Continuidad de negocio

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

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 que comprometa la **continuidad del negocio** de nuestra empresa.

Nuestro **plan para la continuidad de negocio** [1] 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].

1.2. Objetivos

Diseñar y probar un plan de continuidad de negocio [3] (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.

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.	☐
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	**Caducidad del PCN** Actualizas el plan de continuidad de negocio de tu empresa cada _____.	☐
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 la aparición de un desastre.	☐
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.	☐

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. Para ello nos basaremos en los activos críticos de la clasificación de activos de información [10].
- **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]**.** 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.
- **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.
- **Caducidad del plan de continuidad del negocio.** Con el fin de mantener actualizado nuestro plan de continuidad de negocio, determinaremos la periodicidad con la cual debería revisarse. Asimismo, analizaremos la necesidad de actualizar nuestro plan tras acometer cambios importantes en nuestros sistemas de información.
- **Elegir la estrategia de continuidad.** Determinaremos que estrategia es la más adecuada para nuestra empresa. Implantaremos políticas de copias de seguridad [6], donde definiremos la información que debe incluirse en dichas copias, qué tipo de soporte se utilizará, con qué periodicidad y en qué instalaciones físicas. Asimismo, se deberían definir pruebas periódicas para verificar la integridad y la correcta recuperación de la información. Por otro lado, estudiaremos la conveniencia de implantar un centro de respaldo [7] 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 [8].
- **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.
- **Desarrollar actividades para verificar, revisar y evaluar el plan de continuidad del negocio** [9]**.** 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. Estas actividades se tendrán en cuenta sobre todo tras acometer cambios sustanciales en nuestros sistemas.

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – ¿Qué te interesa? – Plan de Contingencia y Continuidad de Negocio https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio

[2]. Incibe – Protege tu empresa – Blog – Sube a la nube, pero no estés en «las nubes» sin continuidad de negocio https://www.incibe.es/protege-tu-empresa/blog/no-estes-en-las-nubes

[3]. Incibe – Protege tu empresa – Blog – ¿No tienes un Plan de Crisis? ¿Estás esperando al desastre? https://www.incibe.es/protege-tu-empresa/blog/plan-de-crisis

[4]. Incibe – Protege tu empresa – 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

[5]. Incibe – Protege tu empresa – ¿Qué te interesa? – Plantilla ejemplo para inventario de activos para BIA https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio

[6]. Incibe – Protege tu empresa – ¿Qué te interesa? – Políticas de seguridad para la pyme – Copias de seguridad https://www.incibe.es/protege-tu-empresa/que-te-interesa

[7]. Incibe – Protege tu empresa – Blog – Frío o caliente… o quizá templado, ¿qué sitio de recuperación me conviene? https://www.incibe.es/protege-tu-empresa/blog/frio-o-caliente-que-sitio-de-recuperacion-me-conviene

[8]. Incibe – Protege tu empresa – Blog – Pon un CPD seguro en tu empresa https://www.incibe.es/protege-tu-empresa/blog/cpd-seguro-empresa

[9]. Incibe – Protege tu empresa – Blog – Las pruebas de continuidad no son una opción, sino una obligación https://www.incibe.es/protege-tu-empresa/blog/pruebas-continuidad-no-opcion-si-obligacion

[10]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Clasificación de la información https://www.incibe.es/protege-tu-empresa/herramientas/politicas

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD