

UNIVERSIDAD ABIERTA PARA ADULTOS

UAPA



**DIRECCIÓN ACADÉMICA DE POSGRADO
MAESTRÍA EN CIBERSEGURIDAD**

**PLAN DE CONTINGENCIA Y CONTINUIDAD DE NEGOCIO ANTE UN ATAQUE DE
CIBERSEGURIDAD A LA INFRAESTRUCTURA TECNOLÓGICA DE LA
UNIVERSIDAD ABIERTA PARA ADULTOS (UAPA) OCTUBRE – DICIEMBRE 2022**

**INFORME FINAL DE INVESTIGACIÓN PRESENTADO COMO REQUISITO PARA
OPTAR POR EL TÍTULO DE MAGISTER EN CIBERSEGURIDAD**

POR:

**ING. JOEL MIESES MARINE
LIC. MARINO SALVADOR GÓMEZ REYNOSO**

ASESOR(A):

CARMEN LUISA AYBAR DE NICASIO

**SANTIAGO DE LOS CABALLEROS
REPÚBLICA DOMINICANA
DICIEMBRE 2022**

TABLA DE CONTENIDO

RESUMEN	9
ABSTRACT	¡Error! Marcador no definido.
Agradecimientos	¡Error! Marcador no definido.
Dedicatoria.....	¡Error! Marcador no definido.
Introducción.....	¡Error! Marcador no definido.
CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN	¡Error! Marcador no definido.
1.1 Planteamiento del problema	¡Error! Marcador no definido.
1.2 Objetivos de Investigación.....	¡Error! Marcador no definido.
1.2.1 Objetivo general	¡Error! Marcador no definido.
1.2.2 Objetivos específicos	¡Error! Marcador no definido.
1.3 Justificación	¡Error! Marcador no definido.
1.4 Descripción del contexto	¡Error! Marcador no definido.
1.4.1 Misión.....	¡Error! Marcador no definido.
1.4.2 Visión	¡Error! Marcador no definido.
1.4.3 Valores.....	¡Error! Marcador no definido.
1.4.4 Objetivos.....	¡Error! Marcador no definido.
1.5 Delimitación	¡Error! Marcador no definido.
1.6 Limitaciones	¡Error! Marcador no definido.
CAPÍTULO II: MARCO TEÓRICO.....	¡Error! Marcador no definido.
2.1 Antecedentes de la Investigación	¡Error! Marcador no definido.
2.2 Infraestructura tecnológica	¡Error! Marcador no definido.
2.2.1 Infraestructura en la nube	¡Error! Marcador no definido.
2.2.1.1 Tipos de infraestructuras en la nube.	¡Error! Marcador no definido.
2.2.1.2 Tipos de servicios en la nube.....	¡Error! Marcador no definido.
2.2.2 Modelo OSI	¡Error! Marcador no definido.

2.2.3 Seguridad de la red	¡Error! Marcador no definido.
2.2.3.1 Tipos de redes informáticas.....	¡Error! Marcador no definido.
2.2.3.2 Tipos de ataques a las redes.....	¡Error! Marcador no definido.
2.2.3.3 Protección.....	¡Error! Marcador no definido.
2.2.3.4 Detección.....	¡Error! Marcador no definido.
2.2.3.5 Reacción.....	¡Error! Marcador no definido.
2.2.4 Configuración de sistemas.....	¡Error! Marcador no definido.
2.2.4.1 Niveles de Aplicación.....	¡Error! Marcador no definido.
2.2.3 Cifrado.....	¡Error! Marcador no definido.
2.2.4 Desarrollo Seguro	¡Error! Marcador no definido.
2.2.7 Seguridad en la nube.....	¡Error! Marcador no definido.
2.2.8 Gobierno	¡Error! Marcador no definido.
2.3 Concepto y definición de ciberseguridad.....	¡Error! Marcador no definido.
2.4 Vectores de ataque.....	¡Error! Marcador no definido.
2.4.1 Etapas de un ataque	¡Error! Marcador no definido.
2.5 Ciberespacio	¡Error! Marcador no definido.
2.5.1 Evolución del ciberespacio.....	¡Error! Marcador no definido.
2.5.2 Ciberamenaza	¡Error! Marcador no definido.
2.5.3 Cibercrimen	¡Error! Marcador no definido.
2.5.3.1 Actores en el cibercrimen.....	¡Error! Marcador no definido.
2.6 El riesgo en ciberseguridad.....	¡Error! Marcador no definido.
2.6.1 Amenaza	¡Error! Marcador no definido.
2.6.2 Activo	¡Error! Marcador no definido.
2.6.3 Vulnerabilidad	¡Error! Marcador no definido.
2.6.4 Impacto	¡Error! Marcador no definido.
CAPÍTULO III: MARCO METODOLÓGICO	¡Error! Marcador no definido.
3.1 Tipo de investigación	¡Error! Marcador no definido.

