Plan de Continuidad del Negocio y Plan de Respuesta a Incidentes

Ciberseguridad – FPUNA

Clase 2024-05-09

Seguridad de la Información

- La protección de los activos de Información va más allá del Plan de Seguridad de la Información. Implica planificar y desplegar varias acciones para que el Plan de Seguridad de la Información sea consistente.

Seguridad de la Información

Plan de Seguridad de la Información

Plan de Continuidad del Negocio

Plan de Respuesta a Incidentes

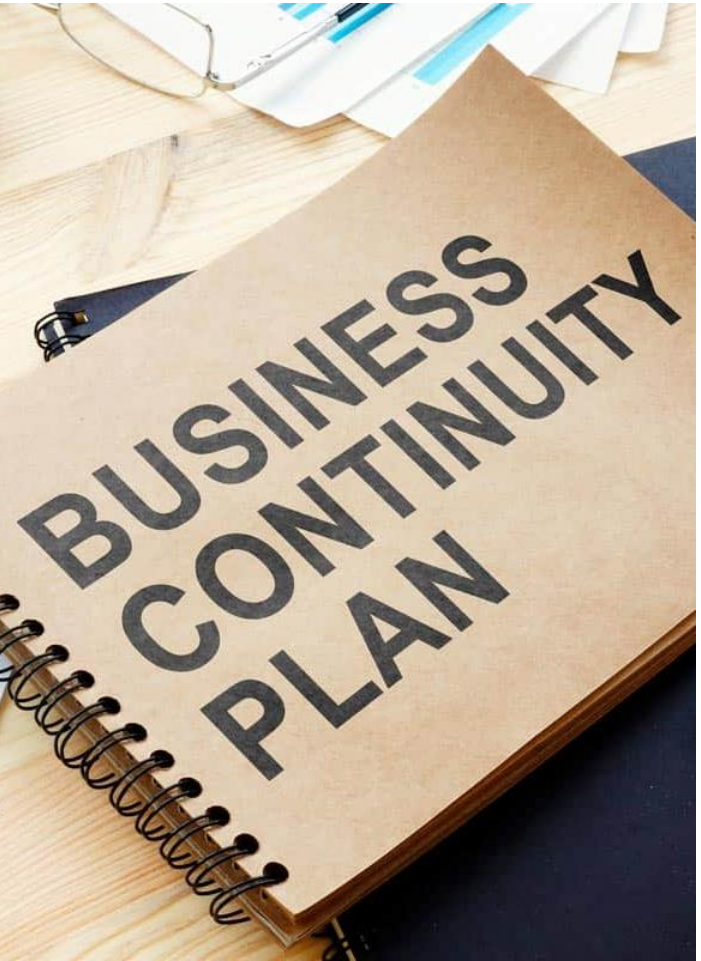
Plan de Gestión de Riesgos

Plan de Auditoría de Seguridad de la Información

Plan de Seguridad de la Información

- Define las políticas y procedimientos de seguridad que se deben seguir en la organización para proteger los activos de información. Incluye medidas de seguridad **físicas**, **técnicas** y **administrativas** que se deben implementar para proteger la información contra amenazas internas y externas.
- El estándar ISO 27001 establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) y proporciona un marco para la implementación de medidas de seguridad para proteger los activos de información de una organización.

