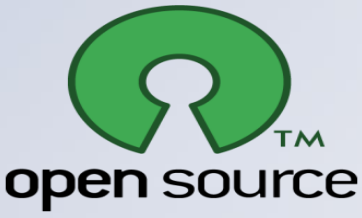
CIBERSEGURIDAD

Planes de Contingencia y Planes de Continuidad del Negocio



Índice

PLAN DE CONTINUIDAD Y PLAN DE CONTINGENCIA, UNA FORMA DE SALVAR TU NEGOCIO 3

RINCÓN DE LOS JÓVENES 6

AGIC PRINT 6

ASPECTOS A CONSIDERAR EN LA ELABORACIÓN DEL PLAN DE CONTINGENCIAS Y SEGURIDAD INFORMÁTICA 7

RECUPERACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN FRENTE A DESASTRES 10

CAPACITACIÓN EN CIBERSEGURIDAD Y ANTIMALWARE 13

RINCÓN DE LOS EXPERTOS 16

ANATOMÍA DE UN PLAN DE CONTINUIDAD DEL NEGOCIO 16

NOVEDADES 17

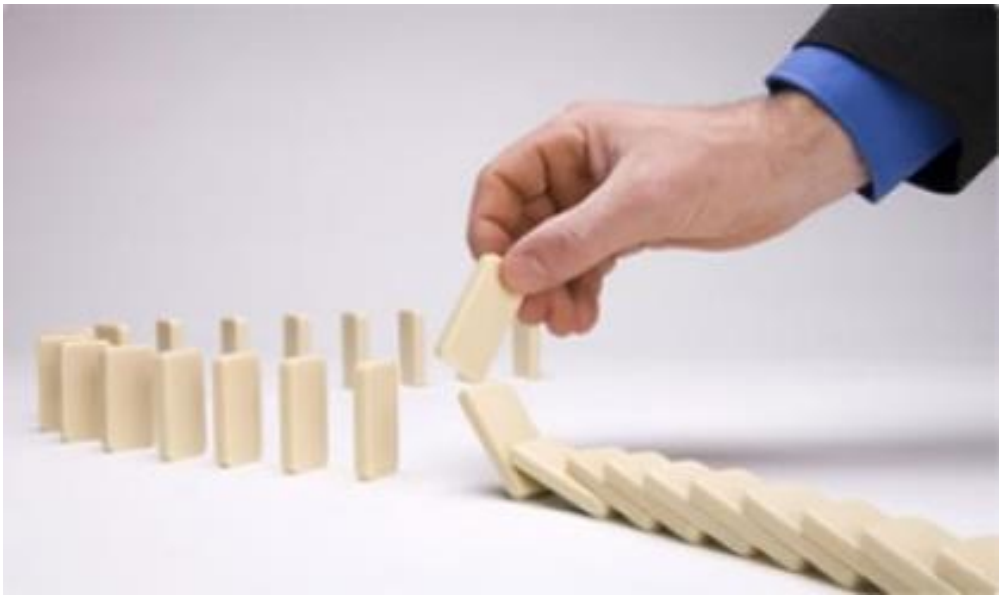
SCPROGRESS Y SU LÍNEA DE SOLUCIONES OPEN SOURCE 17

HUMOR 18

NOTICIAS 19

GUÍA PARA PREVENIR Y ENFRENTAR UN ATAQUE INFORMÁTICO 19

CUATRO PASOS PARA ARMAR UN PLAN DE CONTINUIDAD DEL NEGOCIO 22



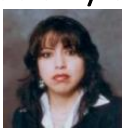
“No harán muy grandes cosas los vacilantes que dudan de la seguridad”

— ELIOT, Thomas Stearns —

CRÉDITOS:

Revista virtual de seguridad informática, recopilación de los mejores artículos de la prensa internacional.

Recopilación y edición:



Consuelo de la Torre
c.delatorre@scprogress.com (+593 979003123)

Marco de la Torre
m.delatorre@scprogress.com (+593 998053611)

Editores Invitados:

Micaela de la Torre

Revisado por:

Arturo de la Torre

adltorre@scprogress.com (+593 999025294)

SCProgress

www.scprogress.com

Facebook

Twitter

Plan de Continuidad y Plan de Contingencia, una forma de salvar tu negocio

En la actualidad las empresas se encuentran realizando el fortalecimiento continuo de sus infraestructuras tecnológicas, para salvaguardar la información de amenazas internas y externas y que pueden afectar los negocios o el funcionamiento normal de las instituciones.

Siendo la información el activo más valioso de cualquier tipo de institución o empresa, se considera de suma importancia, razón por la cual dan cabida al nacimiento y actualización permanente de los planes de contingencia y los planes de continuidad, para minimizar los riesgos de pérdida, substracción o daño permanente de la misma.

SCProgress en esta nueva edición, realiza el análisis y expone las mejores prácticas de los planes de contingencia y los planes de continuidad, que faciliten y guíen a nuestros lectores en su elaboración y mantenimiento para que sus instituciones cuenten con la metodología necesaria, para continuar sus tareas de manera segura y confiable.

Debido a los últimos acontecimientos mundiales, en todas las empresas se deben evaluar las previsiones que se toman para salvaguardar la información de la empresa. Muchas veces, se cree que el Plan de Contingencia, Plan de Recuperación de Desastres y de Continuidad del Negocio son lo mismo; estamos equivocados.

Un **Plan de Contingencia** consiste en restar el impacto financiero que puede causar un "incidente" inesperado en la compañía dentro del marco de los procedimientos habituales de la empresa, este plan trabaja para recuperar a la compañía de los imprevistos especiales que se puedan dar, y que por su causa interrumpen el sistema de producción.

Este plan debe expresar claramente:

- Qué recursos materiales son necesarios.
- Qué personas están implicadas en el cumplimiento del plan.
- Cuáles son las responsabilidades concretas de esas personas y su rol dentro del plan.
- Qué protocolos de actuación deben seguir y cómo son.

Un **Plan de Continuidad** está enfocado a asegurar la continuidad del negocio, cuando de repente ocurre un incidente inesperado. Este plan lo que intenta es no detener la productividad de la empresa, e intentar que la situación que ha

sucedido en ese momento nos afecte lo menos posible.

Los objetivos principales del plan de continuidad de negocio, pueden ser resumidos también de la siguiente forma:

- Prevenir: Limitar al máximo la probabilidad de que tenga lugar cualquier interrupción.
- Contener: Reducir el impacto de cualquier interrupción.
- Recuperar: Asegurar una pronta recuperación.
- Transferir el riesgo residual

Un **plan de recuperación de desastres** (RD en español, o, DRP, por sus siglas en inglés) se refiere al plan de recuperación del área de tecnología.

Para asegurar la continuidad del negocio, es recomendable partir de la siguiente premisa: "Siempre desear lo mejor y planear para lo peor". En un buen plan existen diferentes factores que hay que tomar en cuenta. Por lo que se debe considerar dos fases que son:

Prevención:

1. Enviar respaldos fuera de sitio semanalmente para que en el peor de los casos no se pierda más que los datos de una semana. Incluir el software así como toda la información de datos, para facilitar la recuperación.
2. Si es posible, usar una instalación remota de reserva para reducir al mínimo la pérdida de datos.
3. Redes de Área de Almacenamiento (SANs) en múltiples sitios son un reciente desarrollo (desde 2003) que hace que los datos estén disponibles inmediatamente sin la necesidad de recuperarlos o sincronizarlos.
4. Protectores de línea para reducir al mínimo el efecto de oleadas sobre un delicado equipo electrónico.
5. El suministro de energía ininterrumpido (SAI).La prevención de incendios - más alarmas, extintores accesibles.
6. El software del antivirus, a través de la instalación de **Avira**, desarrollado en el concepto Alemán de calidad, no produce molestias al cliente y el altamente eficiente.
7. El seguro en el hardware, mediante la instalación de **CYBEROAM** NEXT GENERATION FIREWALL, el único Firewall de Siguiente Generación del mercado que utiliza la identificación de Usuarios (Capa 8) a través de las capas 2 – 7, permitiendo a las empresas tener un mejor control y seguridad en sus redes.

Recuperación:

1. Comprar nuevo equipo (el hardware) o reparar o quitar virus, etc.
2. Llamar el abastecedor de software e instalar de nuevo el software.
3. Recuperar los discos de almacenaje que estén fuera de sitio.
4. Reinstalar todos los datos de la fuente de respaldo.
5. Volver a ingresar los datos de las pasadas semanas.
6. Tener estrategias periódicas de respaldos de base de datos.
7. Monitorear el proceso.

FUENTES:

- http://blog.segu-info.com.ar/2013/03/plan-para-la-recuperacion-de-desastres.html
- http://www.audea.com/plan-de-continuidad-y-plan-de-contingencia-una-forma-de-salvar-tu-negocio/ https://www.inbest.me/comunidad/la-importancia-de-los-planes-de-contingencia-drp-y-continuidad-de-negocio
- http://www.ibs-cobanma.hn/noticias/122-plan-de-contingencias-y-continuidad-empresarial.html
- http://www.tecnologiapyme.com/recursos/guia-de-inteco-para-establecer-un-plan-de-continuidad-del-negocio

SECaaS Security as a Service

SCProgress brinda el servicio más completo de seguridad informática optimizando los recursos y garantizando la Confidencialidad, Integridad y Disponibilidad de los sistemas.

FireSecure: El primer nivel de servicio que ofrece detalles de evaluaciones a los firewall, manejo de políticas de seguridad, verificaciones de cumplimiento de políticas, fortalecimiento de los Firewall, así como, políticas de remediación.
Con éste servicio se realiza una (1) auditoría por año.

SecurePlus: Una vez realizado el proceso de FireSecure, se brinda a los clientes el servicio SecurePlus, con el cual se ofrecerán reportes mensuales en los siguientes temas:

- Threat Intellicenge (Análisis de Amenazas)
- Breach Detection (Análisis de Vulnerabilidades)
- Event Correlation (Correlación de eventos)
- Incident Response (Respuesta a incidentes)
- Proactive Monitoring (Monitoreo constante de la seguridad de la plataforma)

Vulnerability Assessment & Pen Testing (Evaluación de Vulnerabilidades y Tests de Penetración): El nivel mas alto de evaluaciones de vulnerabilidades de los sistemas en toda la red, se elabora un informe detallado de test realizados y amenazas encontradas.

SCProgress recibe los mensajes automatizados del Centro de Operaciones en los casos de que exista detección de nuevas vulnerabilidades, ransom o amenazas, para coordinar las acciones a tomar con el cliente junto con el equipo de remediación (técnicos).

Inteligencia de amenazas

Alertas de seguridad en tiempo real

Administración de eventos y logs

Análisis y correlación de eventos

Monitoreo 24x7x365

Gestión de respuesta a incidentes

Auditoría y solución de errores del firewall

VAPT

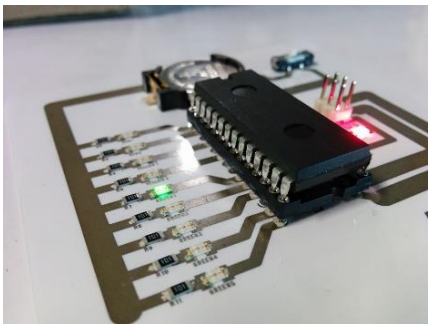
Gestión total del perímetro de seguridad

SCProgress

Rincón de los Jóvenes

AgIC Print

Un circuito eléctrico es el recorrido por donde se desplazan las cargas eléctricas. Usualmente se utilizan cables para conectar las fuentes de poder hasta el final del trayecto, pero la empresa AgIC simplifico este proceso. Con su invento AgIC Print, usando una impresora totalmente normal ahora es posible imprimir tus propios circuitos.

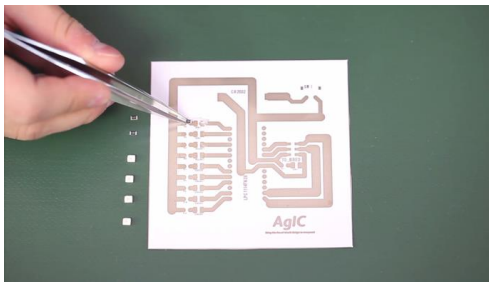


Los diferentes avances en ciencia han hecho posible la manufacturación de una tinta conductora. Esta tinta contiene pequeñas partículas de plata (cabe recalcar que este mineral es uno de los mejores conductores eléctricos que existe). Esta tinta sirve para crear prototipos de circuitos, y mientras se está en el proceso de creación de la impresión es posible revisar y cambiar su forma para que se adapte a las características que se necesitan, haciendo el proceso mucho más simple y estéticamente más atractivo que el común.

Las impresoras tienen una altísima precisión comparada a cualquier otro equipo de fábrica del mismo precio, eso hace que cualquier circuito que se quiera imprimir sea extremadamente preciso, y todo desde la comodidad de casa. Los creadores de esta innovadora idea no solo pensaron en el funcionamiento del invento, sino que también pensaron en el arte que se puede realizar con él. Los cables suelen ser feos, desorganizados y estresantes, con esta idea los circuitos no tienen por qué ser aburridos y nada atractivos.

Con herramientas como Adobe Illustrator o Corel Draw los usuarios pueden usar toda su imaginación para crear elementos de un circuito totalmente funcionales. Y al decir que se puede explotar toda la imaginación de una persona, con esto me refiero a que con una hoja de papel y tinta pueden conseguir un objeto que vuela, un sensor inteligente o un aparato para llevar en tus manos.

Esta empresa incluso ha creado un marcador (AgIC Pen), que al usar en un tipo especial de papel, sirve para el mismo propósito, crear tus propios circuitos. Y a la vez crearon el primer borrador de tinta conductiva, para poder editar cualquier creación realizada a mano con el AgIC Pen o con la AgIC Print. Si cometiste un error al crear un circuito, vas a poder arreglarlo al instante. Las opciones son infinitas.



FUENTES:

- https://www.kickstarter.com/projects/1597902824/agic-print-printing-circuit-boards-with-home-print/description
- https://www.kickstarter.com/projects/1597902824/erasable-circuit-marker-draw-and-edit-circuits-smo/updates

Aspectos a considerar en la Elaboración del Plan de Contingencias y Seguridad Informática

Las organizaciones están constantemente expuestas a contingencias o riesgos de diferente tipo, algunos de carácter natural como los terremotos, inundaciones, erupciones volcánicas, tormentas eléctricas, etc., y otros provocados por el hombre como ataques terroristas, sabotajes, etc., los cuales pueden finalizar en grandes incendios que de no ser atendidos de manera oportuna, pueden causar graves daños a las instalaciones y a las personas, inclusive causando la muerte.

Por otra parte, cada vez son más los ataques informáticos que amenazan a las instituciones tanto públicas como privadas, los ataques a su vez son mucho más sofisticados, esto hace que el personal técnico de las áreas de comunicaciones como informáticas estén preparando planes que les permita seguir operando si en algún momento el ataque, surte el efecto deseado.

Los ataques van desde el secuestro de la información, inyección de ataques, control de los sistemas, etc., todo esto puede causar graves y a veces irreparables daños a las instituciones, de ahí la necesidad de contar con sistema de seguridad apropiados y a su vez, con planes de contingencia.

El plan de contingencia informático debe implicar por lo menos los siguientes pasos:

- Análisis de los amenazas físicas (desastres naturales o antrópicos) e informáticas.
- Probabilidad de ocurrencia de un desastre o ataque.
- Análisis de nuestros recursos humanos y materiales (plataformas).
- Análisis de nuestras fortalezas y debilidades.
- Análisis de los datos sensibles o críticos de las plataformas tecnológicas.
- Análisis de horarios críticos, tales como la noche o fines de semana.
- Análisis del tiempo máximo que la organización puede estar sin operar.
- Posibles alternativas de solución.
- Proveedores que pueden ayudar en caso de desastres.
- Análisis de costos.
- Desarrollo del plan de contingencia.
- Desarrollo del plan de recuperación.
- Seguimiento y evaluación del plan.

Si bien es cierto la unidad de TICs es la encargada de la implantación de medidas de seguridad informática y del desarrollo y evaluación del plan de contingencias, este debe involucrar a todos los miembros de la institución, quienes deben saber de acuerdo a su nivel, las responsabilidades y actividades que deben cumplir para que el plan surta el efecto deseado.

El alcance del plan debe guardar correlación con la infraestructura de comunicaciones e

informática, así como los procedimientos relevantes asociados con la plataforma tecnológica. La infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función del negocio. Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).

El objetivo de un plan de contingencia es implantar un apropiado sistema de seguridad físico y lógico en previsión de desastres (incendios, inundaciones, terremotos, ataques terroristas, ataques informáticos, etc.) de tal manera de establecer medidas destinadas a salvaguardar la información y restaurar los servicios en forma rápida, eficiente, con el menor costo y pérdidas posibles.

La base del plan de contingencia y su posterior recuperación, es establecer prioridades claras sobre qué tipo de procesos son los más esenciales. Es necesario por tanto la identificación previa de cuales de los procesos son críticos y cuáles son los recursos necesarios para garantizar el funcionamiento de las aplicaciones de gestión.

Las simulaciones son esenciales para verificar la eficacia del plan, estás deben realizarse en forma frecuente y en diferentes ambientes, cuando se encuentra todo el personal laborando hasta cuando se dispone de personal al mínimo como es el caso de los fines de semana o días feriados, de igual manera se debe considerar los horarios críticos como el ingreso a las labores por la mañana, también considerar diferentes niveles de riesgo, desde un ataque informático hasta un ataque terrorista.

Las organizaciones deben garantizar la integridad, autenticidad y disponibilidad de la información de sus clientes, eso le hará más competitiva frente a sus adversarios y por ende más efectiva, por tanto la seguridad de sus sistemas debe ser lo más importante para proteger la información y los datos.

Dependiendo del lugar, región, situación política, etc., la probabilidad de que ocurra un desastre puede ser alto o bajo, sin embargo por lo general, el impacto podría ser tan grande que resultaría fatal para la organización, de ahí la necesidad de realizar un adecuado análisis de las amenazas, probabilidad de ocurrencia y su impacto.

Es importante considerar la seguridad informática tanto desde el punto de vista físico como desde el lógico. La seguridad física se refiere a la seguridad de los componentes de los equipos informáticos (hardware) e instalaciones, a la seguridad lógica se refiere a la seguridad de la información y los programas de almacenamiento en un equipo o una red de datos.

La seguridad de información y por consiguiente de los equipos informáticos, es un tema que llega a afectar la imagen institucional de las empresas, incluso la vida privada de personas. Es obvio el interés creciente que día a días se evidencia sobre este aspecto de la nueva sociedad informática. Ladrones, manipuladores, saboteadores, espías, etc. reconocen que el centro de cómputo de una institución es su nervio central, que normalmente tiene información confidencial y a menudo es vulnerable a cualquier ataque.

Los planes de contingencia deben contemplar tres fases:

- Preventiva: Acciones para evitar o disminuir los efectos de los desastres.
- Correctiva: Acciones cuando ocurrió el desastre o ataque.
- Recuperación: Acciones para recuperarse de los efectos causados por los desastres o ataques.

Las organizaciones deberán tener claramente definidos los sistemas de información con los que cuenta, tanto los de desarrollo propio, como los desarrollados por empresas externas. Ello permitirá establecer las acciones que se deben observar para recuperar los servicios, ya sea con el personal propio de la empresa o con los proveedores.

De manera general los servicios que proporcionan las organizaciones son:

- Sistema de comunicaciones (telefonía, video conferencia, etc.)
- Servicio de correo corporativo
- Servicios Web: Publicación de páginas Web.
- Internet.
- VPN: servicios de acceso privado a la red desde cualquier lugar.
- Servicio de monitoreo y vigilancia.
- Servicios de seguridad.
- Servicio de antivirus.
- Servicios de control de personal.

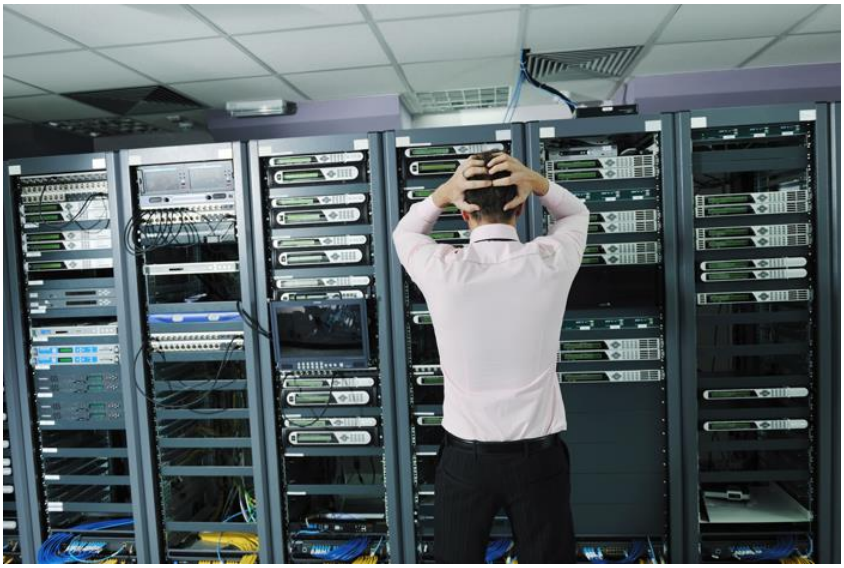
El éxito en la implantación de un plan de contingencias y seguridad informática depende en gran medida, del nivel de preparación del personal, del conocimiento profundo de la organización y sus medios así como de la importancia que le den sus máximas autoridades, es por tanto trascendental que desde los niveles más altos se apoye en forma total en la implementación de medidas preventivas, correctivas y de recuperación. Las organizaciones deben aliarse con proveedores que tengan experiencia en este tipo de acciones, tal como SCCPROGRESS que cuenta con personal altamente capacitado para orientar en la elaboración de planes y la implantación sistemas de seguridad informática.

FUENTES:

- http://www.monografias.com/trabajos101/plan-contingencia-y-seguridad-informacion/plan-contingencia-y-seguridad-informacion.shtml#ixzz4nEJwx2Ss
- www.forodeseguridad.com/artic/discipl/4132.htm
- https://es.wikipedia.org/wiki/Plan_de_contingencias

Recuperación de Tecnologías de la Información Frente a Desastres

Si bien son ciertos y tangibles todos los beneficios de las nuevas tecnologías, existen problemáticas que resultan impredecibles aún para los grandes avances. Los desastres son hechos naturales o provocados que afectan de manera negativa a la cotidianidad, son intempestivos y desembocan en cambios permanentes. En este artículo, proporcionamos información referente a la elaboración del plan de recuperación de desastres de tecnologías de la información (TI), señalaremos los pasos que a nuestra consideración deben seguirse, y los aspectos más importantes que deben considerarse en su elaboración.



Los planes de recuperación de desastres (RD) proporcionan un enfoque estructurado y procedimientos detallados a seguir para responder a los incidentes no previstos que ponen en peligro la infraestructura de TI, compuesta por hardware, software, redes, procesos y personas. Proteger las inversiones realizadas por su firma en la infraestructura tecnológica y garantizar la capacidad empresarial para ejecutar sus operaciones corporativas son las principales razones para poner en marcha un plan de recuperación de desastres en TI.

Todo plan integral de recuperación de desastres debería incluir también a todos los proveedores relevantes, las fuentes de experiencia para recuperar los sistemas afectados y una secuencia lógica de los pasos a seguir hasta alcanzar una recuperación óptima.

Posterior a la evaluación de riesgos e identificación de amenazas potenciales a nuestra infraestructura de TI, el siguiente paso es determinar qué elementos de dicha infraestructura son los más importantes para las operaciones corporativas. Asumiendo que todos los sistemas y redes TI funcionan con normalidad, nuestra empresa debería ser plenamente viable, competitiva y sólida desde el punto de vista financiero. Cuando un incidente -interno o externo- afecta negativamente a la infraestructura de TI, las operaciones corporativas pueden verse amenazadas.

Según la NIST SP 800-34 [PDF], Contingency Planning for Information Technology Systems (Planificación de contingencias para los sistemas de tecnologías de la información), del National Institute for Standards and Technology (NIST, o Instituto Nacional de Estándares y Tecnología) de los Estados Unidos, lo que viene a continuación resume la estructura ideal de un plan de recuperación de desastres TI:

1. Elaboración de la declaración de políticas para el plan de contingencia. Contar con unas directivas formales proporciona la autoridad y orientación necesaria para elaborar un plan de contingencia efectivo.
2. Realización del análisis de impacto sobre el negocio (BIA). El análisis del impacto sobre el negocio ayuda a identificar y priorizar los sistemas y componentes críticos de TI.
3. Identificación de controles preventivos. Medidas que reducen los efectos de las disrupciones al sistema y pueden aumentar su disponibilidad y reducir los costos de contingencia del ciclo de vida.

4. Desarrollo de estrategias de recuperación. Tener una estrategia integral garantiza que el sistema se recuperará de manera rápida y efectiva después de una disrupción.
5. Desarrollo de un plan de contingencia TI. El plan de contingencia debería contener orientaciones y procedimientos detallados para la restauración del sistema dañado.
6. Prueba, formación y ejecución del plan. La prueba del plan identifica lagunas en la planificación, mientras que la formación prepara al personal de recuperación para la activación del plan; ambas actividades mejoran la eficacia del plan y la preparación general de la entidad.
7. Mantenimiento del plan. El plan debería ser un documento vivo que se actualiza regularmente para mantenerlo al día con mejoras al sistema.

Mantener un plan de recuperación ante desastres (DR) puede ser una tarea ardua. Cada plan de DR es diferente. Algunos planes requieren una revisión anual, otros de forma mensual y algunos necesitan ser revisados cada vez que un producto o el entorno, sufre algún cambio. Cada organización debe decidir cuándo es conveniente revisar y/o cambiar el plan de DR, pero ¿cómo determinar cuál es el momento idóneo para realizar una actualización o revisión? En última instancia, usted deberá actualizar el plan de recuperación ante desastres cada vez que se produzca un cambio en un factor importante de su organización, al margen de que dicha variable sea interna o externa. Y el marco temporal en que se producen esos cambios es impredecible. Actualizar frecuentemente los planes de recuperación ante desastres hace que éstos sean más completos y fiables, lo cual genera un entorno de trabajo más seguro en caso de desastre.

Aspectos clave a considerar al planificar la recuperación de desastres TI:

Apoyo de la alta gerencia. Asegúrese de tener el apoyo de la alta gerencia a fin de lograr alcanzar los objetivos del plan.

Tomarse en serio el proceso de planificación de RD de TI. Aunque la recopilación y análisis de los datos para el plan de RD de TI puede llevar mucho tiempo, no es necesario que tenga docenas de páginas. Los plantes simplemente necesitan la información correcta, y esa información debería ser actual y precisa.

Disponibilidad de estándares. Entre los estándares relevantes que podemos usar a la hora de desarrollar los planes de RD de TI están los siguientes: NIST SP 800-34, ISO/IEC 24762 y BS 25777.

La sencillez es un grado. Es esencial reunir y organizar la información correcta.

Estudiar los resultados con las unidades de negocio. Una vez finalizado el plan de recuperación de desastres, debemos cotejar sus conclusiones con los líderes de las unidades de negocio para comprobar que nuestras premisas son correctas.

Cabe destacar que un DRP es una de las mejores inversiones que puede realizar una empresa. Sin embargo, es mucho más que adquirir equipamiento, instalarlo y mantenerlo en operación. Debemos asegurar que dicho capital nos otorgue los mejores rendimientos, por lo que lo más recomendable es que los departamentos de TI cuenten con un proveedor especializado y experimentado que durante una contingencia garantice los recursos apropiados en cuanto a personal certificado, procesos y herramientas para reaccionar apropiadamente.

SCProgress cuenta con las herramientas necesarias de hardware y software de clase mundial, reconocida por sus altos estándares de calidad, productos y servicios a nivel Latinoamérica por Latin American Quality Institute (LAQI), protegerá y facilitará permanentemente la continuidad del negocio.

FUENTES:

- http://blog.segu-info.com.ar/2013/03/plan-para-la-recuperacion-de-desastres.html
- http://searchdatacenter.techtarget.com/es/consejo/Aspectos-basicos-del-plan-de-recuperacion-de-desastres-Actualizacion-y-revision
- http://mundocontact.com/6-pasos-para-crear-un-plan-de-recuperacion-de-desastres-en-la-empresa/

Capacitación en Ciberseguridad y Antimalware

"La necesidad de capacitación surge por la diferencia entre lo que uno debería saber y lo que sabe realmente"

El personal responsable de las áreas de sistemas, así como los usuarios, deben conocer sobre la infinidad de ataques informáticos amenazas, ataques a la información y a las infraestructuras tecnológicas, los mantienen como áreas vulnerables permanentes, facilitando las actividades fraudulentas de hackers, quienes han visto como un gran negocio lucrativo, la sustracción de datos, ya sea personal, financiera, confidencial, etc.

La capacitación en seguridad informática, se vuelve relevante e importante para evitar que las empresas e instituciones, se vean afectadas ante este tipo de amenazas.

SCProgress cuenta con asesores altamente especializados a nivel internacional, lo que nos permite brindar cursos de capacitación en diversos temas tecnológicos, especialmente en el área de seguridad informática, su amplia experiencia y conocimientos, les ha permitido participar en eventos nacionales e internacionales como la conferencia organizada por la CEPOL Research & Science Conference (Organismo acreditado de la Unión Europea), realizada en Budapest el año 2016.

En esta ocasión SCProgress, consiente de la importancia que prestan las instituciones a la seguridad de la información, y ante el incontrolable crecimiento de las amenazas, ha organizado y pone a disposición de sus lectores y clientes, capacitación en los siguientes temas:

Certificación en Ciberseguridad de la RED	Introducción al análisis y comportamiento del malware
Contenido: • Fundamentos de red de computadoras y defensa • Amenazas, vulnerabilidades y ataques a la red • Controles, protocolos y equipos para la seguridad de la red Diseño e implementación de políticas de seguridad en la red • Seguridades físicas • Seguridades en los Host • Configuración y administración segura de Firewalls • Configuración y administración segura de IDS • Configuración y administración segura de VPNs • Protección de redes inalámbricas • Monitoreo y análisis del tráfico de la red • Gestión de riesgos y vulnerabilidades • Data backup y recuperación de datos • Respuesta y manejo de incidentes	**Contenido:** • Análisis de malware • Indicadores de infección • Malware signatures • Categorías de malware • Mass vs Targeted malware • Metodología de análisis de malware • Herramientas Antimalware • Malware empaquetado y oculto • DLL Hijacking • Magic labels • Formatos de archivos • Dynamic Link Libraries • Detección de virtualización de malware • Dependency Tracing • Modificación de registros • Manipulación de archivos del sistema • Análisis de tráfico de la red • Sandboxes

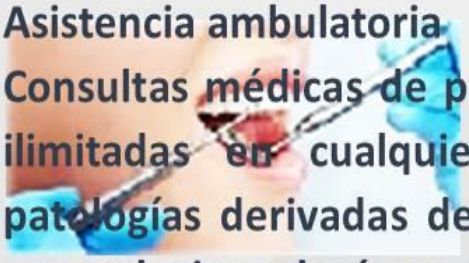
Los cursos se dictan en las instalaciones de SCProgress ubicadas en el edificio Plaza de Vizcaya, tercer piso, en La Pradera E7-21 y Mariana de Jesús,

Para mayor información visite nuestra página web: **www.scprogress.com**, o comuníquese directamente al correo electrónico: **ventas@scpgrogress.com**.

Cooperativa de Ahorro y Crédito "General Rumiñahui"

Promoviendo el desarrollo y bienestar de sus socios militares y civiles desde 1993.

- **Créditos sin garante hasta 3.000 dólares.**
- **Otorgamos créditos para consumo, emprendedores y microempresarios.**
- **Las tasas de interés más bajas del mercado.**
- **Inversiones a plazo fijo.**
- **Pagos de créditos y ahorros, a través de ventanillas o con autorización de débitos bancarios del Banco Pichincha, General Rumiñahui e ISSFA.**



- **Asistencia ambulatoria**
- **Consultas médicas de primer nivel ilimitadas en cualquiera de las patologías derivadas de: medicina general, ginecología y pediatría.**
- **Cobertura en asistencia dental.**
- **Examen clínico y diagnóstico.**
- **Higiene dental, alivio del dolor.**
- **Rayos X periapical, profilaxis (Limpieza dental profunda).**
- **Restauraciones en resina simple.**
- **Extracciones simples.**

Calle Manuel Cabeza de Vaca N53-240 y Av. Los Pinos a 30 mts. Del Cuartel Rumiñahui.
Teléfonos: 2411-731 / 2406-117 / 0984977204
www.cooprumi.fin.ec

Rincón de los Expertos

Anatomía de un plan de Continuidad del Negocio

Si la organización no posee un plan definido de continuidad del negocio, hay que empezar por evaluar los procesos principales del negocio. Determinar qué áreas son vulnerables y las pérdidas potenciales que puedan resultar de fallas en los procesos críticos. Es fundamental realizar en primer lugar un BIA (Business Impact Analisys).

A continuación, tendremos que desarrollar un plan que involucra los 6 siguientes pasos:

1. Identificar el alcance del plan.
2. Identificar los puntos más críticos del negocio.
3. Identificar las funciones críticas.
4. Identificar las dependencias entre varias áreas de negocio y las correspondientes funciones.
5. Identificar un valor máximo de caídas y fallos del sistema, que pueden ser considerados aceptables.
6. Crear un plan para mantenerse trabajando durante las fallas críticas.

Una herramienta común para planificar la continuidad del trabajo, en caso de fallas críticas, es una lista de verificación (checklist) que incluya todos los suministros y equipos, la localización de los respaldos de datos; donde el plan es aplicable y quienes pueden mantenerlo funcionando. Así como también, la información de los principales contactos en caso de existir un evento de emergencia.

Recuerden que el plan de recuperación ante desastres (DR) es parte del plan de continuidad del negocio. Por tanto desarrollar un plan de DR en caso de no tenerlo, debería ser parte de todos sus procesos. Adicionalmente, si Usted no posee un DR, no asuma que es imposible, todos los elementos necesarios puede encontrarlos fácilmente en el mercado. Usted acepte que es necesario un tiempo de recuperación, y que el mismo debe estar claramente definido y responder a las expectativas del negocio.

En los casos en que Usted mismo sea autor de sus planes, considere una entrevista personal a aquellas personas que hayan superado fallas de recuperación de desastres y sus casos sean de éxito. La gente regularmente disfruta de contar sus experiencias profesionales, y los pasos o procedimientos utilizados para superar los problemas. Estas personas pueden darle ideas y procedimientos de invaluable contenido para superar las crisis.

Authorized GSMK CryptoPhone Distributor
El teléfono inteligente más seguro del mundo

Novedades

SCProgress y su Línea de Soluciones Open Source

Hoy en día existe una gran variedad de aplicaciones y soluciones de software libre, por lo que SCProgress ofrece a todos sus clientes soluciones tecnológicas altamente competitivas, con la garantía y experiencia de todos sus técnicos.

La implementación de dichas soluciones, permite que se pueda controlar, gestionar y administrar sus infraestructuras tecnológicas con total independencia de los proveedores de hardware y software.

Dentro de la línea open source cuenta especialistas altamente calificados en:

- **Red Hat**: líder mundial como proveedor de soluciones de código abierto, a través de un enfoque basado en la comunidad que le permite ofrecer tecnologías fiables y de alto rendimiento en la nube, virtualización, almacenamiento, Linux y middleware.

- **Moodle:** software diseñado para ayudar a los educadores a crear cursos en línea de alta calidad y entornos de aprendizaje virtuales. Tales sistemas de aprendizaje en línea son algunas veces llamados VLEs (Virtual Learning Environments) o entornos virtuales de aprendizaje.

- **Zabbix** es un Sistema de Motorización de Redes. Está diseñado para monitorizar y registrar el estado de varios servicios de red, servidores, y hardware de red.

  Usa MySQL, PostgreSQL, SQLite, Oracle o IBM DB2 como base de datos. Su backend está escrito en lenguaje C y el frontend web está escrito en PHP. Zabbix ofrece varias opciones de monitorización.

- **Zimbra:** la suite de colaboración Zimbra es un programa informático colaborativo o Groupware que consta de un servicio de correo electrónico creado por Zimbra Inc. Posee tanto el componente de servidor como su respectivo cliente.

  El servidor ZCS hace uso de proyectos de código abierto existentes como Postfix, MySQL, OpenLDAP y Lucene. Cuenta con una interfaz de programación de aplicaciones basada en SOAP para toda su funcionalidad y actúa como servidor IMAP y POP3 de correo electrónico.

Adicionalmente es muy importante destacar que SCProgress, desarrolla aplicaciones open source con otras tecnologías, para satisfacer a sus dilectos clientes que requieran soluciones más personalizadas, para que empresas e instituciones sean líderes en tecnología de la mejora calidad.

Si requiere mayor información sobre los productos, visite la página web: www.scprogress.com, si usted prefiere un asesoramiento personalizados con nuestros técnicos, escríbanos directamente a ventas@scprogress.com, o comuníquese directamente a nuestro teléfono: (02) 2900865.

Humor

AMOR, CAMBIASTE LA CONTRASEÑA?
SI CARIÑO
ME PUEDES DECIR CUAL ES?
SI! LA FECHA EN QUE NOS CONOCIMOS
VARIAS HORAS PENSANDO....
ME LLEVA...

AY, OSCAR... UN BUEN RESTAURANTE, RICO VINO, EXQUISITA COMIDA, VELAS... ¿ME QUIERE PROPONER ALGO?
QUE PAGUEMOS A MEDIAS

ME SIENTO FRENTE A LA COMPUTADORA Y SE ME DESPIERTA EL HAMBRE
...DEBE SER POR EL RATÓN
Periotti

NUESTRA VIDA MODERNA:
TRABAJAR
DESCANSAR
JUGAR
DORMIR
www.gran-angular.net

Noticias

Guía para prevenir y enfrentar un ataque informático

El caso de WannaCry solo fue una muestra de los desafíos que enfrentan empresas y usuarios.

El último ataque cibernético mundial, protagonizado por el programa malicioso WannaCry, les recordó a las compañías y a los ciudadanos que los sistemas informáticos no son infalibles ni invulnerables. Fue un manifiesto de la existencia de un lado oscuro del ámbito virtual donde ya no solo actúan "lobos solitarios" ávidos por superar desafíos o de suscitar caos por mera diversión, sino organizaciones criminales, "enormes equipos de personas", cuya principal motivación es el dinero.

El impacto económico de WannaCry fue estimado en 4.000 millones de dólares. Los criminales bloquearon el acceso a los datos de cerca de 250.000 computadores y pedían un pago de entre 300 y 600 dólares por liberar la información cautiva. El botín final de los bandidos se estima en alrededor de 100.000 dólares. Aunque se preveía una segunda ola de ataques en los días posteriores a la primera epidemia, la crisis suscitada por WannaCry se ha apaciguado.

Sin embargo, los ataques continuarán. Según el experto en seguridad de la información Iván Castellanos, de la firma Etek International, WannaCry fue un caso de considerable impacto mediático, pero no excepcional. "Habrá más arremetidas de los ciberdelincuentes, tal vez con peores consecuencias pero menos llamativos", alertó.

Muchos de esos ataques serán silenciosos, como aquel perpetrado por cibercriminales en 2015, cuando robaron hasta 1.000 millones de dólares de más de 100 bancos en 30 países. Fue calificado como el mayor robo de la historia en su momento y fue ejecutado de forma metódica.

Los ciberdelincuentes instalaron 'software' espía en los computadores del banco. Aprendieron cómo operaban los empleados y los sistemas de las diferentes entidades infiltradas y después empezaron a transferir dinero a sus cuentas. Tomaron entre 2,5 y 10 millones de dólares de cada una de sus víctimas y así fueron acumulando un botín multimillonario.

El “software” de cibersecuestro, como lo fue WannaCry, seguirá existiendo, y tal vez no atacará a miles de computadores a la vez, pero sí podría afectar al computador de cualquier ciudadano o empresa. Las cifras avalan la alerta: se estima que sean 12 programas maliciosos por segundo. A diario son atacadas más de 400 empresas y los cibercriminales han robado más de 3.000 millones de dólares en los últimos tres años.

Sepa qué debe hacer para prevenir ataques futuros o cómo responder en caso de haber sido víctima de uno de ellos.

Cuando llega la ofensiva

De acuerdo con Juan Mario Posada, consultor en seguridad informática de la firma EY, las máquinas infectadas deben ser aisladas y desconectadas de la red para evitar que sean fuente de propagación.

“En la medida en que se traten los primeros casos, se previenen contagios”, dice. El experto asegura que es necesario activar los planes de respuesta a incidentes y que estos casos no se deben tratar solo como un tema de tecnología, sino como un problema que afecta a todas las divisiones de la organización.

Para las empresas es muy importante que se conserve evidencia del proceso en caso de requerirse una investigación y es recomendable que las copias de seguridad se ubiquen en unidades de almacenamiento que se encuentren fuera de línea.

Para las copias de seguridad, se recomienda implementar un plan para probar, con regularidad, que los respaldos funcionen de forma correcta en caso de que sea necesario usarlos.

Si cae presa de un “software” de cibersecuestro, también conocido como “ransomware”, absténgase de pagar. “Debe tener en cuenta que está lidiando con delincuentes y pagar el rescate no le garantiza que vaya a recuperar el acceso a su información. Además, esto incentiva a que los ataques continúen y se incrementen, ampliando las probabilidades de que incluso usted mismo vuelva a ser víctima nuevamente”.

Consejos para prevenir agresiones informáticas

Primero hay que ser consciente de la existencia de amenazas informáticas, cuando se haga una evaluación de riesgo en una empresa, cuando se empiezan a implementar nuevas tecnologías, se debe priorizar la seguridad como parte esencial del proceso.

Esto afecta, sobre todo, a las pequeñas y medianas empresas. Este tipo de entidades se están transformando para entrar a la era digital, pero su foco es incrementar sus cifras e impulsar el negocio. Creen que la seguridad informática es más un gasto que una inversión. Ese es el primer error.

Los sistemas operativos deben estar actualizados y protegidos. Deben optimizarse los tiempos de mantenimiento y mejorar los equipos para evitar caer presa de una brecha de seguridad.

Una de las razones por las que WannaCry tuvo impacto fue porque, aunque ya existía una cura para el problema desde marzo, muchas empresas habían relegado el proceso de actualización y mantenimiento de sus sistemas.

“La red empresarial debe ser segura. Se debe saber quiénes se conectan a ella. Quienes la administran deben contar con una visión completa del funcionamiento de la misma en

todo momento. También es imperativo diseñarla de modo que, en caso de ataque, existan opciones para segmentar la red y aislar las infecciones".

También se debe invertir en la capacitación de los empleados. Según la consultora EY, los ataques responden, en un 83 por ciento, a empleados descuidados. "En la mayoría de los casos, las campañas de cibercrimen no solo involucran el desarrollo de códigos maliciosos, sino todo un proceso de investigación previa. Los cibercriminales preguntan cómo funciona la red, se infiltran en la compañía y engañan a su personal para obtener información".

Otro factor que llevó a la propagación de WannaCry fue que los creadores del programa malicioso usaron una técnica de vieja data, la de propagación automática, un mecanismo de expansión de infecciones común en la década pasada, pero que fue una rareza para la época actual.

FUENTES:

- http://www.eltiempo.com/tecnosfera/novedades-tecnologia/consejos-para-prevenir-y-enfrentar-ataques-informaticos-92972

Cyberoam®

Cuatro pasos para armar un Plan de Continuidad del Negocio

Al hablar de "continuidad del negocio" nos referimos a la capacidad de "sobrevivir a las cosas malas" que pueden tener un impacto negativo en la empresa: desde un brote de virus informático hasta un brote de virus biológico, y todos los demás peligros entre ambos, como incendios, inundaciones, tornados, huracanes, terremotos y tsunamis. El estándar internacional para la continuidad del negocio, ISO 22301, la define como la "capacidad de una organización de continuar la prestación de productos o servicios en los niveles predefinidos aceptables, tras incidentes de interrupción de la actividad". La Gestión de la Continuidad del Negocio, también llamada BCM por sus siglas en inglés, es el proceso de lograr esta capacidad y mantenerla.

En el presente artículo, describimos los puntos básicos de un BCM, además suministramos una lista de recursos que la organización puede utilizar para mejorar la capacidad de sobrevivir a cualquier cambio imprevisible e indeseado.

La continuidad del negocio no es sólo para tecnología de la información.

La mayoría de las organizaciones de hoy son sumamente dependientes de la tecnología de la información, TI. Los procesos informáticos se dan en equipos portátiles, servidores, tabletas y hasta smartphones, pero queda claro que esta tecnología puede verse afectada por una amplia gama de incidentes potencialmente desastrosos.

Éstos van desde cortes en el suministro de energía provocados por tormentas hasta la pérdida de datos causada por equivocaciones de los empleados o por criminales informáticos.

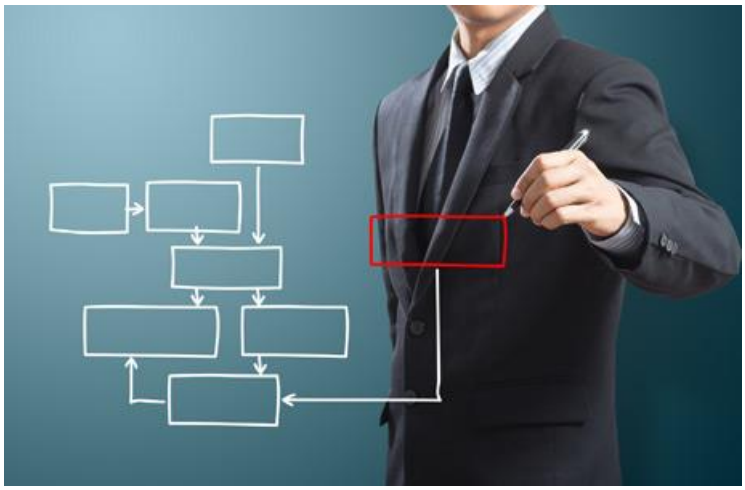
Desde los albores de la TI, estaba claro que las organizaciones iban a necesitar estrategias para prepararse para dichos incidentes, responder a ellos y recuperarse de ellos. Por ese motivo, gran parte de los primeros trabajos sobre el manejo de incidentes de interrupción de la actividad provino de la comunidad de TI.

No obstante, con el paso del tiempo, la disciplina de "recuperación ante desastres" evolucionó a "un proceso de gestión holístico" que "identifica amenazas potenciales para la organización y el impacto que su materialización podría ocasionar en las operaciones corporativas, y que proporciona un marco para crear resistencia corporativa de modo que pueda dar una respuesta eficaz que proteja los intereses de sus grupos de interés, reputación, marcas y actividades de creación de valor fundamentales". Hay que tener en cuenta que, aunque la empresa no necesita tener certificación ISO 22301 para

sobrevivir a un desastre, algunas corporaciones desean conseguir esta certificación para mejorar su programa de BCM y a la vez para ganar más mercado. Por ejemplo, es evidente que ciertas empresas esenciales para la cadena de suministro de algunas industrias reciben más solicitudes por el seguro de continuidad del negocio en las negociaciones contractuales, y su adherencia a ISO 22301 ciertamente contribuye a esta cuestión.

Un programa básico de BCM en cuatro pasos

Desafortunadamente, algunas empresas deben cerrar cuando las alcanza un desastre para el cual no estaban preparadas adecuadamente. Es lamentable porque el camino para dicha preparación está bien documentado. Cualquier empresa de cualquier tamaño puede mejorar las posibilidades de superar un incidente de interrupción de la actividad y quedar en una pieza, con la marca intacta y sin merma en los ingresos, si sigue ciertas estrategias probadas y de confianza, más allá de que desee obtener la certificación ISO 22301 o no.



A continuación, un resumen de los cuatro pasos principales:

Identificar y priorizar las amenazas

Cree una lista de las amenazas y los incidentes de interrupción que pueden provocar. Considere que las amenazas varían según la ubicación, por ejemplo, terremotos, incendios forestales, tsunamis, etc.

En esta etapa, una buena técnica es reunir personas de todos los departamentos en una sesión de intercambio de ideas. El objetivo de la reunión es crear una lista de escenarios ordenados por probabilidad de ocurrencia y por potencial de causar un impacto negativo.

Realice un análisis del impacto en la empresa

Determine qué partes de la empresa son las más críticas para que sobreviva. Una manera es comenzar detallando las funciones, los procesos, los empleados, los lugares y los sistemas que son críticos para el funcionamiento de la organización. Para ello, deberá entrevistar a los empleados de cada departamento y luego elaborar una tabla de resultados que liste las funciones y las personas principales y las secundarias.

A continuación determine la cantidad de "días de supervivencia" de la empresa para cada función. ¿Cuánto puede resistir la empresa sin que una función en particular provoque un impacto grave?

Ordene el impacto de cada función, por ejemplo, utilice una escala de 1 a 4, donde 1 = impacto crítico en las actividades operativas o pérdida fiscal, y 4 = sin impacto a corto plazo. Si luego se multiplica el impacto por los "días de supervivencia", se puede ver cuáles son las funciones más críticas. Al principio de la tabla quedarán las funciones con un impacto mayor y con sólo un día de supervivencia.

Cree un plan de respuesta y recuperación

En esta etapa deberá catalogar datos clave sobre los bienes involucrados en la realización de las funciones críticas, incluyendo sistemas de TI, personal, instalaciones, proveedores y clientes. Deberá incluir números de serie de los equipos, acuerdos de licencia, alquileres, garantías, detalles de contactos, etc.

Necesitará determinar "a quién llamar" en cada categoría de incidente y crear un árbol de números telefónicos para que se hagan las llamadas correctas en el orden correcto. También

necesitará una lista de "quién puede decir qué cosa" para controlar la interacción con los medios durante un incidente.

Deberán quedar documentados todos los acuerdos vigentes para mudar las operaciones a ubicaciones e instalaciones de TI temporales, de ser necesario.

Los pasos para recuperar las operaciones principales deberían ordenarse en una secuencia donde queden explícitas las interdependencias funcionales. Cuando el plan esté listo, asegúrese de capacitar a los gerentes sobre los detalles relevantes para cada departamento, así como la importancia del plan general para sobrevivir a un incidente.

Pruebe el plan y refine el análisis

La mayoría de los expertos en BCM recomiendan probar el plan al menos una vez al año, con ejercicios, análisis paso a paso o simulaciones. La prueba permite sacar el mayor provecho en la creación del plan, y no sólo encontrar fallas y dar cuenta de los cambios corporativos con el transcurso del tiempo, sino que también causa una buena impresión en la gerencia.

No cabe duda de que estos cuatro pasos significan un enorme trabajo, pero es una tarea que las empresas ignoran bajo su propio riesgo. Si el proyecto parece demasiado desalentador para aplicar a la empresa completa, considere comenzar por unos pocos departamentos o una sola oficina. Todo lo que vaya aprendiendo en el proceso se podrá aplicar en mayor escala a medida que progrese. Evite a toda costa pensar que las cosas malas no suceden, porque sí lo hacen. Sólo tiene que estar preparado. Y no pretenda que cuando ocurra algo no será tan malo, porque podría serlo.

FUENTES:

- https://www.welivesecurity.com/la-es/2014/05/14/gestion-continuidad-negocio-cuatro-pasos/
- https://www.securityartwork.es/2013/04/04/continuidad-de-negocio-tipos-de-proyectos/

SCProgress cuenta con todo lo que necesita para su infraestructura de cableado estructurado

Los sistemas de cableado estructurado constituyen una plataforma universal para la transmisión de voz, datos y video, el diseño e implementación de infraestructuras de fibra óptica y cableados que cumplan con los estándares se vuelven cada vez más imprescindible para el éxito de sus empresas.

SCProgress brinda el mejor servicio en:

- Diseño e instalación de sistemas de cableado estructurado con las mejores marcas.
- Certificación de sistemas de cableado estructurado
- Diseño e instalación de fibra óptica.
- Asesoría técnica para la implementación de sistemas de cableado estructurado.
- Personal altamente calificado, certificado y con amplia experiencia.

En caso de requerimiento del cliente, nuestro personal cuenta con experiencia en marcas como Panduit, Dexon, así como marcas nacionales.

Para más información no dude en contactarnos en ventas@scprogress.com

GESRICA
COMPAÑÍA DE GESTIÓN DE RIESGO Y CAPACITACIÓN S.A.

Nuestro país se encuentra ubicado sobre el cinturón de fuego del pacífico, por lo que nos encontramos expuestos a eventos naturales que pueden afectar nuestras actividades, razón por la cual, debemos tomar acciones y ejecutar procedimientos para mitigar posibles siniestros, ya sean causados por la fuerza de la naturaleza o por accidentes humanos.

Contamos con personal especializado en la gestión, planificación, capacitación e implementación de estrategias para la reducción de riesgos y ponemos a su disposición , asesoramiento en la elaboración de planes de gestión de riesgos, diseñados exclusivamente para las características de su empresa, así como, capacitación en áreas a fines, principalmente en:

- ***Primeros auxilios.***
- ***Brigadas de emergencia.***
- ***Prevención de incendios***
- ***Seguridad industrial.***
- ***Normas de seguridad.***
- ***Prevención y manejo de emergencias y evacuaciones.***

www.gesrica.com
E-mail: info@gesrica.com
Teléfonos: 0984489267 - 0996620889 – 0979003123
Dirección: 18 de Septiembre 07-04-009 y Panamericana Norte.

www.scprogress.com

Julio 2017