nubosperta

aws partner network

Advanced Consulting Partner

Guía para un
Plan de Recuperación de Desastres efectivo

nubosperta

Todas las empresas están expuestas, para algunas industrias el daño puede ser menos crítico que para otras, sin embargo es de suma relevancia estar preparados.

Guía para un Plan de Recuperación de Desastres efectivo

Hoy con la transformación digital, las empresas han migrado de sistemas analógicos a digitales y en su mayoría, gran parte de su operación diaria depende de sistemas de cómputo conectados a la web: una laptop, un smartphone, el servicio de mail, los servicios de mensajería, CRMs y más.

Con este cambio, llegó uno más profundo: la vulnerabilidad de los sistemas; es un hecho que no estamos completamente seguros en la web, existen muchos tipos de delitos y riesgos a los que estamos expuestos y muchas veces, simplemente, los desconocemos.

Estos riesgos latentes deben ser mitigados de alguna manera, muchas empresas cuentan con un equipo especializado para mantenerse atentos a posibles ataques, otras más piensan que el peor desastre al que se pueden enfrentar son a los desastres naturales, y algunas apenas cuentan con un sistema de antivirus, que no es tan efectivo o poderoso.

En el siguiente whitepaper te daremos a conocer la importancia de la seguridad en tus sistemas, para mantener la integridad de tu información, la continuidad de tu negocio a través de un Plan de Recuperación de Desastres.

¿Por qué es importante un Plan de Recuperación de Desastres?

Como lo mencionamos, mantenerse protegido ante incidentes que puedan generar algún tipo de pérdida o interrumpir la operación de tu negocio, es de suma importancia. Cuando los sistemas de información y cómputo interrumpen tu servicio o exponen de alguna manera a tus clientes, corres el riesgo de perder su confianza y tener una baja significativa en los ingresos.

Un Plan de Recuperación de Desastres (DRP por sus siglas en inglés), considera todos los riesgos a los que tu negocio puede estar expuesto, y cuida la reputación de la empresa. Se basa en una serie de análisis que determinan la cantidad y nivel de riesgos a los estás expuesto, planea cómo combatir o mitigar dicho riesgo, y cuenta con protocolos de actuación ante un incidente no deseado.

Nadie desea que al hacer uso de un servicio éste no funcione correctamente o que su información sea robada; un DRP previene que esto suceda, y más importante, tiene una respuesta si algo grave sucede.

78%
de los ejecutivos consultados coinciden en que las bajas tasas de incidentes no se correlacionan con la reducción del riesgo.

De acuerdo con la última Encuesta Global de Gestión de Riesgo Operativo de DuPont[1], el 78% de los ejecutivos consultados coinciden en que las bajas tasas de incidentes no se correlacionan con la reducción del riesgo; dos terceras partes de ellos, sin embargo, reconocen sentirse seguros al ver datos que indican que las tasas de incidentes son bajas o que tienden hacia el cero, lo cual ocasiona una baja en la prevención de incidentes, tanto externos como internos.

Esto puede conducir a alcanzar niveles críticos de inseguridad y de interrupción de la operación, como fue el caso del ataque del ransomware WannaCry del 2017, que obligó a Renault y a Nissan a detener algunos de sus establecimientos en Europa; o el caso de Ford Motor Co. que enfrentó un gran incendio en 2018 y se vio obligada a paralizar sus operaciones, con afectaciones a 4 mil empleados[2].

Un Plan de Recuperación de Desastres permite estar atento a diversas amenazas que pueden poner el riesgo la operación, calcular su costo en caso de pérdida y recuperarse rápidamente del incidente. Todas las empresas están expuestas, para algunas industrias el daño puede ser menos crítico que para otras, sin embargo es de suma relevancia estar preparados.

Amenazas y riesgos

Las amenazas y riesgos a las cuales las empresas están constantemente expuestas se dividen en tres grupos primordiales, cada una con sus variables. Cabe resaltar que dependiendo del giro de la empresa de la se hable, estos riesgos tendrán más o menos probabilidad de ocurrir, sin embargo debemos estar atentos todo el tiempo y tomar precauciones.

