TiES Revista de Tecnología e Innovación en Educación Superior

IMPORTANCIA DE LA SEGURIDAD FÍSICA EN LA INFRAESTRUCTURA DE REDES, CENTROS DE DATOS Y TELECOMUNICACIONES DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

https://doi.org/10.22201/dgtic.26832968e.2021.3.5

Carmen Humberta de Jesús Díaz Novelo
Jaime Olmos de la Cruz
https://www.ties.unam.mx/

Fecha de recepción: 18 de agosto de 2020 • Fecha de publicación: abril de 2021 Abril 2021 | número de revista 3 • ISSN 2683-2968

Acervos Digitales, Dirección General de Cómputo y de Tecnologías de Información y Comunicación, UNAM

Carmen Humberta de Jesús Díaz Novelo
Jaime Olmos de la Cruz
https://doi.org/10.22201/dgtic.26832968e.2021.3.5
Abril 2021 • Número 3 • ISSN 2683-2968
https://www.ties.unam.mx/

IMPORTANCIA DE LA SEGURIDAD FÍSICA EN LA INFRAESTRUCTURA DE REDES, CENTROS DE DATOS Y TELECOMUNICACIONES DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

Resumen

La infraestructura de las redes, los centros de datos y las telecomunicaciones de las Instituciones de Educación Superior (IES), permite el transporte de los datos y la interconexión hacia la red de redes (Internet). Por ello, es de vital importancia crear una conciencia sobre las acciones que las áreas estratégicas de Tecnologías de Información y Comunicación (TIC) deben tomar en lo referente a las inversiones y el otorgamiento de los recursos necesarios para asegurar la continuidad de los servicios, así como la implementación y el mantenimiento de sus proyectos. Se observa en las IES una necesidad apremiante por trabajar con un enfoque de gestión de riesgos, ya que, en cuanto a amenazas y vulnerabilidades a las que está expuesta la infraestructura, en todos los casos, el costo asociado a los riesgos no atendidos puede ser mucho mayor que el suficiente para implementar la protección requerida. Las metodologías de gestión de riesgos deben considerar las amenazas y las vulnerabilidades por fenómenos meteorológicos, ocasionadas por la geografía donde están ubicados los campus de las IES.

Palabras clave:

Seguridad física, Redes, Telecomunicaciones, Centros de Datos, Infraestructura, Administración de Riesgos

IMPORTANCE OF PHYSICAL SECURITY IN NETWORK INFRASTRUCTURE, DATA CENTERS AND TELECOMMUNICATIONS OF HIGHER EDUCATION INSTITUTIONS

Abstract

The infrastructure of networks, data centers and telecommunications of the Institutions of Higher Education (IES), allow the transport of the data and the interconnection to the network of networks, Internet. For this reason, it is important to raise awareness about the actions that Information and Communication Technologies (ICT) strategic areas should consider in investments and the granting of the necessary resources for the prevention, maintenance and implementation of their projects that guarantee the continuity of services. It is observed the urgent need to work with a risk management approach in the IES since, in terms of the threats and vulnerabilities to which the infrastructure is exposed, in all cases, the cost associated with the risks not attended can be higher that necessary to implement the required protection; risk management methodologies must consider the threats and vulnerabilities to meteorological phenomenals caused by geography where the campuses of the IES are located..

Keywords:

Physical security, Networks, Telecommunications, Data Centers, Infrastructure, Risk Management.

TiES Revista de Tecnología e Innovación en Educación Superior

Importancia de la Seguridad Física en la Infraestructura de Redes, Centros de Datos y Telecomunicaciones de las Instituciones de Educación Superior
Carmen Humberta de Jesús Díaz Novelo
Jaime Olmos de la Cruz
https://doi.org/10.22201/dgtic.26832968e.2021.3.5
Abril 2021 • Número 3 • ISSN 2683-2968
https://www.ties.unam.mx/

IMPORTANCIA DE LA SEGURIDAD FÍSICA EN LA INFRAESTRUCTURA DE REDES, CENTROS DE DATOS Y TELECOMUNICACIONES DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

Introducción

Un modelo de operación de la infraestructura, considera elementos de gestión de la tecnología, el talento humano y la tecnología requerida. Además, otorga las herramientas necesarias para asegurar la continuidad del servicio en las Instituciones de Educación Superior (IES) [1], enfrentando los riesgos potenciales a los que pueden estar expuestos la infraestructura de redes, los centros de datos y las telecomunicaciones.

Por otra parte, en años recientes se ha observado a nivel global y en México, la necesidad de retomar los tópicos relacionados con la infraestructura de redes y las telecomunicaciones, ante las iniciativas para dotar de Internet a todos los rincones del mundo y el país, además de fortalecer las telecomunicaciones existentes. Esta iniciativa proviene de organizaciones internacionales y nacionales, proveedores de servicios de Internet e instituciones de educación superior.

La Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES), realizó encuestas entre sus asociadas, durante los años 2016, 2017, 2018 y 2019. Los resultados publicados en documentos presentan el estado actual de las TIC en IES de México. Estos documentos cuentan con una sección dedicada a la seguridad de la información. Entre las incidencias de seguridad que se presentaron en las IES, se encontraron las siguientes: fallas en la energía eléctrica, incidentes relacionados con el agua, la humedad y temperaturas extremas, fallas en equipos por condiciones ambientales adversas, desastres naturales (inundaciones, sismos, huracanes, etc.) e incendios [2]. También se preguntó a las IES sobre daños ocasionados por robo, vandalismo y control de acceso, sin embargo, los porcentajes no fueron significativos, por lo que no se consideran en este trabajo. En el cuadro 1 se presentan los porcentajes de los incidentes de seguridad física entre 2016 y 2019.

En los resultados también se observa un lento avance de las IES en la aplicación de alguna metodología de gestión de riesgos; en la implantación de planes de recuperación de desastres, y en la puesta en marcha de planes de

Año	2016	2017	2018	2019
Número de IES que participaron en el estudio	140	149	144	137
Fallas en energía eléctrica	81%	83%	80%	80%
Agua, humedad, temperaturas extremas, etcétera	25%	43%	40%	42%
Fallas en equipos por condiciones ambientales inadecuadas	37%	38%	35%	36%
Desastres naturales (inundaciones, sismos, huracanes, etcétera)	12%	13%	19%	12%
Incendios	0%	1%	2%	1%

Cuadro 1.
Incidentes de seguridad física que se presentaron en las Instituciones de Educación Superior de México entre los años 2016 y 2019. Fuente: elaboración propia.

https://doi.org/10.22201/dgtic.26832968e.2021.3.5
Abril 2021 • Número 3 • ISSN 2683-2968
https://www.ties.unam.mx/

continuidad de negocio que incluyen análisis de impacto [2]. En el cuadro 2 se presentan dos indicadores relacionados con la continuidad del negocio, que permiten ver los porcentajes de avance de las IES entre 2016 y 2019.

Observando los cuadros 1 y 2, se puede concluir que es importante que las IES aborden la seguridad física y gestionen los riesgos asociados a la infraestructura, los centros de datos y las telecomunicaciones, ya que ante los cambios climáticos y los desastres físicos que provocan, cobra una gran relevancia, y se vuelve necesario analizar las vulnerabilidades que pueden presentarse en las IES. Un ejemplo es el paso destructivo del huracán *Dorian* en 2019, cuando la Sociedad de Internet hizo un llamado a la comunidad, ya que "los desastres naturales no van a desaparecer e incluso podemos esperar que tengan un mayor poder destructivo en el futuro. Aunque no podemos luchar contra la naturaleza, no hacer nada no es una opción" [3].

Año	2016	2017	2018	2019
Número de IES que participaron en el estudio	140	149	144	137
La IES cuenta con un plan de continuidad de negocio que incluye análisis de impacto	4%	3%	4%	11%
La IES cuenta con una política de continuidad para la operación de los servicios de T.I.	13%	14%	11%	15%

Cuadro 2.
Estado de avance de los planes de continuidad de negocio en las Instituciones de Educación Superior de México entre los años 2016 y 2019. Fuente: elaboración propia.

Amenazas y vulnerabilidades

En este contexto se considera valioso analizar brevemente algunas de las amenazas relacionadas con la infraestructura, los centros de datos y las telecomunicaciones, a las que se encuentran expuestas las IES, como son: cortes a enlaces de fibra óptica, huracanes, falta o falla de protección eléctrica, daños por agua, explosión, descargas atmosféricas y altas temperaturas, que son las amenazas más reportadas por las IES, de acuerdo con los resultados del estudio de la ANUIES [1]. La autora entrevistó a directores de TI de 25 IES de los siguientes estados: Baja California Sur, Chihuahua, Ciudad de México, Quintana Roo y Yucatán. Se les preguntó acerca de las lecciones aprendidas ante desastres físicos en su infraestructura de Telecomunicaciones, encontrando como resultado siete tipos de amenazas y sus vulnerabilidades. Los resultados coinciden con los estudios de la ANUIES, que a continuación se describen.

