ENTRENAMIENTO, PRUEBAS Y AUDITORÍA

ING. FREDY BUSTAMANTE

TEMAS A TRATAR

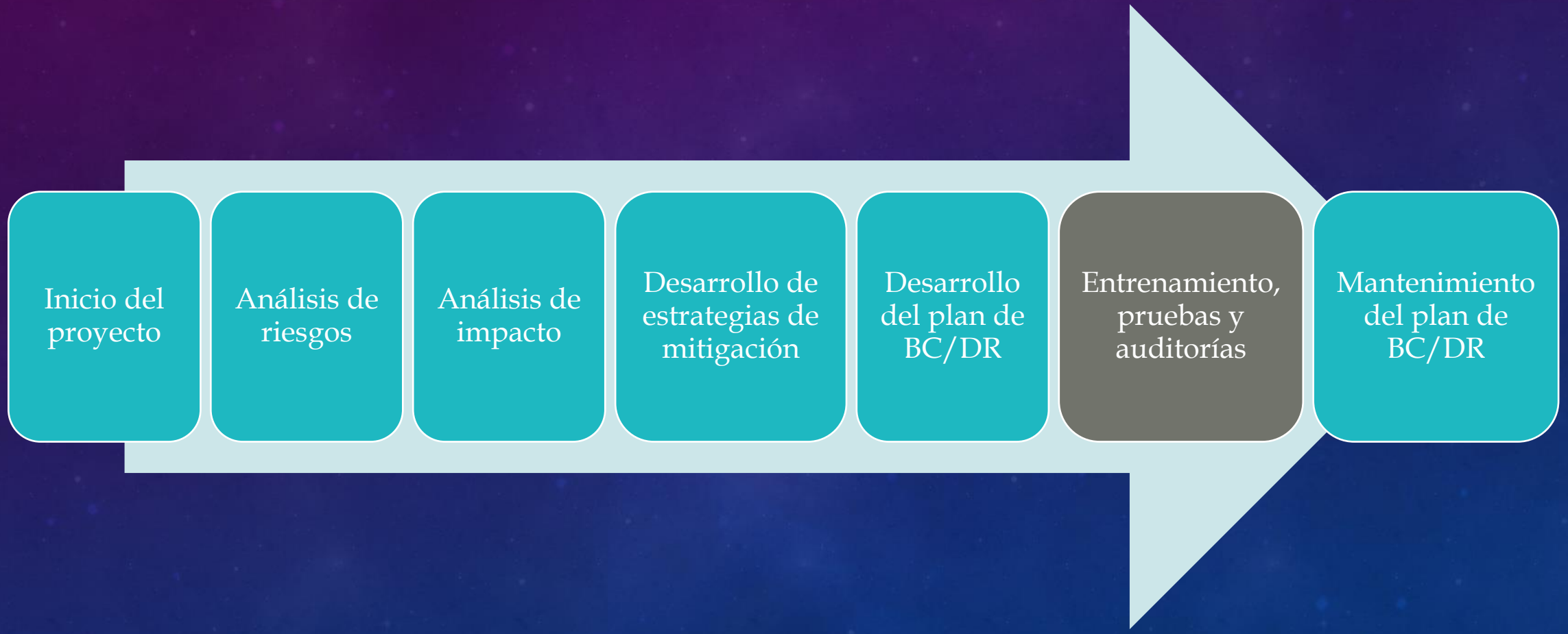
- Capacitación para respuesta a emergencias, recuperación ante desastres y continuidad del negocio
- Pruebas del plan de continuidad del negocio y recuperación ante desastres
- Realización de auditorías de sistemas de TI

INTRODUCCIÓN

Si el plan de BC/DR no se mantiene actualizado y no es entendido por todos los que puedan participar en la respuesta a una emergencia y su recuperación se vuelve **inútil**.

Por eso es crítico el entrenamiento periódico, pruebas y auditoría del plan como parte de las tareas administrativas regulares.

INTRODUCCIÓN



ENTRENAMIENTO PARA RECUPERACIÓN DE DESASTRES Y CONTINUIDAD DEL NEGOCIO

Dos enfoques del entrenamiento BC/DR:

- Respuesta física ante una emergencia.
- Implementación del plan BC/DR.

El entrenamiento en recuperación de desastres (DR) y continuidad del negocio (BC) se enfoca en dos áreas. La primera es cómo reaccionar físicamente ante emergencias (como incendios o inundaciones). La segunda es entrenar a los equipos responsables de implementar el plan de BC/DR, asegurando que tengan las habilidades necesarias para restaurar sistemas y seguir protocolos.

