Fragmentación jurisdiccional y almacenamiento exclusivo en HSM.
2. **Infraestructura de Servidores (Nodos)**
    a. **Riesgo:** Acceso no autorizado a "Cloud Chats".
    b. **Matriz:** Probabilidad (04) x Impacto (05) = **Extremo (20)**.

c. **Política:** Aislamiento de nodos y cifrado de datos particionado.

3. **Talento Humano (Núcleo de Ingeniería)**
    a. **Riesgo:** Fuga de conocimiento crítico o "Bus Factor".
    b. **Matriz:** Probabilidad (04) x Impacto (04) = **Extremo (16)**.
    c. **Política:** Dispersión geográfica y protocolos de salida segura.
4. **Mitigación de ataques DDoS**
    a. **Riesgo:** Caída sistémica de la plataforma por saturación.
    b. **Matriz:** Probabilidad (05) x Impacto (05) = **Extremo (25)**.
    c. **Política:** Filtrado en Capa 4 y redundancia con múltiples proveedores Anycast.
5. **Redes de Administración Interna**
    a. **Riesgo:** Movimiento lateral de atacantes hacia el núcleo.
    b. **Matriz:** Probabilidad (04) x Impacto (05) = **Extremo (20)**.
    c. **Política:** Acceso mediante Zero Trust y llaves físicas (MFA).
6. **Código Fuente del Protocolo MTProto**
    a. **Riesgo:** Descubrimiento de vulnerabilidades críticas por ingeniería inversa.
    b. **Matriz:** Probabilidad (03) x Impacto (05) = **Muy Alto / Extremo (15-20)**.
    c. **Política:** Auditorías criptográficas constantes y control estricto de repositorios.

II. Riesgo Muy Alto (10 - 15)

Riesgos con impacto severo que pueden comprometer la operación.

7. **Proveedores de Pasarelas de SMS (OTP)**
    a. **Riesgo:** Interceptación de códigos (SS7) para secuestro de cuentas.
    b. **Matriz:** Probabilidad (05) x Impacto (03) = **Muy Alto (15)**.
    c. **Política:** Priorizar verificación interna y rotación de proveedores.
8. **Red Blockchain**
    a. **Riesgo:** Fallo en contratos inteligentes o pérdida de activos.
    b. **Matriz:** Probabilidad (03) x Impacto (04) = **Alto (12)**.
    c. **Política:** Auditoría matemática de TVM y nodos descentralizados.
9. **Bases de Datos de Metadatos**
    a. **Riesgo:** Perfilamiento de usuarios por filtración de grafos sociales.
    b. **Matriz:** Probabilidad (04) x Impacto (03) = **Alto (12)**.
    c. **Política:** Cifrado en reposo y purga de logs efímeros.
10. **Proveedores de DNS**
    a. **Riesgo:** Redirección de tráfico mediante secuestro de dominios.
    b. **Matriz:** Probabilidad (03) x Impacto (05) = **Muy Alto (15)**.
    c. **Política:** Implementación obligatoria de DNSSEC y Registry Lock.
11. **Documentación Técnica y Arquitectura**
    a. **Riesgo:** Manual de instrucciones para un atacante externo.
    b. **Matriz:** Probabilidad (02) x Impacto (05) = **Alto (10)**.
    c. **Política:** Cifrado de documentos y acceso por necesidad de saber.

12. **Entornos CI/CD**
    a. **Riesgo:** Inyección de malware en las actualizaciones oficiales.
    b. **Matriz:** Probabilidad (03) x Impacto (05) = **Muy Alto (15)**.
    c. **Política:** Firma de código multi-etapa y aislamiento de compilación.

III. Riesgo Medio / Bajo (04 - 09)

Riesgos operacionales manejables con controles preventivos.

