INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 17

9 DE ENERO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

Son herramientas cuyo objetivo es planificar planes de actuación y contingencia destinados a mitigar el impacto provocado por cualquier incidente de seguirdad.

Contingencia y continuidad.

¿Qué es?

Son herramientas cuyo objetivo es planificar planes de actuación y contingencia destinados a mitigar el impacto provocado por cualquier incidente de seguridad, constituidos por un conjunto de recursos de respaldo y procedimientos de actuación, encaminados a conseguir una restauración ordenada y progresiva de los sistemas y los procesos de negocio considerados críticos en cualquier organización.

Están muy enfocadas a la recuperación ante desastres e incidentes de seguridad, la externalización se ha convertido en un elemento fundamental de este tipo de herramientas, como las soluciones de copia de seguridad remota, la virtualización, así como la seguridad en la nube (cloud computing).

Es necesario proteger los principales procesos de negocio a través de un conjunto de tareas que permita a la organización recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad.

De esta forma se garantiza puede dar una respuesta planificada ante cualquier fallo de seguridad

Tipos

- Software de Recuperación de Desastres (DRP):

Herramientas diseñadas para facilitar la recuperación rápida y eficiente de sistemas y datos críticos en caso de un desastre.

- Planes de Continuidad Empresarial (BCP):

Herramientas y servicios que ayudan en la creación, mantenimiento y prueba de planes de continuidad empresarial, que son estrategias para garantizar la continuidad de las operaciones comerciales durante y después de eventos adversos.

- Sistemas de Respuesta a Incidentes (IR):

Productos que facilitan la detección y respuesta rápida a incidentes de seguridad, incluyendo herramientas de monitoreo, análisis de registros y capacidades de respuesta automatizada.

- Infraestructura de Recuperación (RI):

Incluye servicios y productos relacionados con la creación y gestión de infraestructuras alternativas o secundarias que pueden activarse en caso de interrupciones en la infraestructura principal.

- Almacenamiento y Respaldo Seguro:

Soluciones para almacenamiento y respaldo de datos, asegurando la integridad y disponibilidad de la información crítica.

- Simulacros y Ejercicios de Continuidad:

Herramientas que facilitan la realización de simulacros y ejercicios para probar la efectividad de los planes de continuidad y mejorar la preparación de las organizaciones.

- Gestión de Crisis y Comunicaciones de Emergencia:

Plataformas que ayudan en la gestión de crisis y la comunicación efectiva con los empleados, partes interesadas y el público durante eventos de emergencia.

- Análisis de Riesgos y Evaluación de Impacto Empresarial:

Herramientas que facilitan la identificación y evaluación de riesgos, así como la determinación del impacto potencial en las operaciones empresariales.

- Servicios de Consultoría en Continuidad Empresarial:

Consultores y expertos en continuidad empresarial que brindan asesoramiento personalizado para el desarrollo e implementación de estrategias de contingencia y continuidad.

Recomendaciones

- Realizar un Análisis de Riesgos:

Identificar y evaluar los posibles riesgos y amenazas que podrían afectar a la organización. Esto ayuda a priorizar la planificación y la asignación de recursos.

- Desarrollar un Plan de Continuidad Empresarial (BCP):

Crear un plan detallado que incluya procedimientos específicos para mantener las operaciones críticas durante y después de un evento adverso. El plan debe ser comprensible y accesible para todo el personal relevante.

- Mantener Copias de Seguridad Actualizadas:

Realizar copias de seguridad regulares de datos críticos y almacenarlas en ubicaciones seguras y fuera del sitio. Asegurarse de que los procedimientos de restauración se prueben y sean efectivos.

- Implementar Soluciones de Recuperación de Desastres (DRP):

Utilizar soluciones de DRP que permitan la recuperación rápida de sistemas y datos esenciales. Asegurarse de que estas soluciones se prueben regularmente para garantizar su efectividad.

- Establecer un Centro de Operaciones de Emergencia (EOC):

Designar y equipar un centro desde el cual se pueda coordinar la respuesta a situaciones de emergencia. Esto incluye la gestión de recursos, la comunicación interna y externa, y la toma de decisiones.

- Capacitar al Personal:

Proporcionar capacitación regular al personal sobre los procedimientos de contingencia y continuidad. Asegurarse de que todos estén familiarizados con sus roles y responsabilidades durante una crisis.

- Conducta de Simulacros y Ejercicios:

Realizar simulacros y ejercicios periódicos para probar la eficacia del plan de continuidad. Esto ayuda a identificar posibles áreas de mejora y garantiza que el personal esté preparado para enfrentar situaciones de crisis.

- Establecer un Sistema de Comunicación de Emergencia:

Implementar un sistema de comunicación eficiente que permita la rápida difusión de información crítica durante situaciones de emergencia. Esto incluye la comunicación con empleados, clientes, proveedores y otras partes interesadas.

- Revisar y Actualizar Regularmente:

Revisar y actualizar el plan de continuidad de manera regular para garantizar que esté alineado con los cambios en la organización y en el entorno empresarial. Los riesgos y las amenazas pueden evolucionar con el tiempo.

- Contar con un Equipo de Respuesta a Incidentes:

Establecer un equipo de respuesta a incidentes capacitado para abordar situaciones de emergencia. Este equipo debe estar listo para actuar de manera coordinada y efectiva.