1. **Situaciones de cortes a enlaces de fibra óptica (FO).** A pesar de parecer únicamente notas periodísticas, los accidentes automovilísticos son fuente de daños frecuentes a postes, donde se encuentra la infraestructura de fibra óptica. La reparación de este tipo de daño involucra a las autoridades de la propia institución, empresas prestadoras de servicios, autoridades municipales y, en algunos casos, hasta estatales. Por otra parte, el acceso sin control a sitios de Telecomunicaciones, donde se encuentra instalada infraestructura de fibra óptica, deja a ésta expuesta a daños o desconexiones por descuidos o errores humanos. Otra amenaza son los trabajos de excavación o cortes de cable, debido a construcciones en la Institución (nuevos edificios, avenidas, puentes, jardines, estacionamientos, etc.), por no considerar las rutas de la fibra óptica. Una última situación que se expone, es el robo en registros de fibra óptica (Imagen 1) [4].
2. **Huracanes.** Algunos estados de la República Mexicana se ven afectados periódicamente por los huracanes, que pueden ocasionar daños en, los postes de operadores de Internet o de la Comisión Federal de Electricidad, dejando sin electricidad, Internet y teléfono a las IES. La caída de árboles también puede ocasionar fallas en la energía eléctrica y variaciones en el voltaje. La intermitencia durante el restablecimiento de la energía eléctrica afecta gravemente a los equipos electrónicos.
3. **Falta o falla de protección eléctrica.** Es común que con el tiempo se incrementen los equipos en los centros de datos y los sitios de telecomunicaciones, pudiéndose saturar los equipos UPS (nombre en inglés Uninterruptible Power Supply, también llamado Sistema de Alimentación Ininterrumpida) y la planta de emergencia. Los directores de TI entrevistados mencionaron situaciones en las que un daño en los transformadores provoca una interrupción de la energía eléctrica en el centro de datos y afecta la climatización, con un incremento de temperaturas en los equipos (Imagen 2). Una planta de emergencia, a pesar de ser un ele-

https://doi.org/10.22201/dgtic.26832968e.2021.3.5
Abril 2021 • Número 3 • ISSN 2683-2968
https://www.ties.unam.mx/

Figura 1.
P. Rodríguez y B. Kenigsztein, "Ejemplos de daños a estructuras de cableado. (a) Daño afecta servicio de Cable & Wireless en Chilibre, (b) Causas más extrañas y molestas de rotura de cables de fibra óptica," 2016. [Fotografía]. Disponible en: https://www.tvn-2.com/nacionales/Dano-servicio-Cable-Wireless-Chilibre_0_4543795659.html y https://www.xatakamovil.com/conectividad/las-10-causas-mas-extranas-y-molestas-de-rotura-de-cables-de-fibra-optica [Consultado en junio 22, 2020].

mento de seguridad para mantener el suministro de energía, en ocasiones presenta situaciones físicas como el fallo de algún componente, fallas mecánicas de algún interruptor y hasta errores humanos, como la omisión en el abastecimiento de combustible.

4. **Daños por explosión**. En dos casos compartidos por directores de TI de las IES, las explosiones fueron ocasionadas por fugas de gas cercanas a los centros de datos. En otro caso, la explosión ocurrió en una de las subestaciones eléctricas que alimentaba al centro de datos, debido a falta de mantenimiento. Otras de las principales causas de explosión se deben a componentes calientes que no reciben el enfriamiento adecuado, chispas por corto circuito, electricidad estática, relámpagos, campos electromagnéticos muy intensos y reacciones químicas de laboratorios mal ubicados.

Figura 2.
Sysmiami, "Daños en equipos de telecomunicaciones por falta de protección eléctrica," 2020. [Fotografía]. Disponible en: https://www.sysmiami.com/halloween-pesadillas-tenologicas/?lang=es [Consultado en junio 22, 2020].

5. **Daños por descargas atmosféricas**. Los casos relacionados con descargas atmosféricas siguen en aumento y fueron de los más mencionados por los directores de TI, incremento que puede deberse a los cambios climáticos, ocasionando daños de puertos en equipos de comunicaciones por inducción, a pesar de contar con terminales de sacrificio (pararrayos). Otra situación es la descarga atmosférica en las torres de acceso, que daña los equipos de comunicación inalámbrica entre edificios (imágenes 3 y 4) [5].
6. **Daño por agua**. Las filtraciones de agua, ocasionadas por diversas situaciones, como lluvias fuertes, pueden causar la inundación de un centro de datos. Uno de los casos extremos que se compartieron, fue el de las lluvias prolongadas que produjeron el desbordamiento de ríos. Se han registrado casos en que el agua ha subido más de un metro en un centro de datos (Imagen 5) [7].

Carmen Humberta de Jesús Díaz Novelo
Jaime Olmos de la Cruz
https://doi.org/10.22201/dgtic.26832968e.2021.3.5
Abril 2021 • Número 3 • ISSN 2683-2968
https://www.ties.unam.mx/

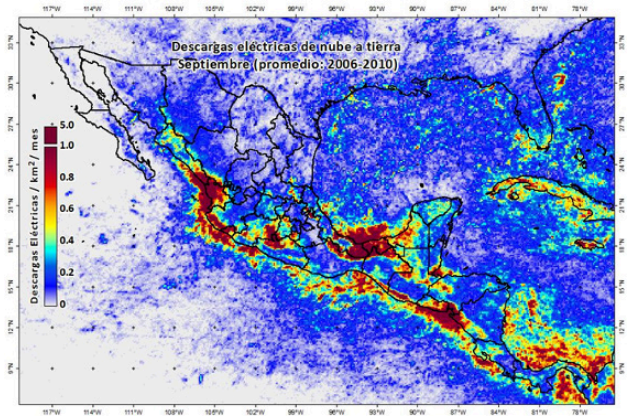

Figura 3.
Descargas eléctricas de nube a tierra. Fuente: Tomada de [6]

Figura 4.
Redwallpapers, "Descarga atmosférica," 2020. [Fotografía]. Disponible en: https://www.redwallpapers.com/tags/lightning?page=4 [Consultado en junio 22, 2020].