13. **Código Fuente de Aplicaciones Cliente**
    a. **Riesgo:** Creación de clones maliciosos de la app.
    b. **Matriz:** Probabilidad (04) x Impacto (02) = **Medio (08)**.
    c. **Política:** Repositorios públicos y Reproducible Builds para validación.
14. **Registros de Auditoría (Logs)**
    a. **Riesgo:** Manipulación de huellas tras una intrusión.
    b. **Matriz:** Probabilidad (03) x Impacto (03) = **Medio (09)**.
    c. **Política:** Logs inalterables (Write-Once) y monitoreo de anomalías.
15. **Infraestructura de Centros de Datos (Terceros)**
    a. **Riesgo:** Acceso físico al hardware por personal del hosting.
    b. **Matriz:** Probabilidad (02) x Impacto (04) = **Medio (08)**.
    c. **Política:** Servidores Bare Metal con cifrado de disco total (SED).
16. **Dispositivos Finales de Usuarios (Endpoints)**
    a. **Riesgo:** Acceso local por robo del teléfono o malware.
    b. **Matriz:** Probabilidad (05) x Impacto (01) = **Medio (05)**.
    c. **Política:** Autodestrucción de mensajes y borrado de caché local.
17. **Plataformas de Distribución (App Stores)**
    a. **Riesgo:** Eliminación de la app por censura gubernamental.
    b. **Matriz:** Probabilidad (03) x Impacto (03) = **Medio (09)**.
    c. **Política:** Canales de distribución alternativos (APK, Web).
18. **Redes de ISPs**
    a. **Riesgo:** Bloqueo regional o inspección profunda de paquetes.

b. **Matriz:** Probabilidad (04) x Impacto (02) = **Medio (08)**.
c. **Política:** Protocolos de ofuscación y sistemas de proxy (MTProto).

19. **Pasarelas de Pago de Terceros**
    a. **Riesgo:** Exposición de datos de facturación de usuarios.
    b. **Matriz:** Probabilidad (02) x Impacto (03) = **Bajo (06)**.
    c. **Política:** Tokenización total y separación de identidad financiera.
20. **Redes CDN Descentralizadas**
    a. **Riesgo:** Caché de contenido manipulado.
    b. **Matriz:** Probabilidad (02) x Impacto (02) = **Bajo (04)**.
    c. **Política:** Exclusividad de contenido público y verificación de hashes.

Definir la Ley dentro del Marco de Referencia

Telegram opera en un "limbo" legal estratégico, definición del marco legal que aplica según su operación:

- **GDPR (Reglamento General de Protección de Datos - UE):** Obligatorio porque procesan datos de ciudadanos europeos. La ISO 27001 es el mejor vehículo para demostrar cumplimiento con el GDPR.
- **Ley Federal de los EAU (No. 2 de 2019):** Al estar su sede operativa en Dubái, deben cumplir con las leyes de protección de datos de salud y telecomunicaciones de los Emiratos Árabes Unidos.
- **Leyes de Privacidad de las Islas Vírgenes Británicas:** Donde está registrada la entidad legal principal, regulando su gobernanza corporativa.
- **Ciberseguridad:** Normativas internacionales de lucha contra el cibercrimen que obligan a la cooperación limitada (aunque Telegram es famoso por su resistencia en este punto).

SECCIÓN 7: SOPORTE

CARTA DE CONFORMIDAD Y NOTIFICACIÓN DE SEGURIDAD (PSI)

DEPARTAMENTO: Ciberseguridad e Infraestructura – Telegram FZ-LLC

CÓDIGO DE DOCUMENTO: TLG-SEC-POL-2026

1. DATOS DEL COLABORADOR

- **Nombre completo:** _____
- **Puesto / Área:** _____
- **ID de Empleado:** _____ **Fecha:** _____

2. GESTIÓN DE COMPETENCIA Y RECURSOS

En cumplimiento con la gestión de recursos de la organización, se ha determinado lo siguiente:

- Se han definido los conocimientos y competencias necesarios para su puesto, determinando que la apertura de puertos de red no esenciales no forma parte de sus herramientas requeridas para la operación diaria.
- El entorno de materiales e infraestructura (su computadora) ha sido configurado bajo el estándar de **"Menor Privilegio"**.

3. CONCIENCIACIÓN DEL SGSI Y PSI

El colaborador declara ser consciente de los lineamientos del **Sistema de Gestión de Seguridad de la Información (SGSI)** de Telegram:

- **Protección de Activos:** Entiendo que el cierre de puertos lógicos es una medida de protección para la información valiosa de la empresa y reduce la superficie de ataque ante posibles intrusiones o malware.
- **Aceptación de Políticas:** Reconozco que los puertos de mi equipo de trabajo han sido cerrados/bloqueados preventivamente como parte de la **Política de Seguridad de la Información (PSI)** vigente.

