ISSN: 2805-1807
XX Congreso Nacional de Ciencia y Tecnología
30 de septiembre al 3 de octubre 2025

Avances en la Implementación del Servicio de Sincronización al UTC(CNMP) por NTP de Manera Segura

Solis Betancur, Raúl Fernando
CENAMEP AIP
Ciudad de Panamá, Panamá
ORCID: 0000-0003-1043-4294

Abstract

With the increasing need for synchronization to keep processes and equipment under control, such as the synchronization needs of IoT devices or the need for time traceability in the financial sector, access to reliable time sources is extremely important, especially when cyberattacks on Information Technology and Operational Technology infrastructures are in increase, with the aim of affecting the time transfer chain. Therefore, the Primary Time and Frequency Laboratory, responsible for safeguarding of the Time and Frequency National Standards (Atomic Clocks) and developing the UTC(CNMP), together with the Time and Frequency Dissemination Laboratory, responsible for providing time dissemination services traceable to the UTC(CNMP), began a development of strengthening their processes against possible cyberattacks, resulting in a UTC(CNMP) synchronization service using the Network Time Protocol, more secure and reliable for its customers.

Keywords: UTC(CNMP), NTP, timing, cybersecurity, GNSS.

Resumen

Con el incremento de la necesidad de sincronización para tener bajo control los procesos y los equipamientos, como es el caso de las necesidades de sincronización de los dispositivos IoT o las necesidades de rastreabilidad de tiempo en el sector financiero, el acceso a fuentes de tiempo confiable es sumamente importante y más cuando se están incrementando los ciberataques a las infraestructuras de las Tecnologías de la Información y las Tecnologías Operativas con el objetivo de afectar la cadena de transferencia de tiempo. Por ello, el Laboratorio Primario de Tiempo y Frecuencia, encargado de custodiar los Patrones Nacionales de Tiempo y Frecuencia (Relojes Atómicos) y desarrollar el UTC(CNMP), en conjunto con el Laboratorio de Diseminación de Tiempo y Frecuencia, encargado de brindar servicios de diseminación de tiempo rastreable al UTC(CNMP), iniciaron un proceso de robustecimiento de sus procesos frente a posibles ciberataques, y teniendo como resultado un servicio de

https://doi.org/10.33412/apanac.2025.13

sincronización al UTC(CNMP) empleando el Network Time Protocol, más seguro y confiable para sus clientes.

Palabras claves: UTC(CNMP), NTP, sincronización, ciberseguridad, GNSS.

1. INTRODUCCIÓN

El empleo de fuentes de tiempo estables y seguras es una de las piedras angulares en los conceptos de IoT, sistemas financieros y entornos digitales, porque nos permiten saber cuándo los eventos ocurren, lo que nos da una secuencia de la ocurrencia de los eventos, que nos permiten correlacionarlos y obtener más información del proceso o de las características de seguridad. Por ello, se recomienda emplear relojes de referencia rastreables al Tiempo Universal Coordinado (UTC) o al GNSS (Global Navegation Satellite System) y, en algunos casos, es requerido obligatoriamente su empleo: de manera mundial la Unión Internacional de Telecomunicaciones (ITU), la Unión Europea (EU) y Estados Unidos (EE. UU.), lo requieren en sus procesos financieros y de ciberseguridad, mostrado en la Tabla 1.

Tabla 1. Normativas donde se requiere el empleo obligatorio de UTC.

Dominio	Normativa	Descripción
ITU	ITU-R TF.1876	Fuentes de tiempo confiable para autoridades de estampado de tiempo (firma digital)
UE	ETSI EN 319-421 y ESTI EN 319-422	Time Stamping Units deben estar sincronizados con UTC
UE	MiFID II / MiFIR	Las entidades financieras deben sincronizar sus relojes con referencia a UTC/GNSS para reporte de órdenes y transacciones
UE	ECB TARGET2 / TIPS	Los mensajes de pago instantáneo deben llevar timestamps en UTC
EE. UU.	FINRA / SEC / CAT	La sincronización del “Business Clocks” es a UTC(NIST)
EE. UU.	Guías NIST (SP 800-53, SP 800-171)	En ciberseguridad, se requiere timestamps a UTC

Como los ciberataques ahora se están dirigiendo a atacar las cadenas de transferencia de tiempo desde dos frentes: el frente de las Tecnologías de la Información (TI) y el frente de las Tecnologías Operativas (TO), normas de ciberseguridad como la ISO 27001:2022 (Anexo A, Controles de Seguridad, A.8.15 — “Uso de relojes”) exige el control del reloj de referencia. Y por ello, muchos usuarios consideran que cuando se emplea el protocolo NTP (Network Time Protocol) [1] o su versión simple, el SNTP, se satisfacen muchos de estos requerimientos.

