CONTINUIDAD DE NEGOCIO

POLÍTICAS DE SEGURIDAD PARA LA PYME

Colección

PROTEGE TU EMPRESA

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. CONTINUIDAD DE NEGOCIO

1.1 ANTECEDENTES

Es imposible garantizar la seguridad total, por lo que las empresas deben estar preparadas para **protegerse ante un posible desastre** que pudiera paralizar su actividad. Hoy en día, la información es un activo esencial en cualquier organización, y los sistemas de información se apoyan en **tecnologías complejas y novedosas** que también están expuestas a amenazas de seguridad. Por todo ello, es conveniente tener elaboradas unas **pautas** que indiquen cómo actuar en caso de que haya un fallo de seguridad que comprometa la **continuidad del negocio** de nuestra empresa.

Estas pautas quedarán debidamente recogidas en un **plan de contingencia y continuidad de negocio** [1] que asegurará la respuesta efectiva por parte de la organización a incidentes o desastres inesperados (como ciberataques, desastres naturales, fallos tecnológicos, etc.), de forma que se minimice el impacto en la operativa del negocio.

Los principales objetivos de contar con un plan de continuidad de negocio son **minimizar las interrupciones en las operaciones críticas y proteger los activos empresariales tangibles e intangibles**. De esta forma, se podrá retomar la actividad de la empresa lo antes posible, garantizando la continuidad del negocio.

1.1 ANTECEDENTES

Nuestro **plan para la continuidad de negocio** debe tener en cuenta las personas responsables de aplicarlo, las operativas a seguir (por ejemplo: implementar un mecanismo de respaldo para nuestra información más crítica), los activos implicados (tanto personales como físicos), indicadores, etc. Una vez que tengamos el plan de continuidad debemos **comprobar** que sabemos ponerlo en marcha.

Cuando contratemos **servicios tecnológicos** (en la nube o a proveedores externos) o que impliquen el tratamiento de nuestra información, debemos exigir y comprobar que tienen planes de contingencia disponibles que se adecuen a nuestra política para la continuidad del negocio [2].

Tan importante como la elaboración del plan de continuidad de negocio es su **difusión**. Los trabajadores de la empresa tienen que ser conocedores de la existencia de un protocolo de recuperación ante incidencias. Principalmente, para saber qué papel le corresponde a cada uno en el procedimiento de recuperación. Que cada agente tenga claros sus roles será la clave de una **ejecución óptima del plan de continuidad**.

En este contexto, la **Norma ISO 22301**, aplicable a cualquier tipo de organizaciones independientemente de su sector y tamaño, es un **marco normativo internacional** que ayuda a las empresas en la implementación y mejora del sistema de gestión de continuidad de negocio.

Esta normativa proporciona una base sólida para **garantizar la continuidad del negocio de las empresas**, reduciendo el riesgo de interrupciones y la recuperación ante ellas, minimizando el impacto, a la vez que demuestra a clientes y proveedores el compromiso de la organización y facilita el **cumplimiento normativo** relacionado con la continuidad de negocio.

1.2 OBJETIVOS

Diseñar y probar un plan de continuidad de negocio (PCN) que nos permita recuperar en un plazo razonable la operativa habitual de nuestra empresa para garantizar la continuidad del negocio.

1.3 CHECKLIST

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a la **continuidad del negocio**.

Los controles se clasificarán en dos niveles de **complejidad**:

- **Básico (B):** el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- **Avanzado (A):** el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- **Procesos (PRO):** aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** aplica al personal técnico especializado.
- **Personas (PER):** aplica a todo el personal.

1.3 CHECKLIST

Nivel	Alcance	Control	
B	PRO	**Determinar el alcance del PCN.** Analizas para que activos y procesos debes garantizar la continuidad.	☐
B	PRO	**Concretar el flujo de responsabilidades.** Determinas las responsabilidades de las personas que deben llevar a cabo el plan de continuidad en caso de aparición de desastres.	☐
A	PRO/TEC	**Realización del BIA (Análisis del Impacto en el Negocio).** Elaboras detalladamente el BIA de tu empresa.	☐
A	PRO/TEC	**Análisis de riesgos.** Determinas las amenazas que pueden producirse y la probabilidad y el impacto de su ocurrencia.	☐
A	PRO/TEC	**Elegir la estrategia de continuidad.** Eliges la estrategia de continuidad óptima para tu empresa. Teniendo en cuenta si fuera preciso la implantación de un centro de respaldo.	☐
A	PRO/TEC	**Detallar la respuesta a la contingencia.** Detallas los procedimientos y controles específicos a ejecutar ante un incidente.	☐
A	PRO/TEC	**Desarrollar actividades para verificar, revisar y evaluar el plan de continuidad del negocio.** Pruebas y evalúas cada _____ el plan de continuidad de negocio de tu empresa.	☐
B	PRO	**Definir la política de comunicación y aviso a entidades externas.** Defines que tipo de mensajes debe transmitir tu empresa en caso de desastre.	☐
B	PRO/PER	**Concienciación de la plantilla.** Te aseguras de que cada empleado conozca la existencia del PCN y comprenda su importancia.	☐

Revisado por: _____ **Fecha:** _____

1.4 PUNTOS CLAVE

Los puntos clave de esta política son:

- **Determinar el alcance del plan de continuidad del negocio.** Debemos seleccionar los activos para los cuales garantizar la continuidad, priorizando en aquellas áreas esenciales. Para ello nos basaremos en los activos críticos de la clasificación de activos de información [3].
- **Concretar el flujo de responsabilidades.** Para una correcta ejecución del plan de continuidad del negocio tenemos que determinar quién(es) debe(n) hacerse cargo de la situación en caso de desastre. Definiremos las responsabilidades, la secuencia de decisiones y los canales adecuados para establecer las comunicaciones oportunas.
- **Realización del BIA (Análisis del Impacto en el Negocio) [4] [5] [6].** Para calcular el riesgo al que estamos sometidos, debemos estudiar las implicaciones de un incidente grave en los activos de información. Para ello determinaremos, entre otros:
  - Cuáles son las actividades principales de la organización.
  - Las dependencias, con otros procesos o proveedores, de las actividades anteriores.
  - El máximo tiempo que podemos estar sin esa actividad o actividades.
  - El tiempo mínimo de recuperación del servicio a niveles aceptables.
- **Análisis de riesgos [7].** Con la información obtenida previamente, se deberá realizar un análisis de riesgos que determine las amenazas que pueden producirse, la probabilidad con la que podrían ocurrir y el impacto que tendrían sobre la organización. Mientras que el BIA está enfocado al estudio del impacto de la interrupción de los procesos críticos del negocio, este análisis trata de identificar los potenciales riesgos que pueden afectar a la empresa y las medidas que se deben tomar para mitigarlos.
- **Elegir la estrategia de continuidad.** Determinaremos qué estrategia es la más adecuada para nuestra empresa para mitigar los riesgos identificados. Implantaremos políticas de copias de seguridad **[8]**, donde definiremos la información que debe incluirse en dichas copias, qué tipo de soporte se utilizará, con qué periodicidad y en qué instalaciones físicas. Por otro lado, estudiaremos la conveniencia de implantar un centro de respaldo a raíz de los resultados obtenidos durante la elaboración del BIA (Análisis del Impacto en el Negocio). Esto es especialmente importante si el alcance del Plan es el CPD.

1.4 PUNTOS CLAVE

- **Detallar la respuesta a la contingencia.** Se deben detallar los procedimientos y controles que aseguren el nivel de continuidad de los procesos y activos esenciales ante una situación adversa **[9]**, es decir, qué acciones se llevarán a cabo en caso de incidente para recuperar la actividad normal del negocio. Este proceso podrá organizarse en torno a los siguientes elementos:
  - Plan de crisis (o incidentes).
  - Planes operativos de recuperación de entornos.
  - Procedimientos técnicos de trabajo (o de incidentes).
- **Desarrollar actividades para verificar, revisar y evaluar el plan de continuidad del negocio [10][11].** Para garantizar que el plan de continuidad del negocio es válido evaluaremos cada cierto tiempo todos los procedimientos y controles que lo componen, para modificarlos, eliminarlos o añadir nuevos si fuera necesario. Se deberán definir pruebas periódicas para verificar la integridad y la correcta recuperación de la información, así como la periodicidad con la cual deberían revisarse, los activos y el personal implicado. Estas actividades se tendrán en cuenta sobre todo tras acometer cambios sustanciales en nuestros sistemas.
- **Definir la política de comunicación y aviso a entidades externas.** En ciertos casos puede ser necesario determinar qué personas deben notificar las situaciones de desastre a las autoridades pertinentes y a los medios de comunicación. Analizaremos qué tipo de mensaje se debe transmitir y cómo.
- **Concienciar a toda la plantilla de la existencia de un plan de continuidad y de su papel en el mismo.** Cada empleado tiene un determinado papel en el plan de recuperación. Será crucial para la empresa asegurar que los trabajadores conocen el procedimiento a seguir en caso de incidente, ataque o denegación de servicio. De esta forma, se minimizará el impacto y se acelerará la respuesta al incidente. Adicionalmente, tras un incidente, es altamente recomendable recopilar toda la información del evento para ser analizada y estudiada para mejorar en la seguridad e implementar nuevas medidas de mitigación.

2. REFERENCIAS

[1] INCIBE – Empresas – ¿Qué te interesa? – Plan de Contingencia y Continuidad de Negocio https://www.incibe.es/empresas/que-te-interesa/plan-contingencia-continuidad-negocio

[2] INCIBE – Empresas – Blog – TemáTICas: Seguridad en la nube - https://www.incibe.es/empresas/blog/tematicas-seguridad-nube

[3] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Clasificación de la información - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/clasificacion-informacion.pdf

[4] INCIBE – Empresas - ¿Qué te interesa? – Plan Director de Seguridad - https://www.incibe.es/empresas/que-te-interesa/plan-director-seguridad

[5] INCIBE – Empresas – Blog – Pasos a seguir para realizar un análisis de impacto en nuestro negocio - https://www.incibe.es/protege-tu-empresa/blog/pasos-seguir-realizar-analisis-impacto-negocio

[6] INCIBE – Empresas – ¿Qué te interesa? – Plantilla ejemplo para inventario de activos para BIA - https://www.incibe.es/sites/default/files/contenidos/dosieres/plan-contingencia-continuidad-negocio/plantilla-ejemplo-bia.xls

[7] INCIBE – Empresas – Herramientas - ¿Conoces tus riesgos? - https://www.incibe.es/empresas/herramientas/conoces-tus-riesgos

[8] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Copias de seguridad - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/copias-seguridad.pdf

[9] INCIBE – Empresas – TemáTICas – Gestión de incidentes - https://www.incibe.es/empresas/tematicas/gestion-incidentes-seguridad

[10] INCIBE – Empresas – Blog - Que un desastre no te detenga, elabora un plan de continuidad de negocio - https://www.incibe.es/empresas/blog/desastre-no-te-detenga-elabora-plan-continuidad-negocio

[11] INCIBE - Empresas – Blog - Fases de un Plan de Continuidad de Negocio - https://www.incibe.es/empresas/blog/fases-plan-continuidad-negocio

Financiado por
la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

INSTITUTO NACIONAL DE CIBERSEGURIDAD