4. PROTOCOLO DE COMUNICACIÓN

Se establecen los procesos de comunicación oficiales para cualquier solicitud técnica:

- **Qué comunicar:** Cualquier necesidad operativa que requiera una excepción en el firewall.

- **Canal:** Las solicitudes deberán enviarse vía ticket al equipo de Seguridad Informática, incluyendo la justificación técnica.
- **Evaluación:** El equipo de InfoSec evaluará si el usuario posee la competencia y la necesidad real para autorizar dicha excepción de forma temporal.

5. DECLARACIÓN DE CONFORMIDAD

Al firmar este documento, el colaborador acepta que ha sido notificado sobre las restricciones de red en su equipo y se compromete a no intentar vulnerar o modificar la configuración de seguridad establecida por el departamento de IT.

"Entiendo que estas medidas no son una limitante a mi trabajo, sino una responsabilidad compartida para proteger la infraestructura global de Telegram."

Firma del Trabajador	**Sello / Firma de Seguridad Informática**
_____	_____
Nombre:	**Telegram Team**

SECCIÓN 8: OPERACIÓN

01 TRATAMIENTO DE LOS RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN

Activo: Código fuente de las aplicaciones cliente

Riesgo asociado: Desconfianza del usuario o inyección de código malicioso en binarios de las tiendas de aplicaciones que no coinciden con el código público.

1. PLAN (Planificar)

- **Definición de Entornos:** Establecer las especificaciones técnicas de los entornos de compilación "limpios" y efímeros que permitan generar binarios idénticos (Reproducible Builds).
- **Cronograma de Sincronización:** Diseñar el flujo de trabajo para que el repositorio público (GitHub/GitLab) se actualice simultáneamente con el envío de versiones a las tiendas de aplicaciones.
- **Documentación de Compilación:** Crear guías paso a paso para que auditores externos puedan replicar el proceso de construcción desde el código fuente.

2. DO (Hacer)

- **Publicación de Repositorios:** Mantener actualizados los repositorios públicos para iOS, Android y Desktop con cada nueva versión lanzada.
- **Generación de Binarios:** Ejecutar el proceso de compilación en los entornos aislados definidos para asegurar que los artefactos finales sean reproducibles.
- **Firma de Código:** Aplicar las firmas digitales correspondientes tanto al código fuente como a los binarios para garantizar su integridad durante la distribución.

3. CHECK (Verificar)

- **Pruebas de Reproducibilidad:** Realizar comparaciones bit a bit entre los binarios generados internamente y los descargados de las tiendas oficiales (App Store, Google Play).
- **Auditoría de Terceros:** Monitorear y validar los reportes de la comunidad o de auditores externos que intentan verificar la coincidencia del código publicado.
- **Validación de Integridad:** Verificar que el hash del código en el repositorio coincida con la documentación de la versión publicada.

4. ACT (Actuar)

- **Corrección de Desviaciones:** Si se detecta una discrepancia entre el binario y el código fuente, se debe identificar la causa (ej. cambio en las dependencias) y corregir el entorno de compilación inmediatamente.
- **Actualización de Políticas:** Ajustar los manuales de compilación si las herramientas de las plataformas (XCode, Android Studio) cambian y afectan la reproducibilidad.
- **Mejora de Transparencia:** Implementar mejores herramientas de automatización en el CI/CD para reducir el error humano en la publicación de versiones.

Sección 10: Mejora

- **Riesgo Asociado de la Matriz:** I. Riesgo Extremo - No. 6: Código Fuente del Protocolo MTProto.
- **Riesgo Teórico:** Descubrimiento de vulnerabilidades críticas por ingeniería inversa.
- **Valoración en Matriz:** Probabilidad (03) x Impacto (05) = Muy Alto / Extremo (15).
- **Política del SGSI Afectada:** Auditorías criptográficas constantes y control estricto de repositorios.

