PLIEGO DE PRESCRIPCIONES TÉCNICAS DE CONTRATACIÓN DE UN SERVICIO PARA LA ELABORACION DEL PLAN DE CONTINUIDAD Y CONTINGENCIA TIC DE ENRESA Nº EXPTE: 000-CO-SI-2019-0005	Clave: 000-ES-SI-0107 Páginas: 3

Contenido

1 Alcance

El alcance del servicio es elaborar el **Plan de Continuidad y Contingencia TIC de Enresa** que describa las actuaciones a desarrollar y las medidas a implantar para garantizar la continuidad de las actividades de la empresa ante los supuestos definidos de crisis o desastre.

Este plan debe incluir el análisis de la contingencia y recuperación de desastres de los procesos y servicios críticos identificados, bajo los requisitos de seguridad de la información y la infraestructura tecnológica y procedimental de Enresa, definiendo estrategias de: Prevención (análisis de redundancia para las infraestructuras y sistemas); Detección (monitorización continua); Mitigación (de las actividades recogidas en el Plan) y de Recuperación (según el plan de recuperación de desastres).

Debe considerar todos los componentes de los sistemas de Enresa, tales como datos/información críticos, “backups”, equipamiento lógico físico, sistemas de gestión y aplicaciones, comunicaciones, documentación y personal. Incluirá, asimismo, cualquier otro recurso externo que pudiera ser crítico ante cualquier situación de crisis, y pueda afectar al plan de continuidad y seguridad definidos.

El Plan deberá ser desarrollado bajo los estándares de continuidad de negocio en sistemas de gestión ISO/IEC 22301 y de seguridad de la información ISO/IEC 27001, o equivalentes. Formarán parte del alcance del servicio los aspectos que, de manera resumida, se enuncian a continuación:

Análisis y establecimiento de procesos críticos de negocio

- Definición del marco del Plan: Responsables/organización, implementación, pruebas, alcance, criticidades, importancia de procesos.
- Recopilación de la información (operativa y estratégica) de documentación facilitada por Enresa y planificación de trabajos y entrevistas, de cara a determinar los procesos y servicios críticos de negocio, sus activos y recursos soporte, y necesidades. Se realizarán y documentarán entrevistas al Comité de Dirección y a los responsables de los procesos corporativos de Enresa.
- Elaboración del análisis de impacto de las actividades de Negocio (BIA), estimando los parámetros relevantes temporales y de recursos, y de impacto en el negocio, como: tiempos tolerables de recuperación (RTO) y periodos máximos de pérdida de información (RPO) asumibles en los procesos críticos identificados
- Partiendo del Análisis de Riesgos de Enresa y de las entrevistas anteriores, elaboración del análisis de riesgos, considerando las amenazas, sucesos iniciadores, probabilidades de ocurrencia e impacto en los procesos críticos. De aquí saldrán las medidas de tratamiento de los riesgos seleccionados.

Determinación de la estrategia de continuidad

- Identificados los procesos críticos y riesgos, elaboración de los escenarios “envolventes” de las situaciones de crisis que pueden dar lugar a una contingencia, por niveles, en función de los impactos potenciales. Estos escenarios deberán incluir los elementos potencialmente afectables, como: personal, ubicaciones, tecnología, información/datos, tiempos de respuesta de proveedores, etc.
- Identificación de la organización responsable de la toma de decisiones y de los equipos de actuación ante situaciones de crisis, con sus funciones y sus responsabilidades.
- Definición de la estrategia de continuidad corporativa.