3.2 Métodos de investigación	¡Error! Marcador no definido.
3.3 Técnicas e instrumentos	¡Error! Marcador no definido.
3.4 Población y muestra	¡Error! Marcador no definido.
CAPÍTULO IV: DESCRIPCION DE LA PROPUESTA;¡Error! Marcador no definido.	
4.1 Plan de Contingencia y Recuperación de Desastres .	¡Error! Marcador no definido.
4.2 Contextualización del proyecto	¡Error! Marcador no definido.
4.2 Objetivos de la propuesta	¡Error! Marcador no definido.
4.2.1 Objetivo General.....	¡Error! Marcador no definido.
4.2.2 Objetivos Específicos	¡Error! Marcador no definido.
4.3 Carácter innovador del modelo.....	¡Error! Marcador no definido.
4.4 Alcance de la propuesta.....	¡Error! Marcador no definido.
4.5 Propuesta del Plan de Recuperación.....	¡Error! Marcador no definido.
4.5.1 Firmas y Revisiones	¡Error! Marcador no definido.
4.5.2 Actividades de preparación	¡Error! Marcador no definido.
4.6 Servicios críticos de la institución	¡Error! Marcador no definido.
4.7 Integración del Equipo de Respuesta.....	¡Error! Marcador no definido.
4.7.1 Organigrama Equipo de Recuperación.....	¡Error! Marcador no definido.
4.7.2 Diagrama de activación	¡Error! Marcador no definido.
4.7.3 Funciones de los Equipos de Recuperación	¡Error! Marcador no definido.
4.7.4 Funciones del Vocero	¡Error! Marcador no definido.
4.7.5 Funciones del líder del Equipo Coordinador.....	¡Error! Marcador no definido.
4.7.6 Responsabilidades del Equipo Coordinador.....	¡Error! Marcador no definido.
4.7.7 Resumen de actividades	¡Error! Marcador no definido.
4.7.7.1 Actividades de Respuesta y Recuperación.	¡Error! Marcador no definido.
4.7.8 Integrantes de los Equipos de Recuperación	¡Error! Marcador no definido.
4.7.9 Análisis de los servicios críticos.....	¡Error! Marcador no definido.
4.7.10 Estrategia de Recuperación de Desastres	¡Error! Marcador no definido.

- 4.7.11 Análisis de Aseguramiento de la Información **¡Error! Marcador no definido.**
- 4.8 Estrategia general **¡Error! Marcador no definido.**
- 4.8.1 Estrategia para la recuperación..... **¡Error! Marcador no definido.**
- 4.8.2 Niveles de contingencia..... **¡Error! Marcador no definido.**
- 4.8.3 Estrategias de acción **¡Error! Marcador no definido.**
- 4.9 Centro de Control de Crisis (CCC) **¡Error! Marcador no definido.**
- 4.10 Topología de red sugerida **¡Error! Marcador no definido.**
- 4.11 Código de notificación para la activación **¡Error! Marcador no definido.**
- 4.12 Actividades antes de la recuperación..... **¡Error! Marcador no definido.**
- 4.13 Actividades previas del Equipo Coordinador **¡Error! Marcador no definido.**
- 4.14 Actividades previas de los Equipos de Recuperación;**¡Error! Marcador no definido.**
- 4.15 Actividades previas del Equipo de Redes y Comunicaciones;**¡Error! Marcador no definido.**
- 4.16 Actividades previas del Equipo de Tecnología de la Información **¡Error! Marcador no definido.**
- 4.17 Actividades previas del Equipo de Ciberseguridad **¡Error! Marcador no definido.**
- 4.18 Activación del Plan de Contingencia y Recuperación;**¡Error! Marcador no definido.**
- 4.18.1 Identificación del evento y su notificación..... **¡Error! Marcador no definido.**
- 4.19 Análisis y evaluación de daños..... **¡Error! Marcador no definido.**
- 4.20 Procedimientos de respuesta..... **¡Error! Marcador no definido.**
- 4.20.1 Tareas del Equipo Coordinador **¡Error! Marcador no definido.**
- 4.20.2 Tareas de los Equipos de Recuperación **¡Error! Marcador no definido.**
- 4.20.3 Tareas del Equipo de Tecnología de la Información;**¡Error! Marcador no definido.**
- 4.20.4 Tareas del Soporte Técnico **¡Error! Marcador no definido.**
- 4.20.5 Tarea del Equipo de Redes y Comunicaciones ... **¡Error! Marcador no definido.**