Desastres naturales

Cuando las empresas hablan sobre cuáles son los riesgos a los que están expuestos, en general su primera preocupación son aquellos que fácilmente pueden salirse de sus manos: los desastres naturales, y tienen razón al tomarlo en cuenta: sismos, huracanes, tormentas, incendios, entre otros, pueden tener un alto impacto en la organización, sin embargo son los que menos probabilidad tienen de ocurrir.

En el 2017, México vivió dos sismos de alto impacto durante el mes de septiembre, ambos causaron severas afectaciones a la infraestructura de Chiapas, Ciudad de México, Guerrero, Morelos, Oaxaca, Puebla y Tlaxcala, así como el lamentable deceso de 331 personas; a su vez, se afectaron 376 mil 588 establecimientos, cerca del 40% de las unidades económicas de dichos estados suspendieron al menos un día sus operaciones[3].

La afectación económica fue altísima y hasta hoy en día la reconstrucción no ha concluido; no había manera de evitar este desastre, sin embargo, aún cuando México es zona sísmica, la magnitud de estos sismos no se había visto desde 1985.

[1] "¿Complaciente o cómplice? - Encuesta global de gestión de riesgo operativo", DuPont en: https://latam.consultdss.com/complaciente-o-complice/
[2] Ibid
[3] Estadísticas sobre las afectaciones de los sismos de septiembre de 2017 en las actividades económicas, INEGI, 2017 en: http://www.diputados.gob.mx/sedia/biblio/usieg/comunicados/econom

Ataques cibernéticos:
virus, ransomware y otros

En el 2017 el ransomware WannaCry atacó: en mayo de ese año secuestró 230 mil computadoras en al menos 150 países; estos ransomware solicitan un monto económico para liberar los sistemas, y aprovechan para robar información sensible de los usuarios.

Al año siguiente, 2018, el ransomware SamSam infectó a distintos sistemas en el mundo, se le califica como un ransomware dirigido que elige a sus víctimas de forma específica, vigila y luego ataca, a diferencia de WannaCry cuyo ataque es masivo y sin distinción.

Los ataques cibernéticos han disminuido en 20%, pero sus pérdidas financieras incrementaron un 60%

Los ataques cibernéticos han disminuido en los últimos años, sin embargo sus afectaciones han incrementado, de acuerdo con el reporte de la Online Trust Alliance de la Internet Society (OTA), los ciberataques en 2018 disminuyeron un 20%, sin embargo sus pérdidas financieras incrementaron en un 60%. Sólo en Estados Unidos, se calcula que la pérdida por ciberataques fue de $45 mil millones de dólares en 2018[4].

Error humano: corrupción de datos

Si bien ya recalcamos que la tecnología puede fallar en cualquier momento por múltiples razones ajenas al negocio, también es importante poner atención a las personas en la organización.

De acuerdo con Boston Consulting Group[5] la cultura en seguridad digital aún no permea lo suficiente, alrededor del 70% de los ataques cibernéticos exitosos son debido al descuido de las personas: una USB corrompida que es ingresada a una computadora que está conectada a una intranet, visitas a sitios peligrosos sin precauciones o conexiones en ubicaciones fuera de redes seguras.

Sumado a lo anterior, una deficiencia en la configuración de los sistemas puede ser una oportunidad para los atacantes que están a la espera de una ventana abierta para infectar.

[4] 2018 Cyber Incident & Breach Trends Report, OTA, 2018 en: https://www.internetsociety.org/resources/ota/2019/2018-cyber-incident-breach-tre

[5] A Smarter Way to Quantify Cybersecurity Risk, BCG, 2019 en: https://www.bcg.com/capabilities/technology-digital/smarter-way-to-quantify-cybersecurit

Industrias más vulnerables

Un Plan de Recuperación de Desastres debe tomar en cuenta distintas variables -además de los múltiples riesgos existentes-, cada sector, industria y empresa tiene diferentes requerimientos en su operación y por lo tanto en su tecnología y seguridad.

A continuación citaremos aquellas consideradas más vulnerables por su nivel de sensibilidad en datos, la complejidad en su operación y su importancia en la vida cotidiana actual, sin embargo debemos tomar en cuenta que otros sectores no están exentos de correr riesgos y tener graves impactos si no cuentan con un DRP.

La industria de servicios financieros es la más atacada por hackers con el **19%** de los incidentes

Industria financiera

Los servicios financieros migraron a la digitalidad para simplificar su operación, tener registro fiel de sus transacciones y sobre todo, hacer más fácil la vida de sus usuarios. En esta transformación, la seguridad cibernética con la que deben contar es la columna vertebral de su éxito.

Las instituciones financieras cuentan con datos altamente sensibles de sus clientes: información de cuentas bancarias, transacciones millonarias, acceso a sus estados financieros y más. Por ello se convierten en un blanco perfecto para los perpetradores y no se pueden dar el lujo de no asegurarse.

De acuerdo con el reporte X-Force Threat Intelligence Index 2019 de IBM[6], la industria financiera es la más atacada con el 19% de los incidentes sólo en 2018. Esto sucede debido a que la información de los clientes de bancos o los datos de tarjetas bancarias, por ejemplo, pueden ser monetizados rápidamente por los cibercriminales.

[6] X-Force Threat Intelligence Index, IBM, 2019 en: https://securityintelligence.com/challenges-and-opportunities-to-close-the-cybersecurity-gap-in-the-financial-services-industry/

Servicios de transporte

IBM señala en su informe que la segunda industria que registra más ataques es la de transporte: aviones, trenes y autobuses, con un 13% de los incidentes ocurridos en 2018. Esto se debe a que los sistemas de transporte son parte de la infraestructura crítica de las ciudades, es altamente atractivo para los atacantes ya que cuentan con información de propiedad intelectual para el desarrollo de tecnologías.

Por ejemplo, en el caso de las aerolíneas, los cibercriminales buscan acceso a los sistemas satelitales de rastreo, a la información de los viajeros y a las nuevas tecnologías basadas en el Internet de las Cosas (IoT por sus siglas en inglés), afectando a millones de usuarios cada día.

Los minoristas pueden alcanzar a perder hasta **$150 MDD** por ataques cibernéticos.

Retail

La industria del retail ha incursionado en el mundo digitalidad debido a las bondades de la omnicanalidad que le da una mayor apertura a nuevos mercados, y por ello se han convertido en un blanco constante de ataques cibernéticos.

El estudio de IBM, anteriormente citado, afirma que el 11% de los ataques fueron dirigidos a empresas minoristas con infecciones de malware en sus puntos de venta, falsificaciones de tarjetas, ataques sofisticados en sus aplicaciones de e-commerce, copias fraudulentas de sus sitios web para el robo de información de sus clientes. Una sola empresa puede llegar a perder hasta $150 millones de dólares debido a cibercriminales organizados.

Servicios de salud

Si bien en el informe de IBM el porcentaje de ataques a los servicios de salud ascienden al 6% del total, es importante tomarla en cuenta debido a la sensibilidad de los datos que manejan. Tener a la mano la información de un paciente puede ser la diferencia al salvar su vida.

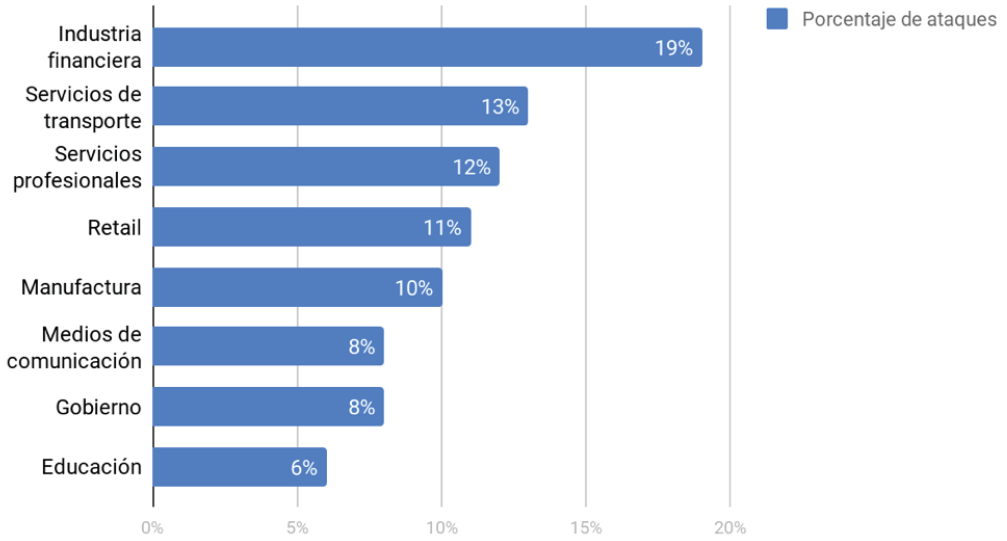
Además, es el sector que mayores pérdidas financieras registra si es atacado, de acuerdo con Ponemon Cost of a Data Breach, los servicios de salud han perdido hasta $408 dólares por víctima registrada[7].

[7] Ibid

Otras industrias vulneradas

De acuerdo con IBM, estas son las industrias que en 2018 sufrieron un porcentaje considerable de ataques cibernéticos, y que vale la pena citar para mantenerse siempre alertas:

Industrias con mayor número de ciberataques en 2018



Most Frequently Targeted Industries in 2018 - X-Force Threat Intelligence Index 2019 de IBM.

RTO y RPO

Para determinar los objetivos de un Plan de Recuperación de Desastres, es de vital importancia conocer la criticidad de la información que una empresa maneja. Este parámetro determinará la tolerancia que tiene el negocio de perder información o tiempo de operación, su tiempo de respuesta ante un incidente y, por lo tanto, sus protocolos de actuación.

Recovery Time Objective (RTO)

Tiempo objetivo de recuperación o RTO por sus siglas en inglés, es el tiempo tolerable que cada empresa determina para recuperarse de un incidente. En algunas industrias, como la de servicios financieros su RTO debe ser cero (o de tolerancia baja), debido a la sensibilidad de sus datos y servicios.

Un banco no puede darse mayor tiempo de recuperación, ya que corre el riesgo de perder reputación ante sus clientes, causar desconfianza o perder una cantidad alta de datos y recursos financieros.

Otras industrias pueden darse un poco más tiempo de recuperación, la industria manufacturera quizá no necesite recuperarse en segundos o máximo minutos, sino que puede tolerar algunas horas o hasta un día entero, antes de que su línea de producción se vea interrumpida.

Estos objetivos se establecen de acuerdo con la criticidad de la operación de la empresa, sus sistemas y su información. Es de suma importancia que un DRP esté determinado con base en esto, para que su tiempo de respuesta sea veloz y cuente con un mayor margen de maniobra antes de ver afectaciones reales.

Recovery Point Objective (RPO)

El punto objetivo de recuperación, como su nombre lo indica, implica el último punto en el que se realizó un respaldo de información confiable. Cada empresa debe tener claro cuánto puede tolerar una posible pérdida de datos en caso de un incidente.

Regresando a la industria financiera, la banca no puede tolerar que su último respaldo de información sea el de un día anterior, o incluso el de una hora antes del incidente, en sólo 60 minutos se pudieron haber realizado miles de transacciones de las cuales debe existir algún tipo de registro.

