					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P23					Título del documento: **Política de sincronización horaria**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineación con normas y reglamentos, cuando corresponda

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	-
ISO/IEC 27002:2022	Control 8	-
NIST SP 800-53 Rev. 5	SC-45, AU-8	-
RGPD de la UE	Artículo 32	-
Directiva NIS2 de la UE	Artículo 21(2)(e)	-
DORA de la UE	Artículos 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Propósito

1.1 El propósito de esta política es garantizar que todos los sistemas, aplicaciones, dispositivos y servicios en la nube de la organización mantengan configuraciones horarias coherentes y precisas mediante la sincronización con fuentes horarias designadas y de confianza.

1.2 La sincronización horaria precisa es esencial para disponer de un registro de eventos fiable, comunicaciones seguras, trazabilidad de auditoría, respuesta a incidentes e investigación forense. La desalineación horaria puede dar lugar a registros no correlacionados, fallos de autenticación e informes regulatorios incompletos.

1.3 Esta política da soporte al control 8.17 del Anexo A de ISO/IEC 27001 y a otras normas internacionales relacionadas, al exigir precisión horaria y detección de la deriva del reloj en todo el entorno tecnológico de TI de la organización.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los componentes de infraestructura, incluidos servidores, estaciones de trabajo, dispositivos de red, cortafuegos y sistemas de Internet de las cosas (IoT)

2.1.2 Entornos virtuales y en la nube (p. ej., AWS, Azure, Google Cloud)

2.1.3 Todos los sistemas que intervengan en el registro de eventos, la autenticación, el procesamiento de transacciones o la correlación de eventos de seguridad

2.1.4 Empleados internos, contratistas y proveedores de servicios externos con responsabilidad sobre sistemas sensibles al tiempo

2.2 Se consideran dentro del alcance los sistemas que generen o consuman registros con marca temporal, como entradas de registro, alertas, registros de actividad de usuario o evidencias forenses.

3. Objetivos

3.1 Definir una arquitectura de sincronización horaria coherente y centralizada mediante fuentes NTP aprobadas o equivalentes.

3.2 Garantizar que todos los sistemas sincronicen sus relojes a intervalos definidos y que cualquier deriva se detecte y corrija automáticamente o con una intervención mínima.

3.3 Mantener la precisión de los relojes en entornos híbridos, en las instalaciones y en la nube para permitir:

3.3.1 Una correlación fiable de eventos y una respuesta eficaz a incidentes

3.3.2 El cumplimiento de normas y reglamentos como ISO 27001, RGPD de la UE, Directiva NIS2 de la UE y DORA de la UE

3.3.3 La protección frente a ataques de repetición y fallos de autenticación basados en el tiempo

3.4 Establecer funciones claras, procedimientos de gestión de excepciones y mecanismos de auditoría para asegurar la aplicación de la política.

3.5 Garantizar que las anomalías relacionadas con el tiempo queden registradas, generen alertas y se escalen cuando superen las tolerancias establecidas.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO)

4.1.1 Es el responsable de esta política y garantiza su alineación con los controles operativos del Sistema de Gestión de la Seguridad de la Información (SGSI) y con los requisitos regulatorios.

4.1.2 Aprueba la selección de las fuentes horarias corporativas y valida los procesos de elaboración de informes de sincronización horaria.

4.2 Responsable de Servicios de Infraestructura / Responsable de Ingeniería de Redes

4.2.1 Mantiene los servidores NTP primarios y secundarios de la organización o la configuración de la fuente horaria designada.

4.2.2 Garantiza que todos los dispositivos conectados a la red y las instancias virtuales sincronicen la hora a intervalos adecuados.

4.2.3 Supervisa los registros de sincronización horaria, las alertas de deriva del reloj y las condiciones de fallo.

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Requisitos de revisión y actualización

9.1 Esta política debe revisarse anualmente, o antes si concurre cualquiera de las siguientes condiciones:

9.1.1 Detección de exploits basados en el tiempo o fallos en el registro de eventos

9.1.2 Cambios en la infraestructura horaria principal (p. ej., nuevos servidores NTP corporativos o actualizaciones de protocolo)

9.1.3 Discrepancias de deriva horaria en plataformas en la nube o cambios en servicios regionales

9.1.4 Hallazgos posteriores a incidentes que identifiquen la desalineación horaria como factor contribuyente

9.2 La revisión será coordinada por el Responsable de Infraestructura, con la participación que corresponda del SOC, Seguridad de Aplicaciones y las partes interesadas de Cumplimiento.