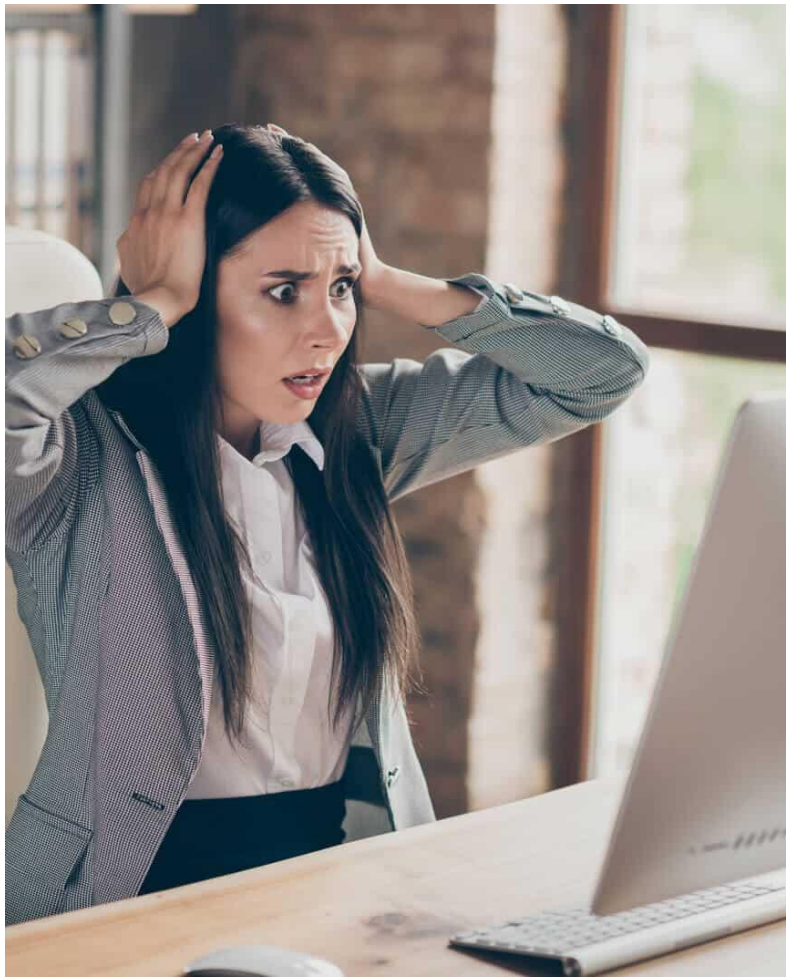
Plan de continuidad del negocio



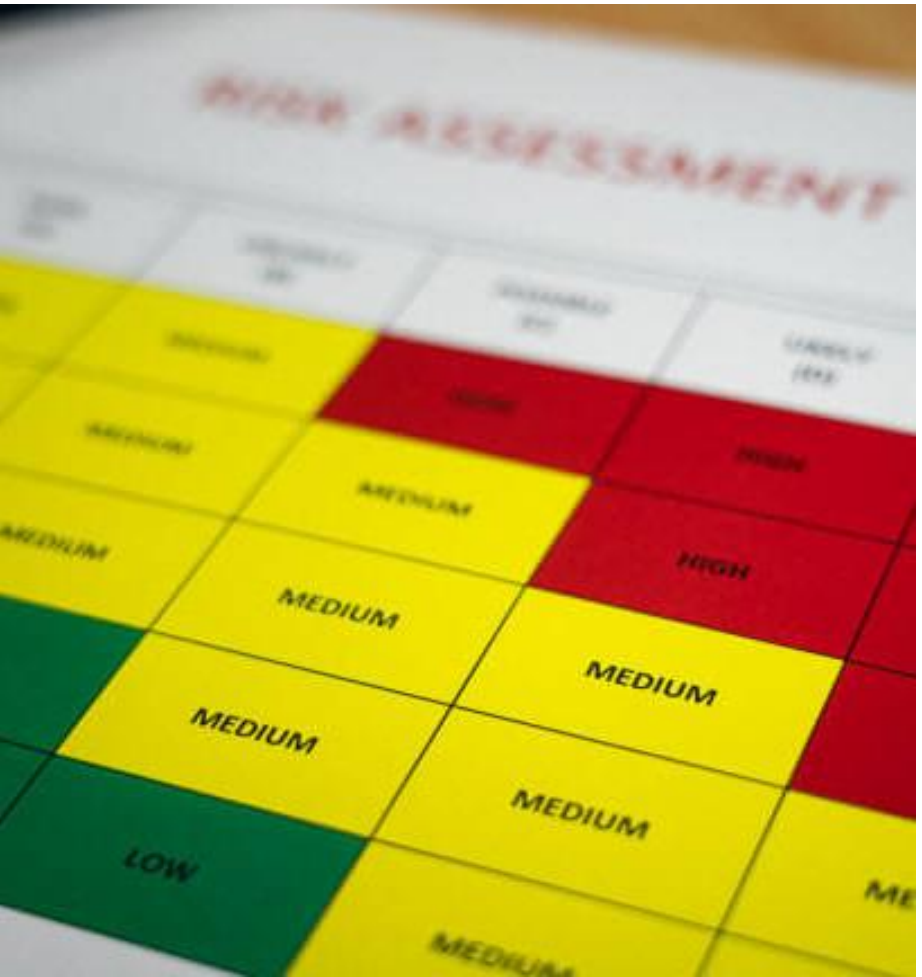
- Se enfoca en garantizar la continuidad del negocio en caso de interrupciones o desastres, incluyendo aquellos relacionados con la seguridad de la información. Define las medidas necesarias para minimizar los tiempos de recuperación y asegurar la disponibilidad de los sistemas y datos críticos.
- El estándar ISO 22301 establece los requisitos para un Sistema de Gestión de Continuidad de Negocio (SGCN) y proporciona un marco para garantizar la continuidad del negocio en caso de interrupciones.