Las industrias que manejan datos altamente sensibles no se pueden permitir ninguna pérdida, por ellos el RPO debe ser igual a cero, o en el peor de los casos en el nivel 1: menos de 15 minutos, -que entre las industrias financieras puede considerarse demasiado tiempo de pérdida-, sin contar el impacto de recursos económicos que éstos incidente pueden causar.

Para determinar los objetivos de un Plan de Recuperación de Desastres, es de vital importancia conocer la criticidad de la información que una empresa maneja.

Ventajas de un DRP en la nube pública

Sólo en 2018, en México se perdieron **$8 MMDD** por ataques cibernéticos.

Ahorro de costos

Los proveedores de nube pública ya cuentan con la infraestructura necesaria y un poco más, para dar a sus clientes sistemas de cómputo escalables, flexibles y seguros. Esto significa que el negocio ya no debe invertir en hardware, en implementaciones largas, ni en mantenimiento. La nube pública ha demostrado ahorrar hasta 99% de los costos de operación una vez implementada[8].

Prevención y mitigación de desastres

Una vez que el negocio ya decidió migrar a la nube pública, contará con expertos certificados en prevención y mitigación de desastres. Para mantenerse seguras, las empresas deben realizar respaldos de manera periódica y consciente, al estar en la nube tendrá procesos automatizados que le ahorrarán la tarea y garantizarán la disponibilidad de su información y su operación.

Expertos certificados y especializados

El proveedor de la nube a la que estés migrando debe contar con expertos y certificaciones que te den certeza de que tu negocio estará seguro. Ellos te ayudarán a crear Planes de Recuperación de Desastres de acuerdo con las necesidades de tu empresa, determinarán el impacto de un posible riesgo, lo mitigarán y te apoyarán en la recuperación.

[8] Amazon Web Services: Enabling Cost-Efficient Disaster Recovery Leveraging Cloud Infrastructure https://media.amazonwebservices.com/ESG_WP_AWS_DR_Jan_2012.pdf

De acuerdo con Infosecurity, México es el país de Latinoamérica que más sufre ataques cibernéticos, calcula que en 2018 las pérdidas ascendieron a $8 mil millones de dólares[9]; un DRP en la nube ayuda a disminuir estas pérdidas al proteger las infraestructuras críticas de cualquier industria.

Hoy, gracias a la automatización y especialización de la nube pública, se ha convertido en una nueva oportunidad para las empresas en lo relativo a la seguridad de sus sistemas.

Seguridad cibernética: compromiso de todos

Es importante resaltar que la seguridad cibernética de la empresa no sólo depende de CEO o el CTO, sino de todos: gerentes, jefes, empleados y proveedores.

Por ejemplo, los trabajadores, sin importar su nivel, deben estar muy conscientes que sin darse cuenta, podrían causar problemáticas serias por malos hábitos. La 21° Encuesta Global de Seguridad de la Información de EY señala que en el mundo se envían 6.4 millones de correos falsos cada día, y sólo en Estados Unidos cerca de mil 400 empleados de gobierno utilizan la contraseña “Password123”.

1,464
empleados de gobierno en EUA utilizan la contraseña **“Password123”**[10]

Los responsables de cada área deben poner atención a estos riesgos al pensar cómo afectaría su trabajo si las aplicaciones de la empresa dejan de funcionar. Todos los C-Level deben estar conscientes que su operación depende de la tecnología, así que deben comunicarse constantemente con el área de TI para educar a sus empleados y hacer equipo para responder a posibles incidentes.

Es importante señalar también, que si la operación de tu empresa ya está en la nube pública, el trabajo de seguridad no es sólo de tu proveedor, sino deben trabajar en un esquema de corresponsabilidad y comunicación para garantizar la integridad de la información de la empresa.

Tu DRP debe ser personalizado

En Nubosperta sostenemos que tu Plan de Recuperación de Desastres debe ser personalizado, esto significa que estará configurado de acuerdo con las necesidades de tu negocio:

- El tipo y cantidad de amenazas a las que puedes estar expuesto.
- La sensibilidad de los datos que manejes.
- Las políticas de seguridad con las que ya cuentes.
- Las soluciones tecnológicas críticas para tu operación.
- El nivel de higiene digital de tus empleados y la cultura de prevención.
- La capacidad de respuesta de tu equipo.