9.3 Las revisiones deben documentarse en el registro documental del SGSI y comunicarse a las partes interesadas internas y externas afectadas.

9.4 Las versiones históricas de la política deben archivarse de forma segura, estar sujetas a control de versiones y ponerse a disposición ante solicitudes de auditoría de cumplimiento o requerimientos legales.

10. Políticas relacionadas y vinculaciones

10.1 P1 – Política de Seguridad de la Información. Establece el mandato general para garantizar la integridad y la trazabilidad de todos los sistemas de información, para lo cual la precisión horaria es un elemento fundamental.

10.2 P5 – Política de gestión de cambios. Regula las modificaciones de las configuraciones del sistema, incluidos los ajustes de las fuentes horarias, garantizando la documentación, las pruebas y los planes de reversión adecuados.

10.3 P22 – Política de registro de eventos y supervisión. Depende directamente de una hora sincronizada para garantizar la secuencia de eventos, la correlación de registros y la integridad de la investigación de incidentes en sistemas diversos.

10.4 P30 – Política de respuesta a incidentes. Depende de marcas temporales precisas para investigaciones forenses, cronologías de incidentes y evidencias de cadena de custodia. Una hora inexacta menoscaba la credibilidad de los informes de incidentes.

10.5 P20 – Política de protección contra software malicioso / malware. Requiere alertado con precisión horaria y análisis de comportamiento para detectar la propagación de malware, el movimiento lateral y las anomalías de acceso.

10.6 P6 – Política de gestión de riesgos. Define el tratamiento de la desincronización como un posible riesgo operativo y forense, y exige los controles definidos en esta política para mitigar su impacto.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 – Planificación y control operacional: exige la integración de controles técnicos precisos, como relojes de sistema sincronizados, para una ejecución operativa fiable.

11.2 ISO/IEC 27002:2022 – Control 8

11.2.1 Refuerza la precisión de los relojes y exige la coherencia organizativa de la hora de los sistemas para facilitar la comparación de registros, la investigación y la validación segura de transacciones.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-45 – Sincronización horaria del sistema: exige la sincronización horaria utilizando fuentes fiables en todos los componentes dentro del perímetro del sistema.

11.3.2 AU-8 – Marcas temporales: garantiza que los eventos estén correctamente marcados con hora y proporciona trazabilidad para la auditoría y la respuesta a incidentes.

11.4 RGPD de la UE (2016/679)

11.4.1 Artículo 32 – Seguridad del tratamiento: aunque no cita expresamente el tiempo, exige el uso de medidas técnicas apropiadas, incluidas pistas de auditoría y registros, cuya validez e integridad dependen intrínsecamente de marcas temporales sincronizadas.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículo 21(2)(e): exige capacidades de registro y detección que presuponen una sincronización horaria precisa para la correlación entre sistemas y una respuesta oportuna.

11.6 DORA de la UE (2022/2554)

11.6.1 Artículo 9 – Gestión del riesgo de las TIC: exige telemetría de sistemas precisa para la supervisión del riesgo y la detección de anomalías, lo que depende de una sincronización exacta de los relojes.

11.6.2 Artículo 10 – Continuidad del negocio de las TIC: impone controles que garanticen la integridad del sistema durante interrupciones, incluidos registros de eventos alineados temporalmente.

11.7 COBIT 2019

11.7.1 DSS05.04 – Supervisar eventos de seguridad: exige la integridad de las marcas temporales para un análisis eficaz de registros y la detección de amenazas.

11.7.2 MEA03 – Supervisar, evaluar y valorar el cumplimiento: la sincronización horaria respalda auditorías de cumplimiento e informes periódicos precisos.