Plan de contingencia del sistema de registro TRD (DLT)

1. Objeto y alcance

   El presente Plan de Contingencia define las medidas organizativas y técnicas destinadas a asegurar la continuidad del registro, la integridad de la información, la disponibilidad operativa y la adecuada gestión de incidentes que puedan afectar al sistema de registro de valores negociables representados en tecnología de registros distribuidos (TRD), para las emisiones en las que URSUS-3 Capital AV, S.A. actúe como ERIR.

   El Plan abarca, con carácter general:

   - La infraestructura y servicios necesarios para la administración del registro.
   - La operativa sobre smart contracts vinculados a las emisiones.
   - Los procesos de seguridad, cumplimiento y gobierno asociados al sistema.
   - Los mecanismos de recuperación, migración y continuidad ante fallos en la red TRD, de proveedores o de componentes internos.

2. Principios de diseño

   El Plan se basa en los siguientes principios:

   - Continuidad operativa y resiliencia: capacidad de mantener la función registral ante incidentes relevantes.
   - Integridad e inmutabilidad registral: preservación de la integridad de las emisiones y de los asientos/estados registrales conforme a las reglas de la red TRD y del sistema.
   - Seguridad de la información y gestión del riesgo: enfoque alineado con estándares de referencia en la materia (incluyendo ISO 27001 e ISO 31000), en la medida aplicable.
   - Minimización de datos on-chain y privacidad: control de la información publicada en TRD, evitando la incorporación de datos personales y preservando la confidencialidad de la vinculación identidad–dirección cuando proceda.
   - Proporcionalidad: medidas acordes con el riesgo, el tipo de emisión y el impacto potencial sobre los titulares.

3. Roles y responsabilidades

   - URSUS-3 Capital AV, S.A. (ERIR): responsable de la administración de la inscripción y registro, incluyendo la gestión de incidentes, la activación del plan de contingencia y la coordinación con los intervinientes.
   - Onyze (socio tecnológico): presta soporte tecnológico a URSUS en el ámbito de seguridad, operación y continuidad; en particular:
     - proporciona a URSUS gestión segura de las claves privadas de administrador necesarias para operar en la red TRD (según el modelo operativo definido),

- apoya la verificación y seguimiento de las redes DLT utilizadas y su adecuación a estándares de seguridad y gestión del riesgo,
- colabora en pruebas técnicas, medidas de recuperación y, cuando proceda, en escenarios de migración de red.

La intervención de terceros proveedores, si existiera, se realizará bajo procedimientos de selección, control y supervisión definidos por la ERIR.

4. Identificación de riesgos y escenarios de contingencia

Con carácter enunciativo y no limitativo, se consideran escenarios de contingencia:

- Incidente de ciberseguridad (intrusión, compromiso de credenciales, denegación de servicio, integridad de APIs).
- Vulnerabilidad o mal funcionamiento del smart contract (error lógico, exploit, configuración incorrecta).
- Interrupción o degradación relevante de la red TRD (congestión severa, interrupción de nodos críticos, eventos de red).
- Cambios de gobernanza de la red con impacto material (hard forks/actualizaciones, cambios de reglas, degradación de condiciones económicas como el gas).
- Incidencias de datos y privacidad (riesgo de reidentificación, acceso no autorizado a bases off-chain, fallos de segregación).
- Fallo de proveedor tecnológico o de componentes internos (servicios de custodia/llaves administrativas, APIs, almacenamiento, monitorización).
- Riesgos operativos (error humano, accesos inadecuados, insuficiencia de formación, indisponibilidad de personal crítico).

5. Medidas preventivas

5.1 Seguridad y ciberresiliencia

- Implantación y mantenimiento de controles de seguridad de la información alineados, cuando proceda, con buenas prácticas equivalentes a ISO 27001 y gestión del riesgo conforme a ISO 31000.
- Pruebas y validaciones para reforzar la resiliencia:
  - pruebas de estabilidad, seguridad y capacidad operativa de los smart contracts,
  - revisión de la resiliencia de la red blockchain seleccionada,
  - integración mediante APIs robustas y monitorizadas,
  - diseño orientado a evitar puntos únicos de fallo y a habilitar recuperación ante desastres.

5.2 Privacidad y protección de datos

- Principio de minimización de información on-chain: las direcciones (wallets) son identificadores alfanuméricos que no identifican por sí mismos a su titular.

5.3 Custodia y control de claves de administrador

- URSUS dispondrá de medidas de seguridad para la custodia y uso de las claves privadas de administrador necesarias para ejecutar sus funciones como ERIR. Onyze proporciona soporte para la gestión segura de dichas claves conforme al modelo operativo acordado (p. ej., políticas de acceso, separación de funciones, autenticación reforzada y controles de autorización).

5.4 Estándares de tokenización y verificabilidad

- Uso de estándares de tokenización reconocidos (p. ej., ERC-3643 o ERC-1400, cuando proceda) como base para mecanismos de validación, control de transferencias y verificación.

5.5 Formación y control de accesos

- Sesiones formativas generales y específicas para personal relevante, en función de su rol y exposición.
- Procedimientos de gestión de autorizaciones y de personal crítico (altas, cambios, revocaciones, segregación de funciones y revisión periódica).

6. Monitorización y detección

- Monitorización continua o periódica, según criticidad, de:
  - estado de la red (congestión, confirmaciones, incidencias),
  - integridad operativa de smart contracts y eventos anómalos,
  - disponibilidad y seguridad de APIs y componentes internos,
  - alertas de ciberseguridad y accesos privilegiados.
- Seguimiento de la gobernanza de la red: revisión de propuestas y cambios aprobados que puedan impactar el funcionamiento esperado y/o las funciones de URSUS como ERIR.