Plan de respuesta a incidentes

- Establece el procedimiento a seguir en caso de que se produzca un incidente de seguridad, incluyendo la identificación, análisis, respuesta y recuperación. También puede definir los roles y responsabilidades de los miembros del equipo de respuesta a incidentes y los procedimientos de notificación de incidentes a las partes interesadas.
- El documento NIST SP 800-61 proporciona directrices para la respuesta a incidentes y establece un marco para la preparación, detección, análisis, contención, erradicación y recuperación de incidentes de seguridad de la información.



Plan de gestión de riesgos



- Se enfoca en identificar, evaluar y mitigar los riesgos asociados con la seguridad de la información. Incluye la implementación de medidas de seguridad adecuadas para reducir los riesgos identificados y el monitoreo continuo para detectar nuevas amenazas y vulnerabilidades.
- El estándar ISO 31000 establece los principios y directrices para la gestión de riesgos y proporciona un marco para la identificación, evaluación y tratamiento de los riesgos asociados con la seguridad de la información.

Plan de auditoría de seguridad de la información

- Establece los procedimientos para evaluar la efectividad de las medidas de seguridad de la organización y la conformidad con las políticas y estándares de seguridad establecidos. Puede incluir la realización de pruebas de penetración, evaluaciones de vulnerabilidades y revisiones de seguridad de los sistemas y procesos.
- El estándar ISO 27007 establece los requisitos para un programa de auditoría de seguridad de la información y proporciona un marco para la realización de auditorías de seguridad para evaluar la efectividad de las medidas de seguridad de la organización y la conformidad con las políticas y estándares de seguridad establecidos.

Plan de Continuidad del Negocio

Plan de Continuidad del Negocio

- Es un conjunto de medidas y acciones destinadas a garantizar la continuidad de las operaciones de una empresa en caso de un incidente de ciberseguridad. El objetivo principal del plan es **minimizar el impacto negativo** que un incidente de este tipo puede tener en la empresa, sus clientes y sus empleados.

¿Qué incluye el Plan de Continuidad del Negocio?

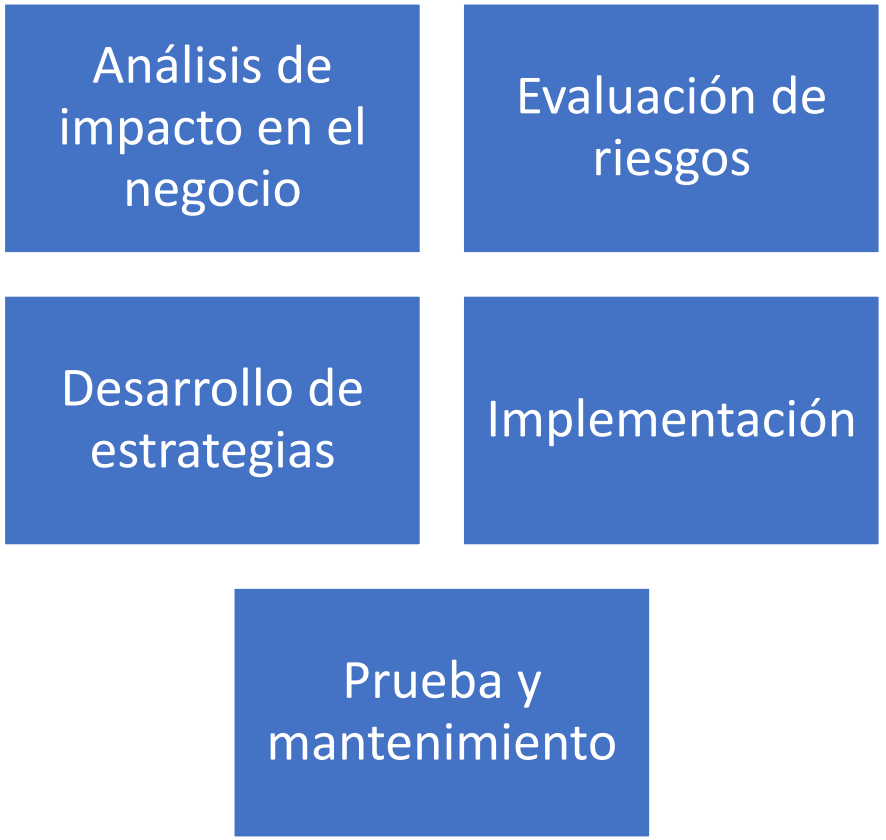
- Debe incluir
  - una **estrategia general** que identifique los sistemas y servicios críticos que deben estar disponibles en todo momento y las acciones necesarias para garantizar su disponibilidad.
  - la definición de los objetivos de recuperación, es decir, el tiempo máximo permitido para restaurar los sistemas y servicios críticos después de un incidente de ciberseguridad.
  - procedimientos detallados de recuperación y restauración de datos y sistemas críticos.
  - las personas responsables de la ejecución del plan, y
  - un plan de comunicación para mantener informados a los clientes y empleados.
- Es importante que el **plan sea probado y validado** regularmente mediante ejercicios de simulación para asegurarse de que sea efectivo y esté actualizado frente a las amenazas emergentes.