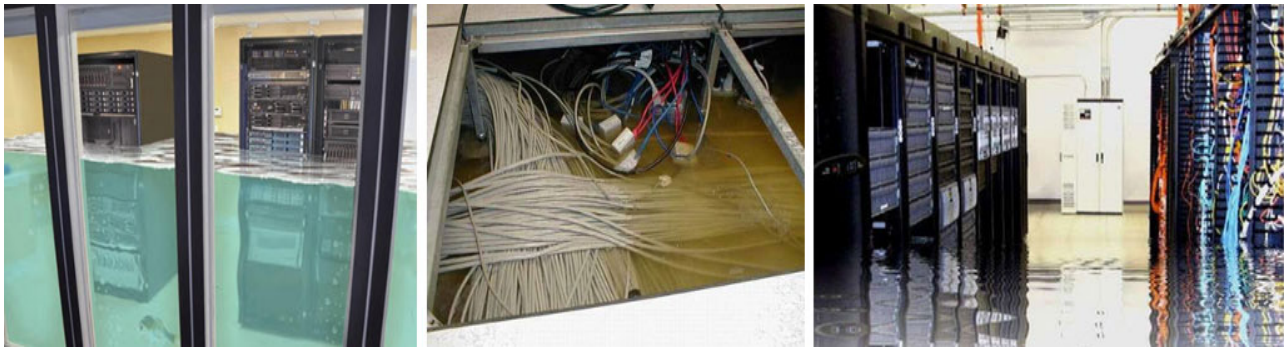

Figura 5.
R. Datacenter, PandoraFMS y Computerworld, "Ejemplos de Centross de Datos inundados, (a) ¿RTO vs RPO?, (b) Octopods flood, (c) calor y lluviasentre los grandes desafíos para la transformación digital del centro de datos," 2013. [Fotografía]. Disponible en: https://revistadatacenter.wordpress.com/2013/12/12/cual-es-la-diferencia-entre-el-rto-y-rpo/ https://pandorafms.com/docs/index.php?title=-File:Octopods_flood.jpg y https://computerworldmexico.com.mx/calor-y-lluvias-entre-los-grandes-desafios-para-la-transformacion-digital-del-centro-de-datos [Consultado en junio 22, 2020].

7. **Altas temperaturas.** Sin duda las altas temperaturas también son un factor de desastres. Algunas experiencias compartidas por los directores de TI, han coincidido en el daño al único aire acondicionado de su sitio de telecomunicaciones, donde se tienen temperaturas mayores a los 39 grados centígrados. Otra circunstancia relatada son los paros laborales o huelgas, que impiden el acceso a los centros de datos, dando lugar a problemáticas en los sistemas de aire acondicionado, al impedirse una atención oportuna a una falla en la climatización.

Acciones estratégicas para fortalecer la seguridad de la infraestructura y telecomunicaciones en las IES

En esta sección analizaremos las lecciones aprendidas y las prácticas compartidas por los directores de TI de IES entrevistados, que servirán de ayuda a otras IES para prevenir o enfrentar las amenazas antes expuestas, considerando la importancia del trabajo colaborativo dentro y fuera de la IES. En ese análisis reflexivo se esbozan algunas acciones estratégicas a considerar.

Carmen Humberta de Jesús Díaz Novelo
Jaime Olmos de la Cruz
https://doi.org/10.22201/dgtic.26832968e.2021.3.5
Abril 2021 • Número 3 • ISSN 2683-2968
https://www.ties.unam.mx/