RESPUESTA ANTE EMERGENCIAS

- El equipo de respuesta ante emergencias (ERT) debe estar identificado y entrenado.
- Especialización según la ubicación y riesgos.
- Capacitación en primeros auxilios y RCP.

Cada empresa debe contar con un equipo de respuesta ante emergencias (ERT) entrenado en las actividades necesarias según los riesgos geográficos (inundaciones, terremotos, etc.). Además, es recomendable incluir capacitación en primeros auxilios y RCP para todos los empleados.

PLANIFICACIÓN DEL ENTRENAMIENTO BC/DR

- Definir objetivos y alcances.
- Evaluar necesidades de capacitación.
- Desarrollar, programar y monitorear el entrenamiento.

El entrenamiento para BC/DR debe seguir un enfoque estructurado. Primero se definen los objetivos, luego se realiza un análisis de necesidades para detectar brechas de habilidades, se desarrolla el plan de entrenamiento, y finalmente se monitorea la efectividad de este proceso.

ALCANCE Y OBJETIVOS DEL ENTRENAMIENTO

- El entrenamiento debe estar alineado con el plan BC/DR.
- Definir cronogramas y objetivos para cada equipo.
- Considerar entrenamiento cruzado para roles múltiples.

El plan de entrenamiento debe estar alineado con el plan de BC/DR, asignando objetivos específicos a cada equipo, como el equipo de respuesta ante crisis (CMT) o el equipo de recuperación de desastres. El cronograma debe considerar las responsabilidades cruzadas de algunos miembros que pertenezcan a varios equipos.

A continuación un ejemplo…

ALCANCE Y OBJETIVOS DEL ENTRENAMIENTO

Entrenamiento del Equipo de Respuesta a Incidentes de Computación (CIRT)

Alcance: Capacitar a todos los administradores de red para monitorear el tráfico en busca de problemas de seguridad. No incluye la configuración de auditorías o habilitación de archivos de log.

Objetivos:

1. Desarrollar conciencia sobre amenazas de seguridad actuales.
2. Entender qué archivos de log monitorear.
3. Identificar qué buscar en los archivos de log.
4. Saber investigar entradas sospechosas en los logs.
5. Responder a actividad sospechosa en la red.

Cronograma:

- Capacitación inicial dentro de 30 días.
- Sesión inicial de 2 horas.
- Refrescos trimestrales de 30 minutos.

Requisitos:

1. Localizar información sobre amenazas y tendencias.
2. Ubicar archivos de log especificados.
3. Interpretar entradas de log.
4. Detectar tendencias.
5. Tomar acciones ante actividad sospechosa.

EVALUACIÓN DE NECESIDADES DE CAPACITACIÓN

- Análisis de brechas de habilidades.
- Identificación de nuevas habilidades requeridas durante las pruebas del plan.
- Evaluaciones periódicas de las habilidades del personal.

Un análisis de brechas de habilidades permite identificar las áreas donde el equipo necesita entrenamiento adicional. Este análisis debe actualizarse periódicamente para asegurar que el personal esté preparado para implementar el plan BC/DR.

DESARROLLO DEL ENTRENAMIENTO

- Capacitación específica y medible.
- Uso de materiales variados (teoría, práctica, ejercicios).
- Importancia de la experiencia práctica.

El entrenamiento debe tener resultados medibles. Para asegurar la absorción de conocimientos, se deben usar diferentes métodos de enseñanza, como clases teóricas, ejercicios prácticos, y simulaciones. Una evaluación final debe verificar que los empleados comprendan los conceptos clave.

No todo el entrenamiento es igual, no es lo mismo entrenar a alguien sobre presionar un botón y parar una máquina que entrenar a alguien para restaurar un sistema que puede tener varios componentes.

PROGRAMACIÓN Y ENTREGA DEL ENTRENAMIENTO

- Desafíos en la programación del entrenamiento.
- Uso de sistemas de aprendizaje flexibles (online o presenciales).
- Importancia de verificar la calidad del entrenamiento.

Programar el entrenamiento puede ser un desafío. Las empresas pueden optar por sistemas flexibles de aprendizaje en línea, pero es importante verificar la calidad de estos programas y que el personal haya aprendido los conceptos clave.

MONITOREO Y MEDICIÓN DEL ENTRENAMIENTO

- Desarrollo de objetivos claros.
- Verificación de habilidades con pruebas teóricas y prácticas.
- Seguimiento de asistencia y cumplimiento del entrenamiento.

Para garantizar la efectividad del entrenamiento, es fundamental desarrollar objetivos claros y evaluar las habilidades adquiridas a través de exámenes y demostraciones prácticas. También se debe monitorear la asistencia y actualizar el entrenamiento según sea necesario.

ENTRENAMIENTO Y PRUEBAS PARA EL PLAN DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRES

Existen cuatro métodos básicos para entrenar al personal y, al mismo tiempo, probar el plan de BC/DR:

- Ejercicios en papel o de escritorio (paper walk-throughs)
- Ejercicios funcionales (functional exercises)
- Ejercicios en campo (field exercises)
- Interrupciones completas (full interruptions)

Los cuatro métodos principales para entrenar al personal y probar los planes de continuidad y recuperación de desastres. Los métodos varían en complejidad, desde simulaciones simples en papel hasta interrupciones completas de las operaciones para verificar la preparación ante emergencias.

ELEMENTOS CLAVE DEL ENTRENAMIENTO PARA LOS PLANES DE BC/DR

- El entrenamiento debe asegurar que los líderes del equipo sepan:
- Cómo y cuándo activar el plan.
- Notificar, reunir y gestionar a sus equipos.
- Operar como parte de un equipo multidisciplinario.
- Comunicar efectivamente en situaciones de estrés.

Estos son los aspectos fundamentales que los líderes del equipo deben dominar para manejar eficazmente una crisis. El entrenamiento se enfoca en habilidades críticas como la activación del plan, la gestión del equipo y la comunicación efectiva bajo presión.

EL PAPEL DEL ENTRENAMIENTO EN BC/DR

- El entrenamiento tiene dos objetivos principales:
- Familiarizar al personal con el plan de BC/DR.
- Reforzar el conocimiento de los procedimientos básicos.

El propósito del entrenamiento no es solo que los empleados conozcan el plan, sino que también estén capacitados para aplicarlo en una emergencia, asegurando que todos los procedimientos sean claros y comprendidos por el personal.

ENTRENAMIENTO PERSONALIZADO PARA ROLES ESPECÍFICOS

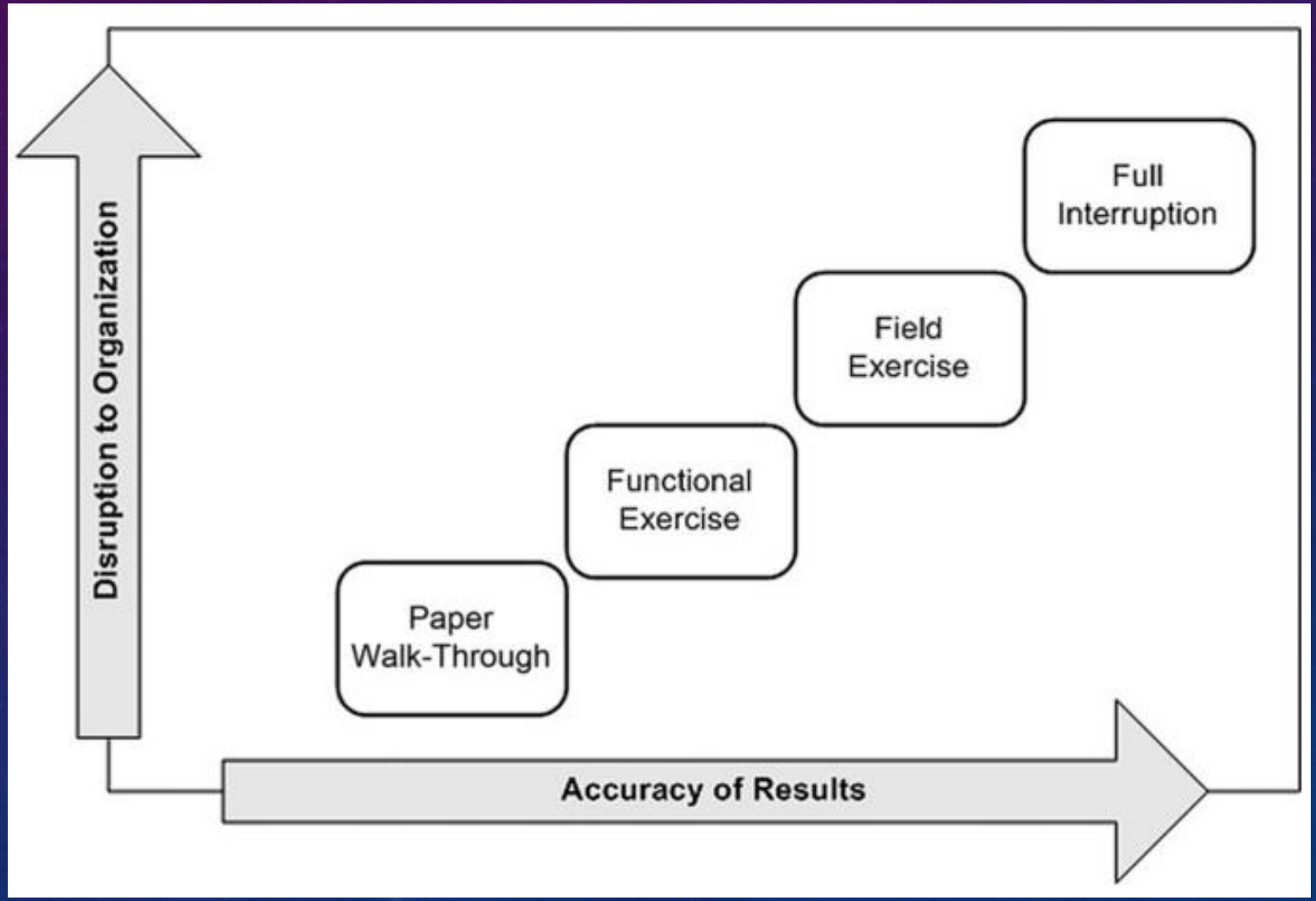
- El entrenamiento debe ser específico para los roles de los participantes. Por ejemplo:
  - Un administrador de bases de datos (DBA) necesita capacitación en evaluación de daños en TI.
  - Un coordinador de crisis debe aprender a utilizar equipo de comunicación de emergencia.