Debido al incremento del NTP/SNTP como mecanismo de sincronización al UTC, el Laboratorio de Diseminación de Tiempo y Frecuencia (LDTF) del Centro Nacional de

https://doi.org/10.33412/apanac.2025.13

Metrología de Panamá (CENAMEP) inicia el servicio de sincronización por NTP al UTC(CNMP) [2] y el LPTF desarrolla un sistema de gestión del laboratorio para mejorar su desempeño en el control del UTC(CNMP) [3]. Pero al llegar la pandemia, se redefine todo lo concerniente a seguridad en el cibermundo, obligando a desarrollar una serie de trabajos con el objetivo de robustecer la seguridad en entornos de TI y también ahora incluimos entornos de TO para garantizar una sincronización segura al UTC(CNMP).

2. MÉTODO

En términos de las referencias de tiempo, se analizó el comportamiento del UTC(CNMP) y los Relojes Atómicos (RA), que son el corazón de los procesos en el LPTF, buscando la deriva (asociado a su predictibilidad) y a su dispersión (asociado a la calidad de la señal de referencia). Para realizar la predicción y mantener UTC(CNMP) bajo control, se emplea regresiones lineales simples en los RA y el resultado se aplica al Generador de Desvíos de Frecuencia [4]. En términos del control de las TO, se trabajó en incrementar la seguridad del enlace con GNSS, empleando mecanismos de detección y mitigación de interferencias radioeléctricas, el control de la redundancia del respaldo eléctrico y el desempeño de los servidores NTP/SNTP (llamados Servidores de Tiempo por Red o STR). En términos del control de las TI se trabajó en analizar las vulnerabilidades de conexión (por ejemplo, empleando el programa Nmap), además del acceso a las configuraciones guardadas por contraseña y el desempeño del Firewall local.

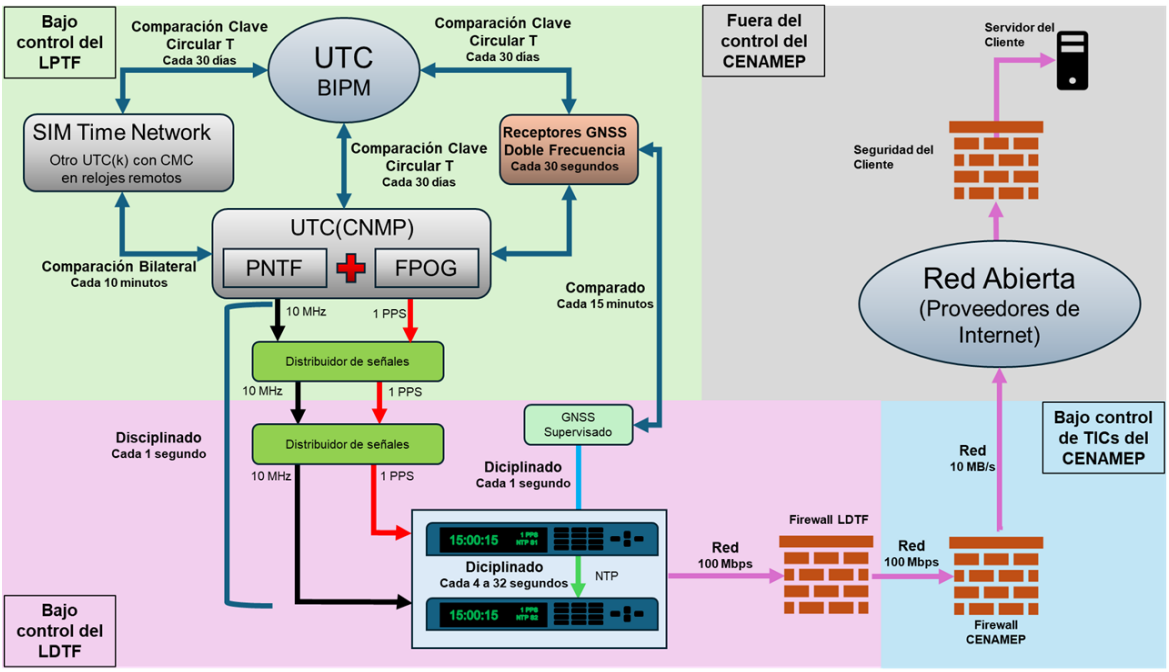

Figura 1. Zonas de control de los laboratorios LPTF y LDTF, el CENAMEP y hasta los clientes.

https://doi.org/10.33412/apanac.2025.13

El trabajo se desarrolló en los procesos que el LPTF y el LDTF tenían bajo control, como se muestra en la Figura 1, mientras que el área de TI del CENAMEP desarrolla sus propios procesos de seguridad.