4.20.6 Tareas del Equipo de Ciberseguridad	¡Error! Marcador no definido.
4.20.7 Taras del Equipo de Desarrollo	¡Error! Marcador no definido.
4.20.8 Tareas del Equipo de Negocio	¡Error! Marcador no definido.
4.21 Procedimientos para declarar el Desastre	¡Error! Marcador no definido.
4.22 Fin de la contingencia.....	¡Error! Marcador no definido.
4.23 Políticas de seguridad	¡Error! Marcador no definido.
4.23.1 Políticas de contraseñas	¡Error! Marcador no definido.
4.23.1.1 Objetivo.	¡Error! Marcador no definido.
4.23.1.2 Alcance.	¡Error! Marcador no definido.
4.23.1.3 Políticas de contraseña.....	¡Error! Marcador no definido.
4.23.2 Políticas de control de acceso remoto.....	¡Error! Marcador no definido.
4.23.2.1 Objetivo.	¡Error! Marcador no definido.
4.23.2.2 Alcance.	¡Error! Marcador no definido.
4.23.2.3 Políticas de control de acceso remoto.....	¡Error! Marcador no definido.
4.23.3 Políticas de cuentas de usuarios.....	¡Error! Marcador no definido.
4.23.3.1 Objetivo.	¡Error! Marcador no definido.
4.23.3.2 Alcance.	¡Error! Marcador no definido.
4.23.3.3 Políticas de cuentas de usuario.	¡Error! Marcador no definido.
4.23.4 Políticas de respaldos	¡Error! Marcador no definido.
4.23.4.1 Objetivo.	¡Error! Marcador no definido.
4.23.4.2 Alcance.	¡Error! Marcador no definido.
4.23.4.3 Políticas de respaldos.....	¡Error! Marcador no definido.
4.23.5 Políticas de seguridad física	¡Error! Marcador no definido.
4.23.5.1 Objetivo.	¡Error! Marcador no definido.
4.23.5.2 Alcance.	¡Error! Marcador no definido.
4.23.5.3 Políticas de seguridad física.	¡Error! Marcador no definido.
4.23.6 Políticas de uso de internet	¡Error! Marcador no definido.

4.23.6.1	Objetivo.	¡Error! Marcador no definido.
4.23.6.2	Alcance.	¡Error! Marcador no definido.
4.23.6.3	Políticas de uso de internet.	¡Error! Marcador no definido.
4.23.7	Políticas de uso de computadores, impresoras y periféricos	¡Error! Marcador no definido.
4.23.7.1	Objetivo.	¡Error! Marcador no definido.
4.23.7.2	Alcance.	¡Error! Marcador no definido.
4.23.7.3	Políticas de uso de computadores, impresoras y periféricos.	¡Error! Marcador no definido.
4.23.8	Políticas de seguridad de los servidores	¡Error! Marcador no definido.
4.23.8.1	Objetivo.	¡Error! Marcador no definido.
4.23.8.2	Alcance.	¡Error! Marcador no definido.
4.23.8.3	Políticas de seguridad de los servidores.	¡Error! Marcador no definido.
4.23.9	Políticas de instalación de software	¡Error! Marcador no definido.
4.23.9.1	Objetivo.	¡Error! Marcador no definido.
4.23.9.2	Alcance.	¡Error! Marcador no definido.
4.23.9.3	Políticas de instalación de software.	¡Error! Marcador no definido.
4.2.10	Políticas de seguridad de base datos	¡Error! Marcador no definido.
4.23.10.1	Objetivo.	¡Error! Marcador no definido.
4.23.10.2	Alcance.	¡Error! Marcador no definido.
4.23.10.3	Políticas de seguridad de base datos.	¡Error! Marcador no definido.
4.23.11	Políticas de seguridad de routers WIFI	¡Error! Marcador no definido.
4.23.11.1	Objetivo.	¡Error! Marcador no definido.
4.23.11.2	Alcance.	¡Error! Marcador no definido.
4.23.11.3	Políticas de seguridad de routers wifi.	¡Error! Marcador no definido.
4.23.12	Políticas de segmentación de red	¡Error! Marcador no definido.
4.23.12.1	Objetivo.	¡Error! Marcador no definido.

