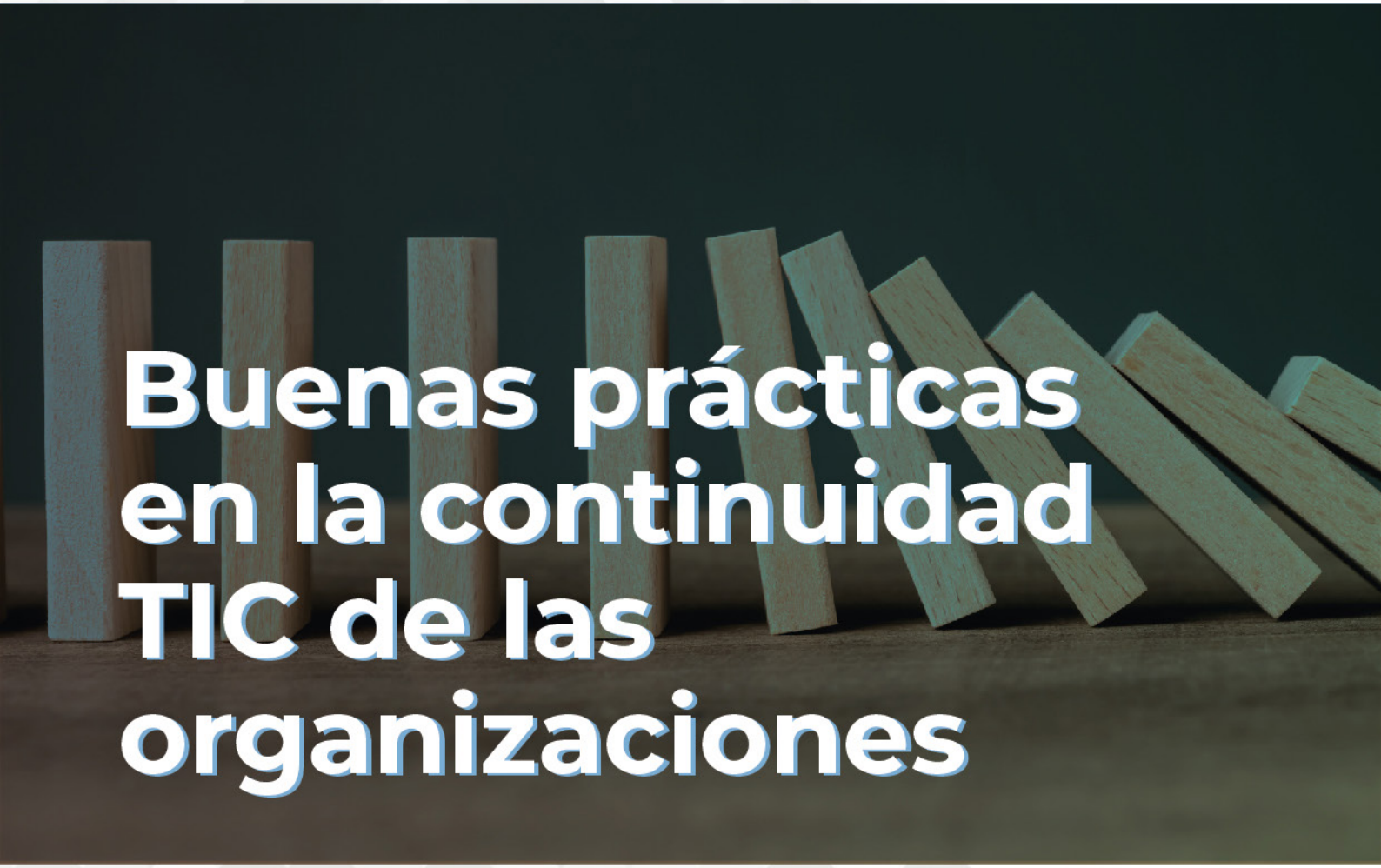
PARC CIENTÍFIC
VNIVERSITAT DE VALÈNCIA



Buenas prácticas en la continuidad TIC de las organizaciones

ISO 22301 | INCIBE | NIST

De la implementación a la certificación

EDITA:
Fundació Parc Científic Universitat de València
c/ Catedrático Agustín Escardino, 9
46980 Paterna (España)
Telf: +34 963 543 841
Kristin Suleng Furió
comunicación.pcuv@uv.es

COORDINADORES:
Jorge Edo Juan
Mariano Serra Bondia

AÑO: 2022

ISBN:
978-84-09-46404-3

DOI:
10.7203/PCUV-11

CON EL APOYO DE:

GENERALITAT VALENCIANA
Conselleria d'Innovació, Universitats, Ciència i Societat Digital

ÍNDICE

1

INTRODUCCIÓN A LA CONTINUIDAD DE NEGOCIO

INTRODUCCIÓN A LA CONTINUIDAD DE NEGOCIO

Francisco Javier
Clemente Ferrández

INTRODUCCIÓN

Un sistema de gestión de la continuidad del negocio (en adelante **SGCN**) se ha convertido en uno de los objetivos prioritarios para las organizaciones, principalmente por la globalización y exigencia de sus clientes o usuarios.

Las empresas quieren mantener una ventaja competitiva y no puede permitirse tener interrupciones en su negocio. En los mercados internacionales deben demostrar su confianza como proveedores a sus clientes, y para ello es fundamental disponer de garantías para responder a cualquier situación que pueda poner en riesgo la interrupción y/o continuidad de su actividad.

Para demostrar estas capacidades, las empresas deben de disponer de un **SGCN** diseñado e implantado correctamente que garantice que en un tiempo estimado puedan reanudar sus operaciones y servicios, ante posibles riesgos que deriven en interrupciones de la actividad.

Por tanto, un **SGCN**, a grandes rasgos, consiste en una preparación proactiva de la organización frente a contingencias de cualquier índole, que puedan generar perjuicios de diferente gravedad, según la importancia del ámbito donde se ha producido el paro y el tiempo de inactividad.

El **SGCN** es la capacidad estratégica y táctica de una organización para planificar y responder ante incidentes o interrupciones del negocio, con el objetivo de recuperar la operación a un nivel aceptable.

Si no se dispone de estas capacidades, una interrupción del negocio grave podría provocar la propia desaparición de la empresa por los daños irreparables que pueda causar.

¿POR QUÉ IMPLEMENTAR UN SGCN?

La implementación de un SGCN permite a las organizaciones tener la capacidad de reanudar la provisión de sus productos o servicios clave a un nivel mínimo aceptable en un tiempo determinado. De ahí la importancia de poner en marcha un SGCN para:

1. Comprender las necesidades de la organización y la necesidad de establecer la política y objetivos de la gestión de la continuidad del negocio.
2. Determinar la operación y el mantenimiento de los procesos, las capacidades y las estructuras de respuesta para asegurar que la organización sobrevivirá a los incidentes disruptivos.
3. Realizar el seguimiento y la revisión del desempeño y la eficacia del SGCN.
4. La mejora continuada basada en mediciones cualitativas y cuantitativas.

COMPONENTES DEL SGCN

El SGCN tiene varios componentes y son los siguientes:

- Política.
- Personas competentes con responsabilidades definidas.
- Procesos de gestión relacionados con esta política. La planificación, la implementación, la operación, la evaluación del desempeño, la revisión por la dirección y la mejora continuada.
- Información documentada de soporte para el control de operaciones y que permita la evaluación de su desempeño.

El propósito de un SGCN es preparar a la organización para proveer y mantener controles y las capacidades para gestionar la habilidad global de una organización para continuar operando durante los incidentes disruptivos.

Al lograr estos objetivos la organización dispondrá de beneficios importantes.

BENEFICIOS

PERSPECTIVA DEL NEGOCIO:

- ✓ Garantizar **el cumplimiento de objetivos estratégicos del negocio**, en caso de contingencia.
- ✓ Crear **ventaja competitiva,** demostrando una **seguridad y confianza** frente a la competencia.
- ✓ Proteger y **fortalecer la reputación** de la organización.
- ✓ Mejorar la **resiliencia** de la organización.

PERSPECTIVA FINANCIERA:

- **Reducir el riesgo legal** porque se va a poder continuar con la provisión de servicios y, por tanto, cumplir con los contratos o las relaciones comerciales.
- **Reducir los costos directos e indirecto**s de los incidentes disruptivos, porque se dispondrá de una planificación.

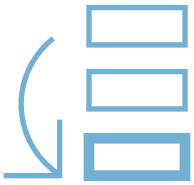
PERSPECTIVA DE LAS PARTES INTERESADAS:

- **Proteger** la vida, la propiedad y el medio ambiente.
- Considerar las expectativas de las partes interesadas para implementar este sistema de gestión.
- **Proporcionar confianza** en la capacidad de la organización.

PERSPECTIVA DE LOS PROCESOS INTERNOS:

- Mejorar la capacidad de **mantenerse eficaces.**
- Demostrar proactividad, identificando amenazas y vulnerabilidades sobre las operaciones del negocio, evaluar su impacto y poder **responder de una forma proactiva** ante incidentes.
- **Integrar la gestión del riesgo en la organización** de forma estandarizada y, por tanto, reducir **al mínimo el riesgo** de que una contingencia puede impactar en el negocio.

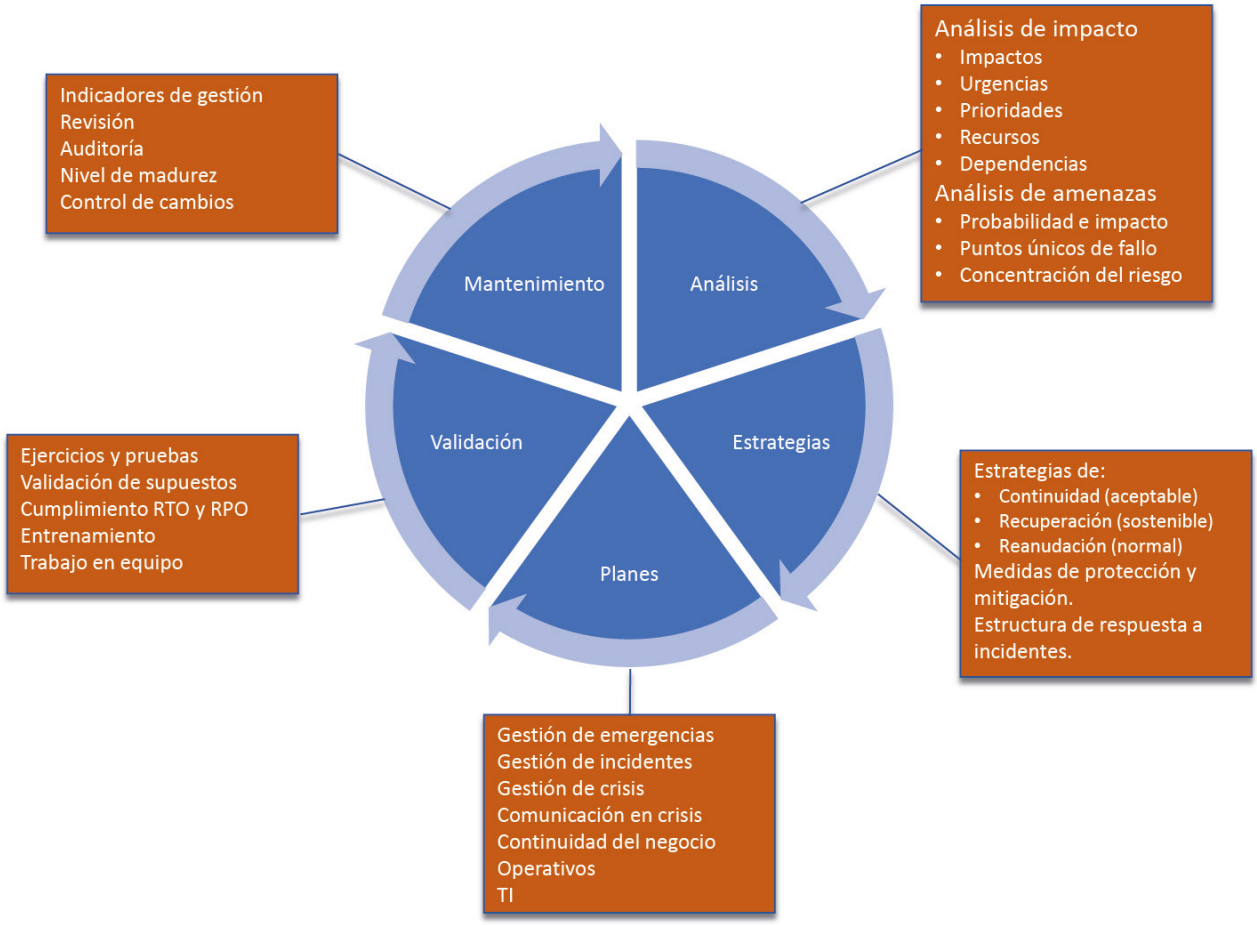
FASES DE LA IMPLEMENTACIÓN DE UN SGCN



Un plan de contingencia es más que la recuperación de la tecnología, es la recuperación de la operativa del negocio. Por tanto, la validez de un plan de contingencia solo se asegura realizando un plan de pruebas exhaustivo y deberá ser actualizado periódicamente para reflejar y responder a los cambios que se vayan produciendo en la compañía.

Se debe implementar un SGCN siguiendo la metodología basada en las normativas actuales de seguridad para el desarrollo de planes de contingencia y de recuperación ante desastres. Previamente hay que definir cuáles son los requisitos del tiempo de la recuperación, de la tolerancia de la pérdida, y la visión de la organización sobre qué operaciones y servicios deben ser recuperados. Conocer en un nivel alto, cuáles son los panoramas posibles de la pérdida para los que el plan se está construyendo y qué limitaciones o ausencias son inherentes en el diseño.

A continuación, se indican las fases de implementación recomendadas:



ANÁLISIS

Es una de las partes más importantes del proceso y, básicamente se trata de relacionar los procesos de negocio identificados con los impactos que se prevé que podría provocar una eventual interrupción de cada uno de ellos. Es lo que se conoce como las actividades BIA *(Business Impact Analysis).*

Resulta pertinente presentar una clasificación de los impactos según su gravedad:

Impactos críticos. Son aquellas interrupciones que pueden provocar un costo no asumible por la organización.

Impactos vitales. Se trata de impactos graves que afectan a procesos importantes, aunque no llegan al nivel de imprescindibilidad de los críticos por existir alternativas paralelas para mantener un cierto nivel de actividad.

Impactos sensibles. Afectaciones sobre procesos que pueden ser desviados o integrados en otros procesos sin que sea necesario restablecerlos a corto plazo.

Impactos no críticos. Eventos que afectan a actividades de importancia menor, por lo que no suponen un costo elevado para la empresa en el caso de que se interrumpan.

En esta fase se definen los escenarios del riesgo que ponga en ejecución las situaciones probables del resultado que requerirían un plan de recuperación. De forma resumida se indican las actividades de análisis que se deben realizar:

Identificación de procesos. Establecer los procesos de negocio que se realizan en la compañía. Para llevar a cabo este proceso suele ser necesario mantener entrevistas en profundidad con profesionales expertos en cada actividad o sector. Podemos dividir los procesos en operativos y procesos de soporte. Los procesos operativos son aquellos que guardan una relación directa con el cliente (comercial, facturación, almacenaje, atención al cliente, etc.). Los procesos de soporte serían aquellos que facilitan los «recursos» para poder llevar a buen puerto los procesos operativos (recursos humanos, gestión financiera, etc.).

Relación de recursos tecnológicos. En este apartado debe recogerse el inventario de los recursos tecnológicos que mantienen los procesos de la organización, a fin de identificar aquellos que den soporte directo a los servicios críticos.

Relación de departamentos y usuarios. Los procesos de la organización están gestionados por departamentos/usuarios. Dentro del inventario de procesos es necesario conocer el personal involucrado en estos.

Determinar los procesos críticos. Esta tarea supone evaluar los impactos económicos y operacionales sobre el negocio en caso de no disponer de la función analizada. La valoración de pérdidas no es una cuestión sencilla, ya que pueden concurrir aspectos intangibles, tales como la imagen de la organización ante sus clientes. Algunos criterios que pueden ayudar a valorar las eventuales pérdidas pueden ser:

- Coste de horas de trabajo perdidas, al no poder usar las aplicaciones que no tengan alternativa manual o cuyo tratamiento manual suponga una pérdida de eficiencia importante.
- Ingresos dejados de percibir.
- Penalizaciones por incumplimiento de contratos con clientes.
- Sanciones administrativas por incumplimiento de leyes debido a la falta de control en situación de desastre.
- Gastos financieros.

Periodo máximo de interrupción. Establecer para cada uno de los procesos críticos definidos, el tiempo a partir del cual las pérdidas económicas afectarían de forma grave a la compañía.

«Es muy importante realizar una estimación real de cara a seleccionar la estrategia de respaldo adecuada a las necesidades de recuperación.»

Se deben de fijar dos parámetros:

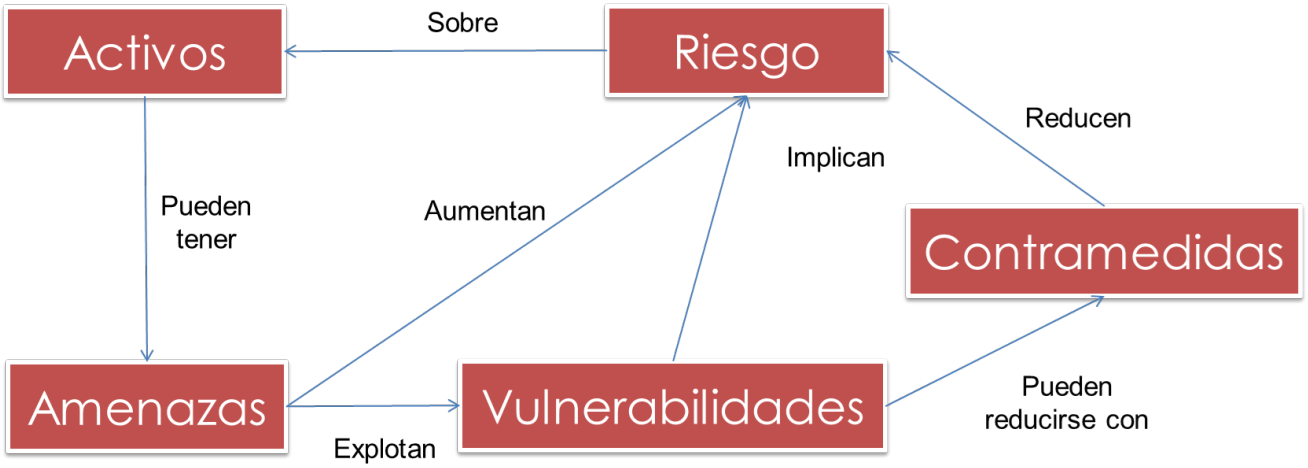
Objetivo de tiempo de recuperación (RTO). Es el período seguido tras un incidente dentro del cual la actividad o recursos deben ser reasumida.

Objetivo punto de recuperación (RPO). Es el punto en que los recursos (humanos, tecnológicos, logísticos...,) han quedado restaurados y, por tanto, se permite la actividad normal.

Una vez recopilada la información se realiza el análisis de riesgos cuyo objetivo es identificar y analizar los diferentes factores de riesgo que potencialmente podrán afectar a las actividades que queremos proteger.

La evaluación de riesgos supone imaginar lo que puede ir mal y a continuación estimar el impacto que supondría para la organización. Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial mediante el desarrollo de un plan de acción adecuado.

Para llevar a cabo el análisis de riesgos seguimos el siguiente flujo con el fin de elaborar la evaluación del riesgo.



En el siguiente capítulo se detalla más información sobre cómo llevar desarrollar un proceso de gestión de los riesgos.

DESARROLLO DE ESTRATEGIAS

Una vez elaborado el mapa de riesgos se inicia la fase del desarrollo del plan de contingencia o recuperación a partir de las estrategias de respaldo que mejor se adecuen a los requerimientos del negocio de cada organización.

Hay tres niveles de estrategias de recuperación:

1. **Continuidad inmediata** a cada proceso para llegar a un nivel aceptable.
2. **Recuperación** para dejar el proceso en un nivel sostenible.
3. **Reanudación** para la vuelta a la nueva normalidad.

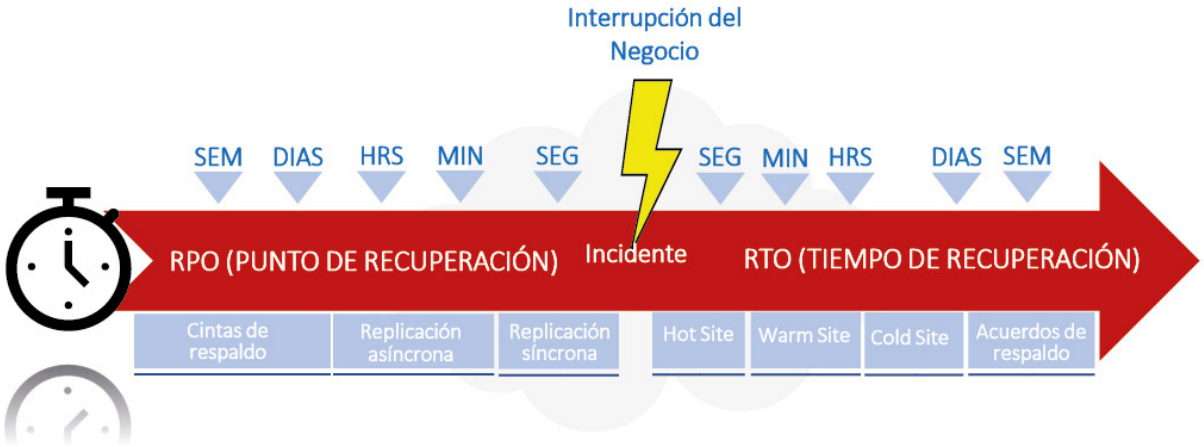
Cada sistema de recursos o de procesos tiene varias estrategias posibles de la recuperación que necesitan ser definidas con cierto nivel de detalle para comparar estas estrategias y conocer sus ventajas, costes y requisitos sobre el tiempo.

El análisis debe cubrir el nivel de dificultad, tiempo necesario para la comunicación previa al plan, así como su preparación, disponibilidad o la fiabilidad de las soluciones propuestas. El análisis de costes y beneficios también se debe tener en cuenta en este paso. El desarrollo de la estrategia necesitará contemplar las diferentes opiniones de la recuperación de los sistemas de información en un plan de recuperación cohesivo y realizable para la organización en su totalidad. Las tolerancias por tiempos muertos necesitarán ser emparejadas con las estrategias integradas de la recuperación. Si el proceso tiene varias opciones para los marcos de tiempo de la recuperación (por ejemplo 24 horas, 48 horas, una semana...), se deben especificar los costes asociados. A veces el plan más lento y el menos costoso puede ser la mejor opción. Las estrategias para un recurso dado a través de diversas unidades de negocio también pueden repasarse ahora de cara a las soluciones y la sinergia comunes.

A continuación, se muestra una tabla que recoge la relación entre el tiempo objetivo de recuperación y la solución de continuidad más adecuada a este objetivo:

TIEMPO OBJETIVO DE RECUPERACIÓN	INTERNAS	CONTRATADO
MESES	Reconstrucción / Realojamiento	----
SEMANAS	Edificios prefabricados On-Site	Contratación de unidades móviles o prefabricados
DIAS	Recuperación "in situ" Trabajo en casa	Subcontratación de procesos en oficinas móviles
HORAS	Localizaciones diversas con empleados formados	Re-localización de un grupo de personas
INMEDIATO	Localizaciones diversas para la misma función	Cambio de funcionamiento a un centro de respaldo subcontratado

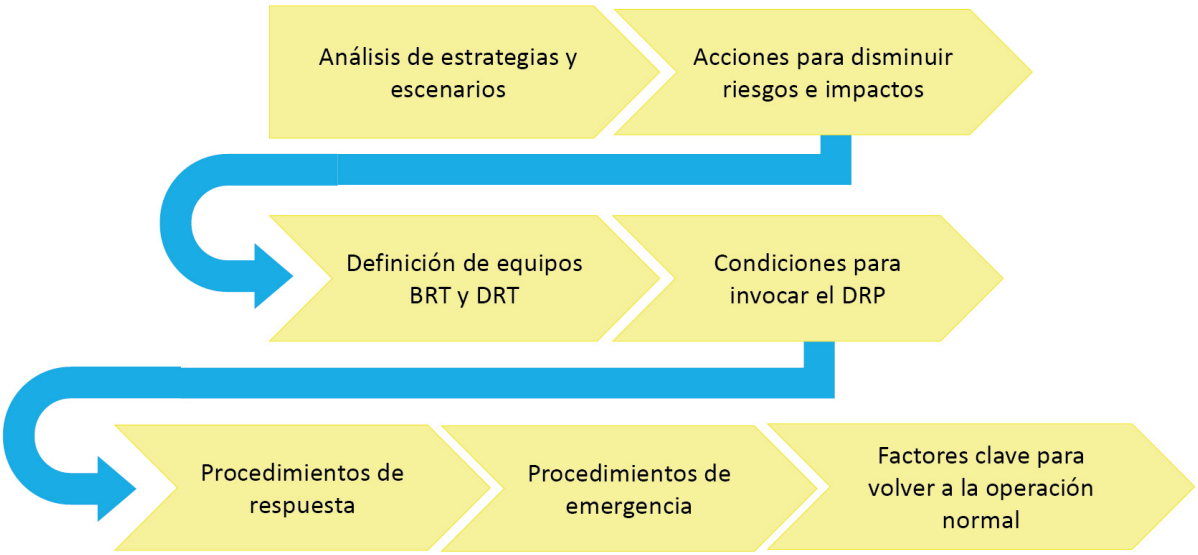
Desde el punto de vista de las TIC, cuando más bajos sean los parámetros de RTO y RPO las estrategias de contingencia deberían estar alineadas con escenarios de recuperación más exigentes, tal y como se indica en la siguiente ilustración:



IMPLANTACIÓN PLANES

A partir de la visión que se tenga de la gravedad del riesgo, y de la estrategia, los planes se pueden desarrollar para presentar las decisiones y los procesos necesarios en un plan de recuperación comprobable y viable. La documentación de los planes (emergencia, gestión de incidentes, gestión de crisis, planes de continuidad operativos, planes continuidad TIC...,) será importante y los compromisos que se adquieran a lo largo plan deberán conciliarse con las decisiones de la visión y del riesgo.

A continuación, se indica el flujo de actividades que se debe desarrollar en la elaboración del plan de contingencia.

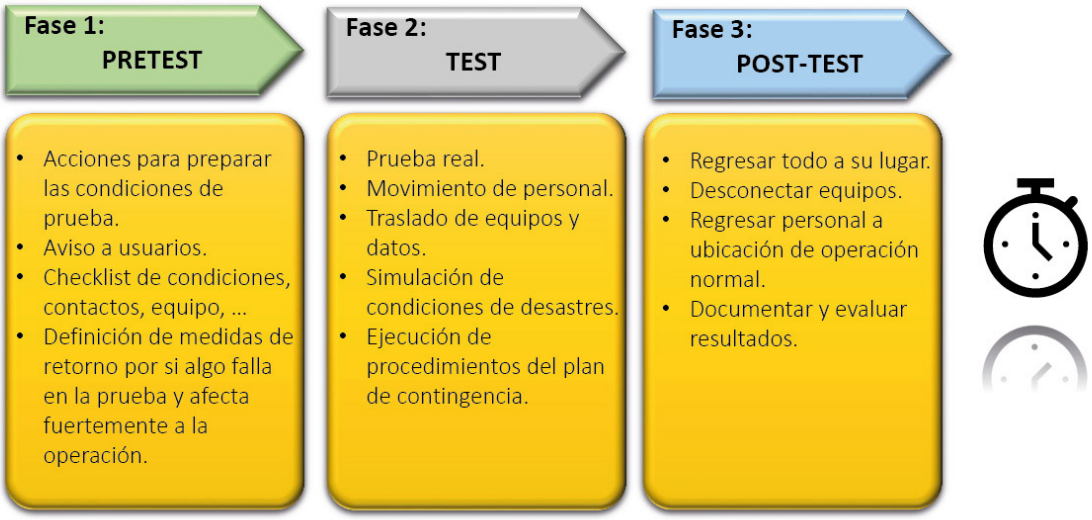


La documentación del plan de la contingencia deberá resolver los siguientes puntos:

- Presentar la visión, requisitos y las obligaciones que se deben asumir.
- Definir los equipos que desarrollarán los componentes del proceso.
- Describir los planes de acción con todos los niveles de detalle.
- Proporcionar un inventario de todos los activos y las localizaciones de las copias de seguridad.
- Proporcionar un inventario de todas las aplicaciones críticas operativas.
- Documentar todas las configuraciones del software de los sistemas.
- Proporcionar un inventario de todas las computadoras, sistemas y otros recursos relacionados.
- Documentar los requerimientos de las telecomunicaciones.
- Documentar un plan de mantenimiento y un test de los procedimientos.
- Proporcionar información de las últimas pruebas y de sus resultados.

VALIDACIÓN DEL PLAN

El plan necesitará ser probado en todos los niveles. Será una prueba integrada que mide la capacidad de la organización de recuperar todas las piezas en los marcos del orden y del tiempo necesario para una recuperación acertada. La unidad de negocio y los procesos de prueba parciales serán un comienzo natural. Las expectativas, la identificación del problema, y las revisiones del plan se deben documentar y comentar formalmente en gerencia. Así, de esta manera cada una de las partes conocerán el estado actual, la capacidad de la recuperación, la toma de decisión estratégica apropiada y la ayuda continuada. Las fases recomendadas para validar el plan son las siguientes:



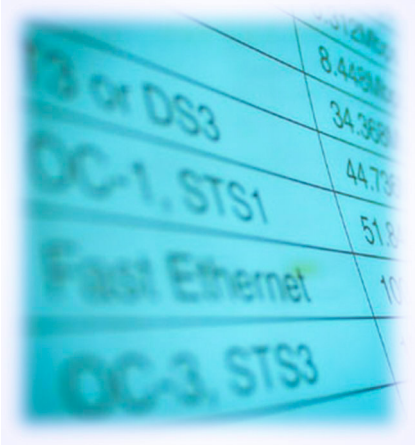
La multitud de pequeños detalles que se deben tener en cuenta (unos aparentemente evidentes, como por ejemplo, el lugar donde se guardan las llaves del acceso al armario donde están las copias de seguridad, los cambios de contraseñas en la máquina de producción real al finalizar las pruebas, etc.) y otros no tan sencillos, como por ejemplo, la designación de las personas autorizadas para dar la orden de activación del plan o las pruebas del este), nos lleva a la conclusión que es imprescindible la realización de pruebas, a pesar del coste que implican.

En la ejecución de las pruebas se validará la solución, y para ello se desarrollarán las siguientes tareas:

- Revisar y optimizar el comportamiento del *hardware/software.*
- Comprobar que toda la solución funciona correctamente y la posibilidad de incorporar algún último ajuste para optimizar en lo posible la solución.
- Llevar a cabo ajustes en el mecanismo de recuperación para asegurar que se cumplen los acuerdos de nivel de servicios acordados.
- Revisar el cálculo de tiempo de recuperación (RTO).
- Medir la consistencia de la información (RPO).
- Verificar las comunicaciones y la operativa del personal usuario.
- Revisar la vuelta a la situación de partida.
- Ejecutar las pruebas y documentarlas para valorar el impacto real de un posible problema.
- Medir la capacitación del equipo de contingencia.

En lo que respecta a la frecuencia de las pruebas, es frecuente contestar con la frase «una al año es poco, pero dos son mucho»; en cualquier caso, es recomendable hacerlas cuando hay cambios en la configuración de la arquitectura o de las aplicaciones.

Si tenemos en cuenta nuestra larga experiencia en este campo, una de las aportaciones más valoradas de la ejecución anual de las pruebas es su incorporación natural a la cultura del personal de la organización, pues se consigue que tanto los responsables de las áreas usuarias como los desarrolladores tengan en cuenta en los diseños la situación de contingencia grave y, por qué no decirlo, la realización de esas mismas pruebas.



Como es bien sabido según los profesionales de este oficio, lo que se cambia rara vez funciona a la primera, de ahí que sea un criterio habitual requerir que no existan, o sean mínimos, los cambios en los procedimientos del día a día de la explotación, sobre todo en el caso de los centros alternativos.

Finalmente, hay que tener en cuenta que ninguna prueba puede ser un reflejo al cien por cien de la situación real pues es inviable efectuar una prueba TOTAL, dado el gran impacto que causaría en la organización. Por ello, para no afectar negativamente el servicio real se eligen los procesos sobre los que realizar las pruebas de contingencia.
Cabría decir, por tanto, que las pruebas tienen un carácter asintótico, por lo que se convierten en una condición necesaria pero no suficiente.

MANTENIMIENTO DEL PLAN

El plan de contingencias requiere una revisión constante para adaptarlo a la evolución de la organización y para garantizar una óptima ejecución cuando sea necesario.

El mantenimiento del plan será accionado por la prueba y la evaluación del plan, así como por los procedimientos de cambio dentro de la organización. Estos harán necesarios cambios correspondientes al programa de recuperación del sistema que experimenta el cambio. Se sugiere un ciclo de seis meses de revisión para repasar el plan.

Se deben determinar los objetivos y las herramientas de monitorización, medición, análisis y evaluación, así como los períodos de desempeño y ejecución.

Dicha monitorización debe estar basada en métricas que sirvan para evaluar, entre otros, los siguientes factores:

- Desempeño de los procesos.
- Conformidad de los estándares internacionales.
- Registro de los datos obtenidos.

Puntos que se deben tener en cuenta en el gobierno y control del SGCN.

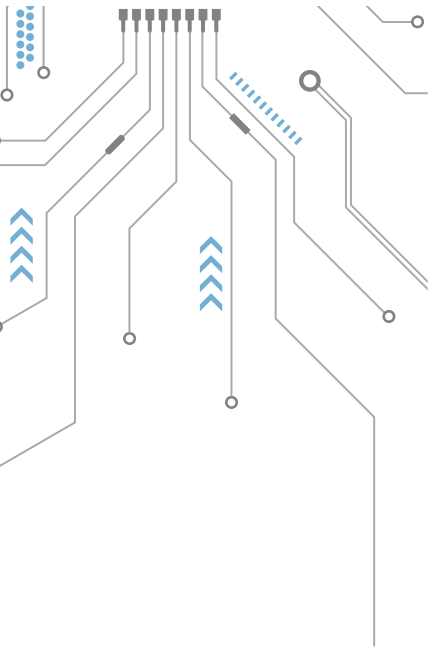
- Determinar un calendario de pruebas mensual, trimestral, semestral, etc.
- Actualizar el plan de contingencia cuando haya cambios sustantivos en el activo implicado: sistemas, funciones o procesos.
- Actualizar la infraestructura de respaldo cuando se pone al día la infraestructura de producción.
- Cambiar las estrategias cuando las criticidades de los sistemas cambien.
- Evaluar los resultados de las pruebas, compararlas y ajustarlas si es necesario.
- Entrenar al nuevo personal cuando haya cambios organizativos.
- Y otros.

La evaluación se debe llevar a cabo mediante **auditorías internas y auditorías externas.**

Las auditorías internas deben estar supervisadas por la dirección o la gerencia de la organización, y su principal objetivo es determinar la conformidad del **SGCN** con los requerimientos de la organización y los estándares internacionales, en especial la norma **ISO 22301**.

A través de estas auditorías y revisiones periódicas, la organización puede lograr los siguientes beneficios:

- Comprobar si la estrategia definida es realmente eficaz para garantizar la continuidad del negocio.
- Implantar las correcciones precisas y necesarias para mejorar el alcance y la efectividad del **SGCN**.
- Comprobar y actualizar los diversos aspectos del **SGCN:** evaluación de riesgos, análisis del impacto, planes de continuidad y procedimientos relacionados.
- Mejorar la monitorización de todo lo relacionado con el **SGCN.**



CONTINGENCIA TIC VERSUS CONTINGENCIA NEGOCIO

Si bien es cierto que se van viendo avances significativos en la comprensión de la contingencia y la continuidad de negocio, de vez en cuando todavía nos encontramos con que no se distinguen del todo algunos conceptos básicos.

Es el caso de los planes de contingencia en relación con los planes de continuidad de negocio (PCN).

Aquí podemos entrar en discusiones del tipo «un plan de contingencia no es exactamente lo mismo que un plan de continuidad de negocio» o «en realidad es un plan de continuidad de negocio, pero solo para el área TIC».

La forma más acertada de abordar el asunto es considerar al plan de continuidad de negocio como un plan de planes. Efectivamente, un buen plan de continuidad contendrá a su vez un cierto número de planes diferentes, como puede ser el plan evacuación, el plan de emergencia, el plan de gestión de incidentes y, cómo no, un buen plan de contingencia TIC.

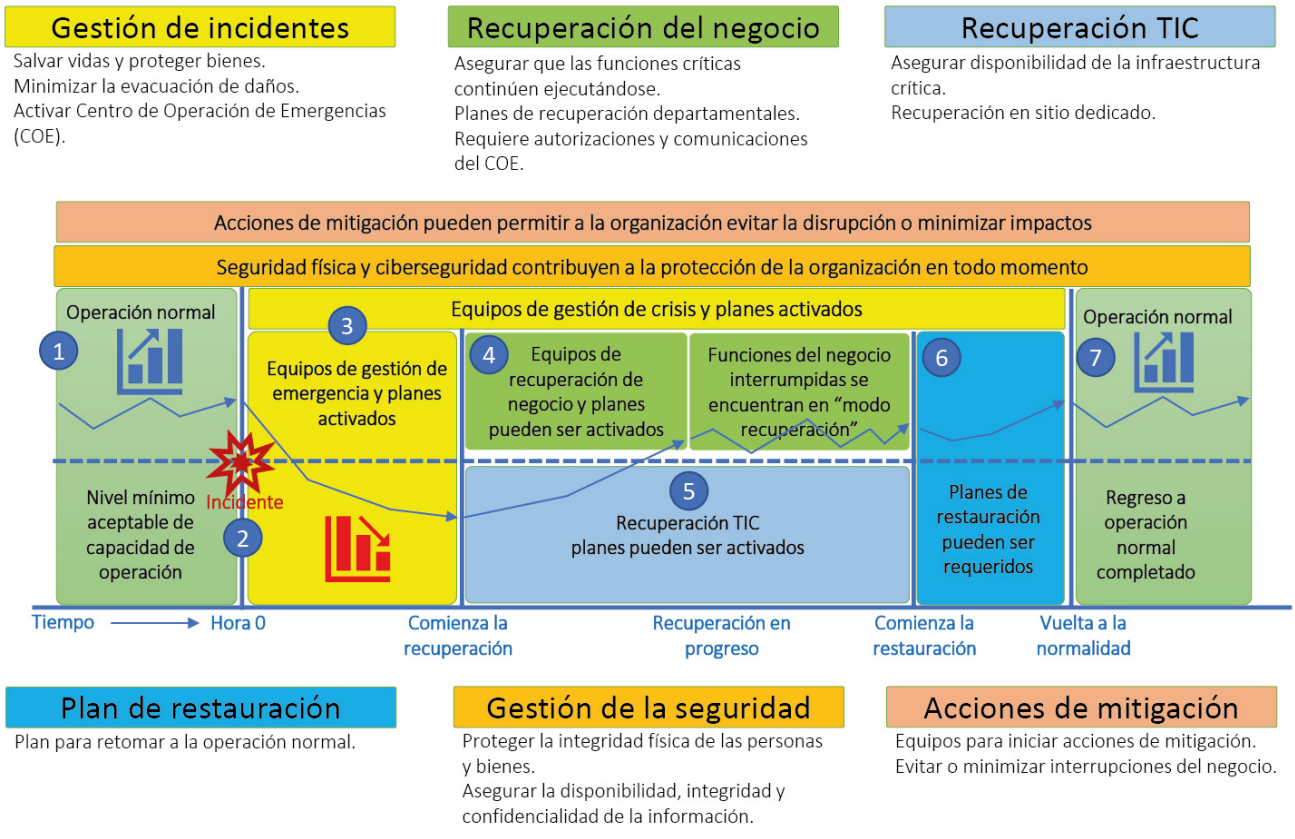
Podemos decir que un plan de contingencia de las tecnologías de la información y las comunicaciones (TIC) consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en el **PCN** de la organización.