7. Integridad y disponibilidad de la información

- Registro en TRD (on-chain): la información registral relativa a la emisión, titularidad y operaciones sobre los valores se mantiene en la red TRD. Por la naturaleza del registro distribuido, dicha información se encuentra replicada en una pluralidad de nodos y protegida mediante mecanismos criptográficos y reglas de validación de la red, lo que proporciona una elevada resistencia a alteraciones no autorizadas y contribuye a la disponibilidad del registro al no depender de un único punto de fallo. En consecuencia, no se realizan copias de seguridad del registro on-chain, al constituir la propia red TRD el soporte del registro.
- Evidencias operativas off-chain (cuando proceda): cuando la operativa requiera componentes off-chain (por ejemplo, herramientas utilizadas por la ERIR para la firma/autorización mediante proveedores terceros), se conservará evidencia operativa adicional. En particular, se mantendrá un registro (logs) de las firmas realizadas por la ERIR a través de dichas herramientas, con fines de trazabilidad, soporte a la gestión de incidencias y auditoría operativa. Estos logs se custodiarán con medidas adecuadas de seguridad y control de acceso conforme a los procedimientos internos aplicables, sin perjuicio de que el registro con efectos registrales sea el reflejado en la red TRD.

8. Gestión de incidentes y activación del plan

- Clasificación e inicio: ante un incidente, URSUS activará el procedimiento de gestión y:
  - clasificará el incidente por severidad e impacto (integridad registral, disponibilidad, privacidad, operación),
  - adoptará medidas de contención,
  - documentará las actuaciones y evidencias.
- Medidas de contención y mitigación (ejemplos)
  - Restricción temporal de operaciones sensibles (p. ej., pausas operativas, controles reforzados) cuando el diseño lo permita y sea necesario.
  - Revocación/rotación de credenciales y claves administrativas (según el modelo de custodia).
  - Desactivación controlada de integraciones afectadas y activación de rutas alternativas.
  - Procedimientos de revisión, parcheo y, cuando proceda, despliegue de versiones corregidas (respetando el gobierno de cambios definido).

9. Continuidad del registro y recuperación ante desastres

- Objetivo y enfoque general: mantener la continuidad de la función registral y la disponibilidad de la información a titulares y público, incluso en caso de incidente o fallo relevante que afecte a componentes internos, integraciones o proveedores. Dado que el registro con efectos registrales se mantiene en la red TRD y se beneficia de su naturaleza distribuida, las medidas de continuidad se orientan principalmente a asegurar (i) la capacidad operativa de interacción con la red (acceso, monitorización y ejecución de funciones, y (ii) la continuidad de los servicios auxiliares necesarios para la administración del registro y la atención a titulares.
- Medidas de continuidad y recuperación (cuando proceda):
  - Restablecimiento del acceso operativo a la red TRD (reconexión de nodos/servicios, recuperación de integraciones y validación de disponibilidad).
  - Conmutación a infraestructura alternativa o redundante para los componentes off-chain de soporte (p. ej., APIs, monitorización, herramientas de firma/autorización, sistemas de consulta y reporting), conforme a procedimientos internos.
  - Recuperación de evidencias operativas (p. ej., logs de firmas y trazas de operación) cuando existan componentes off-chain, para facilitar trazabilidad y soporte a la gestión del incidente.
  - Coordinación con proveedores tecnológicos implicados para la resolución del incidente y la restauración de niveles de servicio, incluyendo la activación de los mecanismos de escalado y respuesta acordados.

10. Red alternativa y criterios de migración

    Como parte del plan de contingencia, se prevé la posibilidad de disponer de una red TRD alternativa para casos en los que resulte relevante migrar (p. ej., por interrupciones del servicio, cambios de gobernanza con impacto material o incrementos significativos y sostenidos de costes operativos como gas).

    La evaluación de red alternativa considerará, entre otros factores:

    - historial de resiliencia,
    - roadmap tecnológico y escalabilidad,
    - grado de descentralización,
    - adopción por proyectos institucionales,
    - adecuación a requisitos técnicos y de cumplimiento definidos por URSUS como ERIR.

    Cualquier migración, de realizarse, se ejecutará conforme a un procedimiento controlado que preserve la integridad del registro y la continuidad de la información, y se reflejará en la documentación pública aplicable.

11. Comunicación y transparencia

    URSUS mantendrá en su web, en lugar visible y accesible:

    - descripción del funcionamiento del sistema de registro,
    - descripción del plan de contingencia y continuidad ante incidencias,
    - procedimientos para certificación de derechos, cargas y gravámenes,
    - procedimiento para el ejercicio de derechos económicos.

    Asimismo, se establecerán mecanismos de comunicación con los titulares cuando un incidente pueda afectar materialmente al registro, a sus derechos o al acceso a información, de acuerdo con los procedimientos internos y el marco aplicable.

12. Pruebas, revisión y mejora continua

    - URSUS declara haber realizado pruebas de las aplicaciones informáticas utilizadas y mantendrá un programa de pruebas periódicas del plan (incluyendo simulacros y pruebas de respuesta).
    - El Plan se revisará y actualizará cuando proceda, especialmente ante:
        - cambios relevantes en la red TRD o su gobernanza,
        - nuevas amenazas o incidentes significativos,
        - cambios en proveedores, integraciones o arquitectura,
        - lecciones aprendidas de pruebas o incidencias.