4.23.12.2 Alcance.....	;	Error! Marcador no definido.
4.23.12.3 Políticas de seguridad de segmentación de red.....	;	Error! Marcador no definido.
4.23.13 Políticas de correo electrónico.....	;	Error! Marcador no definido.
4.23.13.1 Objetivo.....	;	Error! Marcador no definido.
4.23.13.2 Alcance.....	;	Error! Marcador no definido.
4.23.13.3 Política de Correo Electrónico.....	;	Error! Marcador no definido.
4.23.14 Políticas de registro y auditoria de eventos	;	Error! Marcador no definido.
4.23.14.1 Objetivo.....	;	Error! Marcador no definido.
4.23.14.2 Alcance.....	;	Error! Marcador no definido.
4.23.14.3 Políticas de registro y auditoria de eventos ...	;	Error! Marcador no definido.
4.23.15 Políticas de traer tu propio dispositivo (BYOD).....	;	Error! Marcador no definido.
4.23.15.1 Objetivo.....	;	Error! Marcador no definido.
4.23.15.2 Alcance.....	;	Error! Marcador no definido.
4.23.15.3 Política de traer tu propio dispositivo (BYOD).....	;	Error! Marcador no definido.
CAPITULO V: VALIDACIÓN DE LA PROPUESTA. ;Error! Marcador no definido.		
5.1 Validación de la propuesta	;	Error! Marcador no definido.
CONCLUSIONES.....		10
RECOMENDACIONES	;	Error! Marcador no definido.
BIBLIOGRAFÍA	;	Error! Marcador no definido.
APÉNDICE Y ANEXO	;	Error! Marcador no definido.

RESUMEN

El objetivo principal de la presente investigación es crear un Plan de Contingencia y Recuperación de Negocios para la Universidad Abierta Para Adultos, que le permita a la universidad contar con un Manual de Procedimientos ante ataques de ciberseguridad, que se adapte a todos los servicios críticos de la infraestructura tecnológica. La investigación se divide en cinco capítulos. El primero, contiene los aspectos introductorios, la problemática, los objetivos de investigación y otros aspectos que la justifican. El segundo, es el Marco Teórico que sustenta la investigación y ayuda al lector a entender los temas relevantes de la importancia de un Plan de Recuperación, basado en estándares y normas internacionales. En el tercer capítulo, se establece la metodología de investigación que permite a los autores lograr el cumplimiento de los objetivos mediante el uso de técnicas e instrumentos. En el cuarto, se desarrolla el Plan de Contingencia y Continuidad de Negocio, desarrollando la estructura basada en una matriz de riesgo de los servicios críticos de UAPA, en la cual fueron evidenciadas las vulnerabilidades de la plataforma universitaria y falta de controles de seguridad. Finalmente, y el quinto capítulo, se valida la propuesta a través de un cuestionario que permite al personal de TI validar que el Plan de Recuperación cumple con las necesidades de la universidad.

En conclusión, el Plan de Contingencia y Continuidad de Negocio para la Universidad Abierta Para Adultos (UAPA) representa un activo sumamente valioso, porque mitiga los riesgos de las amenazas que puedan afectar la infraestructura tecnológica que representa un punto neurálgico en sus operaciones.

Palabras claves: Plan de Contingencia y Continuidad de Negocios, Plan de Recuperación, Centro Control de Crisis, Ransomware, Recuperación de Desastres, Equipo de Respuesta, Tiempo Objetivo de Recuperación (RTO), Manuales de Procedimientos.

CONCLUSIONES

Las debilidades evidenciadas en el análisis de vulnerabilidades a la infraestructura tecnológica de UAPA, representan un riesgo que puede ocasionar la pérdida total o parcial de la información, pues, la falta de controles de seguridad interna y externa representan una amenaza a la seguridad.

Por otro lado, el departamento de tecnología carece de las herramientas que le permitan desarrollar su trabajo de forma óptima, pues no cuentan con un SIEM para el monitoreo de seguridad en los endpoints, ciertos sistemas se encuentran obsoletos y necesitan ser reemplazos por otros, que se adapten a las necesidades de la universidad y a los estándares de calidad en la gestión de la información. Es importante destacar, que entre las debilidades de la infraestructura está la necesidad de un software para el monitoreo de la infraestructura, lo que no les permite a los administradores de los servidores, monitorearlos para garantizar su seguridad, además, se ha evidenciado que la universidad no es tolerante a fallas, la seguridad se encuentra comprometida en la red interna, carece de controles eficientes de seguridad, no existe segmentación de la red, los equipos no cuentan con controles de seguridad, los respaldos no son verificados, no se cumple el proceso de inhabilitación de usuarios en la red, no existe un sistema de gestión de contraseñas, no hay filtrado de tráfico de la red y tampoco los correos electrónicos, el personal no es capacitado y orientado en temas de seguridad.

En conclusión, el Plan de Contingencia y Continuidad de Negocios no sólo es necesario, sino resulta urgente su implementación y que sean tomada en cuenta las recomendaciones de mejoras para evitar que la Universidad sufra un incidente, que afecte de forma grave su información e imagen ante la crítica que se pueda realizar si esta sufre un incidente por la falta de controles, debido a que, su fuerte en el sistema educativo se basa en la tecnología, por lo que, no se deben estimar esfuerzo para la compra de equipos y aplicativos que sean necesarios para lograr certificar el departamento en los diferentes estándares de seguridad y gestión de la calidad.

BIBLIOGRAFÍAS

Álvarez Velásquez, E.A. (2012) Seguridad en la nube, Revista de Información, Tecnología y Sociedad. Available at: http://www.revistasbolivianas.ciencia.bo/scielo.php?lng=pt&pid=S1997-40442012000200004&script=sci_arttext (Accessed: November 23, 2022).

Arámbula Trejo, J., 2021. Seguridad en redes de computadoras - Monografias.com. [online] Monografias.com. Available at: <https://www.monografias.com/trabajos30/seguridad-redes/seguridad-redes.shtml> [Accessed 8 Nov 2022].

Bustamante Sánchez, R. (2005) Tesis Seguridad en Redes, Universidad Autónoma del Estado de Hidalgo. Available at: <https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf> (Accessed: March 4, 2023).

Caamaño Fernández, E.E., y Gil Herrera, R.J. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional, NOVUM, 1(10), 61 - 80.

Cando-Segovia, M. and Chicaiza, R., 2021. Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. [online] Ojs.3ciencias.com. Available at: <http://ojs.3ciencias.com/index.php/3c-tic/article/view/1134> [Accessed 30 Oct 2022].

CISCO, 2022. ¿Qué es la ciberseguridad? [online] cisco.com. Available at: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html [Accessed 03 Nov 2022].

DeWitt, D. (2021) Cifrado de datos: ¿en qué consiste? Avast. Available at: <https://www.avast.com/es-es/c-encryption> (Accessed: 14 Nov 2022).

Díaz, K. (2022) El aumento de ciberdelitos lleva a las empresas a fortalecer su seguridad tecnológica, Forbes Dominicana. Available at: <https://forbes.do/tecnologia/2022-10->

12/el-aumento-de-ciberdelitos-lleva-a-las-empresas-a-fortalecer-su-seguridad-tecnologica (Accessed: 22 Nov 2022).

Digital Guide, I., 2019. Conoce los tipos de redes más importantes. [online] IONOS Digitalguide. Available at: <<https://www.ionos.es/digitalguide/servidores/know-how/los-tipos-de-redes-mas-conocidos/>> [Accessed 12 Nov 2022].

Gestión de Riesgos. Una Guía de Aproximación para el empresario (2015) INCIBE. Available at: <https://www.incibe.es/protege-tu-empresa/guias/gestion-riesgos-guia-empresario> (Accessed: October 27, 2022).

Gunter, R. E. (1998) Universidad Privada dr. Rafael Belloso Chacín, Universidad Rafael Belloso Chacín. Available at: <https://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/Redes%20de%20Area%20Local%20y%20Metropolitana-cd2/Contenido/RedesdeDatos.pdf> (Accessed: March 3, 2023).