- Se requieren políticas y lineamientos institucionales para precisar con más detalle los puntos y las maneras en que puede participar un área de TI en los comités de obras públicas de las IES. Por ejemplo, se puede conocer y compartir información sobre el diseño y la seguridad de las instalaciones, caminos y nuevas edificaciones, proyectando nuevos consumos de energía y generando esquemas que permitan la señalización adecuada de las rutas de fibra óptica, el aseguramiento de los registros y la integración de todos los documentos relacionados. El área de TI puede compartir buenas prácticas de cableado estructurado y la protección eléctrica de centros de datos. También puede sugerir trayectorias de cableado y la ubicación de áreas de cómputo, además de participar en proyectos de equipamiento de sistemas de voz, cómputo y telecomunicaciones de nuevos edificios [8].
- Tener al menos un plan de recuperación de desastres (DRP, Disaster Recovery Plan), inherente a los fenómenos atmosféricos de cada región, para obtener información de la zona de riesgo, el lugar del acontecimiento y un evento anunciado, así como tener la documentación adecuada y detallada del DRP; es decir, con instrucciones paso a paso sobre cómo ejecutarlo [9]. Las tecnologías de virtualización y de la nube pueden ser aliados para la implantación y las pruebas del DRP, o bien, implementar un sitio remoto con replicado de máquinas virtuales para acelerar la recuperación. No hay que dejar que el DRP se vuelva obsoleto: una vez creado, el plan requiere una revisión periódica.
- Establecer procesos de comunicación efectivos, que permitan hacer notificaciones al personal durante un desastre, considerando también algún acuerdo con asociados y aliados tecnológicos.
- Priorizar los servicios con base en el análisis de riesgos y los objetivos estratégicos de las IES. Esto permitirá mejores políticas para controlar el acceso a los centros de datos, para restaurar los servicios y respaldar la información. Las tecnologías como la nube permiten contar con respaldo en varias áreas geográficas [10] y [11].
- Analizar la ubicación del centro de datos y/o los sitios de Telecomunicaciones, para prevenir algún daño por explosión o inundación, y contar con instalaciones alternas para la operación emergente.
- Contar con sistemas integrales de protección eléctrica (Imagen 6) [12] y climatización. Una vez

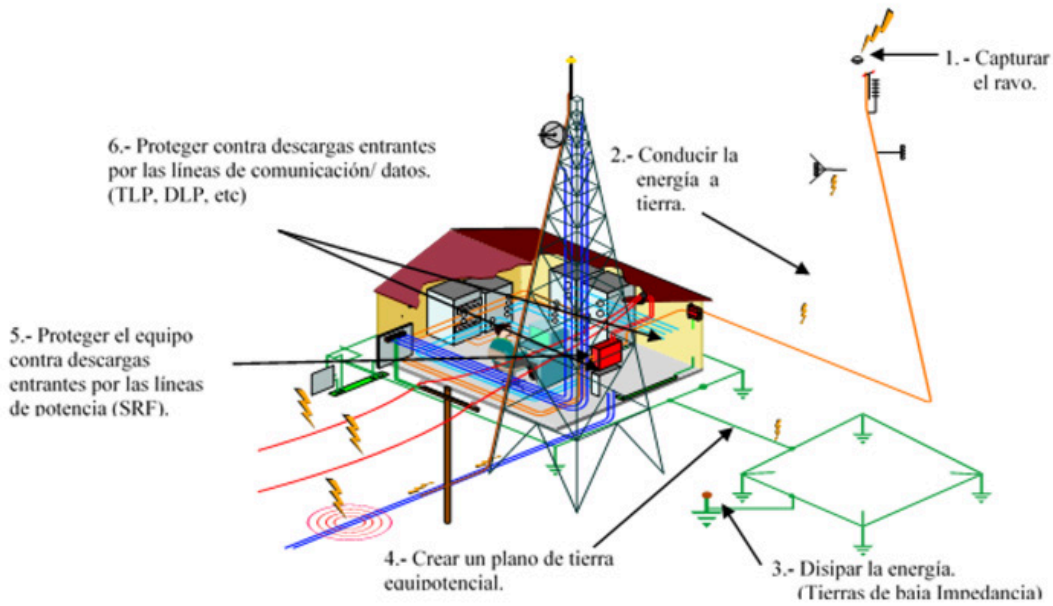

Figura 6.
Erico, "Sistema de protección eléctrica de seis puntos," 2016. [Fotografía]. Disponible en: https://www.erico.com/catalog/literature/E611W-USEN.pdf [Consultado en junio 22, 2020].

Carmen Humberta de Jesús Díaz Novelo
Jaime Olmos de la Cruz
https://doi.org/10.22201/dgtic.26832968e.2021.3.5
Abril 2021 • Número 3 • ISSN 2683-2968
https://www.ties.unam.mx/

implementados, es recomendable no hacer conexiones eléctricas sin un análisis y la documentación de estos diseños. Así, es necesario diseñar adecuadamente la capacidad, el tiempo de soporte y la redundancia, así como dar mantenimiento a los sistemas de protección eléctrica y de climatización, llevando a cabo simulacros periódicamente, para poner a prueba todos los escenarios posibles de fallas de energía básicas. También es imprescindible mantener los sistemas de climatización en condiciones óptimas, mediante un plan de servicios de mantenimiento y diseñar el suministro alterno de aire acondicionado, considerando el suministro de energía eléctrica de emergencia.