El entrenamiento debe adaptarse a las responsabilidades específicas de cada rol. Cada miembro del equipo tiene tareas únicas en una emergencia y requiere la capacitación adecuada para cumplir con sus funciones durante la crisis.

TRABAJO EN EQUIPO MULTIDISCIPLINARIO EN BC/DR

- El equipo de gestión de crisis (CMT) puede incluir líderes de diferentes departamentos que normalmente no interactúan entre sí.
  - Durante una crisis, es probable que los equipos de diversos departamentos deban trabajar juntos de manera fluida. Es importante que todos los líderes estén familiarizados con la estructura de mando y sepan cómo colaborar con otros, independientemente de sus roles habituales.
- La comunicación durante una crisis puede requerir la implementación de planes de contingencia si las herramientas tradicionales de comunicación no están disponibles.
  - La comunicación efectiva es esencial en una crisis. Es importante tener planes alternativos de comunicación en caso de que las herramientas tradicionales, como teléfonos o correos electrónicos, no estén disponibles durante la emergencia.

MÉTODOS DE PRUEBAS DEL PLAN: DISRUPCIÓN VS EXACTITUD



MÉTODOS DE ENTRENAMIENTO: EJERCICIOS EN PAPEL

- Este método de entrenamiento involucra una revisión detallada del plan de BC/DR en un entorno de oficina, donde los participantes discuten cada paso del plan sin activarlo realmente.

Este tipo de ejercicio permite a los equipos repasar el plan sin realizar interrupciones operativas. Es un método sencillo y eficaz para asegurarse de que todos comprendan sus roles y las acciones necesarias ante una emergencia.

MÉTODOS DE ENTRENAMIENTO: EJERCICIOS EN PAPEL

Existen ocho pasos discretos que puedes seguir para realizar una caminata en papel efectiva. Estos pasos también se aplican a otros tipos de entrenamiento (funcional, de campo, etc.).

1. Desarrollar Escenarios Realistas

   Crea escenarios basados en los riesgos determinados por tu evaluación que tengan la mayor probabilidad e impacto. Comienza con un incendio en el edificio, ya que estadísticamente es el desastre más probable que afecta a las empresas.

2. Desarrollar Criterios de Evaluación

   Define criterios para evaluar el éxito del entrenamiento, tales como:

   - Cómo siguieron los participantes el plan.
   - La comunicación entre los equipos.
   - Efectividad de las listas de verificación.
   - Confianza de los participantes en la implementación del plan.

3. Proporcionar Copias del Plan

   Entrega las copias más recientes del plan a los miembros del equipo antes de la caminata. Considera crear un diagrama de flujo para ayudar a los miembros a entender su rol dentro del plan (ver imagen siguiente).