IBM (no date) ¿Qué es infraestructura de ti?, IBM. Available at: <https://www.ibm.com/es-es/topics/infrastructure> (Accessed: November 6, 2022).

INCIBE (2015) Plan de Contingencia y Continuidad de Negocio, Instituto Nacional de Ciberseguridad. Available at: <https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio> (Accessed: October 26, 2022).

Izaguirre Olmedo, J. and León Gavilánez, F., 2018. Vista de Análisis de los ciberataques realizados en América Latina. [online] Revistas.uide.edu.ec. Available at: <<https://revistas.uide.edu.ec/index.php/innova/article/view/837/779>> [Accessed 29 Oct 2022].

KIT de concienciación para empresas (2015) INCIBE. Available at: <https://www.incibe.es/prote-ge-tu-empresa/kit-concienciacion> (Accessed: October 27, 2022).

Levy, P. (2007) Educación, cibercultura e Inteligencia Colectiva, Gazeta de Antropología. Universidad Complutense de Madrid Madrid, España. Available at: <http://www.gazeta-antropologia.es/?p=4403> (Accessed: December 6, 2022).

Marcillo Castro, J., Ortiz Hernández, M. and Mero Lino, E., 2020. Vista de ANÁLISIS DE LAS HERRAMIENTAS Y TÉCNICAS UTILIZADAS EN PRUEBA DE PENETRACIÓN PARA LA DETECCIÓN DE VULNERABILIDADES EN APLICACIONES WEB. [online] 186.101.39.22. Available at: <http://186.101.39.22/index.php/unesumciencias/article/view/316/298> [Accessed 29 Oct 2022].

Meléndez Torres, F., 2020. [online] Prepository.org. Available at: http://prepository.org/xmlui/bitstream/handle/20.500.12475/1065/Articulo%20Final_%20Ferdinand%20Mel%c3%a9ndez.pdf?sequence=1&isAllowed=y [Accessed 30 Oct 2022].

Méndez Olivares, H., 2003. Seguridad de la información. [online] <http://www.ordenjuridico.gob.mx>. Available at: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUK EwjRpNaB84PyAhXylmoFHZA9BSOQFjABegQIAxAD&url=http%3A%2F%2Fwww.ordenjuridico.gob.mx%2FCongreso%2Fpdf%2F114.pdf&usg=AOvVaw17dykPtogi5Bi j9JAXs118> [Accessed 7 Nov 2022].

Morelos, L., 2021. Universidad Rafael Beloso Chacín. [online] www.urbe.edu. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUK Ewii0orZ_YPyAhXMI2oFHbP5AyoQFjABegQIDxAD&url=https%3A%2F%2Fwww.urbe.edu%2Finfo-consultas%2Fweb-profesor%2F12697883%2Farchivos%2FRedes%2520de%2520Area%2520Local%2520y%2520Metropolitana-cd%2FContenido%2FRedesdeDatos.pdf&usg=AOvVaw066aPye1lxkJ3UiIYaJsq6 [Accessed 09 Nov 2022].

Networks, E., 2019. ¿Qué es una red LAN? – ENI Networks. [online] Eninetworks.com. Available at: <<https://www.eninetworks.com/blog-que-es-una-red-lan/>> [Accessed 9 Nov 2022].

Pagnotta, S. (2015) ¡Nueva infografía! Develando la esencia del cifrado de datos, Universidad Veracruzana. Available at: https://www.uv.mx/infosegura/general/noti_cifrado-4/ (Accessed: 14 Nov 2022).

Plan de contingencia y continuidad de negocio - INCIBE (no date). Available at: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf (Accessed: October 26, 2022).

Plantilla ejemplo para el inventario básico de activos para BIA - incibe (no date). Available at: <https://www.incibe.es/sites/default/files/contenidos/dosieres/plan-contingencia-continuidad-ne-gocio/plantilla-ejemplo-bia.xls> (Accessed: October 26, 2022).

Plantilla ejemplo para un plan de recuperación de entornos (2015) INCIBE. Available at: <https://www.incibe.es/sites/default/files/contenidos/dosieres/plan-contingencia-continuidad-nego-cio/contingencia-y-continuidad-de-negocio-plan-de-recuperacion.pdf> (Accessed: October 27, 2022).

Puime Maroto, J., 2019. [online] Dialnet.unirioja.es. Available at: <<https://dialnet.unirioja.es/descarga/articulo/4549946.pdf>> [Accessed 1 Nov 2022].