Por su parte, el **plan de continuidad de negocio** puede ser definido como un conjunto formado por planes de actuación, planes de emergencia, planes financieros, planes de comunicación y planes de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una organización.

Por tanto, no debemos tener dudas al afirmar que el plan de contingencia es uno de los elementos más relevantes de un plan de continuidad de negocio, y que, si tenemos en cuenta la dependencia casi absoluta que las organizaciones y empresas de cualquier tipo tienen de los sistemas de información y de las comunicaciones, nos daremos cuenta rápidamente de que a día de hoy es difícil dar continuidad sin tener contingencia de las TIC. Y decimos «difícil» y no «imposible», pues en ocasiones podremos buscar alternativas «manuales» para aquellas actividades que en condiciones normales hacemos apoyándonos en las TIC.

VISIÓN INTEGRAL DEL SGCN

A continuación, se muestra todo el ciclo del SGCN para que se tenga una visión integral y esquematizada.



1. Operación normal (nivel que permite a la organización cumplir con los objetivos de negocio). También se tiene cuantificado un nivel mínimo aceptable de operación.
2. Ocurre el incidente disruptivo y las operaciones de negocio caen por debajo del nivel mínimo aceptable, incluso a cero.
3. Se convocan los equipos de gestión de crisis para evaluar la situación y tomar las decisiones de cara a activar los planes de recuperación de negocio a partir de los tiempos objetivos de recuperación.
4. Comienza la etapa de recuperación y se activan los diferentes equipos de recuperación para ejecutar la contingencia y recuperar las actividades del negocio afectadas, principalmente las más críticas.
5. Si el alcance del incidente afecta a los centros de datos, también se activan los planes de recuperación TIC y la recuperación está avanzando para recuperar los niveles mínimos de operación marcados por la organización.
6. Una vez estabilizado el nivel de operación por encima del nivel mínimo, se empiezan a aplicar los planes de restauración para volver a un nivel normal de operación.
7. Vuelta a la operación normal.

Durante todo el proceso se debe tener en cuenta el desarrollo de:

- Los planes de continuidad de la seguridad, ya sea a nivel físico de las instalaciones y personas como en el de la ciberseguridad, ya que la información es posible que esté más comprometida.
- Acciones de mitigación para minimizar riesgos y tener que evitar la activación de los planes de contingencia del negocio.

ISO 22301

La ISO 22301 es el estándar reconocido internacionalmente que determina los requisitos para implementar, operar, monitorizar, revisar, mantener y mejorar el SGCN, de manera que se garantice la continuidad de las actividades y la recuperación de los procesos de negocio ante un evento disruptivo, mejorando la capacidad de resiliencia y minimizando las consecuencias de dichos eventos.

La norma ISO 22301 sirve como marco sobre el cual construir un SGCN que permita a las organizaciones estar preparadas para seguir operando durante las disrupciones de negocio. Los requisitos de la norma están destinados a ser aplicados y adaptados a todo tipo de organizaciones, con independencia del tipo, tamaño, sector y naturaleza de la organización.

En el capítulo siguiente se detalla el contenido de la norma y su aplicación.

CONCLUSIONES

- Un **SGCN** es primordial para **asegurar la vida de la organización ante cualquier tipo de desastre.**
- Un **SGCN** permite a la organización **identificar las amenazas conocer sus puntos débiles y poner soluciones.**
- Un **SGCN** es más que la **recuperación de la tecnología, es la recuperación de la operativa del negocio.**
- La validez de un **SGCN solo se asegura mediante la realización de un plan de pruebas exhaustivo.**
- Un **SGCN** deberá ser **actualizado periódicamente** para reflejar y responder a los cambios que se vayan produciendo en la organización.
- Un **SGCN** es un proyecto personalizado a cada organización.
- La tecnología actual nos permite afrontar planes de contingencia acordes a nuestras necesidades operativas y económicas.
- En un **SGCN** debe de estar implicada la dirección general de la organización.

El principal objetivo de un SGCN es permitir la administración, planificación, seguimiento, control y mejora continua de la estrategia de continuidad del negocio de la organización, para garantizar su operación crítica en caso de una contingencia.

2

BUENAS PRACTICAS EN CONTINUIDAD DE NEGOCIO

Imagen de Freepik

2.1

ISO 22301. MARCO DE CONTINUIDAD DE NEGOCIO

Jorge Edo Juan
Jorge Sánchez López

ANTECEDENTES

La norma ISO 22301 es un marco de gestión que define los requisitos y las consideraciones para implementar, gestionar y mejorar un sistema de gestión de la continuidad de negocio, abreviado por las siglas SGCN, cuyo objetivo es tener preparada a la organización para poder hacer frente a cualquier desastre o incidente crítico que pueda afectar a la organización.

La ISO 22301 está basada en la creación de un sistema de gestión, asentado en la continuidad del negocio. Las organizaciones implementan de esta forma sistemas de gestión para mejorar sus operaciones y avanzar en el desempeño de sus operaciones, al mismo tiempo que consiguen aportar más valor a sus clientes.

Podemos encontrarnos con organizaciones en las que existan definidos varios sistemas de gestión, como, por ejemplo:

- Sistema de gestión de calidad: ISO 9001.
- Sistema de gestión de seguridad de la información: ISO 27001.
- Sistema de gestión Ambiental: ISO 14001.

De este modo, como cada vez es más habitual que las organizaciones gestionen varios marcos de cumplimiento simultáneamente, puede resultar interesante que se implemente un sistema de gestión integrado (SGI). Un SGI es un sistema de gestión que integra las distintas ISO que están implantadas en una organización, en un mismo sistema de gestión. Este punto lo desarrollaremos en detalle en el siguiente capítulo (capítulo 3) donde comentaremos la integración de la continuidad de negocio, con otros marcos como pueden ser la seguridad de la información (ISO 27001), y el esquema nacional de seguridad (ENS).

A continuación, vamos a comentar los principales hitos de desarrollo de la ISO 22301 a lo largo del tiempo:

1988. Creación del Instituto de Recuperación de Desastres, DRI.

1994. Creación del Instituto de Continuidad del Negocio, BCI.

2002. Publicación de las directrices de buenas prácticas de la gestión de la continuidad del negocio por parte de BCI.

2003. Publicación de PAS 56 por parte del BCI y el BSI (British Standards Institution).

2006. Publicación de la norma 25999-1 por parte del British Standards. Este estándar fue retirado a principios del 2013 con la publicación de la ISO 22313.

2007. Publicación de la norma 25999-2 por parte de British Standards. Este estándar fue retirado en noviembre del 2012 con la publicación de la ISO 22301.

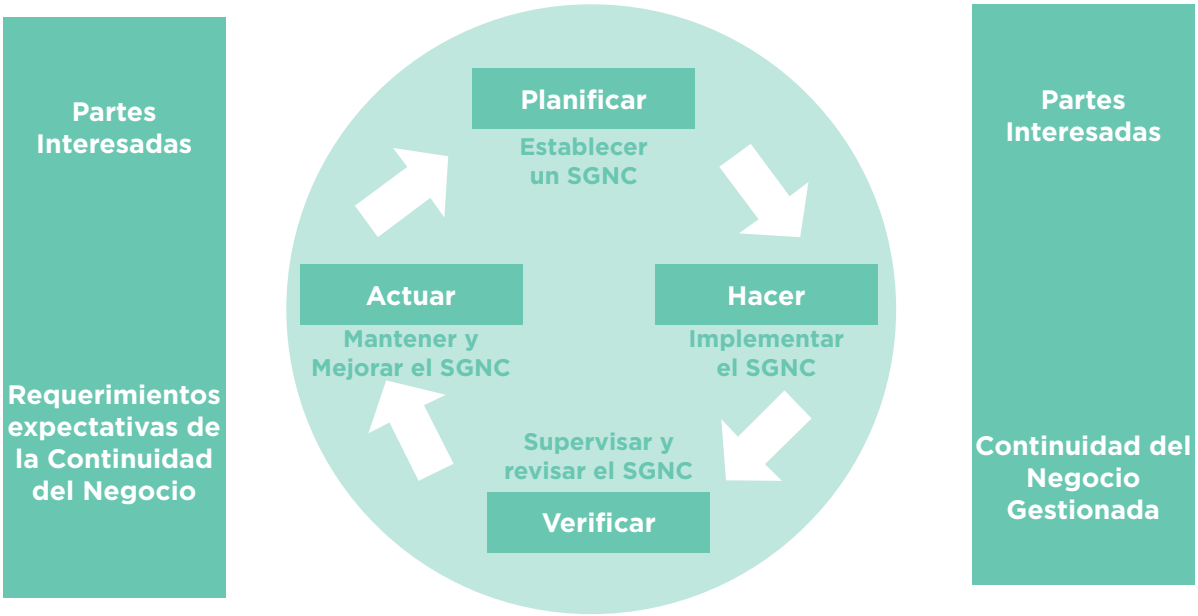
2012. Publicación de la primera edición de la ISO 22301:2012.a

2019. Actualización del marco ISO 22301. ISO 22301:2019.

Junto con la ISO 22301, tenemos que comentar que hay otra norma de la misma familia que proporciona indicaciones y recomendaciones para implantar con éxito un sistema de gestión basado en la ISO 22301. Esta norma es la ISO 22313, que es la equivalente en cuanto a seguridad de la información a la norma ISO 27002. En ambos casos ni la ISO 22313, ni la ISO 27002, son certificables. Posteriormente en el capítulo 4, veremos como una organización puede certificar la ISO 22301.

CICLO DE DEMING

Todos los sistemas de gestión utilizan el ciclo de Deming para la gestión del sistema. Este modelo que vamos a describir en detalle a continuación se aplica a la estructura de todos los procesos del sistema de gestión de continuidad de negocio.



Este método que consta de las fases: planificar, hacer, verificar y actuar, es un método iterativo que ayuda a las organizaciones a poder implementar con éxito, mantener de forma eficaz y mejorar de forma continua el sistema de gestión de continuidad de negocio (SGCN) de una organización.

A continuación, en la siguiente tabla se relacionan las 4 fases del ciclo de Deming: P, D, C, A con las diversas actividades que requiere un proyecto de Implantación de la ISO 22301.

FASE	TAREAS
Plan (P)	Crear y establecer las políticas, objetivos, controles y procedimientos de continuidad de negocio, necesarios para lograr los resultados que se ajusten a la estrategia de la organización.
Hacer (D)	Implementar, comunicar la política, controles, procesos y procedimientos de continuidad del negocio.
Verificar (C)	Supervisar y revisar el rendimiento del sistema de gestión, mediante la realización de auditorías internas y revisiones por parte de la dirección de forma periódica.
Actuar (A)	Mantener y mejorar el SGCN de forma cíclica, mediante la adopción de planes de acción y medidas correctivas basadas en los resultados de las auditorías internas y externas y en la revisión por parte de la dirección.

ESTRUCTURA DE LA NORMA ISO 22301: 2019

Como hemos comentado anteriormente (en el apartado de antecedentes), de acuerdo con la estructura de todos los sistemas de gestión, para posibilitar la integración de diferentes sistemas: ISO 9001, ISO 27001, ISO 22301..., la estructura de las cláusulas de las normas anteriores es idéntica. Este hecho facilita enormemente la integración entre sistemas y define un SGI, como hemos comentado.

Según hemos indicado en el apartado anterior, de acuerdo con el modelo PDCA, las cláusulas 4 a 10 cubren los siguientes componentes:

LA CLÁUSULA 4. CONTEXTO DE LA ORGANIZACIÓN. Presenta los requisitos necesarios para establecer el contexto específico que aplica a cada organización, así como las necesidades, requisitos de las partes interesadas y el alcance del SGCN.

LA CLÁUSULA 5. LIDERAZGO. Define la importancia de la implicación de la alta dirección en el proyecto de continuidad de negocio, así como el establecimiento de una política de continuidad de negocio y como se ha de comunicar dicha política tanto a los empleados, como a otras partes interesadas. Finalmente, otro de los puntos clave en el proyecto será la asignación de los roles adecuados para poder implantar con éxito el SGCN en la organización.

LA CLÁUSULA 6. PLANIFICACIÓN. Describe los requisitos para establecer objetivos estratégicos y principios guía para el SGCN. En este apartado cobra especial importancia tanto la determinación de los riesgos y oportunidades que puedan afectar el SGCN, como el tratamiento de dichos riesgos y oportunidades para obtener un SGCN eficiente y resiliente ante cualquier desastre que se pueda producir. En este punto también hay que definir los objetivos anuales de continuidad del negocio y plantear una adecuada planificación para poder culminarlos con éxito.

LA CLÁUSULA 7. SOPORTE. Determina los recursos necesarios para desarrollar con éxito el proyecto, determina la competencia de las personas que van a llevarlo a cabo y planifica las actividades de concienciación que se deben realizar de forma periódica. También se define en este punto la comunicación con las partes interesadas durante la vigencia del SGCN. Finalmente, un proyecto de estas características implica la creación y el mantenimiento de un sistema documental adecuado a las características y el contexto de la organización.

LA CLÁUSULA 8. OPERACIÓN. Define cómo hay que desarrollar las actividades de planificación y control operacional del SGCN, el análisis de impacto sobre el negocio y la evaluación del riesgo, en función de los diferentes escenarios de riesgo que puedan originarse en la organización, como por ejemplo: caída de las comunicaciones, ausencia del personal clave, corte eléctrico, incendio, inundación... Una vez determinados los escenarios de desastre, se plantearán cuáles son las estrategias para la continuidad del negocio de la organización.

LA CLÁUSULA 9. EVALUACIÓN DEL DESEMPEÑO. Determina los requisitos necesarios para medir el desempeño de la continuidad del negocio, mediante la definición y el mantenimiento de las métricas más adecuadas por un lado a las exigencias de la norma y, por otro, a las características de la organización. En esta cláusula también se plantean los requisitos necesarios para realizar las auditorías internas periódicas, así como los aspectos a tener en cuenta cuando se lleva a cabo la revisión de gestión por la dirección.

LA CLÁUSULA 10. MEJORA. Identifica y actúa sobre las no conformidades del SGCN y la mejora continua mediante acciones correctivas.

A continuación, vamos a explicar el proceso de implantación de un SGCN, y plantearemos con detalle el desarrollo de cada una de las cláusulas anteriores del marco ISO 22301.

CLÁUSULA 4. CONTEXTO DE LA ORGANIZACIÓN

El proyecto de implantación de la ISO 22301 (como el de cualquier sistema de gestión), comienza con la comprensión del contexto de la organización. Para ello es conveniente obtener una visión amplia de la organización, con el fin de entender de forma detallada cuáles son los desafíos en materia de posibles desastres que puedan afectar a su normal funcionamiento. En este punto tendremos en cuenta las siguientes definiciones, que nos va a ayudar a alinear el SGCN con la estrategia de la entidad.

MISIÓN. La misión es lo que justifica y define la existencia de la organización. El que una organización tenga clara cuál es su misión, sirve como punto de referencia para mantener claro hacia a dónde se dirige la organización y qué implicaciones tiene para la gestión de la continuidad del negocio. El SGCN, por lo tanto, debe estar alineado con la misión de la organización.

VALORES. Los valores son las creencias fundamentales compartidas por todos los miembros de una organización. Cabe señalar que, por ejemplo, los valores están relacionados con el apetito de riesgo de la organización (este punto se desarrollará con más en detalle durante el desarrollo de la cláusula 6, Planificación), lo que significa que los valores influyen en la cantidad y los tipos de riesgo que una organización está dispuesta a asumir o tolerar.

OBJETIVOS. Un objetivo es una meta que la organización desea alcanzar. Los objetivos son generalmente predeterminados, cuantificados y con unos plazos determinados. El SGCN debe estar alineado con los objetivos de la organización para mantener la continuidad en caso de un desastre.

ESTRATEGIAS. La estrategia consta de una secuencia definida de tareas encaminadas a la consecución de uno o más objetivos, que se plantee alcanzar la organización.

La misión es lo que justifica y define la existencia de la organización.

A la hora de analizar el contexto de la organización, es fundamental que utilicemos una metodología adecuada para examinarlo de forma conveniente:

ANÁLISIS DAFO (debilidades, amenazas, fortalezas y oportunidades). Esta metodología se utiliza para realizar un análisis exhaustivo de las fortalezas, debilidades, oportunidades y amenazas de una organización, con la finalidad de tomar ventaja con las oportunidades, reducir debilidades, afrontar amenazas, etc.). El análisis DAFO, permite examinar de forma detallada tanto el contexto interno, como el externo.

ANÁLISIS PESTLE (político, económico, social, tecnológico, legal, ecológico o medio ambiental). Este análisis permite a la organización analizar las fuerzas y oportunidades del mercado clasificadas en las seis áreas: política, económica, social, tecnológica. legal y ambiental. Esta metodología sirve únicamente para estudiar el contexto externo de una organización.

ANÁLISIS DE LAS CINCO FUERZAS DE PORTER. El análisis de las cinco fuerzas de Porter examina el nivel de competitividad de las organizaciones mediante el empleo de las cinco fuerzas de Porter.

Estas cinco fuerzas son las siguientes:

- Intensidad de la rivalidad entre los competidores.
- El poder de negociación de los clientes.
- La amenaza de los competidores potenciales en el mercado.
- El poder de negociación de los proveedores.
- Las amenazas de productos alternativos.

Una vez analizado el contexto de la organización, otras actividades que se deben llevar a cabo durante el desarrollo de esta cláusula son las siguientes:

- Identificar los **procesos y actividades clave.**
- Identificar y analizar en detalle las **necesidades y expectativas de las partes interesadas.** A este efecto, se entiendes como partes interesadas: la alta dirección, los proveedores, los empleados, las autoridades, los clientes, los medios de comunicación y los competidores.
- Definir de forma documentada los **requisitos legales y reglamentarios** que afectan a la organización.
- Determinar el **alcance** del SGCN. Para ello, la organización tiene que determinar los límites y la aplicabilidad del SGCN para establecer y definir su alcance. La definición del alcance es un elemento clave que influye de forma considerable en la cantidad de esfuerzo necesario para desarrollar el proyecto con éxito. Un alcance más acotado (que abarque a menos áreas de la organización, será más rápido para poder desarrollarlo), puede ser más conveniente para poder partir de una base sólida y desde ahí en sucesivas iteraciones en años sucesivos poder ampliar dicho alcance inicial.

Finalmente, en este punto de análisis del contexto, es importante reseñar la conveniencia de realizar, con el arranque del proyecto de implantación del SGCN, un **análisis de brechas** (Gap Análisis). Esta técnica se utiliza para determinar las tareas más adecuadas para pasar del estado actual al estado futuro con el proyecto del SGCN implantado.

CLÁUSULA 5. LIDERAZGO

La implicación de la alta dirección en un proyecto de esta magnitud es fundamental, para que este se desarrolle con éxito. Esta implicación puede estar desencadenada por dos situaciones distintas:

1. Implicación directa de la alta dirección en el proyecto. En este caso el liderazgo viene implícito en el proyecto, ya que la alta dirección es su promotora.
2. Creación de un **caso de negocio.** Un caso de negocios es una herramienta excelente, que permite a las organizaciones planificar y tomar decisiones, a partir de unos datos obtenidos de forma objetiva. El propósito más común de un caso de negocio es determinar las consecuencias financieras de una decisión. Así, un caso de negocio bien definido permitirá determinar los beneficios que se alcanzarán con el desarrollo del proyecto, en un tiempo predefinido. Por otro lado, el caso de negocio incluye también los métodos y el sistema utilizado para calcular dichos beneficios, con lo que este será muy útil para que la alta dirección pueda tomar las mejores decisiones referidas a inversiones para cumplir con las estrategias y los objetivos de la organización.

Como hemos comentado anteriormente, el compromiso y la participación de la alta dirección son fundamentales para que el proyecto de implantación del SGCN tenga éxito. Dicho compromiso debe figurar explícitamente por escrito y debe quedar documentado.

Otra de las áreas que requieren de la participación de la alta dirección es la asignación y comunicación de responsabilidades (roles) dentro del SGCN. Generalmente los roles para los que hay que documentar y determinar las funciones y responsabilidades son los siguientes:

- Responsable de la información. Suele ser un representante de la alta dirección.
- Responsable del SGCN. Encargado de la gestión y el mantenimiento de la documentación del SGCN.
- Responsable de seguridad. Desempeñada por el CISO de la organización.
- Responsable de sistemas.

Estos roles definidos anteriormente suelen deben ser ejercidos por miembros de un comité de continuidad de negocio, que tiene la obligación de reunirse periódicamente, y tomar las decisiones de alto nivel en materia de continuidad de negocio.

Otra de las implicaciones que denota el compromiso de liderazgo en materia de continuidad de negocio por parte de la organización es la **política de continuidad de negocio**. Uno de los requisitos de la ISO 22301, en su apartado 5.2.1 establece que la alta dirección debe establecer una política de continuidad del negocio que:

- Sea apropiada para el propósito de la organización.
- Proporcione un marco de referencia para establecer los objetivos de la continuidad del negocio.
- Incluya el compromiso de cumplir los requisitos aplicables.
- Incluya un compromiso por parte de la alta dirección en la mejora continua del SGCN.

Una vez creada y revisada la política de continuidad de negocio, la norma exige que esta sea dada a conocer de forma adecuada tanto a las partes internas, como a las externas a la organización.

CLÁUSULA 6. PLANIFICACIÓN

Dentro de la planificación, tienen un papel muy importante las acciones para abordar los riesgos y las oportunidades. Este apartado tiene su ampliación en la cláusula 8.2, análisis de impacto sobre el negocio y evaluación del riesgo, que se verá posteriormente en detalle.

Adicionalmente, en esta cláusula 6 de planificación, es donde se definen los objetivos de continuidad del negocio y la planificación para poder lograrlos. Los objetivos de continuidad del negocio son un requisito de la norma, y deben definirse con el fin de apoyar a la política de continuidad de la organización, y estar alineados con la estrategia de la organización. Una vez definidos los objetivos, la alta dirección debe validarlos y aprobarlos y, en la revisión, la dirección. Si durante el año, se producen cambios importantes en la organización, los objetivos se pueden modificarse.

Los objetivos de continuidad del negocio deberían diseñarse para cumplir la regla **SMART** y deberían tener relevancia en todos los niveles de la organización:

ESPECÍFICO (S). Debería servir de guía para saber lo que la organización quiere lograr y hasta qué punto.

MEDIBLE (M). La organización debería realizar un seguimiento del progreso y medir los resultados.

ALCANZABLE (A). Los objetivos necesitan ser alcanzables para permitir que se puedan lograr. En el caso de que se fijen objetivos muy poco realistas solo va a crear desesperación y frustración por la imposibilidad de poderlos alcanzar.

RELEVANTE (R). Los objetivos de continuidad del negocio deberían ser relevantes para la organización y estar alineados con la estrategia, la misión y las políticas internas de la organización.

ACOTADOS EN EL TIEMPO (T). Los objetivos de continuidad del negocio deberían tener un tiempo definido para su consecución, de tal forma que permitirá a la organización supervisar cuán cerca están de su cumplimiento, en el tiempo predeterminado.

CLÁUSULA 7. SOPORTE

En esta cláusula se exigen los siguientes requerimientos:

RECURSOS. La organización que está implementando el SGCN debe determinar los recursos que necesita para poder incorporar de forma exitosa el sistema de continuidad de negocio en la organización.

FORMACIÓN. Esto generalmente se suele denominar programa de desarrollo de competencias. La norma establece que la dirección tiene que determinar las competencias necesarias para las funciones y responsabilidades del SGCN. De este modo todas las personas asignadas a funciones dentro del SGCN tienen que disponer de las competencias adecuadas para desempeñar sus funciones correspondientes dentro del sistema de gestión. Este apartado se desarrolla dentro del plan de formación de la organización, donde la organización debe establecer formación de alto nivel de manera periódica. Una vez llevadas a cabo las acciones de formación, la norma establece que hay que evaluar la eficacia de la formación realizada.

CONCIENCIACIÓN. Este apartado va íntimamente unido al anterior. Dentro de los planes de formación de la organización, se exige que se desarrollen de forma periódica (mínimo una vez al año), sesiones de concienciación de más bajo nivel a todos los empleados de la organización. En este punto podemos recomendar el abundante material disponible en el INCIBE (www.incibe.es), como, por ejemplo: videos, píldoras formativas, presentaciones, infografías..., relativas tanto a la seguridad de la información, como a la continuidad del negocio.

COMUNICACIÓN. En este punto se establece que la organización debe determinar las comunicaciones internas y externas adecuadas al SGCN. Generalmente estas comunicaciones, suelen estar asociadas a un **plan de comunicación.** En materia de comunicación, es recomendable seguir los siguientes principios de comunicación eficaz.

Transparencia. Comunicar de forma adecuada a todas las partes interesadas teniendo en cuenta la confidencialidad de la información.

Idoneidad. Hacer que la información proporcionada en la comunicación a las partes interesadas sea la adecuada.

Credibilidad. Comunicar de manera honesta y justa, una información que sea veraz, exacta y relevante.

Respuesta. Responder a las preguntas y preocupaciones de las partes interesadas de manera conveniente y oportuna.

Claridad. Asegurar que los métodos de comunicación y el lenguaje son comprensibles para todas las partes interesadas, con el fin de minimizar la ambigüedad.

DOCUMENTACIÓN. Otra de las exigencias de la norma es que la organización implemente un sistema de gestión de información documentada. Un sistema de estas características garantiza la trazabilidad y protege el acceso a los documentos mediante la asignación de distintos niveles de autorización para el acceso, uso y difusión de la información. Por ejemplo, se puede plantear un sistema de clasificación de la información a cuatro niveles: pública, interna, confidencial (por áreas) y restringida (por personas).

Una de las recomendaciones dentro de este punto, es llevar un registro actualizado de la documentación del SGCN en vigor, donde figure, el autor, el revisor, la versión, la fecha y el documento. Esto facilita una mejor localización de la información, ante las peticiones de las partes interesadas, y el seguimiento durante las auditorías tanto internas como externas.

CLÁUSULA 8. OPERACIÓN

Esta es la cláusula que más tiempo lleva a la hora de desarrollar un SGCN. En este punto es donde se desarrolla tanto la evaluación de impacto (BIA), el análisis de los riesgos y el plan de tratamiento de estos.

Evaluación de impacto (BIA)

Un análisis del impacto en el negocio (por sus siglas BIA) permite que la organización establezca prioridades para reanudar las actividades que se han interrumpido como consecuencia de un desastre que se haya producido. El principal propósito de un BIA es permitir a la organización identificar y clasificar cuáles serían las actividades más críticas de la organización y, en caso de que se produzca un desastre, cuáles serían los procesos por los que empezar la recuperación del negocio.

El BIA debería documentarse incluyendo los siguientes aspectos:

- Identificación de los requisitos legales, reglamentarios y contractuales (obligaciones) y su efecto en los requisitos en materia de continuidad del negocio.
- La aprobación o modificación del alcance del SGCN de la organización.
- La identificación de las dependencias entre productos y servicios, actividades y recursos.

- La identificación de los recursos de soporte necesarios de los que dependen las actividades críticas.
- La identificación de dependencias externas en otras actividades, cadenas de suministro, proveedores y otras partes interesadas.

Las fases para la elaboración de un BIA serían las siguientes:

- Planificación del análisis de impacto.
- Recopilación de los datos para elaborar el BIA.
- Analizar y evaluar los datos anteriores.
- Validar los datos para elaborar el BIA.
- Realización del informe con el BIA.

Análisis de riesgos

Se puede definir el concepto de riesgo en seguridad de la información y continuidad de negocio, como: «El potencial de que una cierta amenaza explote vulnerabilidades de un activo o grupo de activos y así cause daño a la organización». [ISO/IEC 27005:2008]

Vamos a plantear una serie de definiciones de interés:

Activo. Un activo es algo que tiene valor para la organización y, por lo tanto, requiere de una protección adecuada en función de su importancia para la compañía.

Vulnerabilidad. Debilidad inherente al activo. Su presencia no causa daño por sí misma, ya que necesita de una amenaza que la explote. La falta de un control también puede considerarse una vulnerabilidad.

Amenaza. Una circunstancia o evento que tiene el potencial de causar daño a un activo y, por lo tanto, a la organización.

Impacto. Daño causado por una amenaza que explota una vulnerabilidad en un activo y que afecta adversamente el logro de los objetivos de negocio.

En teoría de riesgos, la fórmula que se emplea es la probabilidad por impacto, es decir la probabilidad de que una amenaza afecte a un activo, por el impacto que la ausencia total o parcial de dicho activo impacte en la organización.

$$R = P \times I$$

RIESGO PROBABILIDAD IMPACTO

A continuación, se indican las fases de un proceso de análisis y tratamiento de los riesgos.

Proceso de análisis y tratamiento de riesgos

Fase 1. Enfoque. En esta primera fase se determina cuál es el enfoque que determina la organización para realizar el análisis de riesgos para las escalas de probabilidad e impacto. Enfoque cuantitativo (con números: 1, 2, 3...) o enfoque cualitativo (con niveles: alto, medio, bajo...)

Fase 2. Metodología de evaluación de riesgos. Se recomienda elegir una metodología que esté reconocida en el ámbito internacional como por ejemplo: MAGERIT (España), OCTAVE y NIST 800-30 (EE.UU.), CRAMM (Reino Unido), TRA (Canadá), EBIOS y MEHARI (Francia).

Fase 3. Identificación del riesgo. A partir del inventario de activos, se categorizan estos en grupos, y a cada grupo de activos en función de la metodología elegida en la fase 2, se le aplica el catálogo de amenazas que viene definido en cada una de las metodologías de evaluación de riesgos anteriores.

Fase 4. Análisis de riesgos. Esta fase implica el cálculo de la matriz de riesgos en función de las escalas de probabilidad e impacto. En el gráfico siguiente se muestran dos ejemplos de matrices (en enfoque cualitativo y cuantitativo) de tres niveles tanto en probabilidad como en impacto.

MATRIZ DE EVALUACIÓN DE RIESGOS CUANTITATIVA

		PROBABILIDAD		
		BAJA	MEDIA	ALTA
IMPACTO	BAJO	1	2	3
	MEDIO	2	4	6
	ALTO	3	6	9

MATRIZ DE EVALUACIÓN DE RIESGOS CUALITATIVA

		PROBABILIDAD		
		BAJA	MEDIA	ALTA
IMPACTO	BAJO	MUY BAJO	BAJO	MEDIO
	MEDIO	BAJO	MEDIO	ALTO
	ALTO	MEDIO	ALTO	MUY ALTO

Fase 5. Evaluación del riesgo. En este punto vamos a hablar del concepto de apetito de riesgo, que es el mayor nivel de riesgo que una organización acepta. Por ejemplo, en las matrices anteriores la organización puede determinar que el apetito de riesgo estaría fijado en 4 para la matriz cuantitativa y en medio para la cualitativa.

Una vez fijado dicho valor, no puede haber activos en la matriz correspondiente con valor superior al apetito de riesgo. Para aquellos activos que tengan un riesgo superior a este, hay que aplicar controles para bien evitar o reducir dicho nivel de riesgo.

Fase 6. Tratamiento del riesgo. Tendremos siempre cuatro opciones para poder tratar los riesgos. Dichas opciones serían las siguientes:

Tratar el riesgo. Implementar o modificar controles ya aplicados para reducir el nivel de riesgo por debajo del umbral de riesgo aceptable.

Aceptar el riesgo. Cuando el riesgo se encuentre dentro del nivel aceptable o el coste de los controles sea mayor que la pérdida potencial debida al impacto, la organización puede decidir aceptar las consecuencias del riesgo si este se materializa.

Evitar el riesgo. Eliminación total del riesgo mediante el cese de una actividad o conjunto de actividades mediante la eliminación de la causa raíz que origina la amenaza que puede provocar el riesgo.

Transferir el riesgo. Supone trasladar o compartir el riesgo y su gestión con un tercero (proveedor, empresa aseguradora...).

Fase 7. Aceptación del riesgo. Una vez finalizado el proceso de análisis de riesgos, siempre nos quedará un riesgo residual, en el que aplicamos la siguiente fórmula.

Como podemos comprobar en el gráfico anterior, cuando el riesgo tratado en muy alto (por la aplicación de multitud de controles), el riesgo residual es bajo o muy bajo. Por el contrario, cuando el número de controles implantados en la organización es bajo o muy bajo, el riesgo inherente (riesgo que hay en la entidad antes de aplicar ningún tipo de control) es muy similar al riesgo residual.

Plan de tratamiento de riesgos

Una vez que han sido adoptadas las decisiones sobre el tratamiento de riesgos, deben ser identificadas y planificadas las actividades para poner en práctica estas decisiones.

Las acciones prioritarias se centran generalmente en las actividades de mayor riesgo. El plan de tratamiento al menos debe aclarar las acciones que se deben tomar, los recursos que se deban asignar, las responsabilidades que se deben tomar y la secuenciación de prioridades.

El plan de tratamiento de riesgos, o PTR, es un registro donde, como se refleja en la figura siguiente, se indican los riesgos de la organización, la prioridad a la hora de gestionarlos, los recursos necesarios para tratar los riesgos, los responsables de abordarlos y las fechas de inicio y fin de cada tratamiento.

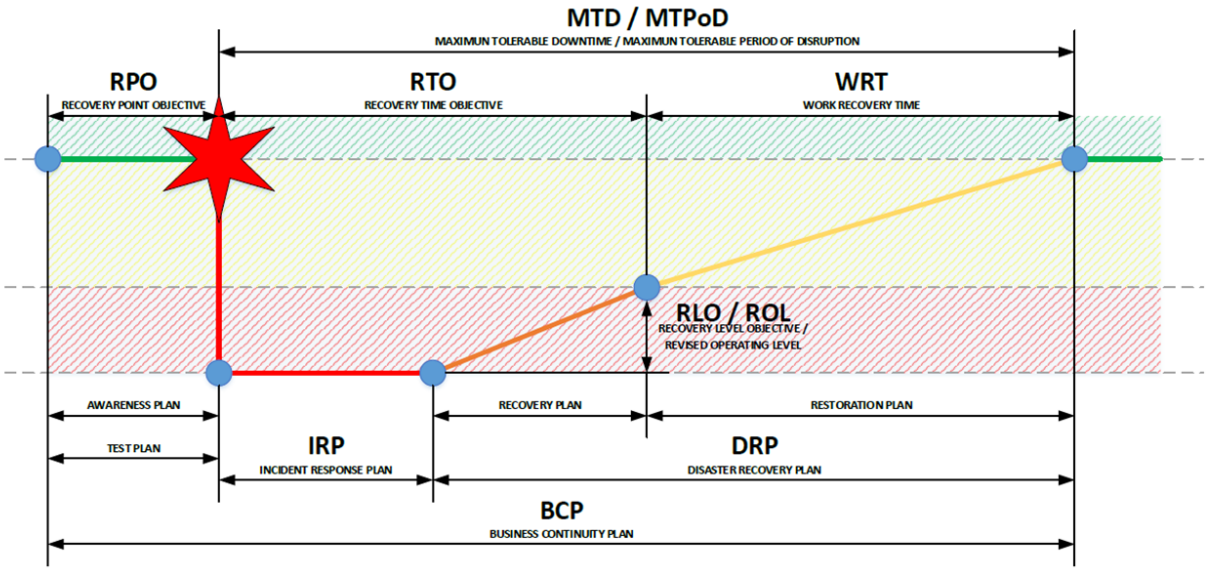
RIESGO	NIVEL DE RIESGO	PRIORIDAD	TRATAMIENTO	DETALLE DEL TRATAMIENTO	RECURSOS	RESPONSABLE	FECHA INICIO/FIN	COMENTARIOS

Estrategias de continuidad de negocio

El objetivo de las estrategias de continuidad de negocio es ayudar a la organización a definir las acciones necesarias para proteger sus funciones críticas del negocio, una vez que se haya producido un desastre, así como posteriormente poder seleccionar las soluciones de recuperación más adecuadas para las funciones críticas del negocio en función del tipo de disrupción que se haya producido. La estrategia de continuidad de negocio debe abordar los hallazgos de la evaluación de riesgos y el análisis del impacto en el negocio, donde dicha estrategia constituye la base de los planes de continuidad del negocio.

En el contexto de la gestión de la continuidad del negocio, la estrategia se relaciona con la determinación y selección de estrategias operativas alternativas que se utilizarán para mantener las actividades críticas de la organización. La experiencia y las buenas prácticas demuestran que la provisión temprana de una estrategia de GCN de la organización, permite garantizar que las actividades de GCN estén en línea con la estrategia de negocio general de la organización.

A la hora definir la estrategia de negocio más adecuada para la organización, entran en juego los términos que se indican en el gráfico siguiente, principalmente los términos: RTO (tiempo de recuperación objetivo) y RPO (punto de recuperación objetivo).



- **RPO:** MÁXIMA CANTIDAD TOLERABLE DE INFORMACIÓN QUE SE PUEDE PERDER EN CASO DE DESASTRE.
- **RTO:** MÁXIMO TIEMPO TOLERABLE QUE PUEDE PASAR DESDE QUE OCURRE UN INCIDENTE HASTA QUE SE RECUPERA EL PROCESO A UN NIVEL MÍNIMO ACORDADO.
- **RLO/ROL:** NIVEL MÍNIMO ACORDADO PARA QUE UN PROCESO PUEDA CONSIDERARSE RECUPERADO.
- **WRT:** MÁXIMA CANTIDAD TOLERABLE DE TIEMPO NECESARIA PARA LA COMPROBACIÓN DE LA INTEGRIDAD DEL SISTEMA O LOS DATOS.
- **MTD/MTPoD:** TIEMPO MÁXIMO TOLERABLE DE NO DISPONIBILIDAD DE UN PROCESO ANTES DE QUE SUPONGA CONSECUENCIAS DESASTROSAS PARA LA ORGANIZACIÓN.

Para garantizar que las actividades prioritarias puedan reanudarse dentro de sus RTO también se deberían establecer RTO compatibles para las dependencias y los recursos de soporte.

En cuanto a estrategias de continuidad de negocio, a continuación, vamos a recoger las estrategias más habituales:

1. Reconstrucción. La contratación de un seguro suele ser la primera de las opciones que se valora a la hora de plantear la estrategia de continuidad del negocio. Esta estrategia es relativamente fácil de poder llevar a término, dado que generalmente solo suelen estar cubiertos por parte del seguro los activos críticos de la organización.

2. Sitio frío (Cold Site). Se trata de una ubicación que solo dispone de una infraestructura básica (red eléctrica, aire acondicionado...), para tener un centro alternativo a un bajo coste. En esta estrategia la ubicación está preparada, pero tiene que ser provisionada con el equipamiento restante una vez se declare la situación de contingencia. La activación de esta estrategia puede tardar varias semanas.

3. Sitio móvil. Esta estrategia se basa en la utilización de un transporte móvil (generalmente un remolque) especialmente diseñado para que se pueda trasladar de forma sencilla de una ubicación a otra.

4. Acuerdo recíproco. En esta estrategia se basa en que varias organizaciones (dos o más) dispongan de infraestructuras tecnológicas similares, lleguen a un acuerdo formal para servir como sitios alternativos entre sí, ante el caso de un desastre. En este tipo de acuerdo se requiere que la secuencia de recuperación de los sistemas de ambas organizaciones se priorice desde una perspectiva conjunta, y que esta sea favorable para ambas partes.