4. Dividir a los Participantes por Equipos

   Si hay miembros de diferentes equipos, agrúpalos para facilitar la comunicación y reducir interrupciones.

5. Usar Listas de Verificación

   Proporciona copias de las listas de verificación de los procesos clave para asegurar que se mantenga la dirección durante la caminata.

6. Tomar Notas

   Asigna a alguien la tarea de llevar notas sobre el flujo general, niveles de preparación, brechas en el plan, etc.

7. Identificar Necesidades de Entrenamiento

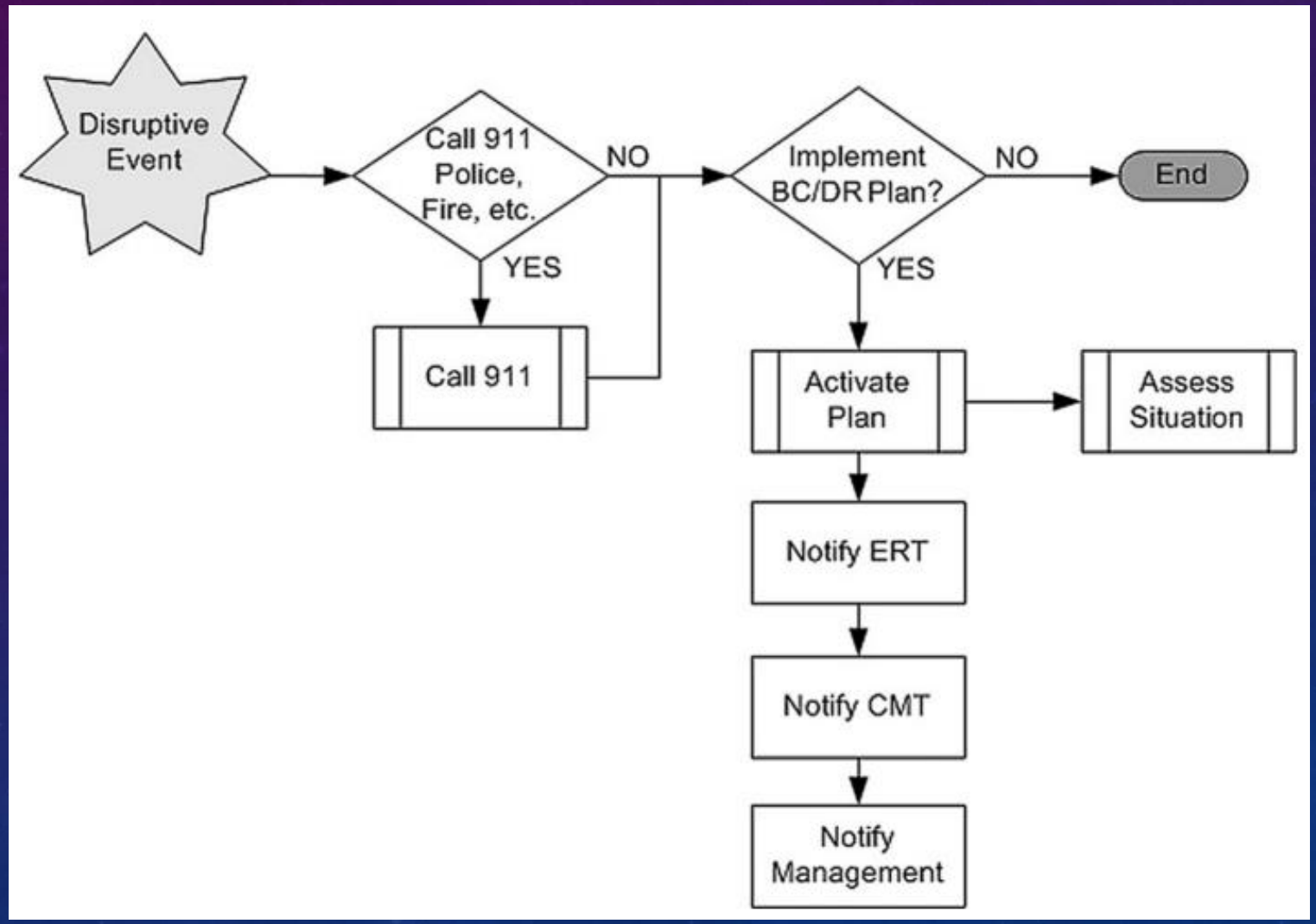
   Mantén un registro de las habilidades que los participantes consideran necesarias para implementar el plan de manera efectiva.