Red Hat (2019) ¿Qué es la infraestructura de ti?, Red Hat - We make open source technologies for the enterprise. Red Hat. Available at: <https://www.redhat.com/es/topics/cloud-computing/what-is-it-infrastructure> (Accessed: November 6, 2022).

RedFibra. 2020. Tipos de redes informáticas. ¿Qué es una red? LAN, WAN, MAN, WLAN, WMAN, WWMAN, SAN, PAN - RedFibra. [online] Available at: <<https://redfibra.mx/tipos-de-redes-informaticas-que-es-una-red-lan-wan-man-wlan-wman-wwman-san-pan/>> [Accessed 9 Nov 2022].

Safety Culture (2022) Análisis de Riesgos: Ejemplo y métodos, SafetyCulture. Available at: <https://safetyculture.com/es/temas/analisis-de-riesgos/> (Accessed: 22 Nov 2022).

Sánchez Vera, F. (no date) Educación, cibercultura e inteligencia colectiva, Gazeta de Antropología. Universidad de Murcia. Available at: <http://www.gazeta-antropologia.es/?p=4403> (Accessed: 16 Nov 2022).

Talero, M., 2022. AUDITORÍA INTERNA - USTA - Los Ataques Informáticos en el Sector Educativo. [online] Auditoriainterna.usta.edu.co. Available at: <https://auditoriainterna.usta.edu.co/index.php/120-los-ataques-de-hacking-en-el-sector-educativo> [Accessed 1 Nov 2022].

Techopedia, 2011. What is a Global Area Network (GAN)? - Definition from Techopedia. [online] Techopedia.com. Available at: <https://www.techopedia.com/definition/7368/global-area-network-gan> [Accessed 12 Nov 2022].

ULL, 2022. Las Universidades exponen sus casos de ciberataques. [online] ULL - Noticias. Available at: <https://www.ull.es/portal/noticias/2022/universidades-exponen-casos-de-ciber-ataques/> [Accessed 1 Nov 2022].

Vaca, C., 2016. Vista de CIBERSEGURIDAD Y GESTIÓN DEL RIESGO TECNOLÓGICO EN EL MARCO DE LA NIIF. [online] Revista.uisrael.edu.ec. Available at: <https://revista.uisrael.edu.ec/index.php/rcui/article/view/9/11> [Accessed 1 Nov 2022].

Valencia, U., n.d. ¿Qué es la seguridad informática y cómo puede ayudarme? | VIU. [online] Universidadviu.com. Available at: <https://www.universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme> [Accessed 8 Nov 2022].

VMWare (no date) What is cloud computing infrastructure?: VMware glossary, VMware. Available at: <https://www.vmware.com/latam/topics/glossary/content/cloud-computing-infrastructure.html> (Accessed: November 7, 2022).

Yarlequé Gutiérrez, A. (2019) Diseño de un plan de Recuperación de Desastres de Ti (DRP ti) para el centro de cómputo de la sede principal de una entidad educativa superior del sector Privado Basado en la Norma Nist SP 800-34, repositorioacademico.upc.edu.pe. Universidad Peruana de Ciencias Aplicadas (UPC). Available at: <https://repositorioacademico.upc.edu.pe/handle/10757/625709> (Accessed: 22 Nov 2022).

INSTRUCCIONES PARA LA CONSULTA DEL TEXTO COMPLETO:

Para consultar a texto completo esta tesis [solicite en este formulario \(https://forms.gle/vx5iLzv1pAMyN3d59 como hipervínculo\)](https://forms.gle/vx5iLzv1pAMyN3d59) o dirigirse a la Sala Digital del Departamento de Biblioteca de la Universidad Abierta para Adultos, UAPA.

Dirección

Biblioteca de la Sede – Santiago

Av. Hispanoamericana #100, Thomén, Santiago, República Dominicana
809-724-0266, ext. 276; biblioteca@uapa.edu.do

Biblioteca del Recinto Santo Domingo Oriental

Calle 5-W Esq. 2W, Urbanización Lucerna, Santo Domingo Este, República Dominicana.
Tel.: 809-483-0100, ext. 245. biblioteca@uapa.edu.do

Biblioteca del Recinto Cibao Oriental, Nagua

Calle 1ra, Urb Alfonso Alonso, Nagua, República Dominicana.
809-584-7021, ext. 230. biblioteca@uapa.edu.do