5. Sitio tibio (Warm Site). En esta estrategia, se parte de la base de que en esta ubicación el sitio está parcialmente configurado, generalmente constituido además de por la infraestructura indicada anteriormente para el sitio frío, por las conexiones de red y unidades de almacenamiento, pero sin los servidores.

6. Teletrabajo. Esta estrategia, sobre todo después de la pandemia de la COVID, se ha implantado en muchas de las organizaciones. Supone trabajar desde los domicilios de los trabajadores de forma remota.

7. Reubicación en otras instalaciones del grupo. Esta estrategia se puede plantear en el caso de que la organización disponga de varias ubicaciones. En el caso de desastre en una de ellas, se llevará a cabo una reubicación.

8. Sitio caliente (Hot site). Los sitios calientes son lugares que están completamente operativos en todos los aspectos, y solo requieren una pequeña parametrización de varias horas. Esta estrategia está destinada a operaciones de emergencia de un período limitado y no para un uso prolongado a largo plazo, dado que esta estrategia conlleva unos altos costes.

Plan de continuidad de negocio

La cláusula 8.4.4.1 indica que la organización debe documentar y mantener planes y procedimientos para la continuidad del negocio. Dichos planes de continuidad del negocio deben proporcionar orientación e información para ayudar a los equipos a responder ante una disrupción y ayudar a la organización en la respuesta y la recuperación. Estos planes de continuidad de negocio se crearán a partir de los BIA y las estrategias de continuidad indicadas anteriormente.

El nivel de detalle de los planes de continuidad de negocio variará de una organización a otra. Dicho nivel diferente de detalle se basará en la criticidad de los procesos, las características específicas de la organización y su complejidad.

El proceso de desarrollo de un plan de continuidad del negocio incluirá, entre otras, las siguientes actividades:

1. Nombrar a una responsable que tenga la competencia adecuada para poder desarrollar el plan.
2. Determinar la estrategia, el enfoque, el alcance y los objetivos del plan.
3. Definir el formato, la estructura y los componentes del plan.
4. Recopilar la información adecuada que se requiera para poder elaborar el plan.
5. Redactar el plan y compartirlo para su posterior consulta y revisión.
6. Publicitar el plan y difundirlo a las partes interesadas.
7. Realizar pruebas periódicas y elaborar los informes correspondientes.
8. Actualizar el plan después de las pruebas y en función de los cambios que se produzcan en la organización.

Pruebas de continuidad de negocio

Según viene definido en la cláusula 8.5, la organización llevará a cabo pruebas de contingencia que:

Sean coherentes con los objetivos de la continuidad del negocio:

- Estén basadas en escenarios apropiados bien planificados con metas y objetivos claramente definidos.
- Posibiliten el trabajo en equipo y las competencias de este.
- Validen las estrategias y soluciones de continuidad del negocio de la organización.
- Generen informes formalizados tras la realización de las pruebas que contengan resultados, recomendaciones y acciones para implementar dichas mejoras.
- Se revisen dentro del contexto de la promoción de la mejora continua.
- Se realicen en intervalos planificados, y cuando se produzcan cambios significativos en el seno de la organización o en el contexto en el cual opera.

Las pruebas constarán de las siguientes fases:

1. Planificar. Durante esta fase, los responsables del desarrollo del programa de ejercicios establecen las actividades clave que deben realizarse durante este.

2. Desarrollar. Durante esta fase, se define el propósito de la prueba, se determinan los objetivos y el alcance, y se seleccionan métodos adecuados para lograr los resultados deseados.

3. Realizar. La realización propia de la prueba de contingencia, se produce durante esta fase, en la que las actividades clave son:

- breve resumen del ejercicio y su propósito;
- información y explicación sobre las funciones y responsabilidades de las personas durante el ejercicio;
- respuesta a las preguntas de los participantes.

4. Evaluar. Se documentan y evalúan las lecciones aprendidas del ejercicio, y se hace una lista de recomendaciones que contiene acciones propuestas que ayudan a la organización a mejorar su capacidad de continuidad del negocio.

Cláusula 9. Evaluación del desempeño

En esta cláusula 9, se nos pide evaluar los siguientes apartados (indicados en negrita) y que se revisan en detalle a continuación:

Seguimiento, medición y análisis

La supervisión, la medición, el análisis y la evaluación son factores críticos en la evaluación del desempeño del SGCN. El objetivo es determinar hasta qué punto los procesos cumplen los objetivos que se han definido de forma periódica en la organización; de esta forma se comparan los niveles reales, de los definidos previamente, de tal forma que finalmente se puede evaluar si la organización cumple los objetivos.

En este apartado, en concreto, se nos piden los siguientes puntos:

1. Determinar lo que se debe medir y controlar.
2. Definir los métodos de supervisión, medición, análisis y evaluación.
3. Recopilar los datos de supervisión, medición, análisis y evaluación.
4. Realizar un análisis y una evaluación de los resultados.

Este proceso de supervisión y medición implica:

- Identificar objetivos de medición.
- Seleccionar objetos que se pueden medir.
- Establecer indicadores de desempeño.
- Evaluar si se han alcanzado los objetivos y si mejoran el sistema de gestión: se debe realizar el proceso de forma periódica.

En este punto cabe señalar como recomendable revisar la norma ISO 27004, la cual proporciona directrices para la medición del desempeño y la eficacia del SGCN.

Auditoría interna

Aunque la información de este apartado exigido por la ISO 22301 se aplica a la auditoría interna, los elementos de un programa de auditoría son los mismos tanto para las auditorías de primera, segunda como de tercera parte. Las herramientas, la metodología, procedimientos y las técnicas son esencialmente los mismos, por lo que este punto se verá en detalle en el capítulo 4, Certificación de la continuidad de negocio.

Revisión por parte de la dirección

Otra de las exigencias de cualquier sistema de gestión, y la ISO 22301, no podía ser menos, es que el sistema se revise a intervalos planificados, de tal forma que en dicha revisión por la dirección se incluyan las decisiones (conclusiones) relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el SGCN para mejorar su eficiencia y eficacia, incluyendo los siguientes puntos:

- Variaciones en el alcance del SGCN.
- Revisión del análisis del impacto, la evaluación del riesgo, las estrategias y soluciones de continuidad del negocio y los planes de continuidad del negocio.
- Revisión y modificación de procedimientos y controles para responder a cuestiones internas o externas que puedan impactar al SGCN.
- Revisión de la eficiencia de los controles.

Esta revisión por parte de la dirección debe de conservarse en un acta en la que se reflejen los aspectos indicados anteriormente como evidencias.

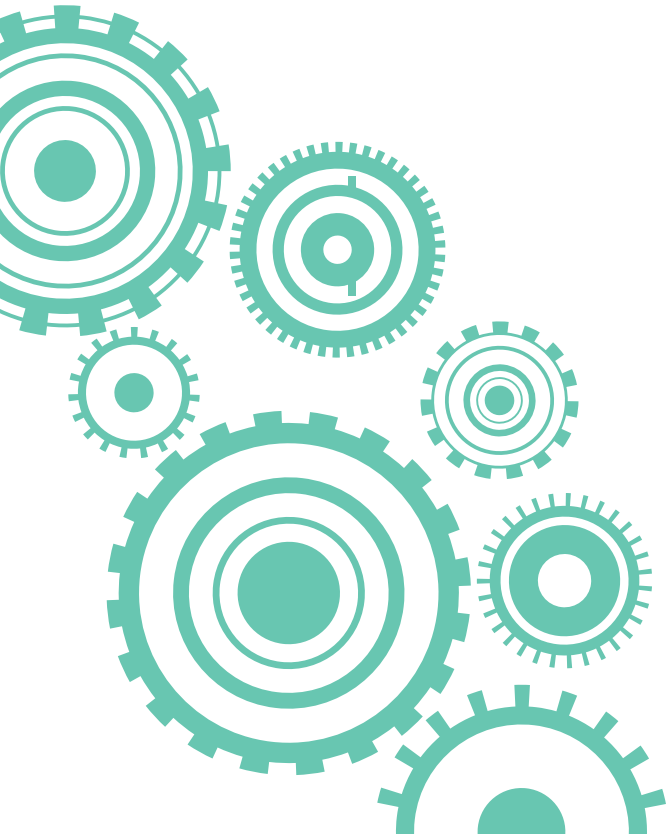
Una vez realizada dicha reunión de revisión hay que llevar a cabo las siguientes tareas:

- La dirección deberá comunicar los resultados de la revisión a las partes interesadas pertinentes.
- Adoptar las medidas apropiadas en relación con estos resultados.

Cláusula 10. Mejora

Esta es la última cláusula de la norma ISO 22301, y la de cualquier sistema de gestión. Las tareas que conllevan el cumplimiento de esta cláusula derivan de las exigencias de la norma en este punto que determina que la organización debe determinar las oportunidades de mejora e implementar las acciones necesarias para alcanzar los resultados previstos de su SGCN.

Esta cláusula corresponde con la fase Act del ciclo de Deming que hemos visto anteriormente, y viene después de la fase de Check del citado ciclo que es el que corresponde a las auditorías (tanto internas como externas), que se desarrollarán en detalle en el **capítulo 4, Certificación de la continuidad del negocio.** Como veremos en el citado capítulo, tanto en las auditorías internas, como externas, tendremos la presencia de no conformidades (incumplimiento total o parcial de las exigencias de la norma). Resolver estas no conformidades, se realizará mediante planes de acción.



En este apartado, la norma nos exige realizar las siguientes tareas:

- Creación de un procedimiento documentado para el tratamiento de las no conformidades.
- Registro de las no conformidades que pueden estar originadas por auditorías (internas y externas), clientes y proveedores.
- Planes de acción para resolver las no conformidades identificadas (recomendable un plan de acción por cada no conformidad detectada).

Bibliografía

AENOR. ISO 31000:2018. Gestión del riesgo. Directrices.
https://tienda.aenor.com/norma-une-iso-31000-2018-n0059900

AENOR. UNE-EN ISO 22301:2019. Seguridad y Resiliencia, Sistema de Gestión de la Continuidad del Negocio. Requisitos.
https://tienda.aenor.com/norma-une-en-iso-22301-2020-n0063818

España (2017). Estrategia de Seguridad Nacional.
https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021

España (2019). Estrategia Nacional de Ciberseguridad.
https://www.boe.es/buscar/pdf/2019/BOE-A-2019-6347-consolidado.pdf

INCIBE. Plan de Contingencia y Continuidad de Negocio.
https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

ISO. ISO 27001:2022. Information security, cybersecurity and privacy protection.
https://www.iso.org/standard/82875.html

2.2 INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE)

Jose Fernández Zapata

ANTECEDENTES

La finalidad de los modelos y marcos de buenas prácticas en materia de continuidad de negocio es tratar de asegurar un nivel adecuado de resiliencia en la organización, entendiendo como tal la capacidad de resistir ante una situación adversa y recuperar su estado de normal funcionamiento lo antes posible.

El desarrollo de buenas prácticas de continuidad de negocio tiene un importante componente en la gestión de los sistemas de información que soportan aquellos servicios de la organización que permiten a esta cumplir con su misión (servicios críticos), ya que el proceso de transformación digital se encuentra actualmente muy avanzado en la sociedad y esto hace que resulte casi imposible encontrar un servicio o proceso de negocio que no requiera para su desempeño del uso de las TIC.

Por lo tanto, el concepto de resiliencia aplicado a las TIC, conocido como ciberresiliencia, va a convertirse en el principal objetivo que se deberá perseguir por parte de las medidas de continuidad aplicadas a los sistemas de información.

Si tenemos en consideración el actual panorama de la ciberseguridad, cuya complejidad se ha acrecentado por la intensa actividad de grupos cibercriminales, frecuentemente respaldados en la sombra por diversos estados, el Gobierno de España adoptó en 2019 la Estrategia Nacional de Ciberseguridad en la que se establecieron diversos objetivos, líneas de acción, medidas, así como una organización de la ciberseguridad incorporada al Sistema de Seguridad Nacional.

En este escenario, uno de los principales instrumentos promovidos por el Gobierno para impulsar el uso seguro del ciberespacio en España es el Instituto Nacional de Ciberseguridad (INCIBE), convertido en un referente en materia de ciberseguridad y con actividades de investigación, prestación de servicios y coordinación con otros organismos competentes en la materia en el ámbito nacional e internacional.

MARCO CONCEPTUAL

La definición de *ciberresiliencia* establecida por el propio INCIBE es la siguiente:

> *Ciberresiliencia es la capacidad de un proceso, negocio, organización o nación de anticipar, resistir, recuperarse y evolucionar para mejorar sus capacidades frente a condiciones adversas, estrés o ataques a los recursos cibernéticos que necesita para funcionar.*

Con el objetivo de evaluar el estado de ciberresiliencia en una organización o sector, el INCIBE ha definido un marco conceptual con el cual estructurar el conjunto de métricas e indicadores necesarios para alcanzar este propósito.

Si bien se trata de un modelo de evaluación, su estructura permite obtener una visión metodológica sobre la que desplegar controles concretos en una organización. Consta de tres niveles que, de más alto a más bajo, serían los siguientes:

Metas (u objetivos generales): Declaración de los propósitos a alto nivel que se desean alcanzar, pudiendo entenderse como fases de gestión del modelo.

Dominios funcionales: Agrupación de diferentes aspectos de la ciberresiliencia que contienen conjuntos de prácticas que la organización debe desplegar.

Objetivos específicos: Modos de alcanzar una o varias metas en materia de *ciberresiliencia* y que se aplican a la arquitectura de los servicios de negocio, su diseño o a los recursos que los soportan. Son equiparables a controles o medidas.

Si tomamos los dos primeros niveles del modelo (que incluye cuatro metas y nueve dominios funcionales) obtenemos una visión esquemática del marco de trabajo de ciberresiliencia aplicable a una organización, donde cada meta se apoya en determinados dominios funcionales:

ANTICIPAR (A)	Política de ciberseguridad (PC) Gestión de riesgos (GR) Formación en ciberseguridad (FO)
RESISTIR (T)	Gestión de vulnerabilidades (GV) Supervisión continua (SC)
RECUPERAR €	Gestión de incidentes (GI) Gestión de continuidad del servicio (CS)
EVOLUCIONAR €	Gestión de la configuración y de los cambios (CC) Comunicación (CM)

Seguidamente describiremos cada uno de los anteriores elementos del modelo:

ANTICIPAR (A). Preparar la organización para proteger sus servicios (o procesos) críticos[1] frente a posibles ciberataques.

Política de ciberseguridad (PC): disponer de una política que defina los objetivos, marco legal, roles y responsabilidades, riesgos de ciberseguridad y la estructura documental de la normativa interna. Esta política debe ser formalmente aprobada por el máximo órgano de gobierno y difundida a toda la organización.

Gestión de riesgos (GR): aplicar una metodología de gestión de riesgos sobre los activos que soportan los servicios críticos que permita su identificación, análisis, evaluación y tratamiento (mitigación).

Formación en ciberseguridad (FO): promover la adquisición de conocimientos, concienciación y capacitación del personal para que pueda desarrollar su cometido en la organización manteniendo un nivel adecuado de ciberresiliencia.

[1] El INCIBE diseñó este marco para su aplicación a Operadores de Servicios Esenciales (OSE) que son los que gestionan las infraestructuras críticas para una nación, según la definición recogida en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (LPIC). Aquí se aplica el modelo a cualquier tipo de organización, por lo que toda referencia a servicios esenciales se ha reemplazado por servicios o procesos críticos (para la organización).

RESISTIR (T). Mantener operativos los servicios críticos tras sufrir un ciberataque.

Gestión de vulnerabilidades (GV): identificar, analizar y gestionar vulnerabilidades en los activos que apoyan la prestación de los servicios críticos.

Supervisión continua (SC): recopilar y distribuir elementos de información sobre el comportamiento y las actividades de los activos (incluyendo sistemas y personas), para detectar y alertar de la presencia de amenazas que puedan afectar a prestación de los servicios críticos.

RECUPERAR (R). Restaurar lo antes posible los servicios críticos cuando se han visto afectados por un ciberataque.

Gestión de incidentes (GI): implantar los procesos para la identificación y análisis de los eventos, detección de incidentes y coordinación de una adecuada respuesta por parte de la organización.

Gestión de continuidad del servicio (CS): planificar el desarrollo de las actividades destinadas a garantizar la continuidad de los servicios críticos en caso de incidente o desastre.

EVOLUCIONAR (E). Adaptar las capacidades de la organización en materia de ciberseguridad para reducir el riesgo de ciberataques.

Gestión de la configuración y de los cambios (CC): implantar los procesos para mantener la normal operación de todos los activos (tecnología, información e instalaciones) necesarios para prestar los servicios críticos.

Comunicación (CM): implantar los procesos para garantizar la comunicación entre todos los roles involucrados en la operación de los servicios críticos, sean internos o externos a la organización.

La metodología de INCIBE, teniendo presente la estructura del marco conceptual antes descrito, divide su proceso de implantación en cuatro etapas que son las siguientes:

1.Delimitación del alcance. Es imprescindible identificar los servicios críticos para la organización, es decir, aquellos cuya interrupción tendría un gran impacto para la consecución de sus objetivos.

2.Análisis (autoevaluación). Se determinará el estado de madurez en la implantación de los objetivos específicos asociados a cada dominio funcional de las diferentes metas. Se recomienda la utilización de un modelo de evaluación como CMMI[2], para establecer niveles de madurez sobre la base de una escala de evaluación de los procesos.

3.Aplicación de medidas correctivas. A partir del anterior análisis y determinando los resultados no satisfactorios para la organización, se identificarán las medidas correctivas que será necesario desplegar para alcanzar un nivel de madurez aceptable.

4.Revisión periódica. Esta etapa implementa el concepto de *mejora continua* en el modelo a través de la repetición de las etapas del proceso a intervalos regulares o cuando se hayan producido cambios relevantes en la organización.

Puesto que la materia fundamental sobre la que versa esta obra es la continuidad, dentro del modelo de INCIBE nos focalizaremos en el dominio funcional de *Gestión de la continuidad del servicio (CS)*, aunque aplicaremos todas las etapas de gestión de esta metodología.

[2] Capability Maturity Model Integration, modelo desarrollado por la Carnegie Mellon University (CMU) y administrado por el CMMI Institute, subsidiraio de ISACA: https://cmmiinstitute.com/company

Los objetivos específicos que este modelo establece dentro del dominio funcional de la continuidad son los siguientes:

- desarrollar planes de continuidad para los servicios críticos;
- revisar periódicamente dichos planes; diseñar un plan de pruebas;
- probar los planes de continuidad, analizar los resultados e introducir las acciones correctivas necesarias;
- establecer procesos para gestionar la continuidad de los servicios y activos críticos que dependen de entidades externas (clientes, proveedores y otras partes interesadas).

Cabe destacar que este modelo describe de forma estructurada qué actividades será necesario desarrollar, pero no cómo deben desplegarse, por lo que será necesario buscar guías específicas de buenas prácticas para concretar la forma de implementarlas en nuestra organización. Por este motivo el propio INCIBE dispone de diversas guías para ayudar a la implementación de los objetivos específicos relativos a un mismo dominio funcional o ámbito de aplicación.

PLAN DE CONTINUIDAD DE NEGOCIO

Como ya se ha mencionado anteriormente, el Plan de Continuidad de Negocio de una organización se apoya en gran medida, aunque no exclusivamente, en la continuidad de los sistemas de información que soportan la prestación de sus servicios críticos, por lo que realmente existen varios tipos de planes que deben desplegarse dentro de la estructura de gestión de la continuidad:

Plan de Continuidad de Negocio (PCN). Este es el plan de más alto nivel que se debe diseñar y cubre todos los aspectos con un impacto relevante en caso de producirse una indisponibilidad de estos: personal, inmuebles, proveedores, suministro de agua y energía, servicios de comunicaciones, logística, infraestructura TIC... Es, por lo tanto, un plan multidisciplinar.

Plan de continuidad TIC (PCTIC). También llamado Plan de Contingencia de Sistemas (PCS), Plan de Continuidad de Sistemas (PCS), Plan de Contingencia TIC (PCTIC)... Se trata de un plan específico para garantizar la continuidad de la operación de los sistemas de información que soportan los servicios críticos para la organización.

Plan de Recuperación ante Desastres (PRD). También conocido por sus siglas en inglés de *Disaster Recovery Plan* (DRP). Es un plan específicamente diseñado para hacer frente a un escenario de desastre en particular (incendio, inundación, huelgas, pandemia, etcétera) que pueda afectar a los sistemas de información, centrándose en las actividades, normalmente de ámbito puramente técnico, que será necesario desarrollar para restablecer su funcionamiento.

Como puede observarse, cada uno de estos planes se va focalizando sucesivamente en aspectos concretos de la continuidad: toda la organización (PCN), los sistemas de información (PCS) o la recuperación de estos en un escenario de desastre en particular (DRP). En este documento nos centraremos en los dos últimos.

El proceso de diseño e implementación de un PCN se puede dividir en seis fases, que incluyen las cuatro de gestión de la ciberresiliencia antes descritas, pero incorporando alguna más para enfatizar la importancia de determinadas actividades:

Fases PCN	Etapas de la ciberresiliencia
Determinación del alcance	Delimitación del alcance
Análisis de la organización	Análisis
Determinación de la estrategia de continuidad	Análisis
Respuesta a la contingencia	Aplicación de medidas correctivas
Prueba, mantenimiento y revisión	Revisión periódica
Concienciación	Aplicación de medidas correctivas

A continuación, vamos a detallar las actividades que se deben desarrollar en cada una de estas fases.

FASE 0. DETERMINACIÓN DEL ALCANCE

En esta fase se identificarán cuáles son los servicios de la organización soportados por el uso de las TIC que son críticos y se van a dotar de mecanismos para garantizar su continuidad en caso de incidente.

Tras identificar los servicios críticos para la organización deberemos identificar todos los activos de la organización que soportan la prestación de estos: instalaciones, personal, equipamiento, *software,* suministros, proveedores, etcétera.

También deberemos analizar la dependencia que existe entre los activos, es decir, cuáles soportan el normal funcionamiento de los demás. Un ejemplo típico es un servicio que se presta mediante la ejecución de una aplicación, que corre sobre un servidor, el cual a su vez se compone de un sistema operativo y un hardware, que se ubican en un CPD, dotado de sistemas de climatización, alimentación ininterrumpida, suministro eléctrico de la red de un proveedor, operado por personal técnico y utilizado por diversos usuarios de la organización. De esta forma se crea un árbol de dependencias que será de gran utilidad para reconocer cómo impactaría en el negocio su indisponibilidad y, posteriormente, hacer un análisis de riesgos en materia de continuidad. Esto es lo que se conoce como **enfoque por proceso** al establecer el alcance del proyecto. Se recomienda este tipo de enfoque en la mayoría de las organizaciones, ya que es muy efectivo y permite abordar el PCN como la suma de los subproyectos derivados de cada uno de los procesos críticos de la organización, simplificando así su desarrollo.

Sin embargo, existe otra posibilidad para determinar el alcance del PCN, que sería el **enfoque por activo,** consistente en focalizarse en uno o varios activos de la organización considerados relevantes para analizar las medidas de continuidad aplicables y determinar posteriormente los procesos o servicios críticos que los utilizan. Este tipo de enfoque se recomienda solamente en pequeñas organizaciones con un número de activos limitado, cuando el proyecto lo va a abordar el departamento técnico o bien en la elaboración de los DRP, ya que estos parten de un escenario concreto de desastre que permite identificar qué activos se podrían ver afectados y las medidas de recuperación aplicables.

FASE 1. ANÁLISIS DE LA ORGANIZACIÓN

Reuniones de entendimiento

Es necesario comprender y analizar cómo se desarrollan los servicios críticos de la organización; cuáles son los flujos de proceso implicados; las entradas necesarias y los productos obtenidos como salida de dichos flujos; identificación de las partes interesadas; medios y recursos empleados; activos TIC que soportan su prestación; proveedores necesarios; tipos de usuarios y clientes; qué tiempos de recuperación son aceptables en cada caso; los medios disponibles para establecer mecanismos de continuidad..., en definitiva, toda la información necesaria para, posteriormente, establecer los requerimientos que deberá satisfacer la solución de continuidad idónea para cada servicio de la organización.

Para ello deberán mantenerse reuniones con los responsables y con el resto de personal implicado en el desarrollo de los procesos y servicios críticos, ya que son los principales conocedores de las características de los servicios que desarrollan cotidianamente.

Análisis de impacto en el negocio

Habitualmente conocido por sus siglas en inglés Business Impact Analisys (BIA), es una tarea fundamental en el proceso de implantación de un PCN, consistente en la determinación de los requerimientos temporales de recursos asociados a la prestación de un servicio:

Recursos necesarios:

- **Humanos.** Hay personal crítico (de difícil o imposible reemplazo) que interviene en la prestación de un servicio bien sea por su capacitación y conocimiento (know-how o saber hacer) o bien por las restricciones de personal en la organización.
- **Tecnológicos.** Aplicaciones, servicios web, correo electrónico, servidores, estaciones de trabajo, impresoras...
- **Físicos.** Oficinas, maquinaria, suministros...
- **Información.** Toda aquella información necesaria para prestar el servicio deberá ser protegida para poder restablecerla en caso necesario.
- **Proveedores.** Hay que identificar a los proveedores críticos, es decir, aquellos sin los cuales no es posible prestar el servicio y dotarnos de medios para hacer frente a su discontinuidad.

RTO (Recovery Time Objective): es el máximo período durante el cual una organización puede asumir la caída de un servicio sin que haya consecuencias perjudiciales para el negocio.

RPO (Recovery Point Objective): es el máximo período durante el cual una organización puede asumir la pérdida de datos de un servicio sin consecuencias inaceptables para el negocio. También puede definirse como el máximo volumen de datos de un servicio cuya pérdida puede asumir una organización sin consecuencias inaceptables para el negocio.

MTD (Maximum Tolerable Downtime): es el máximo periodo durante el cual puede estar caído un servicio antes de que se produzcan efectos desastrosos en la organización y repercuta en el negocio.

ROL (Revised Operating Level): es el nivel mínimo de operación que debe alcanzar un servicio para que se considere recuperado, aunque el nivel de operación no sea el óptimo.

Dependencias: para la prestación del servicio hay que considerar la posible existencia de una relación de dependencia con otros servicios de la organización o con los servicios prestados por un proveedor, en cuyo caso habrá que incluirlos en los planes de recuperación.

Toda la información de un BIA se recoge a través de entrevistas con los responsables del servicio analizado, es decir, los parámetros de recuperación se establecen desde las áreas de negocio, no desde las áreas tecnológicas.

Los activos que son necesarios para la prestación del servicio deberán ser identificados y se les deberá dotar de una alternativa en caso de indisponibilidad. En todo caso, habrá que aportar soluciones de continuidad que garanticen la prestación del servicio según los requerimientos definidos por sus responsables (nunca al revés).

Un ejemplo podría ser un servicio de atención al cliente (SAC). Durante el BIA, elaborado mediante una entrevista al jefe del SAC se determinan los requerimientos de continuidad:

Recursos:

- **Humanos:** un turno único de personal compuesto por diez operadores y un coordinador que trabajan en horario de 08:00 a 15:00.
- **Tecnológicos:** once estaciones de trabajo, una aplicación de gestión de incidencias, once extensiones telefónicas, una centralita con distribución automática de llamadas y correo electrónico.
- **Físicos:** las oficinas donde trabaja el personal (con su mobiliario y servicios de agua y energía).

- **Información:** toda la BBDD de clientes e incidencias alojada en el sistema de información del SAC.
- **Proveedores:** operador de servicios de telefonía.

Nótese que el responsable desconoce la estructura de activos tecnológicos que soportan a los que ha sabido identificar, esa será labor del personal del área TIC, que es quien conoce esa información (servidores, infraestructura de comunicaciones, entornos de virtualización, cabinas de almacenamiento...).

RTO: en caso de disrupción del servicio, este debe recuperarse en menos de cuatro horas o de lo contrario los daños reputacionales y económicos a la organización serían relevantes.

RPO: se asume una pérdida de datos tras la recuperación del servicio que suponga volver al estado existente a la finalización de la jornada anterior (8 horas).

MTD: en cualquier caso, una parada del servicio superior a dos días sería desastroso en criterios de daños a la imagen de la organización e impacto económico por pérdida de clientes y lucro cesante.

ROL: con cinco de los diez operadores se puede mantener un nivel de servicio aceptable para continuar su prestación, aunque la capacidad de atención a los clientes se vería reducida.

Dependencias: existe una total dependencia del operador de servicios de telefonía para poder ofrecer el servicio SAC.

Con esta información queda clara la necesidad de disponer de mecanismos de recuperación capaces de completarse en menos de cuatro horas y que empleen copias de seguridad realizadas el día anterior. En caso de indisponibilidad de alguno de los otros recursos, habría que disponer de alternativas de funcionamiento en menos de dos días.

Deberán contemplarse acuerdos de nivel de servicio mínimo que se deba ofrecer por parte del operador de telefonía, y para ello se exigirá un compromiso contractual que incluya mediciones del nivel de servicio prestado y penalizaciones en caso de incumplimiento.

Análisis de riesgo

El siguiente paso en la fase de análisis de la organización sería llevar a cabo un análisis de riesgos. No entraremos en detalle puesto que no es el objetivo de este documento y hay muchas fuentes de consulta para esta cuestión.

Solamente haremos énfasis en la importancia de confeccionar un catálogo de amenazas derivado de la identificación de las amenazas a la continuidad en la prestación del servicio, bien a través del propio conocimiento y experiencia, bien por el empleo de catálogos confeccionados.

Posteriormente se procederá como en cualquier metodología de análisis de riesgos, es decir, categorizando las amenazas mediante probabilidad de suceso e impacto en la organización, con lo que obtendremos el riesgo potencial.

Con la reducción del riesgo introducida por las medidas de continuidad (controles) desplegadas obtendremos un riesgo residual que se evaluará frente al apetito de riesgo definido en la organización para determinar si es aceptable o si debe ser tratado (las cuatro estrategias frente al riesgo son: transferir, eliminar, asumir o mitigar).

FASE 2. DETERMINACIÓN DE LA ESTRATEGIA DE CONTINUIDAD

Una vez identificados los requerimientos de continuidad y los riesgos asociados a los servicios críticos, es necesario determinar si, cuando se produzca una interrupción, disponemos en la organización de los medios de recuperación adecuados para respetar dichos requerimientos y tratar los riesgos.

En los casos en los que no sea así, habrá que estudiar las estrategias de recuperación que es posible establecer y adoptar la más adecuada. Básicamente se tratará de hacer un análisis diferencial entre los medios existentes y los que serían necesarios, de forma que se identifiquen los medios a incorporar y puedan diseñarse los proyectos de mejora de la continuidad que deberán abordarse para implantar tales medios.

FASE 3. RESPUESTA A LA CONTINGENCIA

Tras definir las estrategias de recuperación, habrá que planificar el despliegue de las medidas necesarias para implementar dichas estrategias, diseñar un plan de crisis y documentarlo junto con el resto de procedimientos necesarios para la recuperación de los sistemas.

Se clasificarán y priorizarán las medidas que se deban implantar, organizándolas en proyectos abordables en función de la disponibilidad de recursos, dotación económica, coste, beneficios obtenidos, etcétera (siguiendo cualquier metodología de gestión de proyectos).

Una parte esencial de esta fase es la elaboración de toda la documentación asociada al desarrollo del PCS.

Plan de crisis (o plan de incidentes)

Este será el documento que guíe al personal de la organización involucrado en el proceso de recuperación de un servicio. Cuando se produce un incidente que afecta a la continuidad del negocio, no es el momento de ponerse a improvisar o probar cosas para ver si funcionan o no. En su lugar hay que tener todas las actividades perfectamente definidas en la documentación de forma que, por si sola, la información que contiene baste para ejecutar el proceso de recuperación, incluso si es desarrollado por personal ajeno a la organización (proveedores, personal voluntario, instituciones tipo CERT, etcétera).

Los elementos fundamentales que debe contemplar un plan de crisis son:

- disparadores. Condiciones que determinan la existencia de una situación de crisis y el consiguiente inicio de las actividades del plan (por ejemplo, la superación, el MTD de un servicio);
- flujos de actividad y de toma de decisiones;
- medios de comunicación y escalado para declarar la situación de crisis;
- personal responsable de la activación y gestión del plan;
- datos de contacto de todo el personal involucrado en la gestión de la crisis;
- priorización para la recuperación de los diferentes activos afectados;
- requisitos temporales para la puesta en marcha;
- planes operativos y personal responsable de su activación.

Planes operativos de recuperación de entornos

Se trata de planes para restablecer el funcionamiento de un entorno en particular, entendiendo como tal el conjunto de activos que soportan la prestación de un servicio TIC concreto, como, por ejemplo, el ERP corporativo, el servicio de correo electrónico, el sistema de gestión de recursos humanos, el sistema de telefonía, etcétera.

Tras el disparo de una situación de crisis, el plan de crisis se pondrá en marcha, incluyendo la determinación de su alcance y los entornos afectados, y se iniciará la ejecución de los planes operativos de recuperación que sean necesarios.

Los planes operativos de recuperación se basan a su vez en documentos más sencillos denominados procedimientos técnicos de trabajo.

Procedimientos técnicos de trabajo (o procedimientos de gestión de incidentes)

Son procedimientos técnicos operativos con instrucciones para la recuperación de determinados activos, como puedan ser un servidor, una BBDD, un enrutador, una aplicación, etcétera.

No son documentos circunscritos a la continuidad del negocio, sino que se emplean en las actividades de operación de los sistemas de información, pero cobran gran relevancia en situaciones de crisis.

Su contenido es eminentemente técnico y está pensado para su uso por parte de personal especializado.

FASE 4. PRUEBA, MANTENIMIENTO Y REVISIÓN

Tras diseñar el plan de crisis frente a contingencias, deberán desarrollarse unos planes de prueba y mantenimiento que permitan evaluar la capacidad de la organización y la efectividad de la respuesta para poner de manifiesto cualquier insuficiencia y corregirla antes de que sea necesario afrontar una incidencia real.

Plan de mantenimiento

Para el correcto funcionamiento de un plan de crisis es vital que la información que contiene esté actualizada, por lo que deberá reflejarse de inmediato cualquier cambio en el personal involucrado, sus datos de contacto, los datos contenidos en los planes operativos (si, por ejemplo, se cambia la infraestructura que soporta un entorno), etcétera.

Descubrir la existencia de un error en los planes en un momento de crisis tiene impacto en su ejecución. Hasta que se consigue detectar y corregir el error, se va a producir una pérdida de tiempo que puede afectará a la consecución de los objetivos temporales de recuperación establecidos por la organización.

Por ello, deberá establecer un plan para la revisión y mantenimiento de la documentación a intervalos preestablecidos y cada vez que se haya producido un cambio que afecte a su desarrollo.

Plan de pruebas

Por otra parte, el mejor y más concienzudo de los diseños no puede considerarse válido si no ha sido puesto a prueba. Para ello se diseñará un plan de pruebas que establezca la realización periódica de pruebas de funcionamiento de distintos aspectos del PCN: escenarios de desastre, entornos para recuperar, coordinación con proveedores críticos...

Para la planificación de las pruebas hay algunos aspectos fundamentales que considerar:

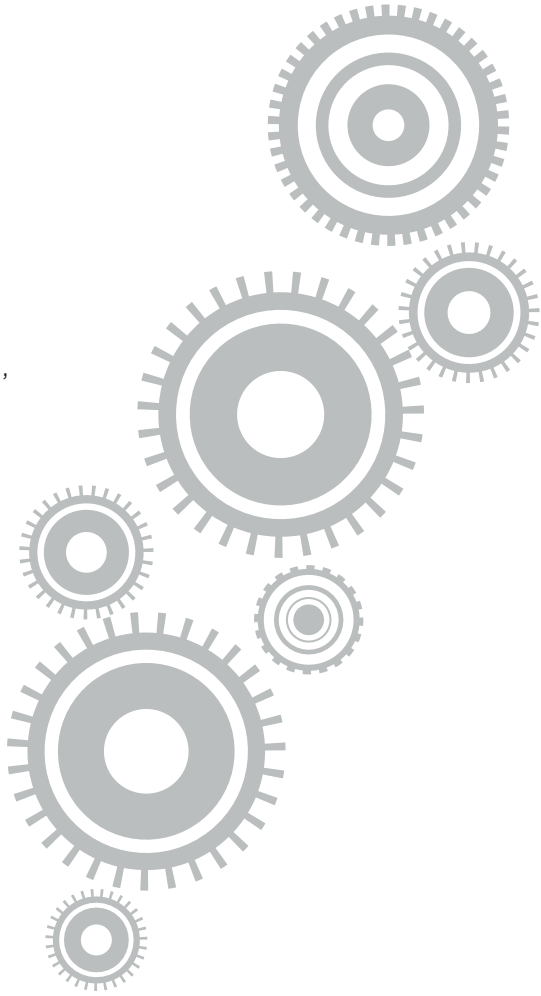
- personal técnico implicado en las pruebas;
- usuarios de la aplicación, servicio o entorno que participarán;
- personal externo (clientes, proveedores, etcétera) involucrado;
- descripción de la prueba que se deba realizar;
- resultado esperado;
- ventana de tiempo para la prueba (fecha y hora de inicio y de fin), ya que puede haber una pérdida de servicio y debe minimizarse el impacto.

Durante el desarrollo de la prueba debe recogerse toda la información relativa a posibles inexactitudes u omisiones en la documentación, detección de fallos o problemas, cronología de actividades, resultados obtenidos, deficiencias de comunicación interna o con personal externo, etcétera.

Con toda esa información se redactará un informe que deberá incluir, además, recomendaciones de mejora, acciones correctivas y lecciones aprendidas.

Algunos ejemplos de pruebas:

- fallo de suministro eléctrico;
- recuperación de una aplicación o entorno con las
- copias de seguridad existentes;
- conmutación de sistemas replicados (clústeres o incluso CPD redundantes si los hay).



FASE 5. CONCIENCIACIÓN

Además del análisis, diseño, implantación y pruebas del PCN, es imprescindible una labor divulgativa para dar a conocer sus objetivos y responsabilidades a todos los miembros de la organización, sin olvidar las particularidades que aplican al desarrollo del PCN en el equipo técnico, en el equipo directivo y también a la plantilla en general.

Esta labor de concienciación debe incluir actividades para la familiarización del personal con los conceptos propios de la gestión de la continuidad (PCN, PCS, DRP, plan de crisis...), así como su participación en pruebas.

Bibliografía

AENOR. ISO 31000:2018. Gestión del riesgo. Directrices.
https://tienda.aenor.com/norma-une-iso-31000-2018-n0059900

España (2017). Estrategia de Seguridad Nacional.
https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021

España (2019). Estrategia Nacional de Ciberseguridad.
https://www.boe.es/buscar/pdf/2019/BOE-A-2019-6347-consolidado.pdf

INCIBE (2014). CIBERRESILIENCIA: Aproximación a un marco de medición.
https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/int_ciber_resiliencia_marco_medicion.pdf

INCIBE (2016). Guía de almacenamiento seguro de la información. Una guía de aproximación al empresario.
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad_0.pdf

INCIBE (2020). IMC_01 - Metodología de evaluación de indicadores para mejora de la ciberresiliencia (IMC).
https://www.incibe-cert.es/sites/default/files/contenidos/guias/IMC/imc_01_metodologia-evaluacion.pdf

INCIBE (2020). IMC_02 - Diccionario de indicadores para mejora de la ciberresiliencia (IMC).
https://www.incibe-cert.es/sites/default/files/contenidos/guias/IMC/imc_02_diccionario-indicadores.pdf

INCIBE. Checklist de buenas prácticas de los departamentos de TI.
https://www.incibe.es/sites/default/files/contenidos/dosieres/buenas-practicas-area-informatica/checklist-buenas-practicas.pdf

INCIBE. Contratación de servicios.
https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_contratacion_de_servicios.pdf

INCIBE. Plan de Contingencia y Continuidad de Negocio.
https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

MITRE (2012). Cyber Resiliency Engineering Framework.
https://www.mitre.org/sites/default/files/2021-11/prs-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf

2.3

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Jose Fernández Zapata

ANTECEDENTES

Consciente de que la irrupción de las tecnologías de la información llevaba aparejada de forma inherente nuevas amenazas específicas, el Gobierno de los EE.UU., ya en al año 1972, decidió establecer su programa de seguridad informática a través del National Bureau of Standards (NBS), que en 1988 pasó a denominarse National Institute of Standards and Technology (NIST), que es como se conoce actualmente a este organismo.

La evolución de las TIC y, por lo tanto, de las ciberamenazas, han convertido al ciberespacio en otro escenario de actuación de criminales y terroristas, lo que ha dado lugar a conceptos como *ciberseguridad, cibercrimen, ciberterrorismo, ciberguerra, ciberdefensa*..., es decir, se han trasladado todos los elementos y planos de actuación relativos a la seguridad, el crimen y la defensa desde el ámbito físico al ámbito cibernético.

Para plantear una mejor defensa frente a las ciberamenazas por parte de las organizaciones y, especialmente, de los sistemas de información que soportan infraestructuras críticas para la sociedad, en 2014, el Gobierno de EE.UU. atribuyó al NIST la función de desarrollar un marco de ciberseguridad de aplicación voluntaria, partiendo del trabajo previamente desarrollado en 2013 que se plasmó en la versión 1.0 del marco.

En el año 2018 se publicó la versión 1.1 del marco que es la vigente y que describiremos a continuación.

MARCO DE CIBERSEGURIDAD

Con el nombre completo de Marco para la mejora de la seguridad cibernética en infraestructuras críticas, se ha construido una metodología formada por tres clases de componentes:

- núcleo;
- niveles de implementación;
- perfil.

NÚCLEO

Se trata de un conjunto de actividades, resultados deseados y referencias aplicables a las organizaciones para la mejora de su postura de ciberseguridad. Se basa en la aplicación de las buenas prácticas de la industria de un modo que permite el alineamiento de las actividades y los resultados en materia de ciberseguridad en toda la organización, desde los órganos de dirección hasta el personal técnico.

El núcleo del marco consta de cuatro niveles que, del más alto al más bajo, están constituidos por los siguientes elementos:

Funciones. Determinan las actividades que se deben desarrollar en el mayor nivel de abstracción del marco. Están íntimamente ligadas a las fases de gestión de las amenazas de ciberseguridad que debe implementar un sistema, es decir:

Identificar (ID). Resulta imprescindible tener un conocimiento del contexto de la organización para poder identificar los aspectos clave que van a condicionar la ciberseguridad: misión y objetivos de la organización, estructura de roles y responsabilidades, medios necesarios para el desarrollo del cometido de la organización, marco normativo aplicable (legal, sectorial, contractual e interno), amenazas...

Proteger (PR). Esta función está orientada al despliegue de las medidas de seguridad preventivas que resulten adecuadas para garantizar la prestación de servicios críticos. Por lo tanto, en esta función se contemplan medidas con capacidad para limitar la probabilidad de suceso de un evento de ciberseguridad.

Detectar (DE). Abarca el despliegue de medidas de seguridad preventivas, o sea, destinadas a identificar la ocurrencia de un evento de ciberseguridad.

Responder (RS). Una vez que se ha producido un evento de ciberseguridad, habrá que contar con medidas de seguridad destinadas a contener el impacto y erradicar la amenaza.

Recuperar (RC). Esta es la función más directamente relacionada con el concepto de *ciberresiliencia*, ya que su propósito es el de recuperar el normal funcionamiento del sistema tras haber sufrido el impacto de un incidente, devolviendo a la organización a su estado de plena operatividad.

Categorías. Constituyen el siguiente nivel de marco de ciberseguridad, dividiendo cada función en ámbitos de ciberseguridad más concretos para el desarrollo de sus actividades: gestión de activos (ID.AM), formación y concienciación (PR.AT), monitorización continua (DE.CM), planificación de la respuesta (RS.RP)...

Subcategorías. Establecen un nivel de concreción más específico dentro de cada categoría del marco, y definen un conjunto de resultados que, aun no siendo exhaustivos, ayudan a determinar las medidas de seguridad necesarias. Algunos ejemplos: «Los sistemas de información externos se catalogan» (ID.AM-4); «Los datos en reposo se protegen» (PR.DS-1); «Las notificaciones de los sistemas de detección se investigan» (RS.AN-1)...

Referencias informativas. El último nivel de la estructura del marco está formado por una selección de controles aplicables a cada subcategoría para alcanzar los resultados que definen. Proceden de diversas fuentes reconocidas internacionalmente, como normas, directrices y prácticas comunes en materia de ciberseguridad. No deben considerarse las

referencias informativas identificadas en el núcleo del marco como un conjunto exhaustivo y limitativo, sino como una orientación que puede ser enriquecida con cualesquiera otros controles que puedan resultar adecuados para las subcategorías en las que se incluyan.

La estructura completa con todos los niveles del marco y la codificación de cada uno de sus elementos puede descargarse del sitio web de NIST.[1]

Niveles de implementación

Otro de los componentes del marco de ciberseguridad, junto al núcleo anteriormente descrito, es el conjunto de niveles de implementación, que permiten valorar el grado de gestión del riesgo en materia de ciberseguridad.

Se tendrán en cuenta tres perspectivas para determinar el nivel de implementación de las medidas de seguridad:

- gestión de riesgos de ciberseguridad;
- programa integrado de gestión de riesgos empresariales (ERM);
- terceras partes (proveedores, clientes, etc.).

El marco emplea cuatro niveles (similares a los del modelo CMMI) para describir el grado de implementación:

Nivel 1: Parcial. Los procesos no están formalizados y los riesgos se gestionan de forma específica y reactiva.

Nivel 2: Riesgo informado. Se informa de los riesgos detectados de manera informal.

Nivel 3: Repetible. La gestión de riesgos se formaliza y se concreta a través de normativa interna, y existe, además, un proceso de actualización periódica.

Nivel 4: Adaptable. Las medidas de ciberseguridad se adaptan a partir de lecciones aprendidas y la recopilación de métricas e indicadores. Existe un proceso de mejora continua y la organización se adapta al escenario cambiante de amenazas.

[1] https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx

Perfil

El último componente del marco de ciberseguridad es el perfil, que es un instrumento que permite alinear el núcleo con los requerimientos de la organización, el apetito de riesgo (o tolerancia al riesgo) y los recursos disponibles. Gracias a esto, las organizaciones podrán utilizar el perfil para establecer una hoja de ruta hacia una postura de seguridad adecuada, y para ello desplegarán las mejores prácticas de la industria. Los criterios de alineamiento con el negocio son tres:

- los objetivos de negocio;
- el marco normativo aplicable en materia de ciberseguridad, y
- las amenazas identificadas.

En la práctica, la elaboración de un perfil se realizará como una tabla en cuyas filas dispondremos los elementos del núcleo (funciones, categorías y subcategorías) y en sus columnas los requisitos derivados de los tres criterios antes mencionados para conseguir el alineamiento con las necesidades de la organización. En cada celda de la tabla se identificará el nivel de implementación de la correspondiente subcategoría (descrita en la fila) necesario para alcanzar la postura de ciberseguridad que responda adecuadamente a cada necesidad de la organización (descrita en la columna). Si una categoría no es adecuada para conseguir un requerimiento, en la correspondiente celda se indicará un «no aplica» o un nivel de implementación nulo («Nivel 0»).

A continuación, se muestra un ejemplo de perfil en su fase de desarrollo, donde se está completando el nivel de implementación para cada requerimiento:

Núcleo del marco			Objetivos de negocio			Amenazas			Requerimientos normativos		
Función	Categoría	Subcategoría	O1: Ofrecer una óptima seguridad para las personas	O2: Mantener un nivel de resiliencia adecuado	O3: Atender eficientemente a los clientes	A1: Fuga de información sensible	A2: Interrupción de los servicios	A3: Ransomware	R1: ENS	R2: RGPD/LOPDgdd	R3: Di
IDENTIFICAR (ID)	Gestión de activos (ID.AM)	ID.AM-1	Nivel 2								
		ID.AM-2	Nivel 2								
		ID.AM-3	Nivel 2								
		ID.AM-4	Nivel 2								
		ID.AM-5	Nivel 4								
		ID.AM-6	Nivel 4								
	Entorno empresarial (ID.BE)	ID.BE-1									
		ID.BE-2									
		ID.BE-3									
		ID.BE-4									
		ID.BE-5									
	Gobernanza (ID.GV)	ID.GV-1									
		ID.GV-2									
		ID.GV-3									
		ID.GV-4									
		ID.RA-1									

Se suelen generar dos tipos de perfiles:

Perfil actual. Recoge los niveles de implementación desplegados en la organización en el momento actual.

Perfil objetivo. Plantea los niveles considerados por la organización como adecuados para satisfacer todos los requerimientos y establece el objetivo que debe alcanzarse.

El plan de adecuación en materia de ciberseguridad que la organización deberá acometer y en el cual se incluirán todas las actividades que se deban desarrollar, se obtendrá de un análisis diferencial de ambos perfiles.

PLAN DE CONTINUIDAD DE NEGOCIO

Tras la descripción del marco de ciberseguridad, su aplicación al ámbito de la continuidad viene determinado por aquellos elementos del núcleo que tienen impacto en esta disciplina.

Si bien hay subcategorías relacionadas con la continuidad, pero que son más transversales en la gestión de la ciberseguridad (como la identificación del entorno, la evaluación de riesgos, la formación y concienciación, etc.), hay algunas cuya aplicación está íntimamente relacionada con la gestión de la continuidad, y podrían destacar las siguientes:

SUBCATEGORÍAS
PR.IP-4. Se realizan, se mantienen y se prueban copias de seguridad de la información.
PR.IP-9. Se encuentran establecidos y se gestionan planes de respuesta (respuesta a incidentes y continuidad del negocio) y planes de recuperación (recuperación de incidentes y recuperación de desastres).
PR.IP-10. Se prueban los planes de respuesta y recuperación.
PR.PT-5. Se implementan mecanismos (por ejemplo, a prueba de fallos, equilibrio de carga, cambio en caliente o hot swap) para lograr los requisitos de resiliencia en situaciones normales y adversas.
RS.RP-1. El plan de respuesta se ejecuta durante o después de un incidente.
RS.CO-1. El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.
RS.CO-3. La información se comparte de acuerdo con los planes de respuesta.
RS.CO-4. La coordinación con las partes interesadas se lleva a cabo en consonancia con los planes de respuesta.
RS.CO-5. El intercambio voluntario de información se produce con las partes interesadas externas para lograr una mayor conciencia situacional de seguridad cibernética.
RS.IM-1. Los planes de respuesta incorporan las lecciones aprendidas.
RS.IM-2. Se actualizan las estrategias de respuesta.
RC.RP-1. El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.
RC.IM-1. Los planes de recuperación incorporan las lecciones aprendidas.
RC.IM-2. Se actualizan las estrategias de recuperación.
RC.CO-3. Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.

Por otra parte, el marco establece una estructura y una metodología, concretando **qué** es lo que se debe hacer, pero dejando en manos de la organización **cómo** desarrollar las actividades identificadas como necesarias, si bien se dan unas referencias informativas relativas a otros conjuntos de buenas prácticas que pueden orientar en su aplicación.

A tal fin, NIST desarrolla en el desempeño de sus funciones mucha documentación de ayuda en el ámbito de la ciberseguridad, incluyendo guías de referencia sobre aspectos concretos que suelen denominarse *Special Publications,* de libre distribución y descarga (en ocasiones traducidas a varios idiomas) cuya consulta es muy recomendable (véase la bibliografía de este documento).

Por lo que respecta a la metodología para establecer un plan de continuidad de sistemas (PCS),[2] NIST considera la existencia de siete etapas en el proceso:

1. Desarrollar la política de continuidad de sistemas.
2. Efectuar un análisis de impacto en el negocio (BIA).
3. Identificar controles preventivos.
4. Crear estrategias de continuidad.
5. Desarrollar un plan de continuidad de sistemas.
6. Establecer pruebas, formación y ejercicios del plan.
7. Realizar un mantenimiento del plan.

En los siguientes apartados desarrollaremos las diferentes etapas del proceso en las que describiremos el conjunto de actividades asociadas a cada una de ellas.

DESARROLLAR LA POLÍTICA DE CONTINUIDAD DE SISTEMAS

En esta primera etapa se abordará el desarrollo de una política de continuidad de sistemas, cuyo principal objetivo es definir y comunicar a toda la organización y a sus partes interesadas, el compromiso de la gerencia con la implantación de buenas prácticas, el planteamiento estratégico que se debe seguir y los requerimientos identificados en materia de continuidad.

[2] Hay algunos conceptos muy empleados en materia de continuidad que son de uso común y que, puesto que se han mencionado anteriormente, no se van a definir de nuevo: PCN, PCS, DRP, RTO, RPO, MTD, BIA...

No obstante, un PCS se integra como una parte del PCN, que contempla todas las perspectivas y escenarios posibles con impacto en el cumplimiento de la misión de la organización, por lo que, generalmente, más que una política de continuidad de sistemas, se diseñará una política de continuidad del negocio, la cual incluirá aspectos relativos a la continuidad de los sistemas. Por esta misma razón el PCS se coordinará con el desarrollo de otros planes del PCN, como el Plan de continuidad de operaciones, Plan de recuperación ante desastres (DRP), Plan de comunicación...

Para que sea realmente efectivo y asegurarse de que el personal comprenda completamente los requisitos del PCS de la organización, estos deben recogerse en el PCN que, a su vez, debe basarse en una política claramente definida. La política debe contener los objetivos de continuidad generales de la organización y ser respaldada, tanto en su divulgación como en su desarrollo, por el máximo órgano de representación de la organización.

En la metodología NIST, los elementos clave de la política son los siguientes:

- *Funciones y responsabilidades.*
- *Alcance.* Como una breve descripción de normas, servicios, funciones, sistemas o cualesquiera otros elementos que definan claramente el ámbito al que se aplica.
- *Requerimientos de recursos.* Normalmente expresados como el apoyo y compromiso de la dirección para dotarse de los recursos que puedan ser necesarios.
- *Requisitos de formación.*
- *Programas de ejercicios y pruebas.*
- *Programa de mantenimiento del plan.*
- *Frecuencia mínima de copias de seguridad y almacenamie*
  medios de copia de seguridad.

EFECTUAR UN ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)

El BIA permite identificar los procesos y servicios críticos para la organización, los elementos de los sistemas de información que los sustentan y la relación de dependencia de los primeros respecto a los segundos, lo que permite establecer de este modo el impacto derivado de una indisponibilidad.

El desarrollo del BIA se divide en tres pasos:

1. **Identificar los servicios críticos y la criticidad de su recuperación.** Es decir, identificar los servicios críticos para el negocio cuya prestación está soportada por los sistemas de información, y determinar además el nivel de criticidad de su recuperación en caso de producirse una interrupción. Se asocia el impacto de una interrupción del sistema con el tiempo de inactividad. Deberá reflejarse el tiempo máximo de interrupción que la organización puede tolerar mientras mantiene la misión.

2. **Determinar las necesidades de recursos.** Para establecer unos objetivos de recuperación realistas es necesaria una evaluación exhaustiva de los recursos necesarios para reanudar los servicios críticos en el menor tiempo posible. Los recursos que deben identificarse incluyen instalaciones, personal, equipo, *software*, archivos de datos, componentes del sistema y registros vitales.[3]

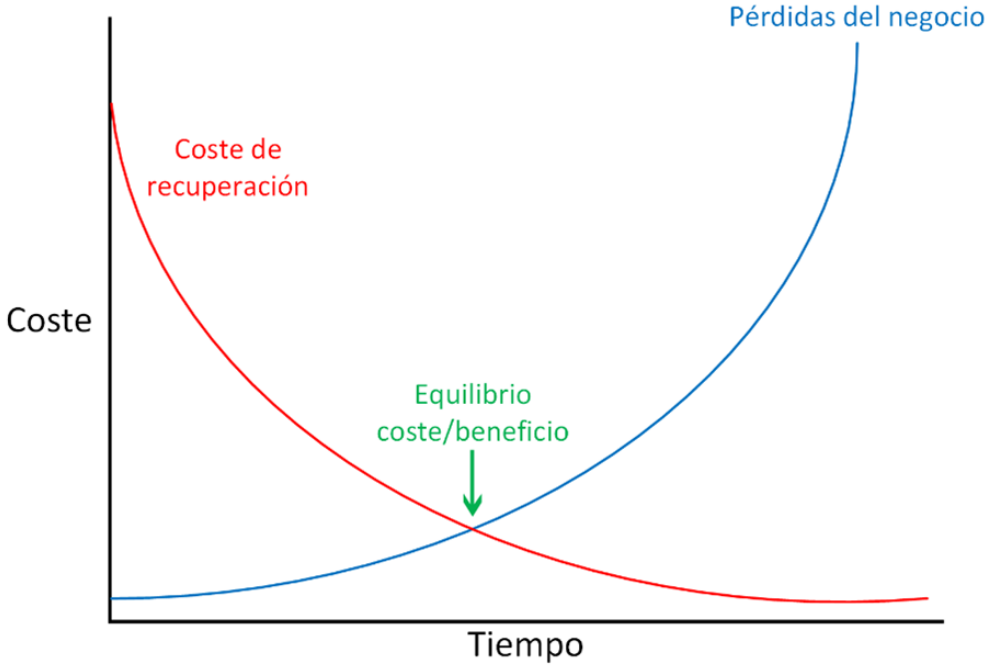
3. **Establecer las prioridades de recuperación para los recursos del sistema.** Sobre la base de los resultados de las actividades anteriores, los recursos del sistema se pueden vincular más claramente a los servicios críticos. Se deben establecer prioridades para secuenciar adecuadamente las actividades de recuperación y los recursos dedicados.

[3] Un registro vital se define como cualquier información registrada, independientemente del formato (papel, fotografía, base de datos, archivo electrónico, etc.), que la organización requiere para poder desarrollar su cometido y que cumple con las siguientes características:
1. es exclusiva de la organización;
2. es imposible de reproducir;
3. es crítica para preservar el estado normal de operación de la organización;
4. es necesaria para restablecer su normal operación tras un desastre.

Si se destruye, la pérdida de un registro vital tendría graves consecuencias para la organización.

En relación con el BIA aparecen de nuevo los conceptos de MTD, RTO y RPO que ya se han definido en anteriores apartados de este documento. Simplemente cabe resaltar la importancia de hacer un análisis coste/beneficio derivado de la aplicación de medidas de recuperación frente al tiempo requerido para recuperar el sistema en caso de disrupción.

Cuando menores sean los requerimientos para el tiempo de recuperación, más pérdidas habrá para el negocio, pero más económico resultará el despliegue de las medidas de recuperación. Por el contrario, cuando mayores sean los requerimientos, menos pérdidas sufrirá el negocio, pero más costosas serán las medidas. Buscar un punto de equilibrio ayudará a determinar qué requerimientos de recuperación son razonables y qué medidas de recuperación serán las más apropiadas (véase la relación descrita más adelante).



IDENTIFICAR CONTROLES PREVENTIVOS

Los impactos en la organización derivados de las interrupciones a sus servicios críticos pueden tratarse mediante el despliegue en el sistema de medidas preventivas (preventivas, disuasorias y eliminatorias) y detectivas. Siempre y cuando sean factibles y rentables, las medidas preventivas son preferibles a las medidas correctivas y de recuperación que pueden ser necesarias para devolver el sistema a su estado de normal funcionamiento después de una interrupción.

En esta actividad de identificación de controles preventivos deben considerarse las medidas efectivas de planificación de la continuidad, así como su mantenimiento de forma continua. Algunas medidas comunes se enumeran a continuación:

- Sistemas de alimentación ininterrumpida (SAI) con un dimensionamiento adecuado (potencia y tiempo de reserva) para proporcionar alimentación de respaldo a corto plazo a todos los componentes del sistema (incluidos los dispositivos de climatización y de seguridad).
- Grupos electrógenos para proporcionar alimentación de respaldo a largo plazo.

  Sistemas de aire acondicionado de potencia adecuada para evitar fallos en ciertos componentes por exceso de temperatura.
- Sistemas de extinción de incendios.
- Detectores de fuego y humo.
- Sensores de agua en el techo y suelo del CPD.
- Contenedores resistentes al calor y al agua para medios de respaldo y registros vitales no electrónicos.
  Interruptor de apagado de emergencia del sistema principal.
- Almacenamiento externo de medios de respaldo, registros no electrónicos y documentación del sistema.
- Controles técnicos de seguridad, como la gestión de claves criptográficas.
- Frecuentes copias de seguridad programadas, incluyendo una ubicación segura para almacenar las copias (en local y en remoto) y con qué frecuencia se reciclan los soportes y se mueven al almacenamiento.

CREAR ESTRATEGIAS DE CONTINUIDAD

Si somos conscientes de la enorme dependencia de las TIC que actualmente tiene la prestación de servicios y procesos de negocio en cualquier organización, es imprescindible gestionar los riesgos asociados al uso de sistemas de información.

Para ello hay que aplicar una metodología que, en el caso de NIST, se desarrolla en tres guías:

- NIST SP 800-53A. Contiene el catálogo de controles de ciberseguridad organizados por familias.
- NIST SP 800-37. Describe la metodología de análisis de riesgos.
- FIPS PUB 199. Establece el proceso de categorización de un sistema de información, el cual determinará el conjunto de controles aplicables.

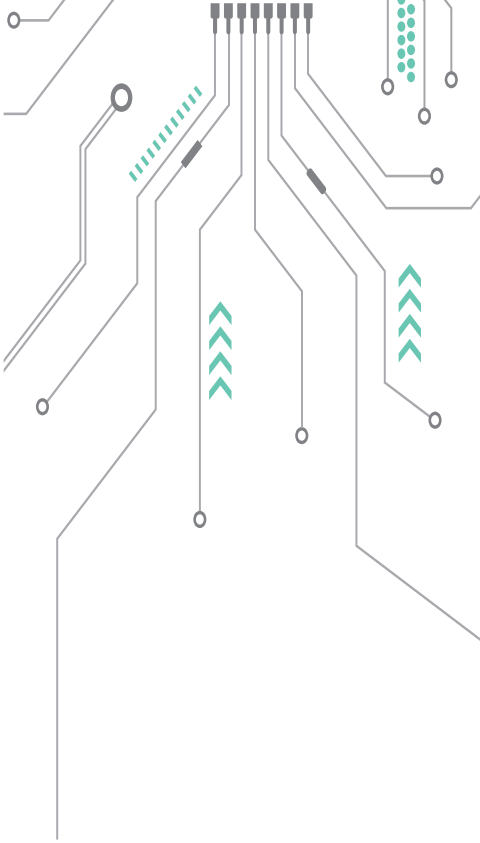
Con el uso de estas tres guías (conocidas generalmente por sus siglas NIST SP 800-53, RMF y FIPS 199) se podrá identificar el conjunto correcto de controles de seguridad adecuados para cada organización.

Las estrategias de contingencia se crean empleando la familia de controles de planificación de contingencia (contingency planning) de la guía NIST SP 800-53, que cubren todo el espectro de controles relativos a copias de seguridad, recuperación, planificación de contingencia, pruebas y mantenimiento continuo.

Copias de respaldo y restauración

Los mecanismos de copias de respaldo y restauración son un medio para recuperar un sistema de forma rápida y efectiva después de una interrupción del servicio. Estos mecanismos deben integrarse en el ciclo de vida del sistema como un elemento más de su arquitectura, teniendo en consideración que deben ser capaces de satisfacer los requerimientos establecidos en el BIA en cuanto al tiempo de recuperación.

La elección del mecanismo de recuperación adecuado dependerá de factores como el tipo de incidente, el tipo de sistema afectado, el nivel de impacto en la organización y los requisitos de operación del sistema. Los métodos de recuperación pueden incluir contratos comerciales



con proveedores de sitios alternativos, acuerdos recíprocos con organizaciones internas o externas y acuerdos de nivel de servicio (SLA) con proveedores de equipamiento.

Además, se deben considerar tecnologías como SAI (si la interrupción es de suministro eléctrico), discos RAID, almacenamiento en red (NAS y SAN), servidores en clúster, sistemas redundantes en alta disponibilidad, etcétera.

Deben plantearse varios enfoques alternativos al desarrollar y comparar estrategias, incluyendo el coste, MTD, RTO, RPO, la seguridad, las prioridades de recuperación y la integración con el PCN (a nivel de organización).

Métodos de copia de respaldo y almacenamiento externo

Es necesario definir en la política de copias de la organización la frecuencia y tipo de las copias que se deben realizar (por ejemplo, semanales completas y diarias diferenciales) dependiendo de la criticidad de los datos y de su frecuencia de modificación. También debe definirse la ubicación de los datos almacenados, la codificación de nombres de los archivos, el tipo de soportes que se deban utilizar, su frecuencia de rotación y el método para transportar los datos a una ubicación externa segura.

Una buena práctica es almacenar al menos una copia de los datos respaldados fuera de la ubicación del sistema de información, lo cual puede conseguirse a través de un proveedor de este tipo de servicios que gestionará la recogida de la información, etiquetado de soportes, transporte y almacenamiento en condiciones de conservación controladas. También puede optarse por la transmisión electrónica de la información al proveedor (como un proceso por lotes diario —*electronic vaulting*— o en tiempo real —*remote journaling*—).

Sitios alternativos

Para aquellos sistemas de información en los que el impacto de un incidente disruptivo sea relevante, la estrategia de continuidad debe incluir la recuperación del servicio en un lugar alternativo que pueda funcionar durante un período prolongado.

El sitio alternativo se puede clasificar aplicando diversos criterios según se muestra en la tabla siguiente:

CRITERIO	TIPO	DESCRIPCIÓN
Propiedad	Propio	Sitio dedicado a ello, propiedad de la organización u operado por esta
	Compartido	Acuerdo recíproco de colaboración con un tercero
	Alquilado	Sitio alquilado
Preparación	Frío	Sitio con espacio e infraestructura adecuada (energía, climatización, comunicaciones...) pero sin equipar
	Templado	Sitio parcialmente equipado (comunicaciones, hardware, software, energía...)
	Caliente	Sitio completamente equipado, configurado y con el personal de soporte necesario
Otros	Móvil	Contenedor portátil y autónomo adaptado a las necesidades de la organización
	Redundante	Sitio con el mismo equipamiento e infraestructura que el principal y con información replicada en tiempo real

Escoger el tipo de sitio idóneo es, una vez más, una cuestión de equilibrio entre el coste y el tiempo de recuperación requerido.

Reemplazo de equipamiento

En previsión de que un incidente haya provocado que el equipamiento del sistema de información haya sufrido daños o que el sitio principal no esté disponible, se requiere diseñar una estrategia de reemplazo de equipos, la cual deberá considerar una vez más el tiempo para tenerlos operativos, respetando los requerimientos del BIA.

Las opciones son:

Acuerdos con proveedores. En este caso es fundamental el establecimiento de SLA adecuados para la entrega del equipamiento y su configuración (si se incluye como parte del servicio).

Equipos almacenados. Se almacenan equipos de respaldo en una ubicación segura. Hay un gran riesgo de que dichos equipos queden obsoletos con el paso del tiempo.

Equipos compatibles existentes. A través de acuerdos de colaboración con terceros o mediante la contratación de proveedores de CPD calientes o servicios en la nube.

Roles y responsabilidades

Una vez establecida la estrategia de continuidad, el plan debe contemplar la estructura del equipo humano necesario para su desarrollo, teniendo en consideración el personal disponible y su capacitación.

Se formarán equipos de trabajo con responsabilidades bien definidas que deberán conocer todos sus miembros, disponiendo además de procedimientos específicos para cada actividad, tiempos objetivo para cada una de ellas y las interdependencias entre los distintos equipos existentes.

Los equipos tendrán un tamaño adecuado para acometer las tareas asignadas y una estructura jerárquica muy clara que estará supeditada a un único coordinador que tendrá la máxima autoridad para la toma de decisiones, incluyendo la activación del plan: el coordinador PCS (frecuentemente el CIO).

Por lo general, los equipos responderán a unas funciones y ámbitos de actuación acordes con las necesidades de la estrategia y respondiendo a perfiles de conocimiento concretos, por ejemplo: equipo de gestión (incluye al coordinador PCS), equipo de comunicación con los medios, equipo de seguridad operativa, equipo de recuperación de servidores, equipo de recuperación de BBDD, equipo de recuperación de red, equipo de recuperación de aplicaciones, equipo de pruebas...

Desarrollar un plan de continuidad de sistemas

El desarrollo del PCS es fundamental dentro de la elaboración de un PCN. Debe incluir los roles, responsabilidades, recursos y los procedimientos detallados para la recuperación del sistema de información tras una interrupción. Es interesante buscar en su redacción un equilibrio entre el nivel de detalle necesario para poder realizar las actividades de forma correcta y la flexibilidad suficiente para hacer el plan escalable y versátil (no concretando en exceso para no restringir su capacidad de adaptación).

La estructura de un PCS se compone de cinco elementos:

- información de apoyo;
- fase de activación y notificación;
- fase de recuperación;
- fase de reconstitución, y
- apéndices.

En su redacción, un PCS debe tener un formato claro, conciso y fácil de seguir en una emergencia, incluso para personal que pueda no estar familiarizado con el sistema de información (proveedores o personal suplente). Siempre que sea posible, se utilizarán listas de verificación y procedimientos paso a paso.

Información de apoyo

En primer lugar, deben describirse el contexto y los antecedentes que permitirán entender, desarrollar y mantener más fácilmente el plan: alcance; objetivos; funciones y responsabilidades; descripción del sistema; supuestos de partida y un breve resumen de las tres fases del plan.

El resto de la información de apoyo para la confección del PCS estará formada por las conclusiones obtenidas del BIA, la estrategia de recuperación, las listas de contactos y los procedimientos existentes que vayan a emplearse.

Fase de activación y notificación

Esta fase define el conjunto de acciones iniciales que deben ejecutarse tan pronto como se produce una interrupción del sistema o esta es inminente. Estas acciones se centran en la notificación al personal implicado en el PCS, una evaluación de la interrupción y la activación del plan. Al finalizar esta fase, todo el personal debería estar listo para comenzar las labores de recuperación del sistema.

A continuación, describiremos las diferentes subfases que componen esta fase.

Procedimiento y criterios de activación

El procedimiento de activación del PCS debe describir el modo de monitorizar el cumplimiento de cualquiera de los criterios de activación definidos por la organización y su validación por parte del coordinador PCS. Los criterios de activación del PCS pueden basarse en la evaluación de tres aspectos fundamentales:

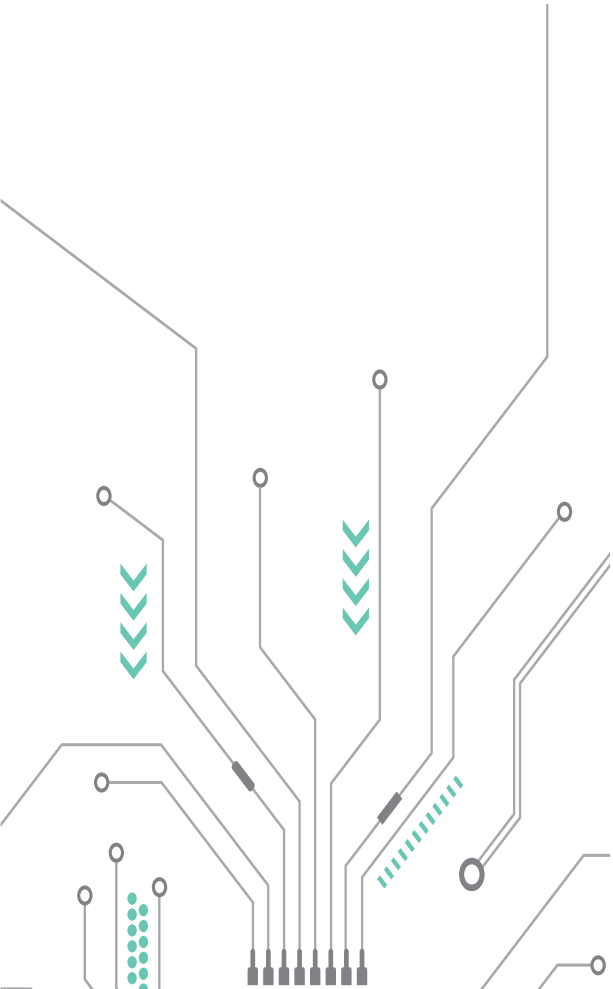
- extensión de los daños al sistema (físicos, operativos o económicos);

- criticidad del sistema o de la misión de la organización (por ejemplo, protección de infraestructuras críticas), y
- se espera que la duración de la interrupción sea mayor que el RTO.

Procedimientos de notificación

Describirán los mecanismos de comunicación para notificar la activación del PCS a todo el personal implicado.

Pueden emplearse una gran diversidad de procedimientos, incluyendo teléfono, correo electrónico, SMS... Se deberán considerar los más adecuados y eficaces, tanto para el horario laboral como para el no laboral. Con frecuencia, una notificación por correo electrónico seguida de una llamada de teléfono puede ser la combinación perfecta para proporcionar información precisa (incluyendo guías, documentación técnica, capturas de mensajes, detalles de la interrupción del sistema, etc.) a la vez que se tiene la certeza de la recepción de la notificación en un plazo de tiempo breve, ya que la consulta al correo puede ser muy esporádica, especialmente en horario de descanso).



Es recomendable establecer un árbol de llamadas para conseguir notificar a todo el personal necesario en un tiempo reducido, de modo que cada persona que reciba la notificación avisará a otras personas preasignadas y así sucesivamente. Cada contacto principal deberá disponer de un contacto alternativo en caso de problemas.

Se incluirá a los POC[4] de las empresas externas involucradas en el desarrollo del PCS. La notificación también se enviará a un equipo de evaluación de interrupciones previamente establecido para que pueda analizar el estado de la situación y organizar los próximos pasos que se deban dar.

Evaluación de interrupciones

Es fundamental para una correcta implementación del PCS evaluar la naturaleza y el alcance de la interrupción del sistema, por ello deberá iniciarse tan pronto como sea posible, y la prioridad será la protección de vidas humanas.

[4] POC *(point of contact)*: identifica la vía de comunicación con una tercera parte implicada en un proceso de la organización para posibilitar la coordinación de actuaciones y el intercambio de información.

El equipo de evaluación de interrupciones debe ser el primero en recibir la notificación de una interrupción. Estará formado por personal que conozca el procedimiento de evaluación de interrupciones y sea capaz de llevarlo a cabo incluso si no se dispone de la documentación de soporte. Una vez analizada la situación, este equipo notificará a los equipos técnicos de trabajo establecidos para cada ámbito de actuación que sea necesario abordar (recuperación de servidores, BBDD, conectividad de red, etc.). Esta notificación incorporará información actualizada de la situación y la respuesta planeada por parte del equipo de evaluación.

Fase de recuperación

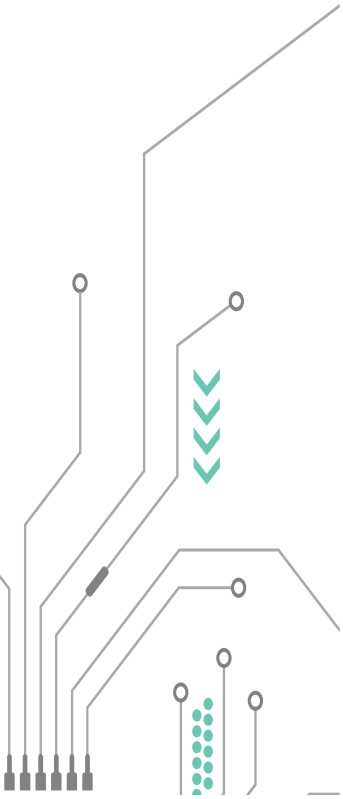
La fase de recuperación del sistema de información comienza después de finalizar las actividades de la fase previa, concretamente:

- activación del PCS;
- evaluación de la interrupción, y
- notificación y activación de los equipos oportunos.

El propósito de esta fase es el desarrollo de las estrategias de recuperación apropiadas para devolver al sistema de información a un estado plenamente operativo, es decir, en el que sea capaz de desempeñar las funciones identificadas como objetivo en el PCS. Puede tratarse de unas funciones temporalmente reducidas que deban acompañarse por la ejecución manual de algún proceso o el uso de un sistema o ubicación alternativos. Incluso puede contemplarse únicamente la recuperación de los activos del sistema identificados como prioritarios en el BIA.

La secuencia de actividades de recuperación debe reflejar la priorización establecida en el BIA y el MTD para evitar impactos significativos en la organización. Del mismo modo, para recuperar sistemas complejos es habitual establecer procedimientos de recuperación que han de desarrollar equipos de trabajo específicos que se deberán coordinar entre sí.

Los procedimientos serán claros, sencillos y redactarse como una secuencia ordenada de pasos.



Los procedimientos de recuperación también incluirán instrucciones para el escalado jerárquico y la coordinación con otros equipos cuando se produzcan problemas, se requieran recursos adicionales, se haya completado un paso clave del proceso, etcétera.

En caso de requerirse la recuperación en un sitio alternativo, toda la logística relacionada con la puesta en marcha en la nueva ubicación debe estar contemplada: traslado de equipamiento, soportes de información, registros vitales... incluyendo requisitos de embalaje, transporte y/o adquisición de material necesario.

Para evitar omisiones y facilitar el seguimiento escrupuloso del PCS, es muy recomendable el uso de listas de verificación.

Fase de reconstitución

Esta fase describe las acciones que es necesario desarrollar probar y validar la capacidad y funcionalidad del sistema de información recuperado. Si la ubicación original del sistema es irrecuperable, la fase de reconstitución será la que incorpore las actividades para preparar una nueva ubicación permanente que permita alcanzar de forma completa los requerimientos del sistema.

Los principales objetivos de esta fase son dos:

VALIDAR LA CORRECTA RECUPERACIÓN DEL SISTEMA. Para ello suelen darse, siempre que las circunstancias lo permitan, los siguientes pasos:

Procesamiento concurrente. Consiste en mantener el sistema en estado operativo en dos ubicaciones separadas de forma simultánea hasta que haya garantías suficientes para determinar que el sistema está recuperado de forma correcta y segura. Esto no siempre será posible, pero sí lo será si, por ejemplo, el sistema principal funciona de forma degradada por haber sufrido daños y se ha levantado uno alternativo.

Pruebas de validación de datos. Es el proceso de probar

y validar los datos del sistema para confirmar que se han recuperado correctamente hasta la última copia de seguridad disponible.

Pruebas de validación de funcionalidad. Es el proceso para probar toda la funcionalidad del sistema y determinar que está listo para reanudar las operaciones.

DESACTIVAR EL PCS. Una vez validada la recuperación, debe llevarse a cabo una notificación formal y coordinada para desactivar el PCS y volver a la normalidad. Para ello es habitual que el coordinador PCS, junto con la gerencia de la organización, monitoricen el comportamiento del sistema y el desarrollo de los servicios/procesos de la organización. En caso de que se hayan producido cambios relevantes, puede ser necesario volver a evaluar la situación antes de autorizar el inicio de la actividad de la organización y el fin del PCS. El proceso de vuelta a la normalidad no es inmediato y requiere de varios pasos previos:

- Notificación (a la plantilla y terceras partes relevantes) del regreso a la normal operación, utilizando los cauces para ello establecidos.
- Limpieza de los espacios de trabajo afectados por las labores de recuperación: desmantelamiento de ubicaciones temporales, reposición de documentación de trabajo a su lugar habitual, reabastecimiento de suministros, etcétera.
- Si se usa un almacenamiento de datos en una ubicación externa, deben devolverse los soportes de copias de seguridad utilizados.
- Hay que realizar tan pronto como se pueda nuevas copias de seguridad en previsión de tener que recuperar nuevamente el sistema.
- Redactar un informe detallado de los eventos y actividades de recuperación y reconstitución, el cual deberá incluir las lecciones aprendidas para la actualización y mejora del PCS.