8. Desarrollar Resumen y Lecciones Aprendidas

   Compila y resume las notas recogidas, programando una reunión de seguimiento para discutir los resultados y las lecciones aprendidas.

MÉTODOS DE ENTRENAMIENTO: EJERCICIOS EN PAPEL

Ejemplo parcial de un flujo de proceso del plan de BC/DR



MÉTODOS DE ENTRENAMIENTO: EJERCICIOS FUNCIONALES

Se utilizan para probar realmente algunas de las funcionalidades del plan. A menudo es útil y adecuado realizar una revisión en papel junto con ejercicios funcionales. Estos entrenan al personal en procedimientos críticos o funciones necesarias para responder y manejar la interrupción.

- Suelen utilizar guiones basados en escenarios y tienen una duración de 2-3 horas.
- El equipo se divide en dos grupos: el equipo principal y los alternos. Los alternos sirven como un segundo grupo para fines de entrenamiento.
- Un guion inicia la secuencia de eventos, que típicamente toma unos 15-20 minutos.
- Los equipos (ERT y CMT) deben responder a los eventos guionizados utilizando su entrenamiento y el plan BC/DR.
- Los alternos actúan como empleados comunes, simulando comportamientos como el pánico o no seguir instrucciones, o pueden tener lesiones simuladas que el equipo de respuesta debe atender.
- El objetivo es que los miembros trabajen en equipo, comprendan sus roles y responsabilidades, y se comuniquen eficazmente bajo condiciones de estrés.
- Se deben definir los objetivos específicos de un ejercicio, por ejemplo:
    - Determinar cuándo es necesario restaurar una base de datos.
    - Acceder a respaldos en bóvedas de datos remotas.
    - Restaurar los datos y verificar la restauración (nombre de archivos, tamaños, ubicaciones).
    - Probar funciones específicas del plan BC/DR mediante instrucciones paso a paso.

Los ejercicios funcionales son una excelente herramienta de entrenamiento y ayudan a probar las capacidades del equipo bajo condiciones simuladas.

MÉTODOS DE ENTRENAMIENTO: EJERCICIOS DE CAMPO

Implican simulaciones bastante realistas basadas en escenarios probables. Estos ejercicios son similares a los que realizan los equipos de respuesta a emergencias en situaciones simuladas, que muchas veces se ven en las noticias locales. Si deseas practicar tu respuesta ante emergencias y recuperación de desastres con ejercicios a gran escala, podrías coordinar estos ejercicios con los equipos de respuesta a emergencias locales.

Beneficios:

- Los equipos de respuesta a emergencias locales pueden estar dispuestos a participar, brindando una excelente oportunidad para probar y afinar habilidades.
- Estos ejercicios no solo pondrán a prueba las habilidades del equipo, sino que también proporcionarán retroalimentación valiosa para la planificación de desastres.

Consideraciones:

- Muchas empresas apenas tienen tiempo o recursos para realizar una revisión anual en papel de su plan, por lo que puede ser difícil realizar un escenario realista completo.
- Sin embargo, si tu empresa trabaja en una industria peligrosa (químicos peligrosos, explosivos, energía, etc.), podrías querer (o estar legalmente obligado) a realizar ejercicios en campo para evaluar y mejorar la preparación.
- Aunque los recorridos en papel y los ejercicios funcionales son útiles, pueden dejar brechas de conocimiento o problemas en el plan que solo se detectan ante una situación real.
- Los ejercicios en campo pueden reducir el riesgo de estas brechas, pero requieren una inversión significativa de tiempo y recursos.
- Para algunas empresas, esta inversión es justificada.

MÉTODOS DE ENTRENAMIENTO: PRUEBA DE INTERRUPCIÓN TOTAL

Al igual que un ejercicio en campo, una prueba de interrupción total puede aplicarse a toda la organización o a sistemas específicos dentro de ella.

Objetivo: Activar todos los componentes del plan y detener todas las funciones críticas de la empresa.

- Incluye la activación de sitios de trabajo alternativos, instalaciones fuera de la sede y almacenamiento externo.
- Puede ser una prueba **anunciada** o **no anunciada**.
  - Las pruebas **no anunciadas** simulan de manera más realista una interrupción o desastre, pero son más disruptivas.
- La mayoría de las empresas son reacias a interrumpir sus operaciones lo suficiente para realizar una prueba completa.
- Sin embargo, en algunas situaciones, interrumpir una unidad de negocio puede ser aceptable para lograr una preparación más realista.

