PLAN DE CONTINUIDAD DE NEGOCIO EN LAS UNIVERSIDADES

BUSINESS CONTINUITY PLAN IN UNIVERSITIES

Autor:

Joaquín Canca Cuenca. Universidad de Málaga. joaquin@uma.es.

Resumen:

En el artículo se reflexiona sobre los riesgos a los que cualquier organización, incluidas las universidades, está expuesta y especialmente los relacionados con los ciberataques. Una de las herramientas para afrontarlos es el denominado Plan de Continuidad de Negocio, que nos va a ayudar a restablecer los servicios después de haber sufrido una interrupción. Para su elaboración existe un marco de buenas prácticas recogido en la norma internacional ISO 22301, de la que describiremos brevemente sus principales elementos.

Abstract:

The article is a reflection on the risks to which any organization, including universities, is exposed and especially those related to cyberattacks. One of the tools to deal with them is the so-called Business Continuity Plan, which will help us to restore services after suffering an interruption. For its preparation, there is a framework of good practices included in the international standard ISO 22301, of which we will briefly describe its main elements.

Palabras clave:

Plan de continuidad de negocio; ISO 22301; Ciberseguridad

Keywords:

Business Continuity Plan; ISO 22301; Cybersecurity

CONTINUIDAD DEL NEGOCIO O PLAN B

El concepto de continuidad de negocio no es más que una traslación al mundo de las organizaciones del concepto de supervivencia ante una crisis.

La referencia a "negocios" en la denominación del plan de continuidad se debe interpretar de manera amplia en el sentido de aquellas actividades que son fundamentales para los fines que justifican la existencia de la organización.

Para sobrevivir, gestionamos y evaluamos riesgos, adoptamos medidas de prevención y, aun así, sabemos que habrá momentos en los que ocurrirán accidentes, provocados o no, que pondrán en riesgo nuestra continuidad. Cuando eso ocurre, es importante que sepamos qué debemos hacer para restaurar la estabilidad perdida, es importante contar con un Plan B.

En el entorno de las organizaciones se ha logrado ir reduciendo significativamente los riesgos accidentales, pero si nos centramos en las tecnologías que apoyan a estas organizaciones, los incidentes intencionados crecen en frecuencia y en intensidad de los ataques. De ser noticia anecdótica hace tan solo unos pocos años, ahora no hay día que no se produzca algún ciberataque muy dañino a empresas u organismos públicos importantes.

EL 12 de mayo de 2017, un ataque mediante WannaCry paralizó numerosas empresas en todo el mundo, incluyendo sistemas sanitarios como el británico. En España fue especialmente destacado el ataque a Telefónica.

Más recientemente en nuestro país, todos recordamos el ataque sufrido por el SEPES (Servicio Público de Empleo Estatal) el 9 de marzo de 2021, o los recibidos por Glovo, Phone House o la Universidad de Castilla-La Mancha en ese mismo año.

Lo que comenzó a principio de los años 70 como una suerte de “cibergamberrismo” ha ido evolucionando a conductas “cibercriminales” con equipos de personas muy formadas y con capacidad para robar datos o inutilizar los sistemas informáticos de casi cualquier

organización que se marquen como objetivo. Si nos convertimos en uno de esos objetivos, difícilmente podremos evitar los daños, aunque sí podemos minimizarlos y, sobre todo, restaurar nuestros procesos en el menor tiempo posible y al menor coste, mitigando así las consecuencias que pueden llegar a ser muy graves para el funcionamiento de nuestra universidad (solamente hay que pensar en una situación en la que perdamos todos los expedientes académicos de nuestros estudiantes, incluidas las copias de seguridad).

Tendemos a pensar que ”no vamos a tener tan mala suerte” pero si atendemos al informe “Cyber Attack Trends: 2021 Mid-Year Report”, los ciberataques se han incrementado en un 29% a nivel mundial respecto al año anterior, llegando en Europa ese incremento al 36%. Los ciberdelincuentes han explotado la pandemia Covid-19 incrementando en un 93% el número de ataques de *ransomware*.

La respuesta a esta situación, peligrosa y probable, es el denominado Plan de Continuidad de Negocio, o cómo levantarnos después de una caída. Tenemos que disponer de un plan que contemple diferentes escenarios, más o menos probables y más o menos predecibles. Esa impredecibilidad es una de las principales características que debe contener un plan de continuidad, pues se trata de plantear escenarios diversos y no necesariamente basados en la experiencia actual. Desastres totales o parciales que afecten a instalaciones, entorno o personas, deben ser contemplados y analizada su respuesta más adecuada, y a cada situación deberá corresponder un plan de acción específico y lo suficientemente flexible como para acoger nuevas eventualidades que ni siquiera hayamos previsto.

Hasta hace bien poco, las universidades, en general, no disponían ni se planteaban seriamente disponer de planes de continuidad, pero noticias como las que acabamos de exponer y más recientemente el uso masivo de los medios *on line* en las universidades, intensificado por la pandemia, ha provocado que nos preocupemos por establecer algún tipo de plan que dé respuesta a la necesidad de restablecer lo antes posible nuestros servicios en caso de crisis, ya sea accidental o provocada. Obviamente, no todos los

servicios son igual de críticos en una organización, por lo que una de las primeras tareas consistirá en determinar un orden en la urgencia de reactivación. Inicialmente son muchas las actividades que nos vienen a la cabeza y, posiblemente, todos querrán estar en la parte alta de la pirámide de prioridades, pero habrá que seleccionar:

- Continuidad de la docencia (presencial u online)
- Continuidad de las pruebas de conocimiento
- Continuidad de los procesos de gestión académica
- Continuidad de la actividad investigadora
- Continuidad de las actividades de ayudas sociales
- Continuidad en la relación con las empresas
- Continuidad de los procesos de la gestión económica
- Continuidad de los procesos de nómina y seguridad social
- Continuidad de los servicios TIC (correo electrónico, internet, VPN…)
- Continuidad de los servicios de biblioteca
- Continuidad de los servicios culturales o deportivos

  …

Podríamos seguir con más procesos y servicios, pero los anteriores bastan para percibir que no será una tarea fácil y que va a ser fundamental que la dirección se involucre de manera importante en la determinación de este conjunto de prioridades poniéndose una vez más de manifiesto la importancia del liderazgo.

Seguramente existen servicios que pueden esperar un mayor tiempo a ser reactivados sin provocar graves inconvenientes, aunque esto no será obvio para sus responsables ni para el personal que trabaja en ellos. Esto nos lleva a destacar una de las características de un Plan de Continuidad de Negocio: tiene que enfocarse a volver a poner en marcha los procesos clave de la institución, pero no necesariamente todos ellos, por lo que puede (y debe) haber planes diferenciados de continuidad de cada uno de sus procesos.

Si observamos lo ocurrido estos meses atrás, las soluciones de continuidad ante la crisis sanitaria provocada por el COVID-19 en nuestras universidades han venido en gran

medida de mano de las tecnologías y del trabajo y enseñanza a distancia, por lo que parece evidente que un plan de continuidad de negocio en nuestro ámbito tendrá que atender muy especialmente a esta área, ya que sin ella difícilmente puede mantenerse el funcionamiento del resto de los procesos, especialmente los académicos y administrativos, y más aún en un entorno no presencial.

Aunque con diferentes niveles de perjuicios, podríamos pensar en la posibilidad de prescindir durante un tiempo de los espacios físicos de aulas, bibliotecas, secretarías o laboratorios, pero más difícil sin correo electrónico, plataformas de enseñanza virtual, servicios administrativos online, o de acceso a internet.

Por este motivo, uno de los principales capítulos de un plan de continuidad para universidades, debe ser el denominado Plan de Continuidad TIC o Plan de Contingencia que no es más que la parte del plan de continuidad que afecta a las TIC.

Por último, haremos mención a que en este Plan de Contingencia deberemos incluir el denominado Plan de Recuperación ante Desastres, para recoger la estrategia de recuperación de la información, el hardware y el software de forma que podamos volver a una cierta normalidad en el menor tiempo posible.

Como vemos, el Plan de Continuidad va a estar constituido por un conjunto de “subplanes” de muy diversa índole y que tratarán de cubrir todos los aspectos que consideremos en nuestro análisis de riesgos: planes de prevención, planes de evacuación, planes de recuperación de servicios, etc.

¿PODEMOS EVITAR LOS DESASTRES?

Esta pregunta tiene una fácil y contundente respuesta: No.

En general, se considera que existen determinadas áreas de peligro que podemos resumir en: Interrupción de los servicios TIC, interrupción de suministro eléctrico, incendios, inundaciones, accidentes naturales, pandemias y terrorismo. Algunas de

estas áreas afectan a otras y todas probablemente terminan afectando a los servicios TIC.

En relación con el tipo de desastres que pueden afectar a la tecnología en la universidad, consideraremos tanto los relacionados con la seguridad física (destrucción de equipamiento y suministros de forma accidental o provocada), como la lógica (los relacionados con los ciberataques, riesgo que estamos comprobando que no es precisamente menor y que causa impacto en los servicios posiblemente mayores que cualquier otro, a excepción de los que provocan daños personales).

Al igual que con las enfermedades o los accidentes, podemos (y debemos) adoptar medidas que reduzcan la probabilidad del desastre, pero esa probabilidad nunca será de cero. Es más, crece conforme los ciberatacantes emplean técnicas más elaboradas, de manera que la lucha llega a ser tremendamente desigual.

Esa desigualdad en los medios, debe ser un acicate para que tomemos muy en serio la necesidad de disponer de un Plan de Continuidad de Negocio en el que analicemos los riesgos a los que estamos expuestos, adoptemos medidas de prevención y también de respuesta para el día en que pueda tocarnos (que nos tocará) esta infame lotería.

¿CÓMO SE HACE UN PLAN DE CONTINUIDAD DE NEGOCIO?

Como posiblemente ya sospecha, existe un marco de buenas prácticas que nos facilitan diseñar nuestro plan de continuidad. Ese marco es la ISO 22301, cuya primera versión es de 2012 mientras que, en 2019, se ha publicado la segunda y última por el momento, y en 2020, la norma española UNE-EN ISO 22301:2020

En la introducción se indica que el documento especifica la estructura y los requisitos para implementar y mantener un sistema de gestión de la continuidad de negocio de acuerdo con el impacto que la organización puede aceptar.

El resultado será la elaboración de un plan que, en su enfoque, deberá tener en cuenta consideraciones como aspectos legales, servicios que se proporcionan, tamaño y estructura de la organización y, por supuesto, los empleados.

Por continuidad de negocio se entiende la capacidad de una organización para continuar la entrega de productos y servicios dentro de marcos de tiempo aceptables tras una interrupción. Una interrupción está provocada por un incidente, ya sea previsto o no, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios de acuerdo con los objetivos de la organización.

ISO 22301:2019. SECURITY AND RESILIENCE - BUSINESS CONTINUITY MANAGEMENT SYSTEMS - REQUIREMENTS

ISO 22301 es la norma internacional para la continuidad de negocio y tiene su origen en la Norma Británica BS 25999. Este estándar internacional especifica los requerimientos para establecer y gestionar un efectivo sistema de gestión de continuidad del negocio ante situaciones como incendios, inundaciones, sabotajes, interrupciones de suministro eléctrico, catástrofes naturales, interrupción de servicios TIC, pandemias o cualquier otro previsto o no previsto.

El propósito último es disponer de planes que eviten la interrupción de la actividad de la organización minimizando en lo posible el impacto negativo de la paralización.

La ISO 22301 está basada en el ciclo de Deming: *Plan – Do – Check - Act* (Planificar – Hacer – Verificar – Actuar):

- **Planificar** implica determinar cuáles son los servicios más importantes que deben mantenerse en caso de una crisis y hasta cuánto podríamos soportar la interrupción de cada uno de ellos. Establece finalmente los objetivos perseguidos con el plan.
- **Hacer** significa realizar una evaluación de riesgos y de impacto para, a partir de ahí, realizar los cambios necesarios que los reduzcan y las medidas que permitan

restablecer los servicios en el menor tiempo posible. Es nuestro plan de respuesta.

- **Verificar** consiste esencialmente en la realización de pruebas periódicas que nos permitan comprobar que las medidas establecidas cumplen con los objetivos propuestos. Si esto no se hace, casi con toda seguridad en poco tiempo nuestras medidas se verán superadas por los cambios tecnológicos y las nuevas modalidades de ataque.
- **Actuar** para, a partir de los resultados del paso anterior, promover los cambios y adaptaciones necesarias para que nuestro plan continúe manteniendo o incrementando su eficacia.

Elaborar un plan de continuidad va a requerir contar durante un tiempo no breve, con recursos materiales y humanos de los que no siempre disponemos. Por ello puede ser recomendable que lo iniciemos abarcando inicialmente unas determinadas áreas que, posteriormente, iremos ampliando.

Los requerimientos del estándar pasan por la consideración de los siguientes elementos:

1. **Contexto.** Cuando establecemos un plan de continuidad, debemos tener en cuenta en primer lugar las necesidades y requerimientos de las partes interesadas (estudiantes, profesorado, proveedores, empresas, otros servicios públicos, sociedad, …) dando un peso a cada una para finalmente, lograr un equilibrio entre ellas. Para lograr este objetivo es fundamental disponer de un conocimiento profundo de la organización y determinar con claridad los límites y el alcance del plan.

2. **Liderazgo.** Dirigir y motivar a las personas que deben contribuir a la redacción del plan, dotar de los recursos necesarios y comunicar los resultados obtenidos.

3. **Planificación.** Describir los objetivos del plan, que deben ser monitorizables y medibles. La planificación debe determinar qué se hará, quién será el responsable, la temporalidad y la forma en la que se llevará a cabo la evaluación de resultados.

4. **Apoyo.** Mediante el suministro de los recursos necesarios, incluyendo las competencias de las personas que deben participar del plan, la forma en que se llevará a cabo la comunicación tanto interna como externa (qué se comunicará, cuándo, a quién, cómo y quién comunicará) y el control de toda la documentación necesaria.

5. **Operación.** Definimos los requerimientos específicos para la continuidad de los servicios. El plan debe incluir:
   a) El propósito, alcance y objetivos.
   b) Los roles y responsabilidades.
   c) Las acciones para implementar.
   d) La información de apoyo necesaria.
   e) Las interdependencias internas y externas.
   f) Los requisitos de recursos.
   g) Los requisitos de información.
   h) Un proceso de retirada.

6. **Plan de mejora.** Determinar las oportunidades de mejora como parte de la mejora continua.

¿Y CÓMO HACEMOS TODO ESTO?

Los pasos que debemos seguir para confeccionar un plan de continuidad son similares a la creación de cualquier plan:

- **Inicio:** Designar los responsables en su elaboración, funciones y metodología de trabajo a seguir.
- **Análisis de riesgos:** Se determina cuáles son los servicios críticos de la universidad que consideramos no pueden interrumpirse, se analizan los riesgos a los que están sometidos y el impacto que tendría la paralización de

cada uno de ellos. Se determinan los recursos que serían necesarios para mantener su continuidad.

- **Estrategia de recuperación:** Se establecen las posibles estrategias de recuperación en caso de que un incidente provoque una interrupción de los servicios.
- **Plan de respuesta:** Se documenta exhaustivamente la estrategia de continuidad elegida para garantizar la continuidad de cada uno de los servicios seleccionados mediante un protocolo de actuación para cada incidente que hayamos previsto.
- **Pruebas:** Se diseñan baterías de prueba que permitan evaluar la eficacia de las medidas de respuesta seleccionadas.
- **Formación:** Es una fase sumamente importante y a la que no se suele prestar el necesario interés. Es fundamental que todo el personal conozca y se sienta corresponsabilizado en la adopción de las medidas que se contemplan en el plan.

¿ES IGUAL EL PLAN PARA CUALQUIER TIPO DE ORGANIZACIÓN?

Sí en la estructura, pero con adecuaciones, ya que cada una tiene sus propias características que definen sus condiciones de continuidad. En el caso de organizaciones basadas en la prestación de servicios, la tecnología tiene un impacto diferente a las basadas en procesos de fabricación o distribución. De alguna forma podemos prestar “menos atención” a otros riesgos, especialmente a los relacionados con la interrupción de la cadena de suministros, que es el principal temor de muchas empresas, ya que los relacionados con las tecnologías constituyen un alto porcentaje de los que pueden causar la interrupción de nuestros servicios de forma prolongada. Los recientes ciberataques a organismos públicos son un claro ejemplo de ello.

También es cierto que mientras el impacto en empresas suele ser fundamentalmente económico y podría incluso provocar su quiebra, en el caso de organismos públicos las

consecuencias son generalmente reputacionales y difícilmente provocarán su desaparición.

En cualquier caso, disponer de planes de continuidad de negocio en las universidades es una necesidad indiscutible y que nos permite documentar adecuadamente los riesgos existentes y la forma de restablecer nuestros servicios con el menor impacto posible. Para ello, la norma ISO 22301 se erige como la herramienta más adecuada.

CONCLUSIÓN

Cuando servicios esenciales para nuestra organización se interrumpen, en muchas ocasiones no disponemos inicialmente de toda la información necesaria para actuar correctamente, la presión sobre los responsables de su restauración se intensifica a cada momento que pasa, muchas personas intervienen o pretenden intervenir, generalmente, de forma descoordinada y redundante. El resto de las personas espera que alguien les informe de lo que está sucediendo y de sus perspectivas de solución.

Elaborar un plan de continuidad ayuda a tener un mejor conocimiento de cada uno de los servicios que prestamos, a conocer los riesgos a los que podemos enfrentarnos, a saber qué debemos hacer y cómo debemos actuar ante cualquier eventualidad que ponga en riesgo nuestra actividad como prestadores del servicio público de la educación superior y a mitigar el posible daño físico o reputacional, que un incidente grave pueda provocar en nuestras universidades pudiendo transformarlo, incluso, en una demostración de eficacia.

REFERENCIAS

- CENTRO CRIPTOLÓGICO NACIONAL. (2021) *Ciber-amenazas y tendencias, edición 2021*. [Fecha de consulta: 02/05/2022]. Disponible en https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html

- CHECK POINT SOFTWARE TECHNOLOGIES. (2021) Cyber Attack Trends: 2021 Mid-Year Report. [Fecha de consulta: 02/05/2022]. Disponible en https://pages.checkpoint.com/cyber-attack-2021-trends.html
- CROWDSTRIKE. (2021) *Global Threat Report 2021*. [Fecha de consulta: 02/05/2022]. Disponible en https://www.crowdstrike.com/resources/reports/global-threat-report-es/
- INSTITUTO NACIONAL DE CIBERSEGURIDAD -INCIBE- (2020) *Plan de contingencia y continuidad de negocio.* [Fecha de consulta: 02/05/2022]. Disponible en https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf
- UNE-NORMALIZACIÓN ESPAÑOLA. (2020) *ISO 22301:2019. Sistema de Gestión de la Continuidad del Negocio.* [Fecha de consulta: 02/05/2022]. Disponible en https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0063818