3. RESULTADOS

A. Mejoras en el control de UTC(CNMP) y los Patrones Atómicos

Se logro establecer las estabilidades en para que cumplieran con parámetros conocidos de telecomunicaciones, y que también mostraran realmente los estados de los RA. Además, se obtuvieron datos que nos permiten mejorar el control del UTC(CNMP) en base a los RA, como se muestra en la Figura 2 y la Tabla 2.

	Límite ITU G.811	CS1 (ns)	CS2 (ns)	CS3 (ns)	CS4 (ns)	CS5 (ns)
Desviación a 1 segundo	± 1E-11	-1.51E-14	-4.15E-14	3.89E-14	6.83E-14	-2.07E-13
TDEV (1 s)	3 ns	0.004	0.004	0.006	0.003	0.003
TDEV (100 s)		0.094	0.098	0.087	0.071	0.079
TDEV (1 000 s)	30 ns	0.296	0.296	0.262	0.211	0.223
TDEV (10 000 s)		0.999	1.143	0.820	0.566	0.860
Datos empleados para predecir la diferencia de tiempo y corregir UTC(CNMP)						
Variabilidad (empleando TDEV)		**CS1 (ns)**	**CS2 (ns)**	**CS3 (ns)**	**CS4 (ns)**	**CS5 (ns)**
V_5: Variabilidad a 5 días		6.2	10.6	7.8	7.2	14.6
V_{30}: Variabilidad a 30 días		8.7	20.4	14.7	13.2	22.1
V_{90}: Variabilidad a 90 días		20.1	38.6	36.7	28.5	48.0
P: Pendiente (ns/mes)		-1.3	-3.6	3.4	5.9	-17.9

Figura 2. Los resultados de la caracterización de los RA en términos de cumplimiento como reloj de referencia (ITU G.811) y en términos de la predictibilidad para sostener el UTC(CNMP).

Tabla 2. Análisis de 2 años de la realización local del UTC del CENAMEP, con respecto a otros institutos de la región.

	UTC(CNMP) Panamá	UTC(NIST) E.E. U.U.	UTC(CNM) México	UTC(ICE) Costa Rica	UTC(INM) Colombia
Promedio (ns)	0,4	-0,1	-1,5	11,0	-65,4
Dispersión (ns)	5,5	1,0	3,6	50,9	60,1
Incertidumbre (k = 2)	11,2	4,0	10,6	14,2	40,8

B. Mejoras en el control de las TO

Las medidas implementadas permitieron mejorar el control de los receptores GNSS y los servidores NTP/SNTP que tienen conexión secundaria a GNSS, además de implementar

https://doi.org/10.33412/apanac.2025.13

mecanismos de mitigación de interferencias tipo Jamming (empleando filtros y medidas de espectro, mostrado en la Figura 3) y tipo Spoofing (implementando mecanismos de validación de satélites como el OSNMA [5]).

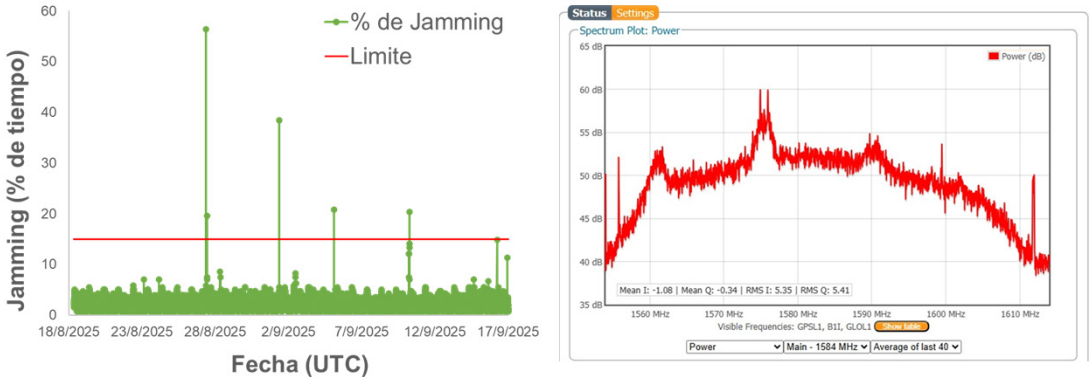

Figura 3. El poder detectar señales de interferencia nos permiten asegurar la calidad del enlace GNSS para las comparaciones por vista común y salvaguardar físicamente los receptores de cualquier daño.