Apéndices

Los apéndices permiten disponer y desarrollar toda la información anterior de manera detallada, incluyendo listas de verificación, listas de recursos necesarios, interconexiones del sistema, identificación de terceras partes implicadas (proveedores y clientes) y los acuerdos de colaboración o acuerdos de nivel de servicio (SLA) existentes.

Pruebas, formación y ejercicios del plan

Para que la organización esté realmente preparada para afrontar un incidente con impacto en la continuidad, es necesario que el personal esté capacitado, entrenado y los sistemas y procedimientos probados. Sería desastroso

descubrir un fallo en la respuesta ante un caso de incidente real, por eso resulta imprescindible establecer programas de prueba, formación y ejercicios que permitan evaluar la capacidad de respuesta y recuperación, con el fin de detectar posibles errores y puntos de mejora para poder corregir el plan.

La organización deberá establecer la realización de pruebas y ejercicios de sus planes de continuidad con una periodicidad determinada. Tras cada actividad llevada a cabo, se elaborará un informe con los resultados y las lecciones aprendidas que permitirán actualizar y mejorar el PCS.

Pruebas

Las pruebas deben realizarse en un entorno tan cerca del entorno operacional como resulte posible, incluyendo todos los componentes del sistema para verificar la eficacia y eficiencia de los procedimientos de recuperación establecidos, incluyendo:

- procedimientos de notificación;
- recuperación del sistema en una plataforma alternativa desde medios de copia de seguridad;
- conectividad interna y externa;
- rendimiento del sistema utilizando equipos alternativos;
- restauración de las operaciones normales;
- pruebas donde se requiera coordinación del PCS con otros
- planes superiores (como el PCN).

En cada prueba diseñada, el coordinador PCS debe evaluar los elementos seleccionados teniendo como referencia los objetivos de la prueba y sus criterios de éxito. El plan de pruebas también debe incluir un cronograma de tiempos para las actividades que se deban desarrollar, el personal que participará, el alcance, el escenario y la logística. El escenario elegido para la prueba puede ser el peor imaginable o el más probable, pero debe imitar la realidad lo más fielmente posible.

Formación

El programa de formación en materia de continuidad se debe focalizar en las funciones definidas en el PCS y los conocimientos necesarios para su desarrollo, de modo que el personal esté preparado para participar en pruebas y ejercicios, así como en incidentes reales de disrupción.
Se efectuará, al menos una vez al año de forma general, y de una forma lo más inmediata posible para el personal recién designado para las funciones del PCS. Uno de los principales objetivos es que el personal sea capaz de desarrollar las actividades que le corresponden incluso sin disponer de la documentación real, ya que podría no estar disponible en los primeros momentos tras una interrupción.

Ejercicios

NIST identifica los dos tipos de ejercicios que se indican a continuación:

Ejercicios de mesa. Este tipo de ejercicios de simulación son similares a un juego de rol donde el formador plantea un escenario de interrupción y hace preguntas a los participantes para abrir un debate entre ellos en torno a sus roles, responsabilidades y la toma de decisiones.

Ejercicios funcionales. En este caso se pretende evaluar la preparación del personal para afrontar un incidente en un entorno de operación simulado. Además, permiten verificar las funciones designadas al personal, el desempeño de sus responsabilidades, los procedimientos operativos, los activos y recursos utilizados, la eficacia de la comunicación y las notificaciones, etcétera. La complejidad de los ejercicios funcionales puede variar desde la comprobación de aspectos muy específicos del PCS hasta ejercicios a gran escala que involucren a todos los elementos del plan.

Mantenimiento del plan

Para garantizar la eficacia del PCS, este debe mantenerse actualizado en todo momento, y se adecuará a los cambios que, con el paso del tiempo, sufran los servicios y procesos de la organización, la estructura de activos del sistema de información, las políticas internas. Los avances tecnológicos también influyen en la forma en que resulta más eficaz acometer situaciones de interrupción.

Adicionalmente, durante la realización de ejercicios y pruebas puede ponerse de manifiesto la existencia de errores, lecciones aprendidas u oportunidades de mejora cuyas acciones correctivas habrá que trasladar al plan.

Por todo ello, en la organización se definirán intervalos de tiempo concretos en los cuales se revisarán la precisión e integridad del plan, así como cada vez que se produzca un cambio relevante en cualquier elemento del plan.

La revisión del plan debe centrarse en los elementos siguientes:

- requerimientos operacionales;
- requerimientos de seguridad;
- procedimientos técnicos;
- hardware, software y otros equipos (tipos, especificaciones y cantidad);
- nombres e información de contacto de los miembros del equipo;
- nombres e información de contacto de los proveedores, incluidos los POC de proveedores alternativos y externos;
- requisitos de instalaciones alternativas y externas; registros vitales (electrónicos y en papel).

Por la información tanto operativa como de personal que contiene un PCS, generalmente se considerará confidencial, por lo que deberá definirse y controlarse su distribución. Debe ubicarse en un lugar seguro, pero accesible, a todo el personal del PCS, incluyendo una ubicación remota en previsión de que las copias locales no estén disponibles. Junto a la documentación del PCS se almacenará otra información importante para su ejecución como pueden ser contratos con proveedores, licencias de software, manuales de usuario, guías de operación, manuales de seguridad y procedimientos operativos.

Todos los cambios al PCS los debe efectuar su coordinador, quien los notificará a los representantes de los planes relacionados. Las modificaciones se anotarán en un registro de cambios con la fecha de ubicación del cambio (página, capítulo, etc.) y una breve descripción del cambio.

Bibliografía

NIST (2004). Federal Information Processing Standards Publication 199. Standards for Security Categorization of Federal Information and Information Systems.
https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

NIST (2006). NIST Special Publication 800-84. Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

NIST (2010). NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems.
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

NIST (2018). Marco de ciberseguridad v1.1.
https://www.nist.gov/cyberframework/framework

NIST (2018). NIST Special Publication 800-37 Revision 2. Risk Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security and Privacy.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NIST (2018). Núcleo del marco de ciberseguridad v1.1 (versión Excel).
https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx

NIST (2020). NISTIR 8183 Revision 1. Cybersecurity Framework Version 1.1 Manufacturing Profile.
https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdfNIST (2019).

NIST (2021). Publicación especial 1271. Guía de inicio rápido del marco de ciberseguridad NIST.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271es.pdf

NIST (2022). NIST Special Publication 800-53A Revision 5. Assessing Security and Privacy Controls in Information Systems and Organizations.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf

NIST Technical Note 2051 Cybersecurity Framework Smart Grid Profile
https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2051.pdf

3

RELACION DE LA CONTINUIDAD CON OTROS MARCOS DE LA SEGURIDAD DE LA INFORMACIÓN

Imagen de Freepik

3.1

CONTINUIDAD DE LOS SERVICIOS DE LAS TI: ITIL E ISO/IEC 20000

Jorge Edo Juan
Jorge Sánchez López

Cada vez es más común que las organizaciones adopten medidas para prevenir el impacto de los efectos adversos que puedan afectar sus intereses. No obstante, nunca desaparece la posibilidad de que ocurra algún evento que amenace con interrumpir los servicios de las tecnologías de la información (TI) que dan soporte a las actividades de la organización. Por ello, es imprescindible disponer de una adecuada estrategia de gestión de continuidad de los servicios de las TI que permita a la organización responder de forma efectiva y eficiente ante cualquier desastre de alto impacto.

La gestión de servicios se puede definir como un conjunto de competencias organizacionales especializadas para entregar el valor a los clientes en forma de servicios. El desarrollo de las capacidades organizacionales especializadas está basado en los siguientes supuestos:

- La naturaleza del valor, entendido como el beneficio percibido, utilidad e importancia de algo.
- La naturaleza y el alcance de las partes interesadas involucradas.
- La manera cómo la creación de valor es habilitada mediante servicios.

En este contexto, la gestión de la continuidad de los servicios de las TI es una actividad de la gestión de servicios que debe orientarse a permitir la recuperación controlada de los servicios y minimizar los tiempos de inactividad, lo que garantizará la continuidad en la entrega de los servicios.

Así, los marcos de trabajo y las buenas prácticas en el contexto de la gestión de servicios de las TI prestan una especial atención a la continuidad de los servicios de las TI. Es el caso de la ITIL (*Information Technology Infrastructure Library*) y la serie ISO/IEC 20000.

A continuación, se describe cómo se desarrolla la continuidad de los servicios de las TI en ambos marcos de trabajo.

ITIL® Y LA CONTINUIDAD DE LOS SERVICIOS DE LAS TI

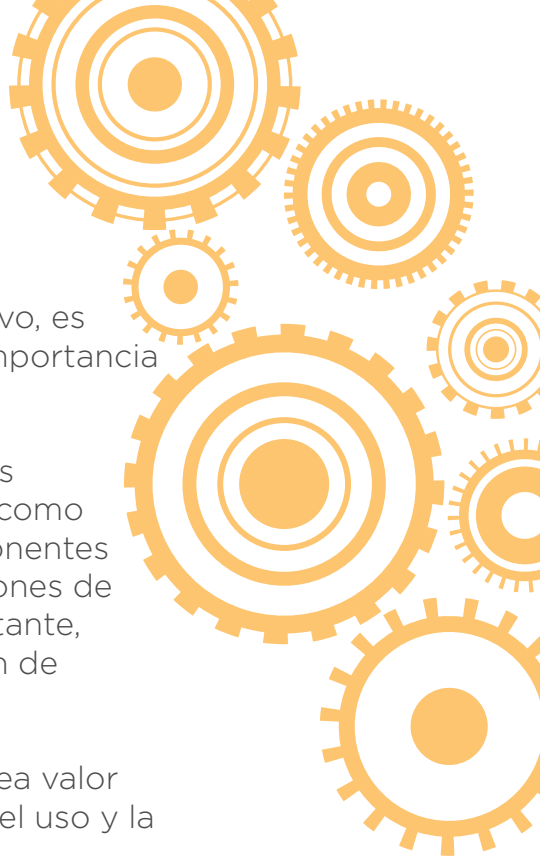
ITIL® 4 es un conjunto de buenas prácticas usadas para la gestión de los servicios de las tecnologías de la información que proporciona a las organizaciones un modelo operativo digital de extremo a extremo para la entrega y operación de productos y servicios habilitados por las TI. ITIL® 4 permite que los equipos de las TI continúen desempeñando un papel importante en la estrategia del negocio, y proporcionan un enfoque integral que contempla otros marcos como Lean, Agile y DevOps.

Los componentes clave de la ITIL® 4 son el sistema de valor del servicio (SVS) y el modelo de cuatro dimensiones.

El sistema de valor del servicio describe las formas en que los diversos segmentos y actividades de una organización están vinculados entre sí. El SVS representa el modo en que los diversos componentes y actividades de la organización trabajan juntos para facilitar la creación de valor mediante servicios habilitados por las TI. El SVS facilita la integración y coordinación y proporciona una dirección fuerte, unificada y enfocada hacia el valor.

Por otra parte, el modelo de cuádruple de dimensiones describe las cuatro perspectivas que son críticas para la facilitación efectiva y eficiente de valor para los clientes y otras partes interesadas en forma de productos y servicios. Este modelo de las cuatro dimensiones de la gestión de servicios se define para garantizar un enfoque global en la gestión de los servicios. Las cuatro dimensiones son:

- Organizaciones y personas.
- Información y tecnología.
- Asociados y proveedores.
- Flujos de valor y procesos.



Para garantizar que el SVS permanezca equilibrado y efectivo, es fundamental dar a cada una de las cuatro dimensiones la importancia debida.

El sistema de valor del servicio de la ITIL® 4 explica cómo los componentes y las actividades de la organización trabajan como un sistema para permitir la creación de valor. Dichos componentes y actividades se pueden configurar en múltiples combinaciones de manera flexible para adaptarse a las circunstancias. No obstante, esta configuración necesita de la integración y coordinación de actividades, prácticas y equipos.

El propósito del SVS es garantizar que la organización cocrea valor constantemente con todas las partes interesadas a través del uso y la gestión de productos y servicios.

Las entradas principales del SVS son la oportunidad y la demanda. Las oportunidades se refieren a las posibilidades que pueden agregar valor para los clientes y partes interesadas, o ayudar a mejorar a la organización. Por su parte, la demanda se refiere a la necesidad de productos y servicios entre las personas o empresas consumidoras.

La oportunidad y la demanda generan actividades que se orientan a la creación de valor. Este valor es la salida o resultado del SVS.

El SVS de la ITIL incluye los siguientes componentes:

Principios guía. Se refiere a las recomendaciones que orientan a las organizaciones en cualquier circunstancia, sin estar ligados a sus objetivos, estrategias o estructura de gestión.

Gobernanza. Contempla los medios por los cuales se dirige y se controla una organización.

Cadena de valor del servicio. Se identifica como un conjunto de actividades realizadas por una organización para entregar a sus clientes un producto o servicio de valor.

Prácticas. Se definen como un conjunto de recursos organizacionales diseñados para acometer un trabajo o lograr un objetivo. La gestión de la continuidad de los servicios de las TI es una de las prácticas definidas en la ITIL® 4.

Mejora continua. Hace referencia a una actividad recurrente desempeñada en todos los niveles con el objetivo de que los resultados obtenidos por una organización cumplan continuamente con las expectativas de las partes interesadas.

Uno de los componentes básicos del SVS son los principios guía que se definen como una filosofía o una idea establecida que orienta a una organización en todas las circunstancias. Se aplican a todas las iniciativas de la organización y a todas las relaciones con las partes interesadas que apoyan una cultura de colaboración y de intercambio.

Cabe señalar que los principios guía respaldan las diferentes acciones y decisiones tomadas por una organización, incluidas sus iniciativas de mejora continua. El propósito es adoptar un enfoque de gestión de servicios y adaptar la orientación de la ITIL® 4 al contexto de la organización.

Estos principios también podemos encontrarlos en otros marcos, métodos, estándares, filosofías e ideas. Los principios guía definidos en la ITIL® 4 son:

1. Enfoque en valor.
2. Empezar donde se está.
3. Progresar iterativamente con retroalimentación.
4. Colaborar y promover visibilidad.
5. Pensar y trabajar holísticamente.
6. Mantenerlo simple y práctico.
7. Optimizar y automatizar.

A continuación, se describen cada uno de estos principios guía:

El principio **Enfoque en valor** se orienta a la creación de valor para los consumidores de servicios. Para alcanzar este valor, las organizaciones deben vincular las diferentes actividades (directa o indirectamente) que realizan de una manera lógica.

El principio **Empezar donde se está** se enfoca a considerar lo que ya está disponible en lugar de comenzar desde cero (o la reutilización). Para lograr esto, es fundamental analizar el estado existente para identificar lo que puede ser útil en la creación de valor.

El principio **Progresar iterativamente con retroalimentación** pone el foco en evitar la búsqueda global de una vez y en recibir la retroalimentación oportuna. Para ello, es necesario dividir el trabajo en componentes más manejables con el objetivo de lograr la iniciativa de manera iterativa.

El principio **Colaborar y promover visibilidad** se centra en eliminar silos de información y generar confianza entre las partes interesadas. De esta manera, es necesario que los miembros de la organización trabajen juntos y compartan información en la mayor medida posible.

El principio **Pensar y trabajar holísticamente** se orienta a una manera integral de trabajar. Para ello, las diferentes actividades de una organización deben centrarse en la entrega de valor.

El principio **Mantenerlo Simple y Práctico** está enfocado a simplificar los procesos y métodos de trabajo complejos. Para lograr esto, se deben identificar y eliminar procesos, servicios, acciones o métricas que no agreguen ningún valor al resultado.

El principio **Optimizar y automatizar** se centra en buscar la mejora en el trabajo realizado por las personas. Este principio plantea que las organizaciones deben automatizar el trabajo en la medida de lo posible a fin de que requiera una intervención humana mínima.

Otro concepto esencial en la ITIL® 4 que ayuda a explicar cómo se desarrolla la gestión de la continuidad de las TI en este marco de buenas prácticas es la cadena de valor del servicio, que se define como un modelo operativo que identifica las actividades clave requeridas para responder a la demanda y permitir la creación de valor a través de la formación y gestión de productos y servicios.

La cadena de valor del servicio de la ITIL incluye seis actividades que conducen a la creación de productos y servicios y, a su vez, de valor.

Las seis actividades de la cadena de valor son:

Planificar. El propósito de esta actividad en la cadena de valor es asegurar una comprensión compartida de la visión, estado actual y dirección de mejora para las cuatro dimensiones y todos los productos y servicios en toda la organización.

Mejorar. El propósito de esta actividad de la cadena de valor es garantizar la mejora continua de los productos, servicios y prácticas en todas las actividades de la cadena de valor y las cuatro dimensiones de la gestión de servicios.

Vincular. El propósito de esta actividad de la cadena de valor es proporcionar una buena comprensión de las necesidades de los interesados, transparencia y compromiso continuo, así como buenas relaciones con todos los interesados.

Diseñar y transicionar. El propósito de esta actividad de la cadena de valor es garantizar que los productos y servicios cumplan con las expectativas de los interesados en cuanto a calidad, costos y tiempo de comercialización.

Obtener y construir. El propósito de esta actividad de la cadena de valor es garantizar que los componentes del servicio estén disponibles cuando y donde se necesiten, y que cumplan con las especificaciones acordadas.

Entregar y soportar. El propósito de esta actividad de la cadena de valor es garantizar que los servicios sean entregados y soportados de acuerdo con las especificaciones acordadas y las expectativas de las partes interesadas.

Las actividades de la cadena de valor representan los pasos que toma una organización para crear valor. Cada actividad contribuye a la cadena de valor, al convertir entradas específicas en salidas.

Las entradas pueden ser demandas externas a la cadena de valor o pueden ser salidas de otras actividades. De esta forma, las actividades interactúan entre sí, allí donde cada actividad recibe y proporciona detonadores para que se lleven a cabo otras acciones.

Para convertir las entradas en salidas, las actividades de la cadena de valor toman diferentes combinaciones de prácticas de la ITIL. Cada actividad puede utilizar recursos internos o de terceros, habilidades y competencias de una o más prácticas.

Por otra parte, un flujo de valor se define como una serie de pasos que una organización realiza para crear y entregar productos y servicios a un consumidor. Un *flujo de valor* es una combinación de las actividades de la cadena de valor de la organización.

Asimismo, en la ITIL®4 una práctica se refiere a un conjunto de recursos organizacionales diseñados para llevar a cabo un trabajo o lograr un objetivo. El sistema de valor de servicio de la ITIL incluye tres tipos de prácticas: prácticas de gestión general, prácticas de gestión de servicio y prácticas de gestión técnica. La mejora continua se aplica a todo el sistema de valor de servicio, así como a todos los servicios de productos, componentes de servicio y relaciones de la organización.

LA GESTIÓN DE LA CONTINUIDAD DE LAS TI COMO UNA PRÁCTICA DE LA ITIL®4.

La finalidad de la gestión de la continuidad del servicio como práctica de la ITIL® 4 es garantizar que la disponibilidad y el rendimiento de un servicio se mantengan en los niveles determinados por la organización en caso de producirse un desastre. Esta práctica plantea un marco de trabajo cuyo objetivo es desarrollar la resiliencia organizativa que proporcione capacidades para una respuesta eficaz orientada a proteger los intereses de las partes interesadas que son clave, así como la reputación y las actividades de creación de valor de la organización.

En relación con lo anterior, un *desastre* puede definirse como un evento repentino no planificado que causa grandes daños o pérdidas graves a una organización. Si nos atenemos a la norma ISO 22300:2021, un desastre se define como «una situación con un alto nivel de incertidumbre que interrumpe las actividades principales y/o la credibilidad de una organización y requiere una acción urgente».

Es importante señalar que la organización debe definir los criterios de impacto organizacional para que una situación pueda identificarse como desastre. La distinción entre desastres, incidentes importantes e incidentes normales debe estar debidamente predefinida, acordada y documentada con una identificación de las condiciones y desencadenantes claros para invocar al siguiente nivel de respuesta y recuperación tan pronto como sea posible.

Una buena práctica que puede seguirse es explicitar la lista de eventos que se consideran desastres. Entre otros, se incluyen:

- Desastres naturales.
- Ciberataques.
- No disponibilidad del personal clave.
- Cortes de suministro eléctrico.
- Incendios.
- Fallos graves en la infraestructura de las TI.

También puede ser de ayuda definir las situaciones que no se identifican como desastre, como puedan ser los eventos que tengan un menor impacto organizativo.

La gestión de la continuidad del servicio contribuye a garantizar que una organización está preparada para responder a incidentes que pueden interrumpir gravemente las actividades de la organización y/o impactar en su credibilidad.

Garantizar la continuidad del servicio es cada vez más importante y complejo. En un contexto de transformación digital donde los servicios digitales tienen una gran importancia, la gestión de la continuidad del servicio se

ha convertido en una actividad imprescindible para las organizaciones actuales.

En la ITIL ® 4, la práctica de gestión de la continuidad del servicio se relaciona de manera directa con otras prácticas para garantizar que los servicios de la organización sean resilientes y estén preparados para mitigar los posibles efectos de los desastres. Entre otras destacan: la gestión de la disponibilidad, la gestión de la capacidad y el rendimiento, la gestión de la seguridad de la información, la gestión de riesgos, el diseño de servicios, la gestión de relaciones, la gestión de la arquitectura y la gestión de proveedores.

Uno de los conceptos esenciales que se manejan en la práctica de la gestión de la continuidad del servicio es el riesgo. Así, se puede señalar que esta práctica se orienta a mitigar los riesgos de alto impacto y baja probabilidad que no se pueden prevenir completamente, entre otras, por la existencia de factores de riesgo que no están bajo el control de la organización.

Por su parte, es interesante señalar que la práctica de la gestión de la continuidad del servicio presenta ciertas similitudes con la práctica de la gestión de incidentes, con la diferencia de que el potencial de daños es mucho más elevado y que el impacto producido puede llegar a condicionar la capacidad de la organización para la creación de valor.

Para recuperarse con éxito de un desastre, la organización debe definir los requisitos de continuidad del servicio, que incluyen lo siguiente:

- Objetivo de tiempo de recuperación (RTO).
- Objetivo de punto de recuperación (RPO).
- Niveles mínimos de continuidad del servicio.

El **Objetivo de tiempo de recuperación (RTO)** puede definirse como el período máximo después de una interrupción del servicio que puede pasar antes de que la falta de funcionalidad organizativa afecte gravemente a la propia organización. En otros términos, es el tiempo máximo acordado dentro del cual se debe reanudar un producto o una actividad, o se deben recuperar los recursos.

Para determinar los valores de RTO, la organización debe tener en cuenta lo siguiente:

- Disminución de la capacidad de la organización para entregar sus productos y/o servicios y los costes asociados a esta reducción.
- Sanciones relacionadas con los acuerdos de nivel de servicio y aspectos regulatorios.
- Pérdidas asociadas a una menor ventaja competitiva y reputación.

Relacionado con el concepto RTO tenemos el término **período máximo tolerable de interrupción/interrupción máxima aceptable** (MAO) que se define como el tiempo que transcurriría para que los impactos adversos se volvieran inaceptables para la organización.

En cuanto al momento en que deberían identificarse ambos conceptos, el MAO debe definirse durante el análisis de impacto organizativo, mientras que el RTO debe identificarse en el proceso de desarrollo de los planes de continuidad del servicio. De esta manera y teniendo en cuenta el apetito de riesgo organizativo, el RTO debe ser menor que el MAO.

Por otra parte, el **Objetivo del punto de recuperación** (RPO) define el período de la pérdida de datos aceptable y se refiere al momento anterior al desastre en el que se debe restaurar la información del sistema impactado para permitir que la actividad funcione de forma eficaz tras la reanudación.

Para estimar los valores del RPO deben tenerse en cuenta los siguientes factores:

- La criticidad del servicio que utiliza el sistema afectado.
- La criticidad de los datos.
- La tasa de producción de datos.

A partir del RPO se definen los requisitos exigidos para la frecuencia de respaldo. La estrategia de continuidad debe garantizar la disponibilidad de una salvaguarda de los datos reciente en caso de desastre.

Durante la recuperación de un desastre puede ser necesario proporcionar un nivel de servicio objetivo mínimo, que se define como el nivel de servicio que acepta la organización para lograr sus objetivos corporativos durante la interrupción. Dependerá de cada organización, pero es importante destacar que lograr un **nivel de servicio mínimo** puede ayudar a minimizar las pérdidas.

Para la definición del nivel de servicio objetivo mínimo se consideran los siguientes factores:

- Funcionalidades que deberían estar disponibles para los usuarios durante una interrupción.
- Grupos de usuarios y/o número de ellos que necesitan acceder a los servicios de las TI durante una interrupción.
- Niveles de carga de trabajo de las TI que la organización requiere durante una interrupción.

En la gestión de la continuidad del servicio es fundamental identificar las funciones de negocio vitales (VBF) y sus dependencias, que pueden incluir proveedores, personas, otros procesos de negocio y servicios de las TI. El análisis de impacto en el negocio (BIA) es una actividad que define los requisitos de recuperación para los servicios de las TI: RTO, RPO y niveles de servicio objetivo mínimos para cada servicio de las TI.

El análisis de impacto en el negocio (BIA) debería incluir:

- Identificación de actividades para el soporte de la provisión de productos y servicios.
- Evaluación de los impactos en caso de ruptura del servicio.
- Establecimiento de los plazos para reanudar estas actividades a un nivel mínimo aceptable especificado.
- Identificación de las dependencias y recursos de soporte para estas actividades, considerando los grupos de interés relevantes: proveedores, socios externos, etc.

Por otra parte, la continuidad del servicio exige disponer de un conjunto de planes claramente definidos orientados a la recuperación y el regreso a una situación previa al desastre, teniendo en cuenta las cuatro dimensiones de la gestión de servicios: **a)** Organizaciones y personas, **b)** Información y tecnología, **c)** Asociados y proveedores y **d)** Flujos de valor y procesos.

Estos planes de continuidad del servicio se convierten en los pasos que se deben seguir orientados a permitir la respuesta, recuperación y restauración de un servicio a los niveles normales después de una interrupción.

Los planes de continuidad del servicio deberían incluir:

Plan de respuesta. Ayuda a definir la manera de reaccionar a un evento disruptivo con el objetivo de evitar los daños que pudieran producirse.

Plan de recuperación. Su objetivo es determinar las acciones orientadas a recuperar el servicio para lograr el RTO y el RPO que haya determinado la organización.

Plan de regreso a las operaciones normales. En este se especificará cómo se reanudan las operaciones normales después de la recuperación.

En algunas ocasiones, también es necesario planificar la continuidad del negocio. Los planes de continuidad del negocio pueden incluir:

- Planes de respuesta de emergencia, que facilitaran la interacción con todos los servicios y actividades de emergencia.
- Plan de evacuación, con el objetivo de garantizar la seguridad de las personas.
- Planes para la gestión de la comunicación y de crisis para el manejo de la comunicación con todas las partes implicadas y de las diferentes crisis, unificando la gestión de los medios.
- Planes de seguridad, orientados a gestionar los aspectos relativos a la seguridad, tanto en el lugar habitual de procesamiento como en los centros de procesamiento alternativo.

En los casos en que los planes de continuidad del servicio se gestionen de manera separada de la gestión de los incidentes debe establecerse un criterio diferente a la activación de los planes de continuidad del servicio.

En tanto que las organizaciones son cada vez más dependientes de los servicios aprovisionados por la tecnología, la alta disponibilidad de los servicios de las TI se ha convertido en un elemento fundamental para la resiliencia y la competitividad de la organización. Las organizaciones alcanzan una alta disponibilidad mediante una combinación de planificación organizativa, robustez de la arquitectura técnica, soporte de disponibilidad, gestión proactiva de riesgos y seguridad de la información, así como a través de la gestión de incidentes y la gestión de problemas.

En la siguiente lista se describen los diferentes componentes de la gestión de la continuidad del servicio en las actividades en la cadena de valor del servicio de la ITIL® 4.

Plan. El liderazgo y el órgano de gobierno de la organización establecen un apetito de riesgo inicial para la organización con un alcance, políticas, estrategias de proveedores e inversión con opciones de recuperación definidos. La gestión de la continuidad del servicio respalda esto con información relevante sobre el estado de continuidad actual de la organización y con herramientas y métodos de planificación y previsión.

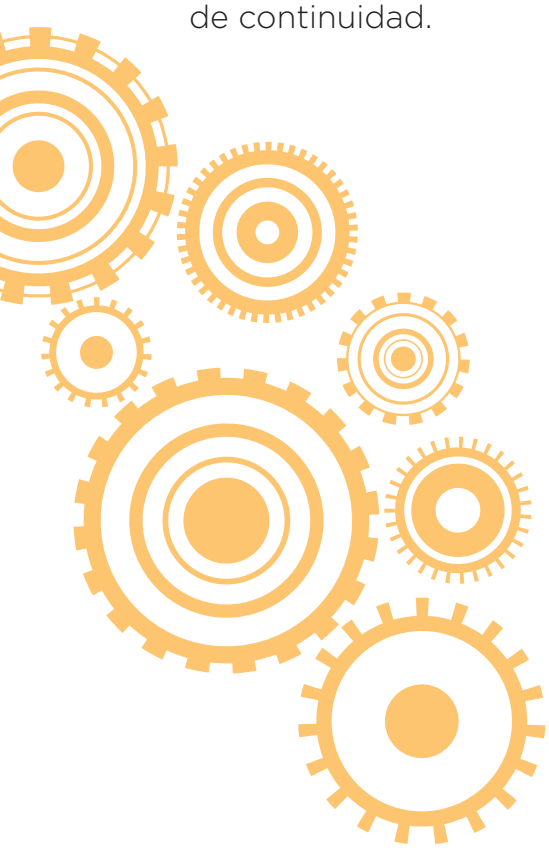
Mejorar. La gestión de la continuidad del servicio garantiza que los planes, medidas y mecanismos de continuidad se supervisen y mejoren continuamente de acuerdo con las circunstancias cambiantes internas y externas.

Contratar. Esta práctica respalda el compromiso con varias partes interesadas para brindar seguridad con respecto a la preparación de una organización para los desastres.

Diseño y transición. La gestión de la continuidad del servicio garantiza que los productos y servicios se diseñen y prueben de acuerdo con los requisitos de continuidad de la organización.

Obtener y construir. La gestión de la continuidad del servicio asegura que la continuidad esté integrada en los servicios y componentes de la organización, y que los componentes y servicios adquiridos cumplan con los requisitos de continuidad de la organización.

Entregar y apoyar. La entrega, las operaciones y el soporte continuos se realizan de acuerdo con los requisitos y las políticas de continuidad.



Por otra parte, en la ITIL® 4 se define un proceso como un conjunto de actividades interrelacionadas o de interacción que transforman las entradas en salidas. Los procesos identifican la secuencia de acciones y sus dependencias. Así, las actividades que se realizan en la práctica de la gestión de la continuidad del servicio de las TI forman cinco procesos:

- Gobernanza de la gestión de la continuidad del servicio.
- Análisis de impacto organizativo.
- Desarrollo y mantenimiento de planes de continuidad del servicio.
- Prueba de los planes de continuidad del servicio.
- Respuesta y recuperación.

Un factor de éxito de la práctica (PSF) es más que una tarea o actividad, puesto que incluye componentes de las cuatro dimensiones de la gestión de servicios. La naturaleza de las actividades y los recursos de los PSF dentro de una práctica puede diferir, pero juntos garantizan que la práctica sea efectiva.

La práctica de la gestión de la continuidad del servicio de las TI incluye los siguientes PSF:

- Desarrollar y gestionar planes de continuidad del servicio.
- Mitigar los riesgos de continuidad del servicio.
- Garantizar la concienciación y la preparación.

Para una respuesta y recuperación eficaces ante los desastres, son imprescindibles los planes de continuidad del servicio, que deben reflejar las estrategias de continuidad del servicio elegidas. Dichas estrategias de continuidad del servicio deben seleccionarse con respecto a los requisitos de continuidad del servicio, que se identifican durante el BIA.

Por otra parte, la práctica de la gestión de la continuidad del servicio de las TI recoge la definición y gestión de controles para gestionar riesgos. Para ello, se utiliza junto con la práctica de la gestión de riesgos y otras prácticas centradas en el riesgo (como la gestión de la disponibilidad, la gestión de la capacidad y rendimiento y las prácticas de la gestión de la seguridad de la información).

Asimismo, los planes de recuperación deben probarse para asegurarse que funcionan según lo previsto. Las pruebas son una parte fundamental de la gestión de la continuidad del servicio y se convierten en la única forma de garantizar que la estrategia seleccionada, las medidas implementadas y los planes funcionan realmente. En la revisión periódica de los planes y procedimientos de la continuidad de los servicios de las TI los equipos de recuperación descubren defectos e ineficiencias que sirven de base para mejorar los planes de continuidad del servicio de las TI.

ITIL® Y LA NORMA ISO/IEC 20000

ISO/IEC 20000 es una norma internacional que describe un conjunto de buenas prácticas que permiten prestar de forma eficaz los servicios de las TI a las empresas y a sus clientes. La primera versión se publicó en 2005 y es el estándar reconocido internacionalmente en la gestión de servicios. La serie ISO/IEC 20000 proviene de la adopción de la serie BS 15000 desarrollada por la British Standars Institution (BSI, entidad de normalización británica).

La serie de normas ISO/IEC 20000 define un conjunto completo y relacionado de procesos de la gestión de los servicios, y se compone de varias partes, entre las que destacan:

La norma ISO/IEC 20000-1:2018, que es la especificación para la gestión de los servicios. Además, establece requisitos para un conjunto de procesos específicos y constituye la base para la certificación.

La norma ISO/IEC 20000-2:2019 que es el código de práctica para la gestión de los servicios donde se describen las mejores prácticas y los requisitos de la parte 1.

Las organizaciones pueden usar ambas partes como ayuda para desarrollar herramientas encaminadas a la gestión de los servicios, productos y sistemas en soporte de la gestión de los servicios basados en las mejores prácticas.

Hasta la versión actual de la norma ISO/IEC 20000-1, la continuidad de los servicios de las TI estaba incluida en un proceso denominado Gestión de la continuidad y de la disponibilidad del servicio. Este proceso junto con la Gestión de la capacidad, Gestión del nivel de servicio, Informes del servicio, Gestión de la seguridad de la información y Presupuestos y contabilidad de los servicios de las TI formaban el grupo de los Procesos de la provisión del servicio.

El objetivo del proceso Gestión de la continuidad y de la disponibilidad del servicio era asegurar que los compromisos de continuidad y disponibilidad acordados con los clientes se cumplieran en todas las circunstancias.

Exigía la identificación de los requisitos de disponibilidad y de continuidad del servicio sobre la base de los planes de negocio, los acuerdos de nivel de servicio (SLA) y las evaluaciones del riesgo.

En cuanto a los planes de disponibilidad y de continuidad del servicio debían desarrollarse y revisarse, al menos, una vez al año, para asegurar que los requisitos cumplen lo acordado en todas las circunstancias, desde la normalidad hasta la pérdida grave del servicio. También, se recomendaba probar los planes de disponibilidad y de continuidad del servicio en los casos en que se producía un cambio importante en el entorno del negocio.

El proceso encargado de evaluar el impacto de cualquier cambio sobre los planes de disponibilidad y de continuidad del servicio es el proceso de gestión de cambios.

Asimismo, se exigía que el plan de continuidad del servicio incluyera la actividad de vuelta a la normalidad.

En la versión actual de la norma, ISO/IEC 20000-1:2018, la continuidad y la disponibilidad del servicio se desarrollan en procesos diferentes. Así, el proceso de la Gestión de la continuidad del servicio, junto con la gestión de la disponibilidad del servicio y la gestión de la seguridad del servicio se encuentra en un grupo denominado Aseguramiento del servicio, dentro del apartado «Operación del sistema de gestión del servicio».

En el proceso de la Gestión de la continuidad del servicio se especifica que los riesgos relacionados con la continuidad deben ser evaluados y documentos periódicamente. Asimismo, establece que la organización deberá determinar los requisitos de la continuidad de los servicios, de manera que estos tomen en consideración los requisitos relevantes del negocio, los requisitos del servicio, los SLA y los riesgos.

Los planes de continuidad deben incluir referencias a:

- Criterios y responsabilidades para invocar la continuidad del servicio.
- Procedimientos que se implementarán en un desastre.
- Objetivos de disponibilidad cuando se invoquen los planes de continuidad.
- Requisitos de la recuperación del servicio.
- Procedimientos para la vuelta a la normalidad.

Los planes deben ser probados regularmente y, también, cuando se produzca un cambio mayor en el servicio. Deben revisarse los planes después de ser invocados con el objetivo de subsanar las posibles deficiencias que se hubieran encontrado. En cualquier caso, debe guardarse un registro de las causas, impactos y las actividades de recuperación siempre que se invoquen los planes.

Bibliografía

Agutter, C. (2020). ITIL Foundation Essentials ITIL 4 Edition-The ultimate revision guide. IT Governance Publishing Ltd.

ISO. (2018). ISO/IEC 20000-1:2018 Information technology - Service management - Part 1: Service management system requirements.

ISO. (2018). ISO/IEC 20000-2:2019 Information technology - Service management - Part 2: Guidance on the application of service management systems.

Van der Haven, D. (2018). A Guide to ISO/IEC 20000-1: 2018 Service Management. ITSM Press.

3.2 ESQUEMA NACIONAL DE SEGURIDAD (ENS)

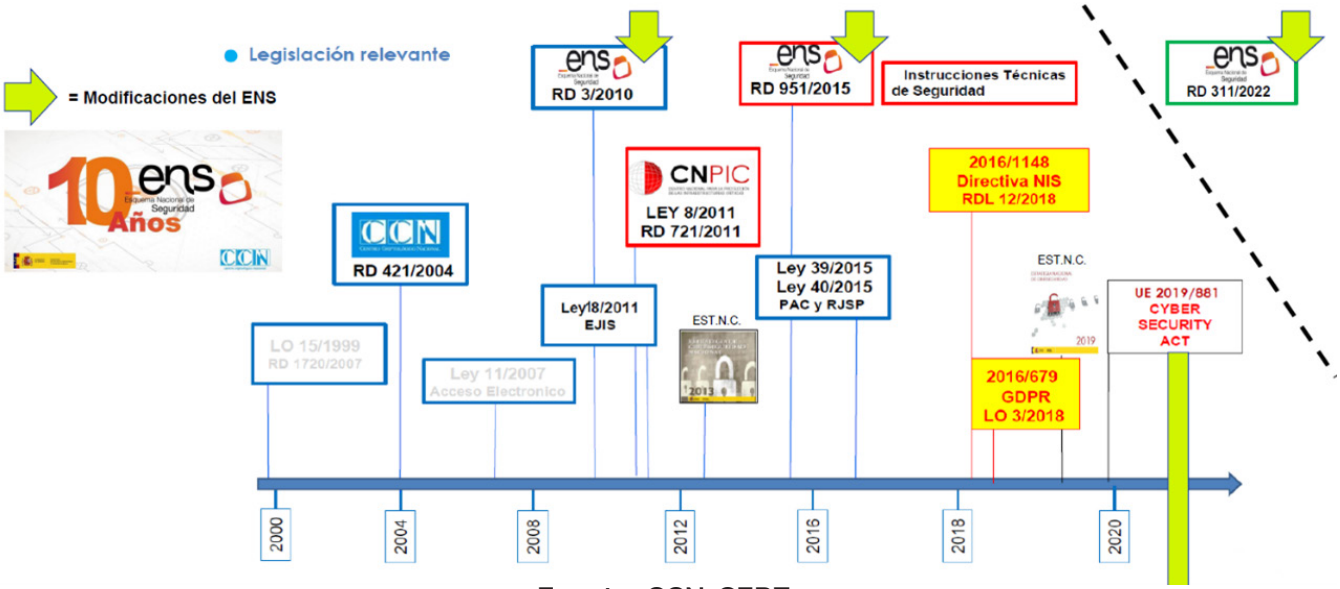
Jorge Edo Juan
Jorge Sánchez López

ANTECEDENTES

El **Esquema nacional de seguridad** (ENS), surge dentro del ámbito de la Administración española, con el objetivo de crear las condiciones necesarias de confianza en el uso de los medios electrónicos. Para ello utiliza medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos. Estas medidas, como veremos posteriormente son de tres tipos: carácter organizativo, control operacional y medidas de protección.