PRUEBAS DEL PLAN DE BC/DR

Razones para probar el plan:

- Asegurar que el plan funcionará en una interrupción real.
- Verificar la comprensión de los procesos por los implementadores del plan.
- Validar la integración de tareas entre unidades de negocio y funciones de gestión.
- Confirmar los pasos desarrollados para cada fase de implementación.
- Identificar los recursos necesarios.
- Familiarizar a las partes involucradas con el flujo de información.
- Detectar fallos o debilidades en el plan.
- Evaluar costos y factibilidad.

COMPRENSIÓN DE LOS PROCESOS

- Las pruebas deben asegurar que los miembros del equipo entiendan los procesos, procedimientos y pasos del plan.
- Deben descubrir procesos faltantes y confirmar dependencias.
- Las funciones críticas deben restaurarse primero, y el plan debe priorizarlas adecuadamente.
- Entender los procesos también incluye el entender las soluciones alternativas y procesos manuales que deben ser implementados durante la recuperación y continuidad del negocio.
  - Y estos deben ser probados.

VALIDACIÓN DE LA INTEGRACIÓN DE TAREAS

- Las pruebas deben involucrar al personal clave de funciones críticas y al equipo de BC/DR.
- Los expertos deben verificar la secuencia correcta de tareas, dependencias y recursos.
- La falta de integración de tareas puede ocasionar un fallo en la implementación del plan.
- **Ejemplo:** Identificar tareas de recuperación de sistemas IT y su interdependencia con otros sistemas y procesos.

CONFIRMACIÓN DE LOS PASOS

- La prueba debe confirmar que los pasos necesarios están listados y en el orden correcto.
- Las pruebas paso a paso ayudan a descubrir errores u omisiones.
- **Ejemplo:** Verificar que el orden de los pasos para iniciar un servicio de TI sea lógico y ejecutable.

CONFIRMACIÓN DE LOS RECURSOS

- Durante las pruebas, es clave preguntar: "¿Qué recursos son necesarios para ejecutar este paso?"
- Recursos pueden incluir personal, habilidades, equipos y suministros.
- **Ejemplo:** Asegurar que dos equipos no requieran simultáneamente los mismos recursos.

FAMILIARIZACIÓN CON EL FLUJO DE INFORMACIÓN

- Las comunicaciones son críticas durante interrupciones.
- Las pruebas identifican quién necesita qué información y cuándo, además de identificar cómo se mueve.
- También debemos identificar cómo fluyen los datos a través de los sistemas de TI para poder estar seguros que un servicio estará realmente funcionando con los datos que necesita.
- **Ejemplos:**
  - Verificar cómo se intercambia información entre equipos de respuesta ante emergencias.
  - Verificar cómo fluyen los datos para alimentar un sistema de venta en línea.

IDENTIFICACIÓN DE DEBILIDADES

- Las pruebas con listas de verificación y simulaciones revelan fallos o debilidades.
- Los escenarios realistas ayudan a detectar problemas que no aparecen en teoría.
- **Ejemplos:**
  - Descubrir omisiones como números de contacto
  - Licencias necesarias para la recuperación
  - Máquinas virtuales que no funcionan correctamente en servidores de recuperación

EVALUACIÓN DE COSTOS Y FACTIBILIDAD

- Las pruebas ayudan a comprender mejor los costos de implementación del plan.
- Identificar la factibilidad de los pasos del plan en situaciones reales.
- Ejemplos:
  - Determinar si un proveedor hará cargos extras por tareas no descritas detalladamente en un contrato.
  - Gastos adicionales de transporte, alimentación, etc.

CRITERIOS DE EVALUACIÓN

- Crear criterios claros para evaluar las pruebas.
- Utilizar preguntas para evaluar la efectividad de cada fase del plan.
- Se puede utilizar las listas o pasos del plan de BC/DR para generar los criterios.
- Ejemplo:
  1. ¿Pudo el miembro principal del equipo comenzar el proceso de notificación con éxito?
  2. ¿Cuántos miembros del equipo fueron contactados?
  3. ¿Cuánto tiempo tomó notificar a los miembros del equipo?
  4. ¿Faltaban números de teléfono o había números incorrectos?
  5. ¿Cuántos miembros del equipo fueron contactados a través de sus métodos principales vs. métodos alternativos?
  6. ¿Cuántos miembros del equipo no estaban en la lista de notificación?
  7. ¿Había nombres en la lista de notificación que no debían estar?
  8. ¿Funcionaría esto si los sistemas telefónicos estuvieran fuera de servicio?

