					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P23S					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

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	cláusula 8	Requisitos de control aplicables
ISO/IEC 27002:2022	control 8	Funcionamiento sincronizado de los sistemas
NIST SP 800-53 Rev.5	SC-45, AU-8	NTP de confianza y precisión de las marcas temporales de los registros
RGPD de la UE	artículos 5(1)(d), 32	Exactitud, responsabilidad proactiva e integridad de los datos personales mediante marcas temporales sincronizadas
Directiva NIS2 de la UE	artículo 21(2)(d)	Capacidades de supervisión y detección respaldadas por registros sincronizados
DORA de la UE	artículos 10, 15	Resiliencia operativa y registros técnicos precisos
COBIT 2019	DSS05.02, MEA03	Eventos con marca temporal y supervisión basada en evidencias

1. Finalidad

1.1 Esta política establece controles obligatorios para mantener una hora precisa y sincronizada en todos los sistemas que almacenan, transmiten o tratan datos de la organización.

1.2 La sincronización horaria es esencial para garantizar la trazabilidad de los registros del sistema, la correlación precisa de los incidentes de seguridad y la fiabilidad de las evidencias durante el análisis forense o la revisión legal.

1.3 La organización establece la sincronización horaria automatizada como requisito fundamental para la integridad de las auditorías, la respuesta a incidentes y el cumplimiento normativo conforme a ISO 27001, el RGPD de la UE, DORA de la UE y la Directiva NIS2 de la UE.

1.4 Esta política garantiza que todos los sistemas utilicen fuentes horarias de confianza, impide la modificación manual de los ajustes de hora y exige la corrección oportuna de la desviación horaria.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los sistemas y dispositivos propiedad de la empresa, incluidos servidores, equipos de sobremesa, portátiles, dispositivos móviles, cortafuegos, routers y máquinas virtuales

2.1.2 Infraestructura remota y alojada en la nube utilizada en las operaciones (por ejemplo, AWS, Microsoft 365, plataformas SaaS)

2.1.3 Sistemas que generan o almacenan registros de eventos, registros de autenticación o pistas de auditoría

2.1.4 Todo empleado, contratista, proveedor o proveedor de soporte de TI responsable de configurar o mantener estos sistemas

2.2 La política también se aplica a los dispositivos BYOD utilizados para acceder a los sistemas de la organización, siempre que dichos dispositivos almacenen o generen datos relevantes para auditoría.

3. Objetivos

3.1 Garantizar que todos los sistemas críticos sincronicen automáticamente la hora mediante servidores del Protocolo de Tiempo de Red (NTP) de confianza o mecanismos equivalentes del proveedor de servicios en la nube

3.2 Evitar discrepancias horarias que puedan menoscabar la fiabilidad o la correlación de los registros del sistema durante auditorías o investigaciones de seguridad

3.3 Permitir la detección y corrección oportunas de la desviación horaria que supere los umbrales aceptables

3.4 Mantener una marcación temporal coherente en todos los entornos (local, en la nube y remoto)

3.5 Cumplir los requisitos técnicos y legales de integridad, trazabilidad y no repudio de registros y eventos

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Aprueba esta política y garantiza su cumplimiento en toda la organización

4.1.2 Supervisa las revisiones periódicas de la precisión horaria a nivel de sistema y de las deficiencias de implantación

4.1.3 Aprueba las excepciones a la sincronización horaria automatizada, cuando estén justificadas y documentadas

4.2 Proveedor de soporte de TI / función interna de TI

4.2.1 Configura la sincronización horaria para todos los sistemas propiedad de la empresa o gestionados por esta

4.2.2 Verifica diariamente, o con la periodicidad establecida, que la sincronización funciona correctamente

4.2.3 Investiga y corrige eventos de desviación horaria, fallos de sincronización o problemas de acceso a NTP

4.2.4 Documenta el estado de la sincronización horaria como parte de las comprobaciones mensuales del estado de los sistemas

[... 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 Revisión programada

9.1.1 Esta política debe revisarse anualmente por el Director General, el proveedor de soporte de TI y el Coordinador de Privacidad

9.1.2 Durante la revisión deben considerarse todos los registros y los informes del estado de cumplimiento de la sincronización horaria

9.2 Actualizaciones motivadas por eventos desencadenantes

9.2.1 Esta política debe actualizarse si:

9.2.1.1 Un fallo del sistema provoca una desviación horaria significativa

9.2.1.2 Una auditoría revela deficiencias en la sincronización horaria

9.2.1.3 La organización adopta nuevos entornos en la nube, híbridos o de virtualización

9.2.1.4 Los cambios legales o normativos introducen nuevos requisitos de integridad temporal

9.3 Control de versiones y comunicación

9.3.1 Todas las actualizaciones deben estar sujetas a control de versiones y fechadas

9.3.2 Los cambios significativos deben comunicarse a todo el personal técnico

9.3.3 Las versiones anteriores deben conservarse durante 3 años como respaldo para auditoría

10. Políticas relacionadas y vinculaciones

10.1 Esta política debe aplicarse conjuntamente con las siguientes políticas SME:

10.1.1 P22S – Política de Registro de Eventos y Supervisión: garantiza una marcación temporal coherente en los registros para la trazabilidad y la correlación forense.

10.1.2 P30S – Política de Respuesta a Incidentes: depende de la precisión de las marcas temporales para reconstruir incidentes, definir cronologías y respaldar decisiones de notificación.

10.1.3 P17S – Política de Protección de Datos y Privacidad: garantiza que los registros de acceso y las cronologías de tratamiento de datos que impliquen datos personales sean precisos y defendibles conforme al RGPD de la UE.

10.1.4 P12S – Política de Gestión de Activos: respalda la identificación de los sistemas que requieren sincronización, en particular los dispositivos móviles y remotos.

10.1.5 P26S – Política de Seguridad de Terceros y Proveedores: garantiza contractualmente que los proveedores que acceden a datos de la organización o los registran apliquen prácticas de sincronización horaria.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001:

11.1.1 cláusula 8.1 – Exige la implantación de los controles necesarios para unas operaciones seguras, incluido el registro de eventos y la marcación temporal.

11.2 ISO/IEC 27002:

11.2.1 control 8.17 – Recomienda la sincronización horaria para todos los sistemas que producen registros o funcionan de forma colaborativa.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Exige el uso de fuentes horarias internas o externas para la precisión de las marcas temporales de los registros.

11.3.2 SC-45 – Especifica el uso de fuentes NTP de confianza y la prevención de cambios manuales de la hora en sistemas críticos.

11.4 RGPD de la UE:

11.4.1 artículo 5(1)(d) – Exige exactitud y responsabilidad proactiva en el tratamiento de datos personales, respaldadas por marcas temporales sincronizadas.

11.4.2 artículo 32 – Exige medidas de seguridad que garanticen la integridad de los datos, lo que incluye intervalos temporales de registro coherentes.

11.5 Directiva NIS2 de la UE:

11.5.1 artículo 21(2)(d) – Exige capacidades de supervisión y detección, respaldadas por registros del sistema sincronizados.

11.6 DORA de la UE:

11.6.1 artículo 10 – Exige resiliencia operativa y requiere registros de incidentes de TIC trazables y con marca temporal.

11.6.2 artículo 15 – Exige a los proveedores de servicios mantener registros técnicos precisos, incluidas pistas de auditoría con marca temporal.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Hace hincapié en la integridad de las marcas temporales para detectar eventos y responder a ellos.

11.7.2 MEA03.01 – Exige supervisión del desempeño basada en evidencias, respaldada por datos precisos y sincronizados temporalmente.