Sistema de Gestión de la Continuidad del Negocio

Otro aspecto importante es la implementación de un Sistema de Gestión de la Continuidad del Negocio. Éste permite a las IES asegurar que todos sus procesos críticos estén siempre disponibles, mediante la planificación, la implementación y el mantenimiento permanente del propio sistema de gestión, viéndose reducida la ocurrencia y quedando de manifiesto la recuperación ante los incidentes [13]. En la imagen 7 se pueden observar los elementos para iniciar un Sistema de Gestión de la Continuidad del Negocio.

La continuidad del negocio debe estar basada en el resultado del análisis de impacto y en la evaluación del riesgo. Estos elementos son vitales porque ayudarán a las IES a identificar, mitigar y controlar las fallas potenciales en la infraestructura y las telecomunicaciones, así como en los procesos críticos relacionados con ellos. Esto permitirá estabilizar, continuar, reanudar y recuperar las actividades, así como determinar los recursos necesarios para su implementación, con el fin de establecer las medidas proactivas y reducir la probabilidad de la interrupción [14].

Experiencias de la Universidad Autónoma de Yucatán

Actualmente, en la construcción de nuevos edificios, la Universidad Autónoma de Yucatán considera la aplicación y el cumplimiento de un esquema de protección eléctrica basado en el modelo de seis puntos de protección. Éste ha demostrado su efectividad y hace posible la contabilización de los eventos que se presentan, pero sobre todo contribuye a proteger la infraestructura de telecomunicaciones, además de los sitios y los centros de datos de la UADY. Con la aplicación de este modelo se han visto disminuidos los incidentes por daños debidos a descargas atmosféricas o fallas eléctricas. Este esquema está implementado en tres centros de datos y catorce dependencias universitarias desde hace trece años. Se ha venido renovando con los servicios, materiales y tecnologías que van surgiendo. Los daños ocasionados por una descarga atmosférica podían ascender hasta a un millón de pesos en un solo sitio, considerando tarjetas, equipos de telecomunicaciones y conmutadores dañados, mientras que con la protección eléctrica estos costos son

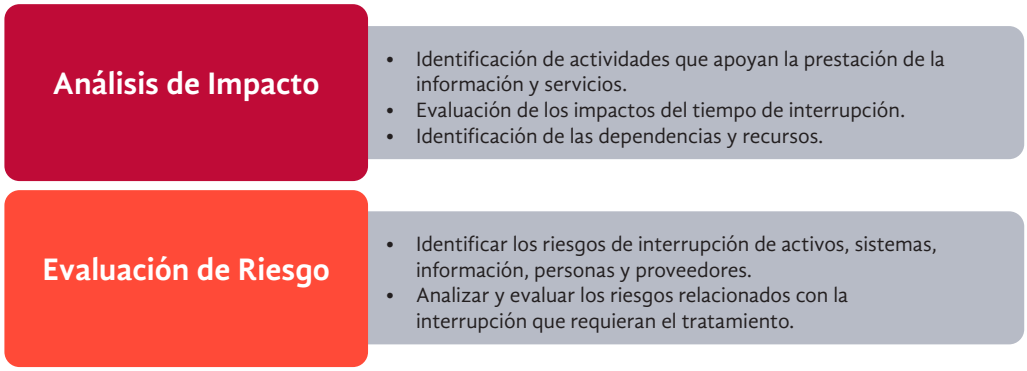

Figura 7.
Elementos requeridos para el Sistema de Gestión de la Continuidad del Negocio. Fuente: elaboración propia.

https://doi.org/10.22201/dgtic.26832968e.2021.3.5
Abril 2021 • Número 3 • ISSN 2683-2968
https://www.ties.unam.mx/

eliminados o insignificantes, pero lo más importante es que la operación de los servicios de TI de una institución no se detienen.

Los antecedentes de esta implementación se detallan a continuación. En 2006 se desarrolló un proyecto para obtener un esquema de protección eléctrica. Este proyecto fue apoyado por primera vez con fondos de financiamiento federales del Programa Integral de Fortalecimiento Institucional (PIFI)[1]. En 2007 alcanzó un 80% la implementación del esquema de protección eléctrica en 14 dependencias universitarias. Posteriormente, año con año se consideró el presupuesto para operar este sistema y proteger los sitios de telecomunicaciones de las dependencias universitarias. A partir de 2008, en los nuevos edificios y construcciones universitarias se considera la inclusión del sistema de protección eléctrica desde el diseño de los nuevos edificios, los sitios de telecomunicaciones y los centros de datos, este es el caso del centro de datos más reciente del Campus de Ciencias Sociales, Económicas y Humanidades, que desde su conceptualización fue planeado para contar con diversos elementos de continuidad en los servicios de TI, siendo uno de ellos el esquema de protección eléctrica.

La implementación de este modelo en la Universidad Autónoma de Yucatán, es parte del plan de continuidad que contempla elementos de seguridad física para la infraestructura [15] y [16], con el propósito de responder ante interrupciones eléctricas, fenómenos meteorológicos como los huracanes y paros por huelgas. Recientemente ha incorporado elementos derivados de la contingencia sanitaria ocasionada por el COVID-19.