Además, se implementaron mejores mecanismos de verificación del desempeño de los STR, con lo que se obtuvo rendimientos por debajo de 200 us en redes internas (mostrado en la Tabla 3), con lo que se establecen criterios de control de su desempeño. También se emplea la Red de Comparación de Servidores NTP [6] para monitorear el rendimiento en redes externas y logrando variaciones por debajo de 10 ms en comparaciones contra NIST (datos abiertos accesibles desde la página https://tf.nist.gov/sim/).

Tabla 3. Se emplea una comparación constante entre servidores para verificar su desempeño y generar referencia para analizar su comportamiento frente a posibles situaciones de seguridad.

Servidor NTP	Stratum de trabajo	Fuente de sincronización	Offset (ms)	Dispersión (ms)	Exactitud (combinación cuadrática, ms)
Servidor Piloto	1	GNSS	0,000	0,002	± 0,002
Servidor A	1	Frecuencia	0,000	0,011	± 0,011
Servidor B	2	Servidor A	1,780	0,273	± 1,801
Servidor C	1	Frecuencia	0,018	0,006	± 0,019
Servidor D	1	1 PPS	0,052	0,034	± 0,062
Servidor E	2	Servidor A	-0,002	0,025	± 0,025

C. Mejoras en el Control de las TI

El trabajo desarrollado resultó que para el control de las TI lográramos:
Mejoras en el control de las contraseñas empleando almacenamiento encriptado mediante

https://doi.org/10.33412/apanac.2025.13

MD5 y el algoritmo 3DES, y se eliminó cualquier configuración en texto plano para los programas desarrollados en los laboratorios.
Analizar y mitigar las vulnerabilidades: Se hicieron pruebas agresivas a cada equipo involucrado. Los sistemas más seguros fueron los STR (diseñados para ser seguros), mientras que los receptores GNSS mostraron vulnerabilidades por configuración (tienen las herramientas de seguridad, pero hay que activárselas manualmente). Los sistemas operativos fueron los entornos menos seguros y requirieron más trabajo de configuración y actualizaciones.
Configurar al Firewall local para que solo permitiera tráfico NTP/SNTP a las zonas delimitadas para los STR a sus puertos asignados, y se activaron sus funciones de reconocimiento de tráfico para robustecer la seguridad en caso de ataques o intentos de intrusión.

4. CONCLUSIONES

Con el desarrollo de este trabajo, se refuerza las capacidades para mantener en control los procesos y su optimización. Se ha mejorado y el robustecido la generación de UTC(CNMP) y su transferencia a los clientes que lo necesitan mediante NTP/SNTP. Además, al incorporar un enfoque de ciberseguridad en las TI/TO, se incrementa la confianza de la prestación del servicio de sincronización empleando NTP/SNTP. Con esto podemos seguir indicando que el LDTF sigue brindando soluciones a necesidades reales con este primer servicio de Sincronización Segura empleando NTP/SNTP, manteniéndonos como referencia en la región de Centroamérica y el Caribe.

Referencias

[1] Mills, D., Burbank, J., & Kasch, W. (2010). Network Time Protocol Version 4: Protocol and Algorithms Specification. https://doi.org/10.17487/rfc5905
[2] Solís Betancur, R. F. (2016). Servicio de Diseminación de Tiempo por Red en el CENAMEP AIP. En Simposio de Metrología 2016 (pp. 211–212). CENAM. https://www.cenam.mx/memorias/
[3] Solís Betancur, R. F. (2016). Desarrollo de un Sistema para la Gestión de la Información para el Laboratorio Primario de Tiempo y Frecuencia. En Simposio de Metrología 2016 (pp. 213–214). CENAM. https://www.cenam.mx/memorias/
[4] R. F. Solís and L. M. Mojica, “Application of SIMT and UTCr timescales for the maintenance of the Universal Time coordinated in Panama,” 2014 IEEE Central America and Panama Convention (CONCAPAN XXXIV), Panama, Panama, 2014, pp. 1-1, doi: 10.1109/CONCAPAN.2014.7000474
[5] “Galileo Open Service Navigation Message Authentication (OSNMA) | European GNSS Service Centre (GSC).” https://www.gsc-europa.eu/galileo/services/galileo-open-service-navigation-message-authentication-osnma
[6] Lombardi, M. , Levine, J. , Lopez, J. , Jimenez, F. , Bernard, J. , Gertsvolf, M. , Sanchez, H. , Fallas, O. , Hernandez, L. , de, R. , Fittipaldi, M. , Solis, R. and Espejo, F. (2014), International Comparisons of

https://doi.org/10.33412/apanac.2025.13

Network Time Protocol Servers, Proceedings of the Precise Time and Time Interval Systems and Applications (PTTI) Meeting, Boston, MA, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=917539 (Accessed October 24, 2025)

Autorización y Licencia CC

https://doi.org/10.33412/apanac.2025.13