Respuesta a la contingencia. Plan de contingencia TIC

- Definición del marco organizativo y procedimental, incluyendo las responsabilidades asignadas en cada etapa definida para la contingencia.
- Con la relación de procesos y servicio críticos de la compañía identificados, revisión de la infraestructura, aplicaciones, y servicios TIC sobre los cuales está soportado cada uno de ellos. Deberán determinarse sus vulnerabilidades.
- Para cada uno de los escenarios de continuidad identificados, definición de las estrategias y orden previsto de recuperación de desastres y los procedimientos de activación, incluyendo los de los centros de respaldo, para el cumplimiento de los RTO y RPO definidos.
  En la respuesta a la contingencia deberá concretarse la recuperación de servicios, entornos y datos/información en cada escenario. Deberán, asimismo, definirse las acciones a realizar, recursos a utilizar y personal a emplear en caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos, así como las tipologías de comunicaciones en estas situaciones de crisis y las medidas de mitigación TIC.
- Preparación del procedimiento de vuelta a la situación normal, una vez superada la contingencia, incluyendo la metodología de lecciones aprendidas.
- El plan de contingencia TIC debe incluir un análisis final y recomendaciones que sirvan de base para la adquisición de nueva infraestructura TIC y recursos necesarios alternativos a los ya existentes para cubrir las necesidades de continuidad definidas en el plan de continuidad.
- Asimismo, deberán considerarse las capacidades necesarias de análisis “forense” que permitan a Enresa, ante una contingencia, analizar su origen y el daño producido, de cara a la futura prevención de situaciones equivalentes y como ayuda para recuperar en el menor tiempo posible el proceso/servicio perdido.
  Deberá incluir un análisis de coste/rendimiento, presupuesto estimado y una propuesta de ubicación del respaldo.

Mantenimiento, Pruebas y Concienciación

- Establecimiento de la metodología de lecciones aprendidas.
- Definición del mantenimiento y revisiones periódicas necesarias, tanto para continuidad como para contingencia
- Diseño de una planificación de pruebas y simulacros periódicos para mantener su efectividad y mejora continua.
- Definición de las necesidades de formación y concienciación para todas las personas involucradas en el mismo.

El alcance está circunscrito, exclusivamente, a la elaboración de los análisis y planes mencionados, dejando fuera de alcance la implantación de las acciones resultantes.

2 Prestación del servicio

El servicio se prestará en dos fases:

- Fase previa: en un plazo de 10 días hábiles a contar desde el siguiente al de formalización del contrato, el contratista deberá presentar una memoria descriptiva que recoja una propuesta de organización de los trabajos, planificación de tareas, metodología de desarrollo del Plan (dentro de los estándares de referencia) y tareas críticas del servicio, en donde se haga especial referencia

a la metodología de elaboración del análisis de impacto de las actividades de negocio y el tratamiento de riesgos. Este documento será validado por el responsable del contrato como paso previo a la fase siguiente.

- Fase de ejecución y entrega del documento final: abarcará la ejecución propia de las tareas recogidas en la planificación de la fase previa y finalizará con la entrega y aceptación por parte del responsable de Enresa del documento final del Plan de continuidad y contingencia TIC.

3 Entregable

Se deberá elaborar y entregar un único informe en formato digital, con las planificaciones en “MS Project”, que constituirá el “Plan de Continuidad y Contingencia TIC de Enresa”, en donde se recoja el análisis y resultados de las actividades definidas en el alcance, integrando el siguiente contenido mínimo:

- Objetivos y alcance
- Recopilación de la información (operativa y estratégica) a través de reuniones y otra documentación
- Análisis de riesgo y análisis de impacto en el negocio (BIA)
- Definición de la estrategia de continuidad corporativa: Organización, escenarios, criticidad, RTO, RPO
- Respuesta a la contingencia: Plan de contingencia TIC: Marco, vulnerabilidades, recuperación de desastres, procedimientos de activación, vuelta a la situación normal
- Análisis final y recomendaciones de adquisición de la infraestructura TIC y recursos para soportar la continuidad y contingencia. Capacidad forense. Análisis de coste/rendimiento, presupuesto estimado y una propuesta de ubicación del respaldo.
- Mantenimiento, pruebas y revisión: Plan de Pruebas y Plan de Mantenimiento
- Formación y concienciación

Este informe contendrá un apartado último, en forma de ANEXO, que incluya un informe ejecutivo resumen con los aspectos clave del mismo.