Conclusión

Los resultados de las encuestas aplicadas por la ANUIES, así como los casos compartidos por las IES, permiten identificar la necesidad de hacer visible la importancia de gestionar los riesgos asociados a la infraestructura, los centros de datos y las telecomunicaciones. Estos riesgos deben ser considerados tanto dentro de los planes de continuidad, como en la gestión de riesgos de una institución.

También cobra relevancia revisar los planes de recuperación de desastres, ya que es probable que los riesgos y los desastres físicos, ocasionados por los fenómenos meteorológicos, se incrementen en las IES, debido a los cambios climáticos, sus edificaciones, la ubicación y las condiciones geográficas.

Las IES deben establecer canales de comunicación y programas de concientización apropiados para las áreas de TI, actores estratégicos y directivos sobre estos temas, para dar la importancia requerida a la seguridad física y a la gestión de los riesgos asociados a la infraestructura, los centros de datos y las telecomunicaciones. Se debe promover la planeación, la implementación y la puesta en operación de metodologías de gestión de riesgos, planes de la continuidad y la disponibilidad de los servicios de TI y la reducción de costos asociados a incidentes de seguridad física de la infraestructura, centros de datos y telecomunicaciones.

[1] Informe del programa de gestión 2007 (PROGES 2007) de la Universidad Autónoma de Yucatán.

https://doi.org/10.22201/dgtic.26832968e.2021.3.5
Abril 2021 • Número 3 • ISSN 2683-2968
https://www.ties.unam.mx/

BIBLIOGRAFÍA

[1] L. G. Díaz, "Las Tecnologías de Información y Comunicación en las Instituciones de Educación Superior: presente y futuro," *Coordinación General de Tecnologías de Información*, noviembre 30, 2016. [En línea]. Disponible en: https://cgti.udg.mx/publicaciones/2016/tic-ies [Consultado en junio 22, 2020].

[2] J. P. López, "Estado actual de las Tecnologías de la Información y Comunicaciones en las Instituciones de Educación Superior en México Estudio 2018," *Publicaciones ANUIES*, 2018. Disponible en: http://publicaciones.anuies.mx/libros/240/estado-actual-de-las-tecnologias-de-la-informacion-y-comunicaciones [Consultado en junio 22, 2020].

[3] Internet Society, "Consolidation in the Internet Economy," *Internet Society*, 2019. Disponible en: https://future.internetsociety.org/2019/introduction/ [Consultado en junio 22, 2020].

[4] TVN/Noticias, "Daño afecta servicio de cable & wireless en Chilibre," *TVN/Noticias*, agosto 03, 2016. Disponible en: https://www.tvn-2.com/nacionales/Dano-servicio-Cable-Wireless-Chilibre_0_4543795659.html [Consultado en junio 22, 2020].

[5] F. M. León, "La red mundial de localización de rayos en tiempo real: WWLLN," *Meteored* Tiempo.com, julio 21, 2012. [En línea]. Disponible en: https://www.tiempo.com/ram/491/la-red-mundial-de-localizacin-de-rayos-wwlln-world-wide-lightning-location-network/ [Consultado en junio 22, 2020].

[6] UNAM, "Descargas eléctricas de nube a tierra," 2020. [Fotografía]. Disponible en: https://atlasclimatico.unam.mx/atlas/Docs/f_lightning.html [Consultado en junio 22, 2020].

[7] Internet Society, "Consolidation in the internet Economy," *Internet Society*, 2019. Disponible en: https://future.internetsociety.org/2019/introduction/ [Consultado en junio 22, 2020].

[8] Bicsi, "ANSI/BICSI N3-20, Planning and Installation Methods for the Bonding and Grounding of Telecommunication and ICT Systems and Infrastructure," *Bicsi*, 2020. [En línea]. Disponible en: https://www.bicsi.org/standards/available-standards-store/single-purchase/bicsi-n3-20-bonding-and-grounding [Consultado en junio 22, 2020].

[9] B. Martin, "Disaster Recovery Plan Strategies and Processes," *SANS*, febrero, 2002. [En línea]. Disponible en: https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564 [Consultado en junio 22, 2020].

[10] AWS, "Seguridad en la nube de AWS," *Amazon Web Services*, 2020. [En línea]. Disponible en: https://aws.amazon.com/es/security/introduction-to-cloud-security/ [Consultado en junio 22, 2020].

https://doi.org/10.22201/dgtic.26832968e.2021.3.5
Abril 2021 • Número 3 • ISSN 2683-2968
https://www.ties.unam.mx/

[11] M. A. Vasquez y G. L. Martínez, "Seguridad en la nube durante los próximos años," *Revista Seguridad*. Vol. 29, pp. 4-8 [En línea]. Disponible en: https://revista.seguridad.unam.mx/sites/default/files/rev_seguridad_29_0.pdf [Consultado en junio 22, 2020].