La finalidad última del ENS es posibilitar a la ciudadanía y a las administraciones públicas el ejercicio de sus derechos y el cumplimiento de sus obligaciones a través de medios electrónicos tanto de forma directa como indirecta.

En el gráfico siguiente podemos apreciar los grandes hitos dentro del ENS.



Fuente: CCN-CERT

Seguidamente, vamos a indicar cuáles son las reseñas más destacables en estos diez años en la vida del ENS.

- **Creación del Centro Criptológico Nacional (CCN-CERT).** RD 421/2004. El CCN, desde su fecha de creación, es el organismo responsable de garantizar la seguridad de las tecnologías de la información y la comunicación (TIC) en las diferentes entidades del sector público, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada.
- Primera versión del ENS (RD 3/2010). Real Decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad en el ámbito de la Administración electrónica.
- Actualización del real decreto anterior y publicación de las instrucciones técnicas de seguridad (RD 951/2015). Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad en el ámbito de la Administración electrónica.
- Publicación de la última y más reciente versión del ENS (RD 311/2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el esquema nacional de seguridad.

¿A QUIÉN SE APLICA EL ENS?

El ENS se aplica a todo el sector público y a sus proveedores tecnológicos del sector privado.

Para ampliar un poco más la frase anterior, podemos concluir, que el ENS se aplica a las siguientes entidades y organizaciones:

- Administración general del Estado.
- Administración de las comunidades autónomas.
- Administración de las entidades locales.
- Entidades de derecho público y privado, pertenecientes al sector público.
- Entidades de derecho privado vinculadas o dependientes de las comunidades autónomas o entidades locales.
- Universidades públicas.
- Agencia Estatal de Administración Tributaria (AEAT), CNI y Banco de España.

- Órganos constitucionales, legislativos y de control autonómico.
- Entidades de derecho privado y fundaciones.
- Empresas del sector privado (proveedores) que presten servicios al sector público.

DIMENSIONES DE SEGURIDAD DE LA INFORMACIÓN EN EL ENS.

El ENS, y a diferencia de la ISO 27001, como veremos en el apartado siguiente, tiene cinco dimensiones de seguridad de la información. A continuación, pasamos a describirlas en detalle:

Confidencialidad. Propiedad de la información, por la que se garantiza que esta está accesible únicamente al personal autorizado para acceder a ella.

Integridad. Propiedad de la información mediante la cual se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.

Disponibilidad. Propiedad de la información, por la cual se garantiza que las personas autorizadas puedan acceder a ella, cuando lo consideren oportuno.

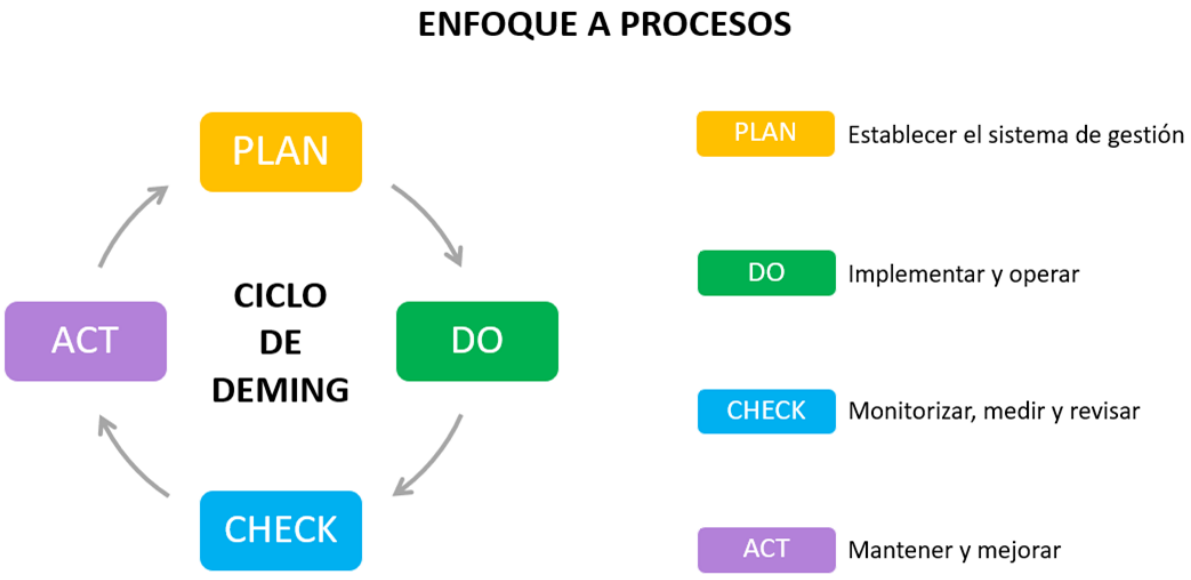
Autenticidad. Esta propiedad garantiza el no repudio, es decir asegura que el mensaje ha sido enviado por parte de quien dice ser. Es decir que la información se haya generado por parte de una fuente fidedigna, o sea que el origen del mensaje sea realmente quien envía la información.

Trazabilidad. La propiedad de trazabilidad aplicada a la información se refiere a garantizar los cambios y las modificaciones de la información, indicando, fecha, hora y autor de dicha alteración.

En el caso de la ISO 27001, como veremos en detalle en el siguiente apartado, en lugar de trabajar con cinco dimensiones, trabaja con solo tres dimensiones de actuación: confidencialidad, integridad y disponibilidad.

CICLO DE DEMING

Como anteriormente hemos visto en la ISO 22301, en el ENS, también se utiliza el ciclo de Deming para la gestión del sistema. Este modelo que vamos a describir en detalle a continuación se aplica a la estructura de todos los procesos del sistema de gestión de seguridad de la información.



Este método consta de las siguientes fases: planificar, hacer, verificar y actuar. Es un método iterativo que ayuda a las organizaciones a poder implementar con éxito, mantener de forma eficaz y mejorar de forma continua el sistema de gestión de seguridad de la información utilizado para gestionar los requerimientos del ENS.

CATEGORIZACIÓN EN EL ENS

El ENS establece tres niveles de valoración en función del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los servicios:

BAJO, MEDIO y ALTO. En función de la categoría, como veremos posteriormente, se aplican unos controles u otros.

Nivel BAJO

Las consecuencias de un incidente de seguridad que afectase a alguna de las dimensiones de seguridad supondrían un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

- La reducción de forma apreciable de la capacidad de la organización para atender eficazmente sus obligaciones corrientes, aunque estas sigan desempeñándose.
- El sufrimiento de un daño menor por los activos de la organización.
- El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
- Causar un perjuicio menor a algún individuo que, aun siendo molesto, pueda ser fácilmente reparable.
- Otros de naturaleza análoga.

Nivel MEDIO

Las consecuencias de un incidente de seguridad que afectase a alguna de las dimensiones de seguridad supondrían un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio grave:

- La reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.
- El sufrimiento de un daño significativo por los activos de la organización.
- El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
- Causar un perjuicio significativo a algún individuo, de difícil reparación.
- Otros de naturaleza análoga.

Nivel ALTO

Las consecuencias de un incidente de seguridad que afectase a alguna de las dimensiones de seguridad supondrían un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:

- La anulación de la capacidad de la organización para atender alguna de sus obligaciones fundamentales y que estas sigan desempeñándose.
- El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.
- El incumplimiento grave de alguna ley o regulación.
- Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
- Otros de naturaleza análoga.

Estos niveles se asignan a cada una de las cinco dimensiones de seguridad (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) tanto de la información manejada como del servicio prestados.

Una vez se dispone de la valoración de impactos en la seguridad de las distintas dimensiones en los servicios prestados e informaciones manejadas por el organismo dentro del alcance del ENS, se procederá a categorizar el sistema de información del cual dependen.

La categoría se determinará según lo indicado en el anexo I del ENS que básicamente especifica que:

1. En cada dimensión de seguridad, el nivel del sistema será el mayor de todas las informaciones y servicios (activos esenciales) que soporta.
2. La categoría del sistema (BÁSICA, MEDIA o ALTA) será equivalente al mayor nivel de seguridad de todas sus dimensiones (BAJO, MEDIO o ALTO).

Ejemplo: Supongamos un sistema de información que soporta los activos de información y de servicios mostrados en la tabla siguiente, donde se puede ver el cálculo tanto de los niveles de seguridad de cada dimensión del sistema, como el de su categoría.

ACTIVO	[D]	[I]	[C]	[A]	[T]	
Información1	0	B	M	B	B	
Información2	0	B	B	0	0	
Servicio1	M	B	M	B	B	
Servicio2	B	B	B	M	B	
Servicio3	B	B	B	B	0	CATEGORÍA
Sistema	**M**	**B**	**M**	**M**	**B**	**M**

Como vemos en la tabla anterior, al tener activos, bien de información o de servicio que tienen en una de sus dimensiones a nivel medio, el sistema entero quedará categorizado como de nivel medio.

MEDIDAS DE SEGURIDAD ESQUEMA NACIONAL DE SEGURIDAD

Las medidas de seguridad son 73 en total en la versión del ENS del 2022 (anteriormente con la versión del 2010 eran 75) y se dividen en tres grupos:

Marco organizativo [org]. Constituido por un conjunto de cuatro medidas relacionadas con la organización global de la seguridad.

Marco operacional [op]. Formado por 33 medidas que se deben tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

Medidas de protección [mp]. Son 36 medidas que se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

La selección de las medidas de seguridad aplicables se hace siguiendo estos pasos:

1. Identificación de los tipos de activos presentes.
2. Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.
3. Determinación del nivel correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.
4. Determinación de la categoría del sistema, según lo definido en el anexo I.
5. Selección de las medidas de seguridad apropiadas de entre las contenidas en el anexo II, de acuerdo con las dimensiones de seguridad y sus niveles o bien de acuerdo con la categoría del sistema, según se indique en el mencionado anexo.

Se recomienda la lectura detenida del anexo II del ENS, así como de la guía CCN-STIC 808 Guía de verificación de cumplimiento del ENS, donde se desarrolla el contenido y la aplicación de todas las medidas de seguridad.

Anexo II: ENS. https://www.boe.es/boe/dias/2022/05/04/pdfs/BOE-A-2022-7191.pdf

Guía CCN-STIC 808: Guía de Seguridad de las TIC, ENS verificación de cumplimiento. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens/file.html

En el apartado siguiente se van a enunciar cada uno de los 73 controles del ENS, para posteriormente en el siguiente apartado, poner el foco en los tres controles relativos a la continuidad de negocio.

MEDIDAS DE SEGURIDAD EN EL ENS:2022

Como hemos indicado anteriormente las 73 medidas de seguridad del ENS (versión 2022) se agrupan en **3 tipos:**

Marco organizativo (4 controles)

org. 1 Política de seguridad
org. 2 Normativa de seguridad
org. 3 Procedimientos de seguridad
org. 4 Proceso de autorización

Marco operacional (33 controles)

op.pl Planificación

- **op.pl.1** Análisis de riesgos
- **op.pl.2** Arquitectura de seguridad
- **op.pl.3** Adquisición de nuevos componentes
- **op.pl.4** Dimensionamiento/gestión de la capacidad
- **op.pl.5** Componentes certificados

op.acc Control de acceso

- **op.acc.1** Identificación
- **op.acc.2** Requisitos de acceso
- **op.acc.3** Segregación de funciones y tareas
- **op.acc.4** Proceso de gestión de derechos de acceso
- **op.acc.5** Mecanismo de autenticación (usuarios externos)
- **op.acc.6** Mecanismo de autenticación (usuarios de la organización)

op.exp Explotación

- **op.exp.1** Inventario de activos
- **op.exp.2** Configuración de seguridad
- **op.exp.3** Gestión de la configuración de seguridad
- **op.exp.4** Mantenimiento y actualizaciones de seguridad
- **op.exp.5** Gestión de cambios
- **op.exp.6** Protección frente a código dañino
- **op.exp.7** Gestión de incidentes
- **op.exp.8** Registro de la actividad
- **op.exp.9** Registro de la gestión de incidentes
- **op.exp.10** Protección de claves criptográficas

op.ext Recursos externos

- **op.ext.1** Contratación y acuerdos de nivel de servicio
- **op.ext.2** Gestión diaria
- **op.ext.3** Protección de la cadena de suministro
- **op.ext.4** Interconexión de sistemas

op.nub Servicios en la nube

- **op.nub.1** Protección de servicios en la nube

op.cont Continuidad del servicio

- **op.cont.1** Análisis de impacto
- **op.cont.2** Plan de continuidad
- **op.cont.3** Pruebas periódicas
- **op.cont.4** Medios alternativos

op.mon Monitorización del sistema

- **op.mon.1** Detección de intrusión
- **op.mon.2** Sistema de métricas
- **op.mon.3** Vigilancia

Medidas de protección (36 controles):

mp.if Protección de las instalaciones e infraestructuras

- **mp.if.1** Áreas separadas y con control de acceso
- **mp.if.2** Identificación de las personas
- **mp.if.3** Acondicionamiento de los locales
- **mp.if.4** Energía eléctrica
- **mp.if.5** Protección frente a incendios
- **mp.if.6** Protección frente a inundaciones
- **mp.if.7** Registro de entrada y salida de equipamiento

mp.per Gestión del personal

- **mp.per.1** Caracterización del puesto de trabajo
- **mp.per.2** Deberes y obligaciones
- **mp.per.3** Concienciación
- **mp.per.4** Formación

mp.eq Protección de los equipos

- **mp.eq.1** Puesto de trabajo despejado
- **mp.eq.2** Bloqueo de puesto de trabajo
- **mp.eq.3** Protección de dispositivos portátiles
- **mp.eq.4** Otros dispositivos conectados a la red

mp.com Protección de las comunicaciones

- **mp.com.1** Perímetro seguro
- **mp.com.2** Protección de la confidencialidad
- **mp.com.3** Protección de la integridad y de la autenticidad
- **mp.com.4** Separación de flujos de información en la red

mp.si Protección de los soportes de información

mp.si.1 Marcado de soportes
mp.si.2 Criptografía
mp.si.3 Custodia
mp.si.4 Transporte
mp.si.5 Borrado y destrucción

mp.sw Protección de las aplicaciones informáticas

mp.sw.1 Desarrollo de aplicaciones
mp.sw.2 Aceptación y puesta en servicio 4

mp.info Protección de la información

mp.info.1 Datos personales
mp.info.2 Calificación de la información
mp.info.3 Firma electrónica
mp.info.4 Sellos de tiempo
mp.info.5 Limpieza de documentos
mp.info.6 Copias de seguridad

mp.s Protección de los servicios

mp.s.1 Protección del correo electrónico
mp.s.2 Protección de servicios y aplicaciones web
mp.s.3 Protección de la navegación web
mp.s.4 Protección frente a la denegación de servicio

Fuente y más información sobre cada uno de los controles anteriores:

- **Anexo II:** ENS. https://www.boe.es/boe/dias/2022/05/04/pdfs/BOE-A-2022-7191.pdf

- De todos los grupos anteriores, las medidas de seguridad especializadas en continuidad de negocio, son las relativas al capítulo op.cont Continuidad del servicio, que como hemos visto está formado por estas tres medidas, que vamos a comentar en detalle en el siguiente apartado:

  op.cont.1 Análisis de impacto
  op.cont.2 Plan de continuidad
  op.cont.3 Pruebas periódicas

CONTINUIDAD DE NEGOCIO EN EL ENS

El esquema nacional de seguridad (ENS) recoge como veremos en el apartado siguiente con la ISO 27001, la continuidad de negocio, dentro de sus medidas de seguridad. En concreto el apartado es el **op.cont Continuidad del servicio**, que seguidamente pasamos a detallar:

Como hemos visto anteriormente existen tres controles específicos de continuidad de negocio.

Op.cont.1 Análisis de impacto

Está medida a partir de sistemas categorizados como de nivel MEDIO, y lo que nos pide es lo que se indica a continuación.

Se realizará un análisis de impacto que permita determinar:

a) Los requisitos de disponibilidad de cada servicio medidos como el impacto de una interrupción durante un cierto período.
b) Los elementos que son críticos para la prestación de cada servicio.

Para ver más detalles sobre cómo realizar un análisis de impacto (BIA), revisar en detalle el capítulo 2.1. ISO 22301, apartado BIA.

Op.cont.2 Plan de continuidad

Está medida a partir de sistemas categorizados como de nivel ALTO, y lo que nos pide es lo que se indica a continuación.

Se desarrollará un plan de continuidad que establezca las acciones que se deban ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Dicho plan recogerá los siguientes aspectos:

- Se identificarán funciones, responsabilidades y actividades que se deban realizar.
- Existirá una previsión para coordinar la entrada en serv de los medios alternativos de forma que se garantice p seguir prestando los servicios esenciales de la organiza
- Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveed correspondientes.

- Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
- El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

Op.cont.3 Pruebas periódicas

Está medida se lleva a partir de sistemas categorizados como de nivel ALTO, y lo que nos pide es que se realicen pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad.

Bibliografía

España (2017). Estrategia de seguridad nacional.
https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021

España (2019). Estrategia nacional de ciberseguridad.
https://www.boe.es/buscar/pdf/2019/BOE-A-2019-6347-consolidado.pdf

Guías CCN-STIC. https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html

INCIBE. Plan de contingencia y seguridad de la información.
https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdfLey Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. https://www.boe.es/buscar/pdf/2007/BOE-A-2007-19814-consolidado.pdf

Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas.
https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10565-consolidado.pdf

Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.
https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10566-consolidado.pdf

Real Decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad en el ámbito de la Administración electrónica (versión consolidada).
https://www.boe.es/buscar/pdf/2010/BOE-A-2010-1330-consolidado.pdf

Real Decreto 4/2010, de 8 de enero, por el que se regula el esquema nacional de interoperabilidad en el ámbito de la Administración electrónica.
https://www.boe.es/buscar/pdf/2010/BOE-A-2010-1331-consolidado.pdf

Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad en el ámbito de la Administración electrónica.
https://www.boe.es/boe/dias/2015/11/04/pdfs/BOE-A-2015-11881.pdf

Real Decreto 311/2022, de 3 de mayo, por el que se regula el esquema nacional de seguridad.
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
https://www.boe.es/doue/2016/119/L00001-00088.pdf

Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el esquema nacional de seguridad.
https://www.boe.es/boe/dias/2016/11/02/pdfs/BOE-A-2016-10109.pdf

Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
https://www.boe.es/boe/dias/2018/04/03/pdfs/BOE-A-2018-4573.pdf

Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
https://www.boe.es/boe/dias/2018/04/19/pdfs/BOE-A-2018-5370.pdf

3.3

ISO 27001. SEGURIDAD DE LA INFORMACIÓN

Jorge Edo Juan
Jorge Sánchez López

ANTECEDENTES

La norma ISO 27001 es un marco de gestión desarrollado por ISO (Organización Internacional de Normalización, en español) con el propósito de ayudar a gestionar la seguridad de la información en una organización.

Actualmente, con alcance mundial, este estándar es la norma de referencia para certificar la seguridad de la información en las organizaciones, independientemente de su tamaño, y estructura, dado que existen organizaciones tanto del ámbito privado, como del público, certificadas; así como organizaciones pequeñas, medianas, grandes o muy grandes.

La ISO 27001, al igual que hemos comentado anteriormente está basada en la creación de un sistema de gestión. Las organizaciones implementan de esta forma sistemas de gestión para mejorar su seguridad al mismo tiempo que consiguen aportar más valor a sus clientes.

Como hemos comentado en el capítulo 2, relativo a la ISO 22301, como cada vez es más habitual que las organizaciones gestionen varios marcos de cumplimiento simultáneamente, puede resultar interesante que se implemente un sistema de gestión integrado (SGI).

A continuación, vamos a comentar los principales hitos de desarrollo de la ISO 27001 a lo largo del tiempo:

1990. Publicado el código de prácticas BS-7799 por el Departamento de Comercio e Industria del Reino Unido.

1995. Se publicó el código de prácticas BS-7799-1.

1998. Se publicó la especificación de seguridad de la información BS-7799-2.

2000. Publicado el código de prácticas del sistema de gestión de la seguridad de la información ISO/IEC 17799.

2005. Publicación de la primera versión del estándar ISO 27001 como tal.

2007. Se publicaron los requisitos del organismo de certificación según el marco 27006.

2008 a 2012. Publicación de otros marcos dentro de la familia de la ISO 27000.

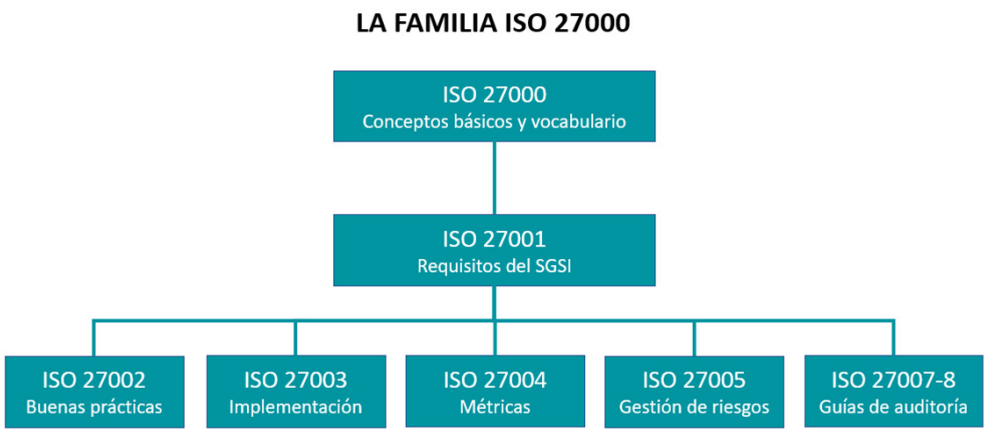
2013. Publicada la versión ISO/IEC 27001: 2013.

Febrero 2022. Revisado el marco de buenas prácticas ISO 27002: 2022.

Octubre 2022. Publicada la versión ISO/IEC 27001: 2022

FAMILIA ISO 27000

La familia de normas ISO/IEC 27000 está dedicada a la seguridad de la información. En el gráfico siguiente, se muestran los marcos incluidos dentro de esta familia:



ISO/IEC 27000. Presenta los conceptos básicos y el vocabulario que se aplica al establecimiento de un sistema de gestión de seguridad de información.

ISO/IEC 27001. Define los requisitos del sistema de gestión de seguridad de la información (SGSI) y proporciona un conjunto de referencias de controles de seguridad en su anexo A.

ISO/IEC 27701. Especifica los requisitos y proporciona orientación para establecer, mantener y mejorar continuamente un sistema de gestión de información de privacidad como una extensión de las normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la privacidad.

ISO/IEC 27002. Proporciona el marco de buenas prácticas para la implementación de los controles de seguridad de la información del anexo A de la ISO 27001.

ISO/IEC 27003. Orientación sobre la implementación o configuración de un SGSI.

ISO/IEC 27004. Directrices para el seguimiento y medición del rendimiento de la seguridad de la información y la eficacia de un SGSI.

ISO/IEC 27005. Directrices sobre la gestión de riesgos de seguridad de la información que cumple con los conceptos, modelos y procesos generales especificados en la norma ISO/IEC 27001.

ISO/IEC 27006. Requisitos para las organizaciones que auditan y certifican un SGSI.

ISO/IEC 27007. Orientación para la auditoría de los sistemas de gestión de seguridad de la información.

ISO/IEC TS 27008. Orientación para los auditores de controles de seguridad de la información.

ISO/IEC 27011. Orientación sobre la implementación de los controles de seguridad de la información en la industria de las telecomunicaciones.

ISO/IEC 27017. Introduce un conjunto de controles complementarios a la ISO 27002, orientados directamente a los servicios desplegados en la nube y a los proveedores que los proporcionan, y propone controles específicos vinculados a la gestión y provisión de servicios seguros en la nube.

ISO/IEC 27018. Marco de buenas prácticas para la protección de información personal (PII) en servicios desplegados en la nube.

ISO 27799. Orientación sobre el uso de ISO/IEC 27002 en la informática médica.

Fuente: https://www.iso.org

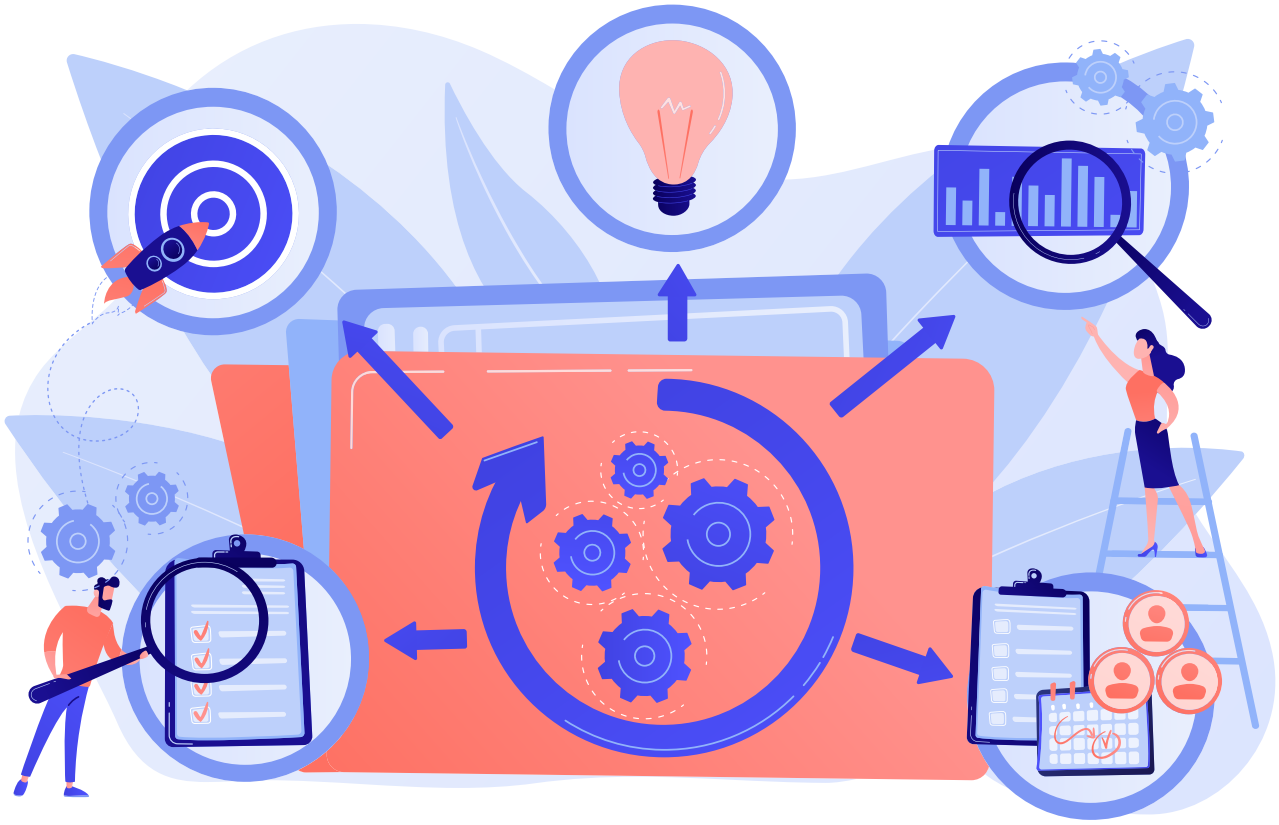


Imagen de vectorjuice en Freepik

CICLO DE DEMING

Como anteriormente hemos visto en la ISO 22301, todos los sistemas de gestión, y la ISO 27001 no podía ser diferente, utilizan el ciclo de Deming para la gestión del sistema.

ESTRUCTURA DE LA NORMA ISO 27001

Como hemos comentado con anterioridad (en el apartado de antecedentes), de acuerdo con la estructura de todos los sistemas de gestión, para posibilitar la integración de diferentes sistemas: ISO 9001, ISO 27001, ISO 22301..., la estructura de las cláusulas de las normas anteriores es idéntica. Este hecho facilita enormemente la integración entre sistemas, y define un sistema de gestión integrado (SGI), como hemos comentado.

Según hemos indicado, en el capítulo 2, apartado 1, donde hemos hablado en detalle de los sistemas de gestión, y más en concreto de la ISO 22301, de acuerdo con el modelo PDCA, las cláusulas 4 a 10 cubren los siguientes componentes, en el caso de la ISO 27001 relativos a la seguridad de la información:

Cláusula 4, Contexto de la Organización. Presenta los requisitos necesarios para establecer el contexto específico que aplica a cada organización, así como las necesidades, requisitos de las partes interesadas y el alcance del sistema de gestión de seguridad de la información (SGSI).

Cláusula 5, Liderazgo. Define la importancia de la implicación de la alta dirección en el proyecto de seguridad de la información, así como el establecimiento de una política de seguridad de la información, la forma de comunicar dicha política tanto a los empleados, como a otras partes interesadas. También en esta cláusula determina los puntos clave para la asignación de los roles adecuados con el fin de poder implantar con éxito el SGSI en la organización.

Cláusula 6, Planificación. Describe los requisitos para establecer objetivos estratégicos y principios guía para el SGSI. En este apartado cobra especial importancia tanto la determinación de los riesgos y oportunidades que puedan afectar el SGSI, como el tratamiento de dichos riesgos y oportunidades para obtener un SGSI eficiente y resiliente ante cualquier desastre que se pueda producir. En esta cláusula también se definen los objetivos anuales de seguridad de la información y se plantea una adecuada planificación para poder culminarlos con éxito.

Cláusula 7, Soporte. Determina los recursos necesarios para desarrollar con éxito el proyecto, determina la competencia de las personas que van a llevarlo a cabo y planifica actividades de concienciación que se deben llevar a cabo de forma periódica. También se define en este punto la comunicación con las partes interesadas durante la vigencia del SGSI. En este punto también se crea y se lleva a cabo el mantenimiento de un sistema documental adecuado a las características y el contexto de la organización.

Cláusula 8, Operación. En este punto se define como hay que desarrollar las actividades de planificación y control operacional del SGSI, la evaluación del riesgo, en función de diferentes escenarios de riesgo que puedan originarse en la organización.

Cláusula 9, Evaluación del desempeño. Determina los requisitos necesarios para medir el desempeño de la seguridad de la información, mediante la definición y el mantenimiento de las métricas más adecuadas por un lado a las exigencias de la norma y, por otro, a las características de la organización. En esta cláusula también se plantean los requisitos necesarios para realizar auditorías internas periódicas así como los aspectos que se deben tener en cuenta cuando se lleva a cabo la revisión de la gestión por parte de la dirección.

Cláusula 10, Mejora. Identifica y actúa sobre las no conformidades del SGSI y la mejora continua mediante acciones correctivas.

ANEXO A. ISO 27001:2013

La norma ISO 27001 ya hemos comentado que dispone de una serie de cláusulas numeradas de la 4 a la 10, que hemos visto en el apartado anterior.

Adicionalmente el cuerpo de la ISO 27001, versión 2013, disponía de 114 controles agrupados en 35 objetivos de control, en controles numerados desde el grupo A.5, hasta el A.18.

Sin entrar en cada uno de los controles de la ISO 27001: 2013 sí que seguidamente indicaremos los apartados en los que están agrupados cada uno de ellos:

A5. Políticas de seguridad de la información;
A6. Organización de la seguridad de la información;
A7. Seguridad relativa a los recursos humanos;
A8. Gestión de activos;
A9. Control de acceso;
A10. Criptografía;
A11. Seguridad física y del entorno;A12. Seguridad de las operaciones;
A13. Seguridad en las comunicaciones;
A14. Adquisición, desarrollo y mantenimiento de los sistemas de información;
A15. Relaciones con proveedores;
A16. Gestión de incidentes de la seguridad de la información;
A17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio;
A18. Cumplimiento.

De todos los grupos anteriores, la familia especializada en continuidad de negocio, es la del grupo A.17, que detallaremos en los próximos apartados.

ANEXO A. ISO 27001:2022

A continuación, vamos a comentar las principales diferencias entre la versión 2013 y la de 2022 tanto en relación con las cláusulas, como con los controles del anexo A.

Cambios en las cláusulas. ISO 27001:2022

Reseñar que los cambios que se han producido en el cuerpo de cláusulas de la ISO 27001, son muy poco relevantes, únicamente indicaremos los siguientes:

- Hay que determinar qué requisitos de las partes interesadas se abordan a través del sistema de gestión de seguridad de la información.
- Hay que determinar las interacciones entre los procesos.
- Los objetivos en el SGSI tendrán que ser monitorizados y documentarse.
- Hay que planificar de forma más detallada los cambios en el SGSI.
- La comunicación con las partes interesadas se simplifica.
- En el control operacional se definirán los criterios necesarios para los procesos y cómo se implementará el control de estos.
- Mayor exigencia de control en relación con los proveedores respecto a los productos y servicios que sean provistos por terceros.
- En la revisión de la dirección hay que evaluar de forma más detallada que anteriormente, los cambios en las necesidades y las expectativas de las partes interesadas que sean relevantes para el SGSI.

Cambios en el anexo A. ISO 27001: 2022

La parte correspondiente a los controles del anexo A, es la que sí que tiene unos cambios mucho más relevantes que los correspondientes a las cláusulas. De entrada, se pasa de **114 controles agrupados en 14 capítulos a 93, agrupados en 4 capítulos**, con lo que integra varios controles de la versión 2013 en otros controles, para reducir así el número de estos.

Por otro lado, se plantean 11 nuevos controles, que vamos a comentar seguidamente:

- **Inteligencia de amenazas (5.7).** Deberemos ser capaces de recoger y analizar información sobre amenazas.
- **Seguridad de la información en el uso de servicios en la nube (5.23).** Este nuevo control requiere que se desarrollen procedimientos específicos para los servicios que tenga la entidad en la nube, y de esta forma se diferencia de los controles A.15 de la versión 2013 sobre servicios prestados por terceros, para diferenciarlos explícitamente de los servicios en la nube.
- **Continuidad de las TIC (5.30).** En la versión del 2022 queda claramente enfocado este control a la continuidad de las TIC, y deja la continuidad del negocio para otros estándares como la ISO 22301. Así, este control se enfoca a la continuidad TIC, diferenciándola de la continuidad del negocio.
- **Monitorización de la seguridad física (7.4).** Será necesario implementar mecanismos de control de acceso que detecten si se producen accesos físicos no autorizados.
- **Gestión de la configuración (8.9).** Este control está orientado a su integración o gestión mediante la norma ISO 20000 o ITIL, ambos marcos específicos de gestión de servicios IT.
- **Borrado de la información (8.10).** Ligado al principio de la limitación del plazo de conservación de la información, está relacionado con los requerimientos del RGPD en este punto.
- **Enmascaramiento de datos (8.11).** Mediante técnicas de anonimización y seudoanonimización para proteger la información en caso de fugas de información y brechas de seguridad que afecten principalmente a datos personales.
- **Prevención de fuga de datos (8.12).** Con la utilización de herramientas que detecten este tipo de fugas.
- **Monitorización de actividades (8.16).** Mediante sistemas SIEM.
- **Filtrado web (8.23).** Con este control, se pretende restringir la navegación de los usuarios, con el objetivo de reducir el riesgo de acceso a contenidos maliciosos que puedan provocar incidentes de seguridad.
- **Control de codificación segura (8.28).** Este control va más allá de las exigencias del control «política de desarrollo seguro» de la versión del 2013, y requiere además de una política, para que se implementen metodologías de desarrollo seguro.

Como hemos señalado antes los 93 controles de la ISO 27001:2022, se agrupan en **4 capítulos:**

Controles organizacionales (37 controles):

5.1. Políticas de seguridad de la información;
5.2. Roles y responsabilidades de seguridad de la información;
5.3. Segregación de funciones;
5.4. Responsabilidades de la dirección;
5.5. Contacto con las autoridades;
5.6. Contacto con grupos de interés especial;
5.7. Inteligencia de amenazas;
5.8. Seguridad de la información en la gestión de proyectos;
5.9. Inventario de la información y activos asociados;
5.10. Uso aceptable de la información;
5.11. Devolución de activos;
5.12. Clasificación de la información;
5.13. Etiquetado de la información;
5.14. Transferencia de la información;
5.15. Control de accesos;
5.16. Gestión de identidad;
5.17. Información de autenticación;
5.18. Derechos de acceso;
5.19. Seguridad de la información en las relaciones con los proveedores;
5.20. Seguridad de la información en los acuerdos con los proveedores;
5.21. Seguridad de la información en la cadena de suministro;
5.22. Seguimiento, revisión y gestión de cambios de los proveedores;
5.23. Seguridad de la información en los servicios en la nube;
5.24. Planificación y preparación de la gestión de incidentes de seguridad de la información;
5.25. Evaluación y decisión sobre eventos de seguridad de la información;
5.26. Respuesta a incidentes de seguridad de la información;
5.27. Aprendiendo de los incidentes de seguridad de la información;
5.28. Recopilación de pruebas;
5.29. Seguridad de la información durante la interrupción;

5.30. Preparación de las TIC para la continuidad del negocio;
5.31. Requisitos legales, reglamentarios y contractuales;
5.32. Derechos de propiedad intelectual;
5.33. Protección de registros;
5.34. Privacidad y protección de datos personales;
5.35. Revisión independiente de la seguridad de la información;
5.36. Cumplimiento de políticas y normativas de seguridad de la información;
5.37. Procedimientos operativos documentados.

Controles de personas (8 controles):

6.1. Filtrado de candidatos;
6.2. Términos y condiciones de empleo;
6.3. Concienciación y formación en seguridad de la información;
6.4. Proceso disciplinario;
6.5. Responsabilidades después de la terminación o cambio de empleo;
6.6. Acuerdos de confidencialidad y no divulgación;
6.7. Teletrabajo;
6.8. Reporte de eventos de seguridad de la información.

Controles físicos (14 controles):

7.1. Perímetro de seguridad física;
7.2. Entrada física;
7.3. Aseguramiento de oficinas, salas e instalaciones;
7.4. Supervisión de la seguridad física;
7.5. Protección contra amenazas físicas y ambientales;
7.6. Trabajo en áreas seguras;
7.7. Política de escritorio y pantalla limpios;
7.8. Ubicación y protección del equipo;
7.9. Seguridad de los equipos fuera de las instalaciones;
7.10. Medios de almacenamiento;
7.11. Utilidades de apoyo;
7.12. Seguridad del cableado;
7.13. Mantenimiento de equipos;
7.14. Eliminación segura o reutilización de equipos;

Controles tecnológicos (34 controles):

8.1. Dispositivos de punto final de usuario;
8.2. Derechos de acceso privilegiado;
8.3. Restricción de acceso a la información;
8.4. Acceso al código fuente;
8.5. Autenticación segura;
8.6. Gestión de la capacidad;
8.7. Protección contra programas maliciosos o malware
8.8. Gestión de vulnerabilidades técnicas;
8.9. Gestión de la configuración;
8.10. Eliminación de información;
8.11. Enmascaramiento de datos;
8.12. Prevención de fuga de datos;
8.13. Copia de seguridad de la información;
8.14. Redundancia de las instalaciones de procesamiento de información;
8.15. Registro;
8.16. Actividades de seguimiento;
8.17. Sincronización de relojes;
8.18. Uso de programas de utilidad privilegiados;
8.19. Instalación de software en sistemas operativos;
8.20. Seguridad de redes;
8.21. Seguridad en los servicios de red;
8.22. Segregación de redes;
8.23. Filtrado web;
8.24. Uso de criptografía;
8.25. Ciclo de vida de desarrollo seguro;
8.26. Requisitos de seguridad de la aplicación;
8.27. Arquitectura de sistema seguro y principios de ingeniería;
8.28. Codificación segura;
8.29. Pruebas de seguridad en desarrollo y aceptación;
8.30. Externalización del desarrollo de software;
8.31. Separación de los entornos de desarrollo, pruebas y producción;
8.32. Gestión de cambios;
8.33. Información de prueba;
8.34. Protección de los sistemas de información durante las pruebas de auditoría.