RECOMENDACIONES BASADAS EN RESULTADOS DE PRUEBAS

- Desarrollar recomendaciones a partir de los resultados de las pruebas.
- Las recomendaciones pueden implicar modificaciones al plan o entrenamiento adicional.
- Ejemplo:
  - Actualización de listas de contacto o inclusión de nuevas áreas de negocio en el plan.
  - Verificación de medios alternos de comunicación.

REALIZACIÓN DE AUDITORÍAS DE SISTEMAS Y SEGURIDAD DE TI

- **Una auditoría es un examen sistemático basado en criterios definidos**.
- Cumplimiento de leyes o regulaciones
  - Si la empresa debe cumplir con leyes o normativas, seguramente ha pasado por auditorías rigurosas.
- Relación con BC/DR
  - Las auditorías que se realizan para cumplir con normativas pueden ser útiles en la planificación de BC/DR y deben incluirse en el plan.
- Una auditoría debe incluir tanto la continuidad del negocio como auditorías de sistemas.
- Ejemplo:
  - Si tu empresa debe cumplir con los estándares ISO/IEC 27001 (Seguridad de la información) o el Decreto 22-2008 (Ley de acceso a la información pública), los planes de BC/DR deben abordar estos temas y la auditoría del plan debe incluir esos parámetros.

AUDITORÍAS DE SISTEMAS DE TI Y SEGURIDAD

Las auditorías de sistemas de TI implican un conjunto de tareas que ayudan a reducir el riesgo de intrusión o ataque. Las auditorías se centran principalmente en asegurar la confidencialidad, integridad y disponibilidad de los datos de la empresa, áreas que comúnmente son blanco de ataques.

EVALUACIÓN SISTEMÁTICA DE SEGURIDAD

- Una auditoría de sistemas de TI se enfoca en:
  - Evaluar la seguridad de varios sistemas de TI.
  - Revisar la configuración física y del entorno de la red.
  - Revisar la configuración del software y el manejo de datos, especialmente los sensibles.
  - Verificar los controles de accesos de los usuarios.
- Estas están asociadas al cumplimiento de estándares por temas legales o exigencias de clientes.
  - Se recomienda realizar auditorías de este tipo incluso si no fuese obligatorio.

FORTALECIMIENTO DE LA SEGURIDAD DE LOS SISTEMAS

El fortalecimiento de la seguridad de los sistemas es una estrategia de mitigación de riesgo que minimiza el área de ataque mediante:

- Eliminación de protocolos de red no utilizados.
- Desactivación de puertos y servicios no utilizados.
- Reducción de permisos al mínimo necesario.
- Eliminación de usuarios no utilizados.
- Automatización de actualizaciones de antivirus y antispyware.
- Etcétera.

AUDITORÍA DEL PLAN BC/DR

La auditoría de sistemas en la planificación BC/DR incluye:

- Asegurar que las estrategias de mitigación de riesgos de TI estén implementadas y configuradas correctamente.
- Asegurar que los sistemas identificados en el plan de BC/DR sigan en funcionamiento y operativos.
- Identificar áreas donde se haya implementado nueva tecnología y que puede no estar incorporada en el plan de BC/DR.
- Identificar áreas donde la tecnología ha sido retirada o modificada, lo que resulta en la necesidad de revisar el plan de BC/DR.
- Revisar los procesos identificados en el plan de BC/DR en relación con los sistemas de TI para garantizar que los pasos y procesos sean aún correctos, completos y relevantes.
- Verificar que el equipo de respuesta a incidentes de TI (CIRT, CERT, o cualquier otro término utilizado) esté operativo y tenga una comprensión clara de roles, responsabilidades y cómo implementar los segmentos específicos de TI del plan de BC/DR.
- Revisar los datos de varios sistemas para garantizar que aún cumplan con los planes de BC/DR. Estos sistemas incluyen sistemas operativos, equipos de redes y telecomunicaciones, bases de datos y aplicaciones, respaldos de sistemas, controles de seguridad, integración y pruebas. Cualquiera de estas áreas está sujeta a cambios frecuentes. Una auditoría puede ayudar a asegurar que el plan de BC/DR funcionará si se implementa

IMPORTANCIA DE LA AUDITORÍA PERIÓDICA

- Las auditorías periódicas son una excelente práctica para mantener actualizado el plan BC/DR.
- Es más sencillo añadir pasos a las auditorías regulares que realizar una auditoría BC/DR separada.
- También facilita encontrar cambios graduales que pueden impactar significativamente la implementación del plan BC/DR.