[12] Aemsys, "Nuestras marcas," *Aemsys*, 2020. [En línea]. Disponible en: http://www.aemsys.com/nuestras-marcas/ [Consultado en junio 22, 2020].

[13] ISOToolsExcelence, "ISO 22301 Gestión de continuidad de negocio en la práctica," *ISOToolsExcelence*, julio 23, 2017. [En línea]. Disponible en: https://www.isotools.org/2017/07/23/iso-22301-gestion-continuidad-negocio-la-practica/ [Consultado en junio 22, 2020].

[14] Diligent, "Las cinco mejores prácticas para la gobernanza de la seguridad de la información," *Diligent*, 2016. [En línea]. Disponible en: http://diligent.com/wp-content/uploads/2016/10/WP0018_ES_Five-Best-Practices-for-Information-Security-Governance.pdf [Consultado en junio 22, 2020].

[15] UADY, "Políticas institucionales de seguridad en cómputo," *UADY*, mayo 27, 2010. [En línea]. Disponible en: https://www.riuady.uady.mx/riuady/UADY-PSI-01-REV03-PoliticasInstitucionalesdeSeguridadenComputo_Rev09.pdf [Consultado en junio 22, 2020].

[16] UADY, "Plan de contingencias para servicios institucionales de TI," *UADY*, septiembre 01, 2012. [En línea]. Disponible en: https://www.calidad.uady.mx/8/0/1/0/0/L-SG-CGTIC-05%20Plan%20de%20Contingencias%20para%20Servicios%20Institucionales%20de%20TI%20Rev02.pdf [Consultado en febrero 24, 2021].

[17] Revista DataCenter, "¿RTO vs RPO?," *Revista DataCenter*, diciembre 12, 2013. [En línea]. Disponible en: https://revistadatacenter.wordpress.com/2013/12/12/cual-es-la-diferencia-entre-el-rto-y-rpo/ [Consultado en junio 22, 2020].

[18] C. E. Betancourt, "Ciberseguridad en los sistemas de información de las universidades," *Dominio Las Ciencias*, vol. 3, no 3, agosto, 2017.

[19] Secretaria de Comunicaciones y Transportes, "Habilidades de ciberseguridad para telecomunicaciones y radiodifusión," *Secretaria de Comunicaciones y Transportes*, mayo 28, 2019. [En línea]. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/479532/conclusiones_habilidades_en_ciberseguridad_para_telecomunicaciones_y_radiodifusion.pdf [Consultado en junio 22, 2020].

[20] ITU Publications, "Global Cybersecurity Index-GCI," *ITU Publications*, 2018. [En línea]. Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf [Consultado en junio 22, 2020].

[21] Gobierno de México, "Estrategia nacional de ciberseguridad," *gob.mx*, 2017. [En línea]. Disponible en: https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad [Consultado en junio 22, 2020].

[22] OEA, "Hacia una estrategia nacional de ciberseguridad," *sites.oas.org*, agosto 02, 2017. [En línea]. Disponible en: https://www.sites.oas.org/cyber/Documents/Mexico%20-%20Consolidacion%20de%20Consultas%20Documento%20ENCS%20(1).pdf [Consultado en junio 22, 2020].

[23] OAS, "NIST Cybersecurity Framework-CSF," *oas.org*, 2019. [En línea]. Disponible en: https://www.oas.org/en/sms/cicte/docs/OAS-AWS-NIST-Cybersecurity-Framework(CSF)-ENG.pdf [Consultado en junio 22, 2020].

https://doi.org/10.22201/dgtic.26832968e.2021.3.5
Abril 2021 • Número 3 • ISSN 2683-2968
https://www.ties.unam.mx/

[24] ISMS, "El libro blanco del CISO," *ISMS Forum spain,* [En línea]. Disponible en: https://www.ismsforum.es/ficheros/descargas/segunda-edicion-del-libro-blanco-del-ciso-de-isms.pdf [Consultado en junio 22, 2020].

[25] J. C. Guel, Ponente, *Webinar MetaRed: Cyberseguridad aplicada a la Educación Superior*. México: 2019

[26] Diligent, "Las cinco mejores prácticas para la gobernanza de la seguridad de la información," *Diligent*, 2016. [En línea]. Disponible en: http://diligent.com/wp-content/uploads/2016/10/WP0018_ES_Five-Best-Practices-for-Information-Security-Governance.pdf [Consultado en junio 22, 2020].

Cómo se cita:

C. D. Novelo y J. O. De La Cruz, "Importancia de la Seguridad Física en la Infraestructura de Redes, Centros de Datos y Telecomunicaciones de las Instituciones de Educación Superior," *TIES, Revista de Tecnología e Innovación en Educación Superior*, n.o. 3, abril, 2021. [En línea]. Disponible en: https://www.ties.unam.mx/ [Consultado en mes día, año].