Fuente y más información sobre cada uno de los controles anteriores:
- **ISO/IEC 27001:2022**
- **ISO/IEC 27002:2022.**

ISO/IEC 27002:2022.

Continuidad de Negocio en la ISO 27001

La norma ISO 27001, como hemos visto más arriba es un marco idóneo para la continuidad de negocio, ya que prepara a la organización ante la interrupción de los procesos en caso de que se produzca un evento adverso y resguarda la totalidad de los procesos críticos de negocio de los efectos que pueden ocasionar dichos desastres, al tiempo que asegura una recuperación de dichos procesos críticos, con la mayor rapidez y agilidad posible.

En el caso del marco ISO 27001:2022, el control que se refiere explícitamente a la continuidad del negocio es el control 5.30 dentro del capítulo de controles organizacionales, el relativo a la **Preparación de las TIC** para la continuidad del negocio, donde el enfoque está claramente orientado a la preparación de un plan de contingencia TIC para la organización. En este punto cabe indicar las siguientes consideraciones:

- La organización debe determinar si la continuidad de la seguridad de la información queda dentro del proceso de continuidad del negocio o dentro del proceso de gestión de la recuperación de desastres.
- Los requisitos de seguridad de información deben determinarse al planificar la continuidad del negocio y la recuperación de desastres.
- En ausencia de planes formales de continuidad del negocio y de recuperación de desastres, la gestión de la seguridad de la información debe asumir que los requisitos de seguridad de la información son los mismos tanto en condiciones adversas como en las condiciones normales de operación.
- Incluir el RTO (tiempo de recuperación objetivo), y RPO (punto de recuperación objetivo) priorizados y los procedimientos para restaurar cada uno de los elementos especificados en el BIA (análisis de impacto). Para más detalles véase el capítulo 2, ISO 22031, puntos relativos a dichos conceptos.

En los siguientes puntos, recogemos los **documentos necesarios** para cumplir este control de la ISO 27001:

- Política de continuidad del negocio;
- Metodología para el análisis del impacto en el negocio;
- Cuestionario sobre el análisis del impacto en el negocio;
- Estrategia de continuidad del negocio;
- Lista de actividades;
- Prioridades de recuperación para las actividades;
- Objetivos de tiempo de recuperación para actividades;
- Ejemplos de escenarios de incidentes disruptivos;
- Estrategia de recuperación de actividades.

Verificación, revisión de la continuidad de la seguridad de la información

Una vez planificado e implementado un plan de contingencia TIC en la organización, hay que comprobar la eficacia de dicho plan a intervalos regulares, siguiendo las siguientes recomendaciones:

- Ejecución y prueba de la funcionalidad de los procesos, procedimientos y controles para la continuidad de la seguridad de la información asegurando que son consistentes con los objetivos de continuidad de la organización.
- Ejecución y prueba del conocimiento y la rutina para operar los procesos, procedimientos y controles de continuidad de la seguridad de la información asegurando que su rendimiento es consistente con los objetivos de continuidad de seguridad de la información.

Finalmente como conclusiones referidas a la seguridad de la información (ISO 27001) y la continuidad de negocio (ISO 22301), podemos indicar que para que la organización disponga de un plan de continuidad de negocio efectivo, es fundamental que dicho plan, se sustente un plan de contingencia TIC que le de soporte.

Bibliografía

AENOR. ISO 31000:2018. Gestión del Riesgo. Directrices.
https://tienda.aenor.com/norma-une-iso-31000-2018-n0059900

AENOR. UNE-EN ISO 22301:2019. Seguridad y Resiliencia, Sistema de Gestión de la Seguridad de la Información. Requisitos.
https://tienda.aenor.com/norma-une-en-iso-22301-2020-n0063818

AENOR. UNE-ISO/IEC 27001:2013. Tecnología de la Información, Técnicas de Seguridad, Sistema de Gestión de Seguridad de la Información (SGSI).
https://tienda.aenor.com/norma-une-en-iso-iec-27001-2017-n0058428

España (2017). Estrategia de Seguridad Nacional.
https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021

España (2019). Estrategia Nacional de Ciberseguridad.
https://www.boe.es/buscar/pdf/2019/BOE-A-2019-6347-consolidado.pdf

INCIBE. Plan de Contingencia y Seguridad de la Información.
https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

ISO/IEC 27001: 2022. Information security, cybersecurity and privacy protection.
https://www.iso.org/standard/82875.html

ISO/IEC 27002: 2022. Information security, cybersecurity and privacy protection - Information security controls.
https://www.iso.org/standard/75652.html

4

CERTIFICACIÓN DE LA CONTINUIDAD DE NEGOCIO

Imagen de Freepik

4.1 CERTIFICACIÓN DE LA CONTINUIDAD DE NEGOCIO

Eva Banegas González

INTRODUCCIÓN

Aunque todos tenemos claro a estas alturas de siglo que la gran mayoría de las empresas se sostienen sobre tecnologías de la información, y la tecnología está integrada en nuestras vidas, no está tan claro que las empresas vean o tengan en mente que un evento disruptivo puede dar al traste con la operatividad de su negocio.

En cuestión de seguridad de la información debemos ser escépticos respecto a la frase «esto nunca nos va a pasar a nosotros», ya que en los últimos años hemos visto como grandes empresas, administraciones públicas y varios sectores críticos han sido objeto de ataques cibernéticos, programas de chantaje o *ransomware* u otros actos disruptivos que han afectado a su continuidad en el negocio.

Hoy por hoy nadie está seguro de que en algún momento sea objetivo para cibercriminales, *hackers*, extorsionadores, etc., en definitiva, cualquier elemento que provoque una caída de nuestros sistemas y, por tanto, consiga una interrupción de nuestro negocio.

En 2010, un periódico de tirada nacional realizaba una encuesta sobre la existencia de planes de continuidad de negocio en el tejido empresarial español. Las conclusiones eran demoledoras: más del 50 % contestaba que no tenía plan de continuidad del negocio, y eran empresas que facturaban entre 30 y 60 millones de euros. Hoy, en 2022, los resultados no serían mucho mejores.

Los objetivos de la mayoría de las empresas son realizar planes de continuidad de negocio y planes de contingencia, pero estos difícilmente se llegan a desarrollar y solo quedan como buenas intenciones para acometer en el próximo año.

Datos más recientes de una encuesta realizada por PwC, la Global Crisis Survey 2021, dice literalmente: «el 95 % de los encuestados expresó que sus capacidades de gestión en continuidad de negocio requieren mejoras como resultado de los eventos vividos». El informe continúa diciendo que la planificación de la continuidad de negocio y los planes de recuperación ante desastres, no estaban alineados con el negocio en la empresa. Por eso su efectividad fue escasa e incluso nula.

Estos datos nos llevan a reflexionar sobre el momento actual para llevar a cabo una evaluación correcta y acorde alineando las estrategias del negocio con las tecnológicas en un proceso holístico en que se consideren todos los activos críticos y las dependencias que lo soportan.

En Kiwa hacemos la certificación estándar internacional para la gestión de la continuidad del negocio, que fue desarrollada para ayudar a las organizaciones a minimizar el riesgo del cese o interrupción de un negocio o actividad.

Las principales aportaciones para las empresas y negocios que realiza la ISO-22301, son:

- Clara definición de la responsabilidad de la dirección.
- Mayor énfasis en la definición de objetivos, seguimiento mediante métricas adecuadas al negocio (KPI).
- Mejora en la planificación de los recursos para garantizar la continuidad del negocio en caso de impacto o interrupción de este.

Consideramos que es un paso más por parte de una organización, empresa o negocio (de manera voluntaria) para realizar un ejercicio de control holístico sobre su operativa de negocio y sus sistemas tecnológicos (sea del sector que sea) para poder asegurar el correcto funcionamiento después de ser impactado por una causa involuntaria que pueda producir una interrupción en la continuidad de su negocio.

La continuidad del negocio garantiza que durante una interrupción la organización continuará brindando los productos y servicios en los que confían sus clientes. Además, la continuidad de negocio ayuda a las organizaciones durante las interrupciones a volver a sus operaciones comerciales normales lo más rápidamente posible

También es una forma de asegurar a terceros con los que tenga un contrato mercantil, y que realice operaciones a usuarios o terceros para asegurar que se encuentra en las condiciones más optimas de seguir operando.

Es un valor seguro y diferencial de cara a optar a una licitación, a un acuerdo B2B, etc., en definitiva, a poder dar crédito de que, si sufrimos una interrupción de nuestro negocio, este se podrá recuperar en un tiempo razonable para continuar operando y no sufrir pérdidas económicas o reputacionales graves.

Muchas empresas están equivocadas en su estrategia al contratar productos de aseguradoras, los llamados ciberseguros, ya que piensan que estos les repondrán el servicio de manera inmediata. ¿Cuál es la realidad?, este año en algunos casos se ha triplicado la prima de estos ciberseguros, ya que han tenido que hacer frente a muchos ciberataques, lo que ha supuesto un gasto enorme para las aseguradoras y un aumento en sus primas. Pero no nos equivoquemos, un ciberseguro no te repone el servicio de manera inminente, hay un peritaje que determina, mediante análisis forense informático, las causas que han llevado a la empresa a sufrir ese ciberincidente, y ese peritaje puede requerir días para su elaboración y para reponer los sistemas impactados. Incluso puede determinar que los sistemas no estaban bien configurados y no hacerse responsables de la reposición de los activos afectados.

Un sistema de gestión de la continuidad del negocio sin embargo aporta beneficios desde las perspectivas comerciales y económicas, ya que el sistema respalda completamente los objetivos estratégicos de la organización, mejora su resiliencia y protege su credibilidad y reputación. Esto le dará a la organización que lo implante una ventaja competitiva en su sector industrial.

Los beneficios económicos al implantar un sistema de gestión de la continuidad de negocio basado en la ISO 22301 incluyen pérdidas reducidas, ya sea que estén directa o indirectamente relacionadas con la interrupción. Además, el riesgo legal y económico se reducirá también.

Finalmente, un sistema de gestión de la continuidad de negocio efectivo ayudará a las organizaciones a fortalecer sus procesos internos. Esto incluye una capacidad mejorada para mantener su eficacia durante las interrupciones al controlar de manera proactiva los riesgos potenciales y garantizar que se hayan abordado todas las vulnerabilidades operativas.

Por eso sabemos que es mejor tener una certificación de un sistema de gestión de la continuidad de negocio, en la que te hagas responsable de su realización, y un tercero externo, en este caso una entidad certificadora, que realice una evaluación a tu sistema de gestión, sujeto a los principios de auditoría de integridad, independencia e imparcialidad, profesionalidad, confidencialidad, un enfoque basado en la evidencia, en el riesgo y en la presentación de conclusiones por los que nos regimos como entidad certificadora basado en la ISO 19011 y acreditados por la ENAC.

SISTEMA DE GESTION DE LA CONTINUIDAD DEL NEGOCIO Y ESTRUCTURA DE LA NORMA ISO 22301

Un sistema de gestión de la continuidad de negocio se encarga de supervisar la implementación, operación, monitorización y revisión de todos los aspectos de la continuidad de negocio.

Para ello se busca que implemente, mantenga y mejore la política de continuidad del negocio, la entrega de productos y servicios, durante una interrupción, a un estado que se considere aceptable y que fortalezca su resiliencia mediante la aplicación efectiva del sistema de gestión de continuidad del negocio.

La estructura de la norma es la siguiente:

Las cláusulas 1 a 3 definen el alcance, las referencias normativas y los términos y definiciones de la norma.

La cláusula 4, Contexto de la organización, describe las necesidades, los requisitos y los elementos esenciales del alcance para definir el contexto del sistema de gestión aplicable a la organización.

La cláusula 5, Liderazgo, resume el papel de la alta dirección en el sistema de gestión de la continuidad del negocio, incluida la comunicación de las expectativas de liderazgo a través de una declaración en la política.

La cláusula 6, Planificación, define los requisitos para establecer los objetivos estratégicos y los principios rectores del sistema de gestión de la continuidad de negocio.

La cláusula 7, Soporte, propone el apoyo para las operaciones del sistema de gestión de la continuidad del negocio relacionadas con la competencia y la comunicación a las partes interesadas, incluida la creación, control, mantenimiento y almacenamiento de la información documentada.

La cláusula 8, Operación, describe las necesidades de la continuidad del negocio, como satisfacer esas necesidades y cómo desarrollar procedimientos para administrar la organización en caso de una interrupción.

La cláusula 9, Evaluación del desempeño, describe los requisitos necesarios para medir el desempeño de la continuidad del negocio y la conformidad del sistema de gestión de la continuidad del negocio con la norma ISO 22301 y para realizar su revisión por parte de la gerencia.

La cláusula 10, Mejora, actúa sobre la no conformidad de sistema de gestión de la continuidad de negocio y la mejora continua a través de acciones correctivas.

PRINCIPIOS FUNDAMENTALES DE LA CONTINUIDAD DEL NEGOCIO

Para tomar la determinación de que un negocio quiera opta a la certificación, debe tener en cuenta los cuatro principios fundamentales.

Responsabilidad de la alta dirección. Es crítico el apoyo de la alta dirección, para apoyar y promover activamente las iniciativas dentro de una organización.

Preparación para grandes interrupciones operativas. Es principalmente de lo que trata un sistema de gestión de la continuidad de negocio. Hay que estar preparado y predeterminar cómo responderá la organización a una interrupción importante, esto ayudará a una organización a actuar de manera adecuada y proactiva si ocurren tales interrupciones.

Comunicación. Es fundamental y uno de los aspectos clave de la recuperación de las operaciones comerciales después de la interrupción. Todos los miembros de la organización deben estar incluidos en el proceso de comunicación. La comunicación es especialmente importante en los primeros momentos de la interrupción, ya que el procedimiento de

comunicación debe determinar a qué empleados les corresponderá transmitir la comunicación tanto interna como externa, incluida la alta dirección, los asesores legales y de cumplimiento, los responsables del sistema de gestión de la continuidad de negocio, etc.
El procedimiento de comunicación abordará cualquier tema relacionado con la interrupción del servicio. También se abordarán los medios alternativos para llevar a cabo una comunicación eficaz de la interrupción.

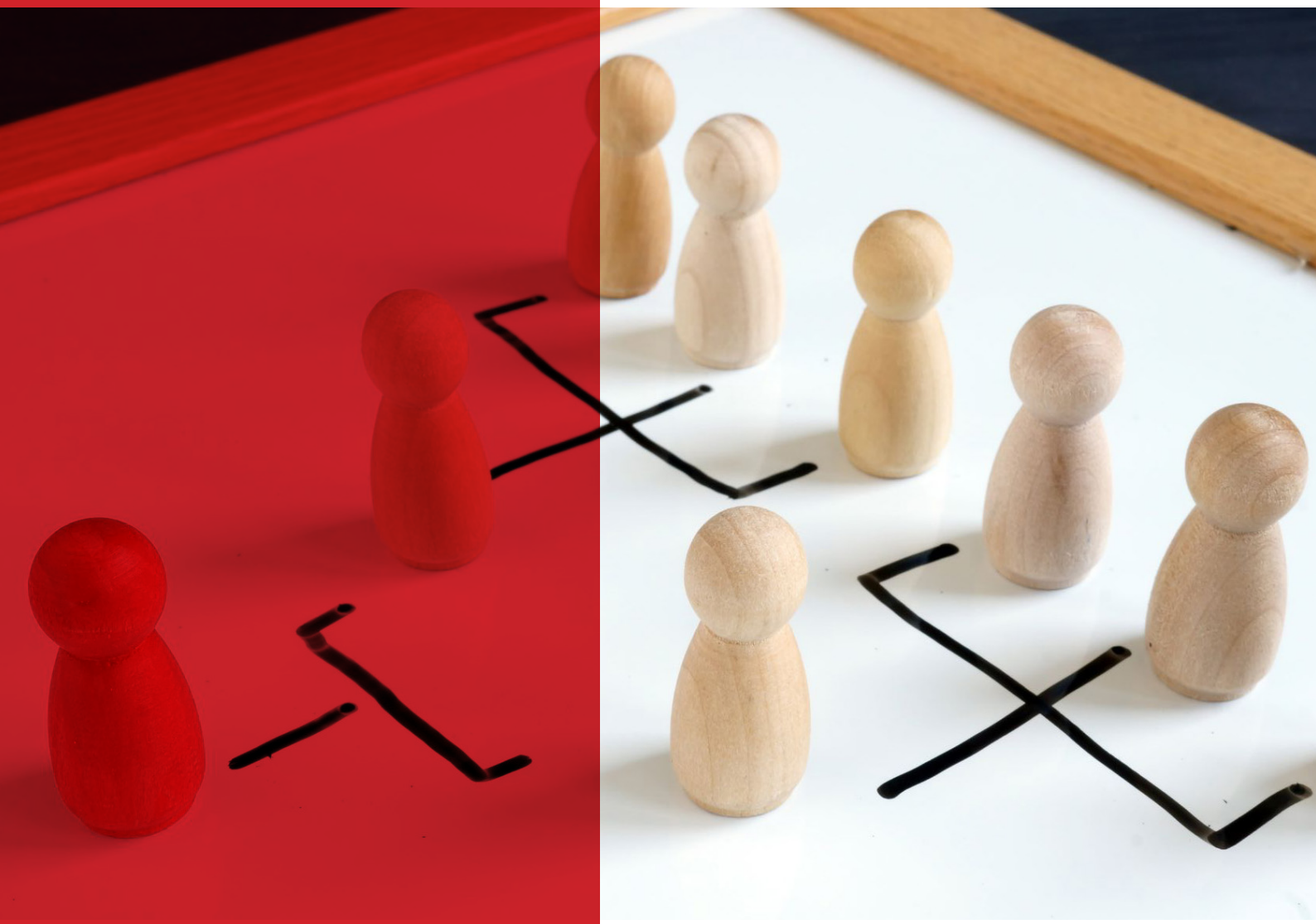
Pruebas. Una organización debe probar su plan de continuidad comercial con regularidad para asegurarse de que todos los empleados lo entiendan y conozcan su función. Las pruebas están diseñadas sobre escenarios potenciales, de modo que los responsables puedan evaluar su efectividad y actualizarlo si fuera necesario. Este nivel de pruebas ayuda a garantizar que la organización sea capaz de recuperar operaciones críticas en caso de interrupción del servicio.
El tipo de pruebas y con qué frecuencia deben hacerse serán determinadas en función de la criticidad de las operaciones. El objetivo de realizarlas es determinar si el sistema de gestión de la continuidad del negocio necesita ser ajustado y esta es la única manera de garantizar su plena eficacia cuando sea necesario.

PROGRAMA DE AUDITORÍA DE SISTEMA DE GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

1. Inicio del proceso de auditoría	2. Fase 1 de la auditoría	3. Preparación para la fase 2 de la auditoría	4. Fase 2 de la auditoría	5. Conclusiones de la auditoría	6. Mas allá del inicio de la auditoría
1.1. Aceptar el mandato del cliente y designar el equipo auditor	**2.1.** Preparar las actividades de la auditoría in situ	**3.1.** Planificar la fase 2 de la auditoría	**4.1.** Llevar a cabo la reunión de apertura de la auditoría	**5.1.** Determinar y acordar las conclusiones de la auditoría	**6.1.** Realizar actividades de seguimiento de la auditoría
1.2. Determinar las fechas	**2.2.** Conducir la auditoría in situ	**3.2.** Asignar el trabajo al equipo auditor	**4.2.** Recoger la información	**5.2.** Redactar las conclusiones	**6.2.** Realizar actividades de vigilancia
1.3. Firma del contrato de la auditoría	**2.3.** Documentar el resultado del estado de la fase 1	**3.3.** Preparar los planes de verificación de la auditoría	**4.3.** Realizar pruebas de auditoría	**5.3.** Llevar a cabo la reunión de cierre	**6.3.** Planificar y realizar la auditoría de recertificación
1.4. Establecer contacto con el auditado		**3.4.** Preparar la documentación para la fase 2 de la auditoría	**4.4.** Determinar los hallazgos de la auditoría, redactar informes de no conformidad y realizar una revisión de calidad	**5.4.** Preparar y distribuir el informe de auditoría	
1.5. Definir la agenda de auditoría				**5.5.** Tomar la decisión de la certificación	

5

CASOS PRÁCTICOS



5.1

AUTORIDAD PORTUARIA DE ENSENADA

Jose Fernández Zapata

En este caso práctico vamos a plantear el escenario de la Autoridad Portuaria de Ensenada, cuyas características definiremos para, a continuación, proceder a la implantación de un plan de continuidad de sistemas (PCS).

CONTEXTO DE LA ORGANIZACIÓN

Una primera suposición para el desarrollo del caso será que la organización, en el momento en que se acomete la implantación de un PCS, lo hace como parte de un plan de continuidad de negocio (PCN) más ambicioso, que no solamente recogerá los aspectos relativos al sistema de información que utiliza, sino todos los elementos organizativos, actividades, recursos y terceras partes implicadas en el normal desarrollo de su misión, es decir, en la consecución de sus objetivos de negocio. Para ello la organización ha decidido seguir las buenas prácticas que recoge la norma ISO 22301 en materia de continuidad de negocio.

Resulta fundamental comprender cuál es la misión de una Autoridad Portuaria. Se trata de un organismo público que gestiona los puertos de titularidad estatal ubicados en su provincia y que, en el caso que nos ocupa, supondremos que son dos, denominados Puerto de Barlovento y Puerto de Tajamar, aunque el núcleo del sistema de información se localiza en el primero de ellos.

El cometido legalmente atribuido a una autoridad portuaria y del que se desprenden tanto sus funciones como su estructura organizativa, se recoge en el Real Decreto Legislativo 2/2011, de 5 de septiembre, por el que se aprueba el Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante (TRLPMM). Su misión y objetivos se describen en un plan estratégico de desarrollo plurianual.

De forma muy resumida, podemos extraer del TRLPMM que los principales servicios gestionados desde una autoridad portuaria son los siguientes:

Gestión del dominio público portuario estatal en su zona de actuación: concesiones y autorizaciones de uso.

Servicios generales

- Ordenación, coordinación y control del tráfico portuario, tanto marítimo como terrestre.
- Coordinación y control de las operaciones asociadas a los servicios portuarios, comerciales y otras actividades.
- Señalización, balizamiento y otras ayudas a la navegación.
- Policía en las zonas comunes.
- Alumbrado de las zonas comunes.
- Limpieza habitual de las zonas comunes de tierra y de agua.
- Prevención y control de emergencias.

Servicios portuarios

- Servicios técnico-náuticos:
  - Servicio de practicaje.
  - Servicio de remolque portuario.
  - Servicio de amarre y desamarre.

- Servicio al pasaje: el embarque y desembarque de pasajeros, la carga y descarga de equipajes, y la de vehículos en régimen de pasaje.

- Recepción de desechos generados por los buques.

- Manipulación de mercancías: carga, estiba, descarga, desestiba, tránsito marítimo y el trasbordo de mercancías.

Servicio de señalización marítima

Servicios comerciales

- Agentes consignatarios, actividades subacuáticas, aprovisionamiento de buques, suministro de combustible, depósito de mercancías, primera venta de productos pesqueros...

La gestión del dominio público portuario, la prestación de los servicios generales y el de señalización marítima son responsabilidad específica de las autoridades portuarias, aunque para su desarrollo se cuente con los servicios de terceros. Sin embargo, la prestación de los servicios técnico-náuticos y comerciales se desarrolla a iniciativa privada, mientras que las autoridades portuarias se limitan a la supervisión de su correcta ejecución.

Requisitos normativos

Otro supuesto de partida para nuestro caso práctico será el de que la Autoridad Portuaria de Ensenada ha sido designada como operador de servicios esenciales (OSE), lo que supone que una interrupción de su actividad tiene graves efectos para la sociedad, por lo que quedará sujeto a la legislación aplicable en materia de protección de infraestructuras críticas (sector transporte, subsector marítimo):

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (LPIC).

Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas (RPIC).

Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (transposición de la Directiva NIS europea).

Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Además, por tratarse de un organismo público, a toda autoridad portuaria se le aplica el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

En la categorización del sistema de obligatoria en aplicación del ENS, la Autoridad Portuaria ha obtenido la calificación de categoría ALTA, puesto que diversas dimensiones de seguridad como la confidencialidad y la disponibilidad se han valorado a nivel alto, por lo que la Declaración de aplicabilidad contendrá todas las medidas correspondientes a la categoría obtenida.

Las actividades y controles destinados a implementar el PCS deberán tener en cuenta toda la legislación aplicable, lo que supone su integración con los instrumentos derivados de dicha legislación como el Plan de Seguridad del Operador (PSO); Plan de Protección Específico (PPE); planes de Protección de los Puertos (PPP); los principios, objetivos, líneas de acción y medidas de la Estrategia Nacional de Ciberseguridad; los mecanismos de coordinación con las autoridades competentes en materia de ciberseguridad (CCN-CERT e INCIBE-CERT); integración con las medidas de seguridad del anexo II del ENS (especialmente con el marco operacional, grupo de continuidad [op.cont])...

Objetivos y alcance

Los objetivos que la Autoridad Portuaria desea conseguir con la implementación de un SGCN, expresados por la dirección general, se concretan en los siguientes:

- Implantar, antes de la fecha xx/xx/xxxx, un SGCN acorde con la norma ISO 22301 y que proteja el desarrollo de las competencias legalmente atribuidas a la Autoridad Portuaria de Ensenada.
- Obtener, antes de la fecha xx/xx/xxxx, la certificación ISO 22301.

Del régimen de prestación de servicios en una Autoridad Portuaria expuesto anteriormente en la descripción del contexto de la organización, se desprende que la continuidad de negocio se focalizará en la gestión del dominio público, los servicios generales y la señalización marítima. Sin embargo, aunque esto es absolutamente cierto, no lo es menos la existencia de otros servicios y procesos de la organización que son necesarios para su buen funcionamiento, más allá de la gestión externamente visible y fundamental del negocio.

Así, para el correcto funcionamiento de cualquier organización, es imprescindible la gestión económico-financiera, la gestión de los recursos humanos, el desarrollo comercial, la gestión estratégica, la gestión de los sistemas de información, los órganos de dirección, etcétera.

Por todo ello, a pesar de la gran importancia de conocer el contexto en el que se desenvuelve la organización, va a ser necesaria, además, una identificación de todos los servicios y procesos críticos para la organización; es decir, aquellos cuya continuidad habrá que proteger. Posteriormente, un análisis del impacto producido por la interrupción de los anteriores servicios y procesos de negocio permitirá determinar los requerimientos de continuidad que será necesario satisfacer para garantizar su continuidad.

La forma de proceder a la identificación de los servicios y procesos críticos es a través del catálogo de servicios de la organización, que es un documento formal y actualizado regularmente que contiene la relación de procesos y negocios, su descripción, responsables de su desarrollo, marco normativo aplicable, recursos necesarios, interrelación con otros servicios/procesos, etcétera. En este catálogo de servicios también se identificarán los que son críticos para que la organización cumpla con su cometido y permitirá hacer la selección de aquellos cuyo impacto en caso de interrupción deberá ser analizado para la adopción de las medidas de protección pertinentes.

Hay que tener muy presente que la elaboración del catálogo de servicios es responsabilidad de los órganos de gobierno de la Autoridad Portuaria, de modo que, si no existe, está obsoleto o no se ha actualizado, no es tarea del área técnica corregir esta situación. Siempre será responsabilidad de la dirección asegurarse de la existencia y mantenimiento de este documento, tanto por su carácter estratégico para la organización como por el conocimiento de negocio que requiere, y del cual los responsables de los servicios y procesos (equipo de gerencia) tienen conocimientos y no el departamento TIC.

Si no existe este documento, la estructura organizativa de la organización (que RRHH debe tener actualizada) y un conocimiento de los sistemas de información que soportan los servicios (cuyo conocimiento sí está en las herramientas de inventario -CMDB- del área técnica) pueden ayudar a establecer un primer punto de partida para su elaboración, aunque hay que insistir en que es una tarea de la dirección.

El proceso de identificación de servicios[1] críticos para la Autoridad Portuaria, se llevará a cabo mediate entrevistas con todos los responsables de los servicios de la Autoridad Portuaria, de forma que se comprendan las características de su prestación, y se complemente la información del catálogo y, sobre todo, se identifiquen aquellos cuya interrupción implicaría pérdidas o daños a la organización por afectar a la consecución de la misión y los objetivos de la organización (paralización parcial o total del negocio). El resultado obtenido es el siguiente:

SERVICIOS CRÍTICOS
Gestión del dominio público
Gestión de infraestructuras
Gestión de operaciones marítimas
Gestión de operaciones terrestres
Gestión de operaciones ferroviarias
Servicio de señalización marítima
Servicios portuarios y comerciales
Gestión comercial y de clientes
Port Community System (PCS)
Facturación
Gestión de la protección portuaria
Gestión de la seguridad industrial
Gestión medioambiental

Con la información disponible del catálogo de servicios y la CMDB (que establece los activos TIC que soportan los servicios), se determinan los responsables de los servicios y el personal de sistemas que formarán parte de los diferentes equipos de trabajo para la recuperación de los servicios dentro del PCS.

Las partes interesadas (gobierno local, autonómico y estatal; proveedores; clientes; ciudadanía) y otros terceros como la competencia, deberán también tenerse en cuenta para establecer los planes de continuidad.

[1] En realidad, también habría que identificar los procesos relevantes dentro de cada uno de los servicios críticos, pero no se incluyen en el caso práctico por simplificación de este.

El modo de incluir todos los aspectos que pueden sufrir el impacto de una interrupción de las operaciones de la Autoridad Portuaria será mediante los criterios de evaluación con los cuales se ejecutará el BIA, los niveles de riesgo definidos en materia de continuidad y el apetito de riesgo establecido por la dirección. Esto lo veremos con detalle en el apartado Planificación.

LIDERAZGO

La implantación de un sistema de gestión de la continuidad de negocio (SGCN) del que forman una parte importante el PCN y el PCS, no es una responsabilidad del área técnica o de cualquier otro departamento, sino que debe ser una necesidad implantada para toda la organización y, por lo tanto, respaldada por los órganos de gobierno.

En determinados casos, cuando la continuidad de negocio no se ha recogido en una organización por desconocimiento o por falta de impulso, sí que es posible que cualquier miembro de la plantilla que detecte la importancia de implantar un SGCN asuma, por responsabilidad, la iniciativa de comunicar y concienciar a los órganos de gobierno, pero la decisión de iniciar el proyecto, el apoyo a este y la involucración deben partir de la dirección.

El liderazgo de la dirección debe materializarse a través varias acciones:

- Comprometerse al cumplimiento de toda la normativa aplicable y buenas prácticas de continuidad.
- Establecer unos objetivos de la organización en materia de continuidad, integrados en los objetivos estratégicos.
- Integrar los mecanismos de continuidad pertinentes como parte de las actividades de ejecución de los procesos de negocio.
- Dotar de los recursos necesarios para la implantación, mantenimiento y mejora continua de un SGCN, incluyendo presupuesto, personal, recursos y, en caso necesario (habitualmente), la contratación de servicios de consultoría externos.
- Designar una o más personas (coordinador de la continuidad de negocio) con la suficiente autoridad para responsabilizarse de la implantación de un SGCN de forma efectiva.
- Asegurarse de que se establecen en la organización los roles, funciones y responsabilidades necesarios para la adecuada gestión y funcionamiento del SGCN, incluyendo la creación de comités y grupos de trabajo específicos.

- Comunicar a todos los miembros de la organización la importancia de la consecución de los objetivos de continuidad establecidos y su implicación.
- Participar activamente en las pruebas y ejercicios.
- Asegurarse de que se realizan auditorías internas periódicas.
- Gestionar las revisiones efectivas del SGCN.
- Dirigir y apoyar la mejora continua.

Política

El contexto de la organización, el marco normativo, el alcance del SGCN y las acciones de liderazgo se recopilan en la redacción de la política de continuidad de negocio de la Autoridad Portuaria, cuyo contenido incluye los anteriores aspectos con un lenguaje claro. En la política también se indican los procesos de aprobación y actualización (con un control de cambios). Finalmente, el documento recoge la descripción y la designación de roles y responsabilidades en materia de continuidad.

Para facilitar el mantenimiento de la política, tanto el marco normativo como los nombramientos designados a los distintos roles, están descritos en documentos específicos e independientes que se referencian desde la política.

La política se ha elevado a la aprobación formal por el máximo órgano de gobierno (consejo de administración) y ha sido divulgada a todo el personal de la organización. Con esto se consigue trasladar a la plantilla el compromiso de la dirección con la implantación de buenas prácticas de continuidad de negocio a través las actividades de un SGCN incluidas en la política, con el fin de buscar su implicación para un eficaz desarrollo.

Roles y responsabilidades

Los principales roles y responsabilidades de la organización de la continuidad de negocio que se describen en la política son, de forma resumida, los siguientes:

Comité de crisis. Equipo de alta dirección con el máximo nivel de decisión en la gestión de los incidentes disruptivos. Sus miembros son: director general, adjunto a la Dirección, jefe del Gabinete de Dirección, secretario general, jefe del Gabinete de Presidencia, jefe de Explotación, jefe de RRHH y jefe de EcoFin.

Responsable de la continuidad del negocio. Responsable del diseño, implantación y mantenimiento del SGCN. Se designa al jefe de Planificación Estratégica de la Autoridad Portuaria. Como parte de su labor, mantendrá actualizada la política e incorporará los cambios normativos y organizacionales que se produzcan, siguiendo un procedimiento de revisión periódica.

Coordinador de la continuidad de Tajamar. Punto de contacto y máximo responsable del SGCN en el puerto de Tajamar, supeditado al anterior rol. Se designa al jefe de comisaría de Tajamar.

Comité de continuidad. Grupo directivo creado para apoyar al coordinador de continuidad en la toma de decisiones y gestión del SGCN. Sus miembros son: jefe de Sistemas, jefe de Explotación, jefe de RRHH, jefe de EcoFin y jefe de Planificación Estratégica.

Equipos de continuidad. Grupos de trabajo especializados, cada uno de ellos, en un ámbito de la continuidad concreto, lo que les permitirá actuar en caso de que una interrupción obligue a adoptar medidas de recuperación.

Equipo de respuesta a incidentes. Está formado por toda la estructura organizativa asignada a la gestión de incidentes, en la cual se determinan las fases de respuesta ante interrupciones de la actividad. Para ello establecerá los criterios de activación del PCN (y, llegado el caso, del PCS) además de los protocolos de escalado jerárquico en función de la gravedad del incidente y la activación de los equipos de continuidad adecuados según su naturaleza.

ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)

Otra información fundamental recogida en las entrevistas con los responsables de los servicios críticos de la organización es la relativa al análisis de impacto en el negocio (BIA). Durante el BIA se ha hecho un estudio del impacto que tendría para la organización la interrupción de cada servicio crítico. Este impacto se cualifica sobre la base de unos criterios de diferente índole y una escala cualitativa de valoración del impacto en tres niveles (bajo, medio y alto, aunque el número de niveles y su denominación es arbitrario):

Criterio	Bajo	Medio	Alto
Económico	Inferior a 50 000 €	Entre 50 000€ y 250 000€	Superior a 250 000 €
Operacional	Reducción apreciable de la capacidad de la organización para atender sus obligaciones.	Reducción importante de la capacidad de la organización para atender sus obligaciones.	Imposibilidad de la organización de atender alguna de sus obligaciones.
Reputacional	Cualquier impugnación a la reputación.	La reputación resulta significativamente amenazada.	Grave pérdida de reputación con difusión en los medios de comunicación.
Cumplimiento	Incumplimiento de alguna ley, normativa o contrato de carácter subsanable.	Incumplimiento formal de alguna ley, normativa o contrato no subsanable.	Incumplimiento formal o material grave de alguna ley, normativa o contrato.
Derechos de las personas	Causar un perjuicio menor y reparable a algún individuo.	Causar un perjuicio significativo de difícil reparación a algún individuo.	Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.

A cada servicio crítico se le asigna un nivel de impacto para períodos de interrupción predefinidos, ya que, cuanto mayor es el tiempo de interrupción, mayor suele ser el impacto producido. Tras esta valoración, se obtienen los requerimientos de RTO y RPO que establecen los requisitos de recuperación, los cuales dependen del nivel de impacto asumible por el responsable cada servicio. Para cada servicio siempre se toma la valoración del criterio que provoca un mayor impacto en menos tiempo.

Un resumen del resultado obtenido tras consolidar los diferentes criterios de impacto es el que se muestra a continuación:

Servicio	1 Hora	4 Horas	8 Horas	24 Horas	48 Horas	72 Horas	7 Días	14 Días	30 Días	RTO	RPO
Gestión del Dominio Público	No aplica	Bajo	Bajo	Bajo	Bajo	Medio	Medio	Alto	Alto	24h	24h
Gestión de Infraestructuras	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	Medio	Alto	Alto	7 días	24h
Gestión de Operaciones Marítimas	No aplica	No aplica	Bajo	Bajo	Medio	Medio	Alto	Alto	Alto	8h	24h
Servicios Portuarios y Comerciales	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	Bajo	7 días	24h
Gestión Comercial y de Clientes	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	72h	24h
Port Community System (PCS)	No aplica	Bajo	Medio	Alto	Alto	Alto	Alto	Alto	Alto	8h	24h
Facturación	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	72h	24h
Gestión de la Seguridad Industrial	Bajo	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	4h	24h
Gestión Medioambiental	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	N/A	N/A

Para determinar el RTO, se ha establecido como tolerable un nivel de impacto bajo, a excepción de aquellos casos en los que el responsable del servicio, por sus características, ha considerado necesario establecer un tiempo de recuperación inferior. El RPO se ha definido en todos los casos como de 24 horas porque la política de copias de seguridad establece la realización de una copia diaria y ningún responsable ha exigido un punto de recuperación más corto.

Además, el BIA recoge los recursos necesarios para el desarrollo de los procesos críticos (infraestructuras, tecnología, personas y proveedores). Estos recursos son aquellos cuya disponibilidad habrá que garantizar, si bien para el PCS se hace foco en los que permiten operar con normalidad a los sistemas de información que soportan los procesos críticos.

ANÁLISIS DE RIESGOS

El análisis de riesgos a la continuidad del negocio parte de un catálogo de amenazas que se caracterizarán con su probabilidad de suceso y el impacto producido en la organización para determinar el riesgo.

Si determinamos los tipos de activos a los que afectan las amenazas, se establecen distintos escenarios de interrupción de la actividad a los que se asociarán el riesgo derivado de las amenazas que los producen y las estrategias de recuperación adecuadas.