Una vez determinados estos puntos básicos, se configura un DRP adecuado que responda eficientemente en caso de desastre.

[9] InfoSecurity México 2019 por Juan Manuel Rodríguez Ospina, Show Director de Infosecurity México en: https://www.revistamasseguridad.com.mx/los-ciber-ataques-mexico-costado-8-mil-millones-dolares/

[10] 21° Encuesta Global de Seguridad de la Información de EY en: https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/$FILE/ey-encuesta-global-seguridad-informacion-2018-

Las mejores prácticas impulsan la seguridad del negocio

La aseguradora AXA afirma que el 95% de las PyMes no cuentan con ningún tipo de póliza que asegure su patrimonio empresarial, esto las deja expuestas a las consecuencias de los desastres naturales; como mencionamos anteriormente, ésta es una de las amenazas a las que las empresas están expuestas.

De acuerdo con Hugo García, CEO de Nubosperta, los proveedores de nube pública deben tomar en cuenta las políticas de seguridad que ya tienen las empresas, y con ello se podrán establecer mejores parámetros de prevención, protección y mitigación de riesgos a través del Plan de Recuperación de Desastres, éstas incluyen las pólizas de seguros previamente contratadas por los negocios.

Además de esto, recomendamos a las empresas que para garantizar su seguridad a través de la nube pública realicen las siguientes acciones:

1. Establecer políticas de seguridad más estrictas en sistemas críticos.
2. Determinar la capacidad de respuesta de los responsables de seguridad.
3. Impulsar una cultura de seguridad cibernética entre los empleados.
4. Únicamente dar los permisos necesarios para cada nivel de empleado.
5. Probar los sistemas de respuesta ante incidentes.
6. Solicitar simulaciones de desastres a tu proveedor de nube pública.
7. Revisar constantemente tu Plan de Recuperación de Desastres.
8. Contratar una póliza de seguros en caso de desastres.
9. Mantener una comunicación constante con tu proveedor de nube pública.
10. Calcular la tolerancia de pérdidas del negocio ante incidentes.

La insistencia en estos puntos ayudará a tu empresa a mantenerse lo más segura posible, la tecnología puede fallar, y es por ello que debemos tomar todas las precauciones que estén a nuestro alcance para evitar vulnerabilidades que se traduzcan en pérdidas millonarias, en falta de confianza del cliente o hasta en una bancarrota.

[11] "Pymes, sin conciencia sobre riesgos" por Ximena Soto en: https://expansion.mx/emprendedores/2014/02/07/pymes-expuestas-

CONCLUSIÓN

Estamos constantemente expuestos a riesgos que pueden salir fácilmente de nuestro control, esto no significa que debamos entrar en pánico, sino que debemos estar conscientes de la necesidad de establecer mecanismos y estrategias eficientes para mitigar y contrarrestar estos riesgos.

Cada industria, sector o empresa está expuesta a más o menores riesgos, es por ello que tu proveedor de nube pública debe garantizar la eficiencia de un Plan de Recuperación de Desastres, que sea a la medida y que asegure la continuidad de tu negocio.

Contacta con nuestro equipo de data specialists.

nubosperta

Nubosperta es una empresa líder del mercado de cómputo en la nube.
Advancend Partner Tier de AWS, y con amplia experiencia en el despliegue de soluciones Big Data.
Cuenta con un equipo de ingenieros, gerentes de proyectos y profesionales de la seguridad quienes ayudan a las empresas a construir y administrar su infraestructura en la Nube de AWS.
https://www.nubosperta.com/

CONTACTO
contacto@nubosperta.com
Jose Vasconcelos # 105 Primer Piso
Hipódromo Condesa, 06100
Ciudad de México