1. Qué ocurrió (Descripción de la No Conformidad y caso hipotético)

El 18 de abril de 2026, un investigador de seguridad externo notificó a través del programa *Bug Bounty* de Telegram el descubrimiento de una vulnerabilidad crítica de desbordamiento de búfer en el componente de cifrado del código fuente del protocolo MTProto 2.0, la cual permitía realizar ingeniería inversa avanzada y deducir fragmentos de memoria efímera. La investigación interna reveló que la vulnerabilidad fue introducida en una actualización menor realizada tres semanas antes. El cambio en el código fuente omitió el control técnico estricto del repositorio y se publicó en producción sin haber pasado de forma obligatoria por la **auditoría criptográfica constante de terceros** estipulada en la política de seguridad, constituyendo una desviación directa al cumplimiento de los controles del SGSI.

2. Medidas de contención y mitigación (Consecuencias indeseables)

Inmediatamente después de la validación del reporte (tiempo de respuesta de 45 minutos):

- **Aislamiento del repositorio:** Se restringió temporalmente el acceso de escritura al repositorio principal del protocolo para congelar cualquier línea de desarrollo adyacente.
- **Despliegue de Parche Criptográfico:** El núcleo de ingeniería senior desarrolló y aplicó un parche de emergencia (*hotfix*) directo al código fuente para neutralizar la vulnerabilidad de ingeniería inversa.
- **Auditoría Retrospectiva Externa:** Se contrató de manera urgente a la firma externa encargada de las auditorías matemáticas del protocolo para analizar el parche en un entorno aislado y certificar de manera exprés que la integridad criptográfica de MTProto había sido completamente restablecida antes de liberar la actualización global a las aplicaciones cliente.

3. La causa raíz del suceso

Tras realizar el análisis mediante la metodología de los *5 Porqués*, se determinó que la causa raíz fue una **falla en la configuración de la automatización (*pipeline*) de control del repositorio en el entorno de desarrollo seguro**.

Específicamente, una regla técnica que debía bloquear de forma mandatoria la fusión de ramas (*merge*) hacia la rama principal si no existía el certificado digital o token de aprobación de la auditoría criptográfica externa, fue desactivada manualmente de forma temporal durante una ventana de mantenimiento previa y no se volvió a activar por falta de una verificación automatizada posterior de cumplimiento técnico.

4. Las medidas adoptadas para eliminar la causa raíz (Acción Correctiva)

Para evitar la recurrencia de este fallo y blindar de forma permanente la política de la organización, se implementaron las siguientes acciones técnico-administrativas:

- **Endurecimiento Técnico de Repositorios (Control Estricto):** Se implementaron reglas de protección de rama inmutables en el control de versiones. A partir de esta fecha, el sistema exige de manera automatizada dos factores de validación inquebrantables: la firma criptográfica del líder del Núcleo de Ingeniería y el hash de aprobación emitido por el sistema de la firma auditora externa. Ningún usuario (incluidos administradores) puede evadir esta restricción.
- **Monitoreo Automático de Cumplimiento:** Se integró un bot de auditoría continua en el sistema de control de repositorios que escanea cada 60 minutos las configuraciones de seguridad de las ramas críticas. Si detecta que alguna regla de protección es modificada o desactivada, alerta instantáneamente al equipo de Ciberseguridad y revoca los accesos de forma preventiva.

5. Evaluación de la eficacia de las medidas adoptadas

Treinta días después de la implementación de las acciones correctivas (18 de mayo de 2026), el área de Seguridad Informática realizó la auditoría de seguimiento:

- Se extrajo el historial de auditoría inalterable (*logs*) del repositorio central, confirmando que se realizaron 8 fusiones (*merges*) de código al protocolo MTProto en este periodo.
- En el 100% de los casos, el entorno exigió y validó de forma correcta tanto la firma del núcleo de ingeniería como la certificación de la auditoría criptográfica externa antes de permitir el empaquetado del código.
- El bot de monitoreo automático reportó un correcto funcionamiento sin caídas.
- **Conclusión:** La acción correctiva se evalúa como **Eficaz**, habiendo mitigado el riesgo de inyección de vulnerabilidades explotables por ingeniería inversa mediante un

control técnico estricto y automatizado del código fuente de nuestro protocolo principal.