El catálogo de amenazas, activos afectados y riesgo[2] manejados en la Autoridad Portuaria de Ensenada son los siguientes:

Amenaza	Tipo de activos a los que afecta				Probabilidad TAO	Impacto	Riesgo
	Infraestructura	Tecnología	Personas	Proveedores			
Inundación	X	X	X		0,01	Alto	Medio
Terremoto	X	X	X		0,01	Alto	Medio
Incendio	X	X	X		0,01	Alto	Medio
Explosión	X	X	X		0,01	Alto	Medio
Escapes tóxicos			X		0,1	Alto	Alto
Corte de energía	X	X			1	Alto	Alto
Fallos tecnológicos (comunicaciones, hardware o software)		X			10	Medio	Alto
Errores humanos		X			10	Bajo	Medio
Enfermedades (pandemia, intoxicación colectiva…)			X		0,1	Alto	Medio
Ausencia de personas clave			X		0,1	Medio	Bajo
Huelga			X		0,1	Medio	Bajo
Ataques cibernéticos		X			1	Alto	Alto
Sabotaje	X	X			0,1	Alto	Medio
Robo		X			0,1	Medio	Bajo
Actos violentos (revueltas, atentados, guerra…)	X	X	X		0,01	Alto	Medio
Fallo en la cadena de suministro				X	1	Medio	Medio

La organización ha establecido un apetito de riesgo bajo, lo que obliga a desplegar medidas frente a las amenazas de riesgo medio y alto, si bien muchas de ellas ya existían en aplicación de buenas prácticas:

- Sistemas contraincendios.
- Sistemas de alimentación redundante (SAI y grupos electrógenos).
- Protección de las zonas críticas frente a inundaciones.
- CPD redundantes.
- Sistema de gestión de la seguridad operativa (plan de autoprotección).
- Sistema de gestión de la seguridad de la información (conforme al ENS).
- Tras calcular el riesgo residual, es decir, considerando los efectos mitigantes de las medidas existentes, se ha identificado una amenaza cuyo valor de riesgo sigue superando el umbral del apetito de la organización y requiere un plan de tratamiento del riesgo para desplegar nuevos controles. Se trata del posible fallo de la cadena de suministro, para cuya mitigación se planifica la implantación de un plan de diversificación de proveedores y la exigencia de SLA de continuidad en los contratos.

[2] Riesgo intrínseco o potencial, es decir, sin considerar el efecto de los controles existentes. Se ha empleado una escala de probabilidad equivalente a la tasa anual de ocurrencia (TAO) y unas escalas de impacto y riesgo cualitativas de tres niveles: bajo, medio y alto.

ESTRATEGIAS DE CONTINUIDAD

Los escenarios de interrupción de la actividad y las estrategias de recuperación asociadas son las que se muestran a continuación:

Escenario de interrupción	Estrategias de continuidad
Indisponibilidad de infraestructuras	Teletrabajo
	Acuerdo de colaboración con terceros (compartición temporal de infraestructura)
	Respaldo entre los puertos de Barlovento y Tajamar
	Centro de trabajo administrativo alternativo (alquiler o cesión de locales)
Indisponibilidad de tecnología	Equipamiento de reserva
	Contratos de reposición y puesta en marcha con proveedores
	PCS y DRP implantados en la organización
Indisponibilidad de personas	Definición de árboles de llamada
	Capacitación multidisciplinar
	Rotación de los puestos de trabajo
	Documentación de procedimientos
	Contratación de personal externo
Indisponibilidad de proveedores	Diversificación de proveedores
	Definición de acuerdos de nivel de servicio adecuados
	Almacén de suministros

Cabe tener muy presente que las estrategias de continuidad seleccionadas son adecuadas para el escenario en el que se incluye, pero siempre en función de las particularidades en las que se concrete dicho escenario. Así, por ejemplo, un escenario de indisponibilidad de tecnología como consecuencia de un incendio grave puede suponer la reposición de todo el equipamiento (red, servidores, puestos de trabajo...) y su reconfiguración, mientras que la indisponibilidad por un ataque de ransomware no requerirá la reposición del equipamiento, pero sí una ardua labor de contención de la amenaza y posterior erradicación mediante el uso de copias de seguridad previas al ataque.

Por este motivo se ha desarrollado un DRP que recoge todos los escenarios específicos que, para la recuperación de los sistemas de información, requieren procedimientos de desarrollo concretos: activos afectados, actividades de recuperación, recursos necesarios, tiempos objetivo, etcétera.

PROCEDIMIENTO DE GESTIÓN DE CRISIS

Se ha desarrollado un procedimiento para la gestión de incidentes que impacten en la continuidad del negocio, el cual incluye los criterios de evaluación de los incidentes para determinar la activación del PCN (incluyendo el PCS cuando así sea necesario) y los mecanismos de comunicación internos y externos (proveedores, clientes y partes interesadas).

PLAN DE PRUEBAS

También se ha diseñado un plan para probar periódicamente el correcto funcionamiento del PCN (y sus partes integrantes como el PCS) y detectar posibles errores o puntos de mejora.

PLAN DE FORMACIÓN

Otra actividad que se ha incluido es el desarrollo de acciones de formación y concienciación de los empleados. Para este fin se ha adaptado a las funciones concretas asignadas dentro del PCN a cada miembro implicado en su ejecución.

PLAN DE COMUNICACIÓN

La Autoridad Portuaria de Ensenada es plenamente consciente de la enorme importancia de un buen plan de comunicación, tanto interna como externa, en caso de producirse un incidente disruptivo, ya que permite coordinarse con terceros y lanzar mensajes a las partes interesadas que, siendo realistas y veraces, ayuden a transmitir seguridad y confianza en la organización a pesar de las circunstancias.

Un plan de comunicación bien diseñado y ejecutado puede incluso reforzar la imagen de la organización tras la gestión adecuada de un incidente. Para ello es necesario escoger adecuadamente el contenido de los mensajes transmitidos, controlar los tiempos, y elegir a los interlocutores adecuados, etcétera.

Bibliografía

AENOR. UNE-EN ISO 22301:2020. Seguridad y resiliencia. Sistema de Gestión de la Continuidad del Negocio. Requisitos. (ISO 22301:2019).
https://tienda.aenor.com/norma-une-en-iso-22301-2020-n0063818

AENOR. UNE-EN ISO 22313:2020. Seguridad y resiliencia. Sistemas de gestión de la continuidad del negocio. Directrices para la utilización de la norma ISO 22301. (ISO 22313:2020).
https://tienda.aenor.com/norma-une-en-iso-22313-2020-n0063819

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630

Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
https://www.boe.es/buscar/act.php?id=BOE-A-2011-8849

Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

Real Decreto Legislativo 2/2011, de 5 de septiembre, por el que se aprueba el Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante.
https://www.boe.es/buscar/act.php?id=BOE-A-2011-16467

Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257

5.2

SALUD

Albert Martínez Aparisi

CASO PRÁCTICO SANIDAD

NOVASALUD es una compañía que ofrece servicios de salud a cerca de un millón de pacientes mediante una red de centros asistenciales. Para ello cuenta con diez hospitales y veinticinco centros de salud distribuidos en el territorio donde desempeña su actividad.

Elena Jover llegó al puesto de directora general de la empresa hace cinco años. Anteriormente, había ocupado el puesto de jefa del Servicio de Anestesiología de uno de los hospitales de NOVASALUD. Desde que se incorporó a la gerencia había demostrado su talante en gestión sanitaria. En una de sus primeras reuniones con los gerentes de los diferentes hospitales manifestaba:

«La asistencia sanitaria es un servicio que exige mucho esfuerzo y es muy valorado por nuestros pacientes. Todos sabemos que, gradualmente, estamos dedicando más recursos a dicha atención y, en consecuencia, se necesita incrementar y mejorar el equipamiento asistencial, las infraestructuras y los profesionales.

No obstante, todo este aumento no es suficiente para garantizar la máxima calidad en la prestación de la asistencia sanitaria, con una optimización y un máximo aprovechamiento de todos los recursos empleados.

Nuestro core consiste, esencialmente, en tomar decisiones para mejorar la salud de nuestros pacientes. En consecuencia, los sistemas de información no son un simple soporte al proceso asistencial y a la gestión sanitaria, sino que están en el propio núcleo del proceso asistencial.

No es posible una asistencia sanitaria eficiente y segura sin las tecnologías de la información y de las comunicaciones, que se han convertido en un componente nuclear de todo el proceso asistencial y un factor indispensable para la gestión sanitaria.»

En las primeras semanas en el cargo, Elena Jover nombró a Cristina Casares directora de sistemas de información de NOVASALUD.

En el primer análisis de la situación que llevó a cabo la nueva directora de sistemas se encontró con:

- Cada hospital disponía de su propio CPD y su propio presupuesto en TI. También se disponía de un CPD en la sede central para dar soporte a las aplicaciones de los diferentes centros de salud.
- Las aplicaciones dedicadas a la asistencia sanitaria no cubrían todo el proceso asistencial y, en algunos casos, eran diferentes en los diferentes hospitales.
- En cada hospital había una media de veinte aplicaciones relacionadas con el soporte al proceso asistencial. Muchas de ellas no estaban integradas.
- No existía evidencia de planes de sistemas completos ni en los hospitales ni globalmente en la empresa NOVASALUD. En algunos casos, se habían encontrado planes de sistemas que no seguían la misma metodología ni pretendían los mismos objetivos.
- El liderazgo del área de tecnologías de la información en los hospitales era muy débil y en la sede central casi inexistente. No se disponía de una documentación clara sobre los componentes de infraestructura hardware ni de software en los hospitales.
- El historial clínico no era único, por lo que los profesionales necesitaban acceder a los sistemas del hospital de referencia de los pacientes para consultar los datos de aquellos a quienes estaban atendiendo.
- Las aplicaciones de gestión administrativa (nóminas, ERP, CRM) se encontraban centralizadas en el CPD de la sede central.
- En los últimos meses se habían producido rupturas de servicio en dos hospitales que habían obligado a una parada de sistemas de cerca de ocho horas, que comportaron un enorme impacto asistencial.

Ante esta situación, la nueva directora de sistemas de información elaboró un informe estratégico que pretendía establecer las bases para capacitar a NOVASALUD y, así, poder afrontar los nuevos retos a los que se enfrentaba. En el informe se destacaron dos grandes líneas de trabajo:

a) Aumentar la integración de los sistemas en los siguientes ámbitos:

Área asistencial. Se implica a todos los sistemas para que puedan intercambiar los datos y permitan definir nuevas iniciativas orientadas a la mejora de la atención sanitaria.

Área de gestión operativa. Se mejoran las capacidades actuales en la gestión de los recursos para evolucionar hacia un contexto de mayor eficiencia y optimización de los recursos empleados.

Área de analítica de datos. Se dota a la organización de un sistema de soporte a la toma de decisiones que ofrezca la información y el conocimiento cuando se necesite, como se necesite y a los implicados en cada una de las decisiones.

b) Mejorar las ventajas competitivas de la organización mediante:

- El aumento de la eficiencia de los procesos asistenciales, llegando a proponer a la organización nuevas maneras de llevar a cabo el proceso asistencial.
- La mejora de los costes operativos, normalizando los procesos y alcanzando economías de escala.
- La colaboración en la mejora de la calidad del servicio, potenciando la aplicación de las tecnologías para acercar el contacto con el paciente.

Asimismo, Cristina Casares incluyó en su informe las ideas generales de las estrategias en los sistemas de información:

- Necesidad de disponer de una historia clínica electrónica (HCE) compartida y accesible por todos los profesionales asistenciales de NOVASALUD que permitan poner al paciente en el centro del proceso asistencial y no tanto en los recursos implicados en dichos procesos.

- Incrementar la lógica en los sistemas que permitan la derivación de los pacientes entre los diferentes centros de NOVASALUD, para los traslados entre los hospitales o la petición de interconsultas clínicas o la realización de pruebas complementarias como las pruebas de diagnóstico por la imagen o de laboratorio.
- Unificar la información de los procesos asistenciales de los centros de salud y los diferentes hospitales, con el objetivo de establecer un continuo asistencial.
- Facilitar unos procesos de gestión comunes mediante la analítica de datos a través de cuadros de mando que relacionen la información de manera fiable y única.
- Evolucionar hacia una organización sin papeles, para lo que se propició una transformación digital que incluyera un cambio disruptivo en la atención sanitaria.
- Orientar la arquitectura tecnológica hacia un contexto de plena interoperabilidad e integración entre los sistemas de la organización.
- Afrontar los nuevos desafíos contando con todas las tecnologías y modelos al alcance de la organización que le permitan lograr los objetivos corporativos, incluyendo cualquier manera de externalización *(cloud friendly).*
- Abrir la organización al paciente para aumentar la calidad de su relación con NOVASALUD mediante sistemas multicanal.
- Interconectar todos los centros y sedes de NOVASALUD con una capacidad operativa que permita alcanzar los tiempos de respuesta que haya definido la gerencia.
- Establecer un centro de soporte técnico único para toda la organización que facilite un aumento de la disponibilidad y calidad de dicho soporte.
- Crear un área específica para la seguridad de información, mediante el refuerzo de las acciones en ciberseguridad.
- Implantar estructuras organizativas para el gobierno de la información.

Una de las decisiones que Cristina Casares tomó al principio fue la implantación de acuerdos recíprocos entre hospitales, que permitían reservar una capacidad computacional para los otros centros en caso de contingencia de alguno de ellos. Esta medida no estuvo exenta de cierto rechazo entre los responsables de los sistemas de información de cada hospital debido, entre otros, a la autogestión y autonomía que se había otorgado desde NOVASALUD a cada uno de los hospitales. Las acciones siguientes se orientaron a la definición e implantación de las nuevas estrategias.

Durante los tres años siguientes desde que Cristina Casares llegó a la dirección de sistemas, NOVASALUD acometió grandes proyectos de tecnologías y sistemas de la información. El más importante fue la implantación de la historia clínica unificada en toda la organización.

Para acometer este proyecto se potenció el Centro de Proceso de Datos de la sede central. Se dotó de capacidad computacional suficiente y se contó con la tecnología de procesamiento, almacenamiento y de comunicaciones más avanzadas.

También se potenciaron los diferentes canales para facilitar al paciente el contacto con la organización.

Las decisiones que se tomaron con relación a la continuidad de las tecnologías de la información (TI) fueron de aplicación gradual y se adaptaron a los cambios estructurales y de sistemas de la organización.

Para ello, la dirección de sistemas se planteó abordar la continuidad de las TI de manera que permitieran:

- Responder al cambiante contexto de riesgos.
- Asegurar la continuidad de los procesos críticos de la organización soportados por los servicios de las TI.
- Prevenirse ante las interrupciones de los servicios de las TI, identificando los eventos o las series de eventos relacionados con los incidentes.
- Capacitarse para responder y recuperarse de incidentes y/o desastres y fallos.

La primera acción del plan de continuidad era llevar a cabo un análisis de impacto del negocio, BIA (*Bussiness Impact Analysis*) para identificar con claridad los procesos críticos de NOVASALUD y analizar el nivel de impacto con relación a la organización.

El entregable de este análisis era un informe que detallaba las funciones y los procesos críticos del negocio. Este documento contenía la información básica de los recursos requeridos y los tiempos de recuperación para poner, de nuevo, en producción los servicios de las TI y, en consecuencia, la continuidad de los procesos de NOVASALUD.

Este análisis ayudó a Cristina Casares a:

- Identificar las funciones y los procesos importantes para la supervivencia de NOVASALUD en el momento de la interrupción. Esto implicaba tener en cuenta qué procesos son claves para priorizar la entrada en operación frente a los de menor prioridad; también se identificaron con claridad aquellos procesos identificados como no tan prioritarios que se debían incluir también en los planes de recuperación.
- Analizar los impactos operacionales y financieros que una interrupción podría tener en los procesos de prioridad alta.
- Realizar estimaciones de tiempos de recuperación, atendiendo los posibles impactos de los procesos considerados de alta prioridad para la operación de las infraestructuras de las TI.

Para evaluar el impacto operacional, que les permitía medir el nivel negativo de una interrupción en el proceso asistencial, se contó con la siguiente escala de valoración:

Nivel A: La operación es crítica para el proceso asistencial.

Nivel B: La operación es una parte integral del negocio, pero no es una función crítica para la organización.

Nivel C: La operación no es una parte integral del negocio.

A partir de este análisis se obtuvo la siguiente información:

Función crítica de negocio	Sistemas/componentes críticos	Impacto	MTD (horas)	Prioridad de recuperación
Laboratorios de análisis clínicos	Sistemas de laboratorio	A	1	1
Triaje de urgencias	Sistema de admisión de pacientes	B	5	2
Historia clínica electrónica del paciente	Estación clínica	A	1	1
Portal NOVASALUD	Sitio web de NOVASALUD	C	24	3
Admisión en urgencias	Sistema de admisión de pacientes	B	5	2
Nóminas	Sistema de nóminas	C	48	3
Comunicaciones	Dispositivos de la red	A	1	1
Imagen médica	Sistema PACS	A	1	1

A partir del BIA y del análisis de los riesgos, la dirección de sistemas tomó las siguientes decisiones:

- Crear un equipo de trabajo para determinar los objetivos y el alcance de un plan para la continuidad de las TI de NOVASALUD.
- Establecer una política de soporte a la continuidad de las TI.
- Una de ellas era la necesidad de disponer de un lugar alternativo para la continuidad de las operaciones.
- Asignar recursos humanos con las competencias y capacidades adecuadas para dar soporte a la continuidad de las TI.
- Determinar un plan detallado de requerimientos, con una categorización de las actividades para la continuidad de las TI, y para ello se definirá el nivel que cada actividad crítica necesitaba para su reanudación. Estas actividades debían contar con un tiempo objetivo de recuperación (RTO) y un punto objetivo de recuperación (RPO) para el objetivo mínimo de continuidad del proceso asistencial en NOVASALUD.
- Establecer actividades de prevención, monitorización, detección, respuesta y recuperación para ser notificadas a la gerencia.
- Definir los niveles de resiliencia requeridos para desarrollar las tareas de prevención de incidentes, detección, respuesta, recuperación y restauración acordes a las exigencias establecidas.
- Iniciar la formación y concienciación de los empleados de NOVASALUD en el plan de continuidad de las TI.

Estas decisiones de Cristina Casares tuvieron impacto en varios niveles de la organización. En el ámbito de las TI se llevaron a cabo las siguientes acciones:

- Dotar de resiliencia a la red de datos añadiendo una redundancia en los componentes de la red local y la extensa. Se definió un nuevo modelo de red para los hospitales y centros de salud, de manera que se incorporaba una tipología homogénea de dispositivos y un esquema lógico que hacía compatibles las diferentes redes. En las redes de área extensa, se añadió una línea de copias de seguridad o backup para cada uno de los centros de salud y hospitales.

- Se contrataron servicios computacionales en la nube con la finalidad de servir de centro de respaldo en espejo. Dadas las necesidades de NOVASALUD, principalmente en las aplicaciones de historia clínica electrónica, se optó por establecer un modelo mixto, con las operaciones distribuidas entre el CPD de la sede central y la nube. Hasta este momento, las tres interrupciones graves que se han producido se han conducido sin apenas impacto en el proceso asistencial. Al mismo tiempo, se ha aumentado el número de sistemas y aplicaciones incluidos en la infraestructura en la nube.

- Formar un equipo interdisciplinar que gobierna la continuidad en las TI. Se ha implicado a la gerente de NOVASALUD, así como a diferentes jefes de servicio asistenciales de los diversos hospitales. Por parte del área de tecnologías de la información participa la directora de sistemas y otros miembros del área de tecnologías de la información.

- Cada seis meses se lleva a cabo una simulación para la activación del plan de continuidad de las TI. Se están alcanzado resultados muy positivos para la adherencia de los empleados a las acciones requeridas por el plan.

Los resultados obtenidos mediante la definición e implantación de los planes de continuidad de las TI han sido muy positivos:

- Ha aumentado la confianza de los profesionales en los sistemas de información.
- Se ha incrementado la relación con el paciente y se ha facilitado su contacto con NOVASALUD.
- Ha generado ventajas competitivas para NOVASALUD.

En la última convención de empleados Elena Jover, gerente de NOVASALUD, trasladó públicamente sus felicitaciones a Cristina Casares por los resultados del plan de continuidad y su contribución a alcanzar los objetivos de la organización.

5.3

Infraestructura científica ARTEMISA. Instituto de Física Corpuscular (IFIC)

Ana Isabel Delgado Belmar
Francisco Albiol Colomer

PLAN DE CONTINUIDAD DEL IFIC

Plan de continuidad de una infraestructura científica: ARTEMISA *Entorno artificial para ML e innovación en computación científica avanzada* del Instituto de Física Corpuscular.

El Instituto de Física Corpuscular (IFIC) es un centro mixto del Consejo Superior de Investigaciones Científicas y la Universitat de València. La misión del IFIC cumple un amplio rango de áreas y subproyectos. En un sentido amplio podemos decir que estudia las interacciones fundamentales (gravitación, electrodébil y fuerte), los bloques constituyentes de la materia y ambos consideran los aspectos teóricos y experimentales. Su misión es entender la naturaleza de estas interacciones y las consecuencias fenomenológicas en los laboratorios, para predecir el comportamiento en futuros experimentos y, como objetivo final, buscar una teoría unificada de todos ellos. Además, se adentra en el deseo de conocer qué física ocurre en el universo y cómo ha evolucionado desde sus condiciones iniciales. En paralelo, está la contribución a la sociedad con desarrollos derivados de estas actividades.

Para llevar a cabo muchas de estas actividades, tanto en el análisis de datos reales como en la simulación de modelos, el IFIC cuenta con una infraestructura de sistemas de información realmente impresionante y conectada a las principales fuentes de datos de todo tipo de experimentos. Por ejemplo, los datos generados en experimentos del LHC son un contrincante digno de las grandes empresas tecnológicas en cuanto a volumen de datos, y está dividido en nodos a lo largo de toda Europa con el principio de divide y vencerás.

Todas estas conexiones especiales con otros centros, así como la necesidad de mantener estos sistemas preparados y operacionales orientaos al propósito para el que están encomendados han sido posibles gracias a la adopción desde el origen (años ochenta) de buenas prácticas y conocimientos, en gestión y operación, aunque no se han visto traducidas en la consecución de objetivos de visibilidad como una ISO certificada externamente.

Asimismo las capacidades y los procesos únicos de estos sistemas de información que, recordemos, no están enfocados a procesos de negocio que puedan afectar al funcionamiento institucional, así como los espacios de trabajo eminentemente de colaboraciones internacionales, dificultan la expresión de un plan de continuidad general asociado a procesos, y de carácter general e institucional.

Además, aunque la infraestructura del IFIC esté gestionada por personal generalmente del CSIC, una parte de la infraestructura que gestiona es propiedad de la UVEG, que tiene sus propios principios.

Por estos motivos, tras la adquisición de Artemisa —una infraestructura que proviene de fondos Europeos, lo que garantiza la continuidad—, y por las oportunidades de visibilidad, se decidió iniciar una ISO27001 en este ámbito, avalada por muchos investigadores del IFIC, y destinada a la inteligencia artificial. En efecto, abrir esta infraestructura a investigadores de otros centros o institutos impone nuevas condiciones de uso ideales encaminados a este propósito.

Desde 2018 se trabaja con la dirección en la implantación de esta norma voluntaria para dar visibilidad a dicha plataforma.

Entre las cuestiones que se han tratado están:

- Las políticas de acceso y uso.
- Las garantías que se pueden obtener.
- Los aspectos orientados a la gestión de riesgos y los procesos de continuidad, que es de lo que trataremos a partir de ahora.

OBJETIVOS DE NEGOCIO

El negocio, como actividad económica, no está dentro de las actividades del IFIC; sin embargo, el tamaño del instituto así como su capacidad o presencia internacional, lo convierten en un foco de proyectos europeos muy demandantes de infraestructura avanzada en muchos aspectos, desde la instrumentación científica hasta capacidades de computación.

Parte de los objetivos de la ciencia, la difusión y la cooperación están incorporados a la lógica y objetivos de esta infraestructura. El IFIC participa dentro del CSIC en el ámbito nacional en las siguientes plataformas:

- Plataforma Temática Interdisciplinar (PTI) de Inteligencia Artificial. Tiene más de seis grupos en su interior.
- Plataforma Temática Interdisciplinar (PTI) de Salud, diagnóstico por imagen. Una plataforma con solapamiento en la anterior, y que fue vertebrada a consecuencia del COVID-19

El nivel internacional de las enumeraciones y fortalezas son incontables, y van desde aplicaciones en la física de partículas en LHC, la cosmología, la astrofísica y las astropartículas, hasta un número muy completo de aplicaciones y estudios de física teórica y experimental tal como se ha enunciado al principio.

Lo que es interesante aquí, es que la decisión política busca una ciencia que cubra dos frentes:

- Una mayor interdisciplinariedad, basada en la colaboración que favorezca la innovación.
- Un mayor espacio de cooperación y usos compartidos de infraestructuras que por su naturaleza no sean posibles de replicar por muchos actores.

Los proyectos de Artemisa en el momento de escribir este punto (https://artemisa.ific.uv.es/web/) incluyen:

- Uso de recursos para el COVID-19.
- Proyectos de salud, orientados a tratamientos innovadores.
- Proyectos de la ESA orientados a la agricultura y el cambio climático.
- Proyectos de modelado de gemelos digitales humanos para aspectos de biomecánica.
- Estudios de tormentas solares, su impacto y su prevención en los sistemas eléctricos
- Estudios de reconocimiento de patrones en audio.
- Estudios de segmentación automática de tejidos en imagen.
- Simulación de ondas cerebrales.
- Búsqueda de anomalías.

- Tráfico.
- Seguridad informática y criptografía, y, por supuesto
- un sinfín de proyectos dedicados a física de partículas.

Las instituciones y centros de los que esta infraestructura se ha nutrido son:

- Numerosos centros del Consejo Superior de Investigaciones Científicas.
- Instituto Biomecánico de Valencia.
- Centro Príncipe Felipe.
- Grupos de teledetección de la Universitat de València.
- Otras universidades.

Dado el carácter de gratuidad y de enfoque científico, esta infraestructura no puede ofrecer garantías comerciales y no está previsto su uso por parte de las empresas; sin embargo, la infraestructura alberga proyectos de colaboraciones muy ambiciosas, en sectores médicos o industriales.

OBJETIVOS Y PLAN DE CONTINUIDAD

Con las definiciones de Artemisa, la continuidad de negocio se centra en dos aspectos:

- Cómo mantener la computación.
- Qué hacer con la gestión de los datos.

Ambos aspectos están centrados en garantizar el control de acceso a la infraestructura por contrato y que de una forma única el usuario pueda acceder a estos datos de forma controlada.

- Artemisa no puede usarse sin un proyecto de calidad científica detrás que avale su uso, es decir un proyecto financiado localmente, a nivel nacional o con un contrato con una empresa o institución.
- Es la dirección del centro de origen quien aprueba a sus usuarios para este acceso.

De esta forma se garantiza que el usuario goza de unos permisos que se asocian a unas obligaciones al uso.

Respecto a la continuidad de la computación —la experiencia de más de treinta años (que en tecnologías de la información es un mundo) en la gestión de este tipo de recursos—,

recordemos que el IFIC puso en marcha su centro de cálculo con sistemas VAX, y empleando los recursos de los Mainframe de IBM de la Universitat de València hasta mediados de los noventa, cuando la computación se pasó a sistemas de clústeres UNIX que llegarían a principios del 2000, cuando esta infraestructura pasó a ser prácticamente exclusiva de High Performance Computing en Linux.

Esto quiere decir que procesos como la instalación y gestión del software de manera global ya son una práctica madura en estos sistemas de información.

Respecto a los datos, las cosas han cambiado mucho en estos últimos treinta años. Las razones son dos:

- La adopción masiva de redes de gran ancho de banda y baja latencia.
- El incremento sostenido y exponencial de la capacidad de los discos o almacenamiento directo que ha crecido de forma asimétrica con los sistemas de respaldo.

La primera razón facilita la movilidad de los datos, aunque también el riesgo de ataques o cuestiones relativas a la seguridad.

La última razón dificulta la capacidad en tiempo y en recursos a la hora de poder mantener una copia diaria de los datos. Sin embargo, una gran parte de las aproximaciones modernas se basan en el uso de ambas características, es decir:

- Alejar los datos mediante réplica de las ubicaciones de cómputo.
- Emplear, si se requieren, las características excepcionales de las redes modernas para que estos datos se repliquen en ubicaciones diferentes.

La diferencia esencial en Artemisa, es que no existe una réplica de Artemisa como tal, que es lo que generalmente ofrecen proveedores de servicios de *cloud*, pero sí que existe una réplica de los datos por *diseño*.

- Los sistemas de adquisición y colaboraciones mantienen una copia de los datos en las distintas ubicaciones que participan en estas.

- El uso de datos por parte de entidades externas facilita que la responsabilidad de la copia se transfiera a las entidades usuarias.

Es decir, Artemisa elimina las características de banco de datos que tiene que ser proporcionado por el usuario.

Artemisa facilita la recuperación y el mantenimiento del servicio que es donde se centra el plan de recuperación.

Por su parte, los aspectos recogidos en el plan de continuidad y recuperación incluyen:

- Mantenimiento y actualizaciones del software requerido de operación.
- Procesos de reinstalación automática y de salvaguarda de datos críticos de operación (configuraciones, usuarios, permisos).
- Sistemas físicos de extinción, acceso y ambiente de las instalaciones.
- Identificación de responsabilidades y recursos para el mantenimiento y la operación.

ANÁLISIS DE PROCESOS CLAVE PARA LA DEFINICIÓN DEL PLAN DE CONTINUIDAD EN EL IFIC

Hasta llegar a disponer del plan de continuidad se ha de realizar mucho trabajo e implicar a gran parte de la organización.

La herramienta del sistema de gestión de la seguridad de la información, certificado de acuerdo con la norma ISO 27001: 2013 que da soporte a Artemisa, como se ha comentado anteriormente, nos ha proporcionado un marco de trabajo ordenado en el que, por requisito, no se pueden obviar los procesos clave que señalamos y que hemos decidido abordar en este caso práctico. Para las organizaciones que no dispongan de un sistema de gestión normalizado sería una ayuda comenzar con una planificación de tareas que permita asegurar un análisis completo de los procesos y de los riesgos asociados a estos, ya que esta información será sobre la que se fundamente todo el plan.

Desde nuestra experiencia, los procesos que consideramos clave para la definición de un plan de continuidad adecuado empiezan con el análisis del contexto y la definición del alcance. Antes de realizar un análisis de riesgos (que por supuesto también consideramos clave) frente al que definir el plan de continuidad es importante contextualizar la organización, los procesos y el entorno donde se llevan a cabo, y definir los límites, el hasta dónde debemos y hasta dónde estamos «comprometidos» a responder.

Estas circunstancias particulares de cada organización dependen de su naturaleza y sus objetivos y, como hemos visto en la introducción a este artículo, el caso de Artemisa es diferente de un proyecto empresarial en estos aspectos: tiene una naturaleza institucional y sus objetivos no son de negocio.

Estrategia de implantación

Artemisa es una infraestructura pionera y con objetivos muy relevantes, cuyo funcionamiento requiere, por tanto, un nivel de conciencia operacional exigente dentro de la organización.

Idealmente, las normas surgen en forma de arriba abajo o top-down, es decir, al ser la decisión de la dirección la que facilita la implantación de normas, es esta la que debe proponerlas a partir de sus intereses.

En general, si bien hay alicientes para la implantación de normas voluntarias como la 27001, que a diferencia de las reguladas requieren esfuerzo, el retorno a la hora de la implantación no está claro. El problema es que implica concienciar también a la organización y requieren un trabajo importante de implantación.

Gracias a los fondos recibidos por la Agencia Valenciana de la Innovación, en reconocimiento a las características únicas en la Comunidad Valenciana del IFIC, se constituyó con fondos de esta agencia la UCIE, la Unidad Científica Empresarial. Gracias a que estos fondos llegaron en paralelo a Artemisa y al carácter multidisciplinar de la infraestructura muy ligada a la innovación, la dirección entendió perfectamente la necesidad de diferenciar esta infraestructura, la primera del IFIC abierta por diseño a otros usuarios, del resto de sus infraestructuras de computación.

Esto permite adicionalmente, y si fuese necesario, extender esta actividad a otras infraestructuras que gestiona el IFIC, pero esta es de especial complejidad debido a su uso externo.

Toda esta implicación ha tenido un efecto positivo:

- El entendimiento de las políticas por parte de la dirección.
- La implicación en todos los aspectos de esta que incluyen los sistemas de información, programas y recursos necesarios, lo que permite comprender dónde van los recursos.
- Una mejor comunicación de un departamento horizontal en cuanto a servicios y necesidades de los usuarios.

El IFIC como centro mixto de investigación funciona con arreglo a procedimientos y requisitos de las dos instituciones que lo forman. La iniciativa del instituto para elaborar un plan de continuidad en el marco de un sistema de gestión de la seguridad de la información certificado ha resultado pionera en el marco institucional y se ha alineado a la perfección con los sistemas de la Universitat de València, que es una de las pocas universidades en España certificadas en el Esquema Nacional de Seguridad (ENS).

El hecho de que el plan de continuidad no haya sido un requisito de ninguna de las partes, si no que ha surgido como una iniciativa del propio instituto, supone que para ambas instituciones el IFIC es un referente frente a futuras implantaciones de sistemas de gestión de seguridad de la información y también para la redacción y mejora de los planes de continuidad.

Definición del alcance del plan

En el instituto se llevan a cabo muchos proyectos, de la misma forma que en una empresa se realizan diferentes procesos de negocio, que afectan o dependen de infraestructuras y responsables concretos. En la definición del alcance implicamos a determinados procesos y con ello todo aquello que los soporta (recursos, personas, procesos de gestión...), por eso lo consideramos un aspecto clave.

El alcance del plan de continuidad y del sistema de gestión de seguridad de la información certificado que lo respalda, implica solo a los procesos de Artemisa. Esto no quiere decir que no afecte a otros procesos o infraestructuras del IFIC, y de ahí la importancia de empezar analizando profundamente el contexto.

Análisis del contexto operacional

El contexto operacional consiste en el entorno en el que se llevan a cabo los procesos. En el análisis y la definición del contexto se han tenido en cuenta los factores inherentes a su ubicación física y ambiental así como los asociados a su administración, mantenimiento e institucionalidad.

Entre las particularidades del contexto de Artemisa destacan su carácter de institución mixta y sus objetivos «de negocio». Estas han supuesto algunos retos en la planificación del sistema y del plan de continuidad, pero también importantes oportunidades. Cabe destacar aquí, por ejemplo, todos los servicios de apoyo que cuentan con un alto grado de organización previo a la definición del plan. Los servicios de mantenimiento, informática, administración y gestión consolidados han facilitado la integración de nuevos planes y procedimientos.

Análisis del contexto de responsabilidad

Artemisa es una infraestructura operada con fondos públicos. En principio, solo las instituciones de investigación sin ánimo de lucro tienen derecho a utilizar la plataforma. No obstante, conforme está previsto en los términos generales de uso y servicio pueden preverse acuerdos especiales con organizaciones lucrativas estudiando caso por caso.

Las condiciones o garantías a las que se compromete el instituto mediante los acuerdos con terceras partes y, por tanto, a las que debe dar continuidad en caso de contingencia son:

- Seguridad a niveles de mercado (*zero-day-exploit,* controles de acceso, seguridad física, seguridad lógica manteniendo la conectividad, disponibilidad).
- Disponibilidad (aprovisionamiento de cómputo: es a repartir entre proyectos y se revisa de *call a call* o si hay requerimientos especiales).
- Disponibilidad (acceso a la infraestructura externa, que depende del origen, y de cuestiones tales como la interna (UVEG) o la local (IFIC).

Aunque estas condiciones pueden compararse con los niveles de seguridad de mercado, los procesos y los datos dentro del alcance implican que los impactos y, por tanto, las acciones necesarias para un plan de continuidad adecuado sean diferentes a las requeridas en los procesos de negocio de otros tipos de organizaciones.

Análisis de riesgos

La naturaleza de los riesgos identificados y tratados en el sistema es similar a la de otras organizaciones en lo relativo a infraestructuras de gestión, tales como el correo, las bases de datos de usuarios, etcétera, y se diferencia en cuanto a las infraestructuras de servicio científico, las propias de alojamiento y computación.

En los riesgos asociados a estas últimas, las acciones para su tratamiento persiguen la eliminación del riesgo o la limitación en los niveles de riesgo que se pueden alcanzar mediante el establecimiento de requisitos de uso de la infraestructura, en línea con los objetivos del proyecto como tal.

En este aspecto somos conscientes de que se eliminan grandes amenazas de seguridad al limitar el acceso a la infraestructura a proyectos e instituciones de investigación. Además, al análisis de riesgos generales, en nuestro caso, se añade un análisis de riesgos particulares de cada proyecto que se aborda en el proceso de evaluación de solicitudes.

Esta fase del proceso de admisión no existe en el acceso a otras infraestructuras de computación, por lo que, además de un requisito, suponen un valor añadido a la seguridad. Actualizar la evaluación de riesgos periódicamente es una tarea importante para tener en cuenta nuevas amenazas, experiencias, incidencias y oportunidades de mejora detectadas de cara a la revisión del plan de continuidad.

Elaboración y actualización del plan de continuidad

Para que la elaboración y actualización del plan de continuidad sea un proceso eficaz es importante trabajarlo de forma conjunta con todos los departamentos y responsables afectados en el ensayo de escenarios y respuestas. De esta forma, en el momento de definir las acciones que se deban tomar en cada escenario se dispone de toda la información necesaria y se facilita la propuesta de alternativas y la coordinación por parte de los responsables de los procesos.

En la elaboración del plan de continuidad de Artemisa han participado de una forma u otra todos los servicios de gestión y soporte de actividades del IFIC (administración, informática, mantenimiento) y también el propio comité de seguridad de la información, formado en este caso por un miembro del departamento de IT, la propia dirección y un investigador certificado CISA de ISACA.

Está previsto que todos participen de igual modo en las actualizaciones. Las necesidades de actualización pueden surgir en cualquier ámbito: desde cambios en proveedores de servicios, modificación de personal responsable o tan solo de números de teléfonos de contacto hasta la incorporación de nuevos escenarios.

El plan establece los procedimientos necesarios para recuperar los sistemas de información críticos del proyecto dentro del proyecto. Se incluyen en este las alternativas básicas de contingencia, los procedimientos de operación, la secuencia de eventos y los procedimientos de recuperación que se deban utilizar inmediatamente después de un desastre, con el objeto de volver lo antes posible a la normalidad.
Aunque inicialmente se considere completo, garantizar la adecuación del plan requiere la realización de pruebas y el tratamiento y análisis posterior de resultados.

Aprobación y comunicación del plan

Una vez aprobado el plan es fundamental que se comunique y se ponga a disposición de los afectados de una manera eficaz. Si el plan es totalmente adecuado pero no está a disposición de las personas que han de poner en marcha las acciones en caso de contingencia, todo el trabajo resultará inútil.

Además, para cada escenario posible se han previsto procedimientos y líneas concretas de comunicación, diferentes en cada caso.

En el IFIC los procesos de comunicación están bastante consolidados y están soportados por recursos independientes del proyecto Artemisa. Esto permite que la implantación y actualización de estos procedimientos no haya supuesto nuevos retos para la organización.

Para cualquier actualización del plan, sea cual sea la naturaleza del cambio, hay prevista una nueva distribución controlada del documento a todas las partes intervinientes y afectadas.

EXPERIENCIA OPERATIVA: PUESTA EN MARCHA DEL PLAN DE CONTINUIDAD

Los escenarios de posibles contingencias y planes de recuperación y continuidad establecidos son: incendio/ terremoto, inundaciones, situación de alarma/excepción, cortes eléctricos, no funcionamiento de los equipos de climatización del CPD, cortes en servicio de Internet, fallos en elementos de la red, caídas de servicios críticos y de servicios replicados, servidores de almacenamiento y plagas de roedores.

Existen, por tanto, escenarios en los que la identificación de la contingencia es inmediata y clara, pero hay otros en los que es necesario el uso de métricas para el seguimiento de los procesos y la evaluación objetiva de su estado. Resulta necesario definir responsables en la supervisión y el seguimiento de estas métricas para garantizar la identificación de necesidades de puesta en marcha del plan de continuidad ante determinados escenarios.

PARC CIENTÍFIC
VNIVERSITAT DE VALÈNCIA

GENERALITAT VALENCIANA
Conselleria d'Innovació, Universitats, Ciència i Societat Digital