Fases generales de Implementación de un BCP

- Análisis de impacto en el negocio
- Evaluación de riesgos
- Desarrollo de estrategias
- Implementación
- Prueba y mantenimiento

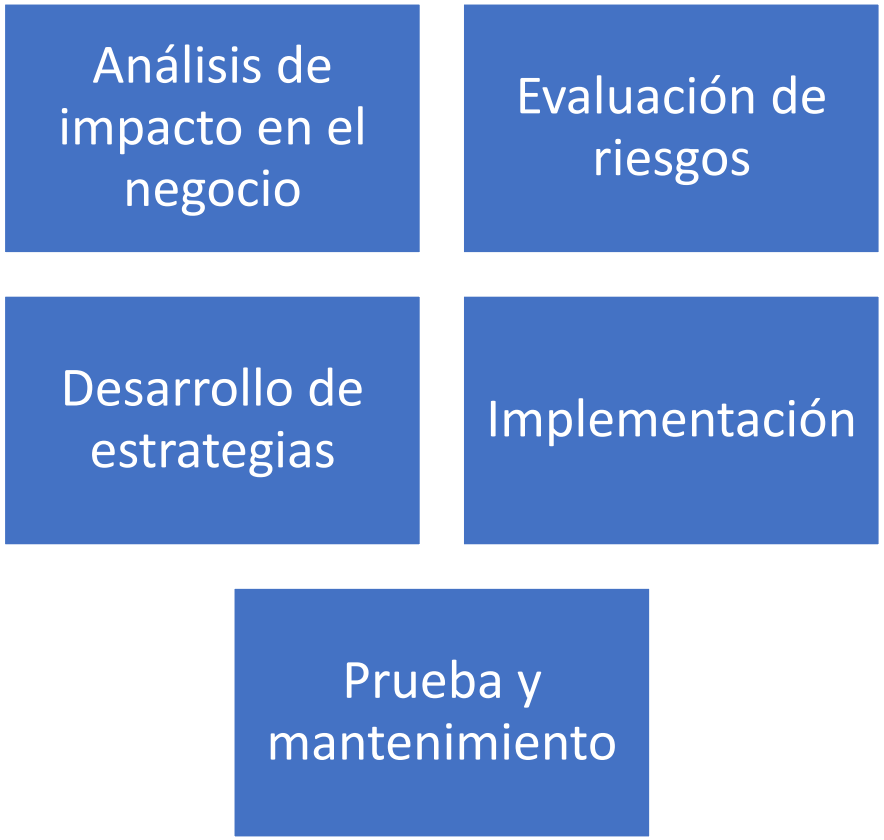
Análisis de impacto en el negocio

- Esta fase implica la identificación de los procesos críticos de la organización y los recursos necesarios para mantenerlos en funcionamiento. Se debe realizar un análisis detallado de los efectos potenciales de un evento de ciberseguridad en la organización, como la interrupción de servicios, la pérdida de datos, el daño a la reputación y las pérdidas financieras.



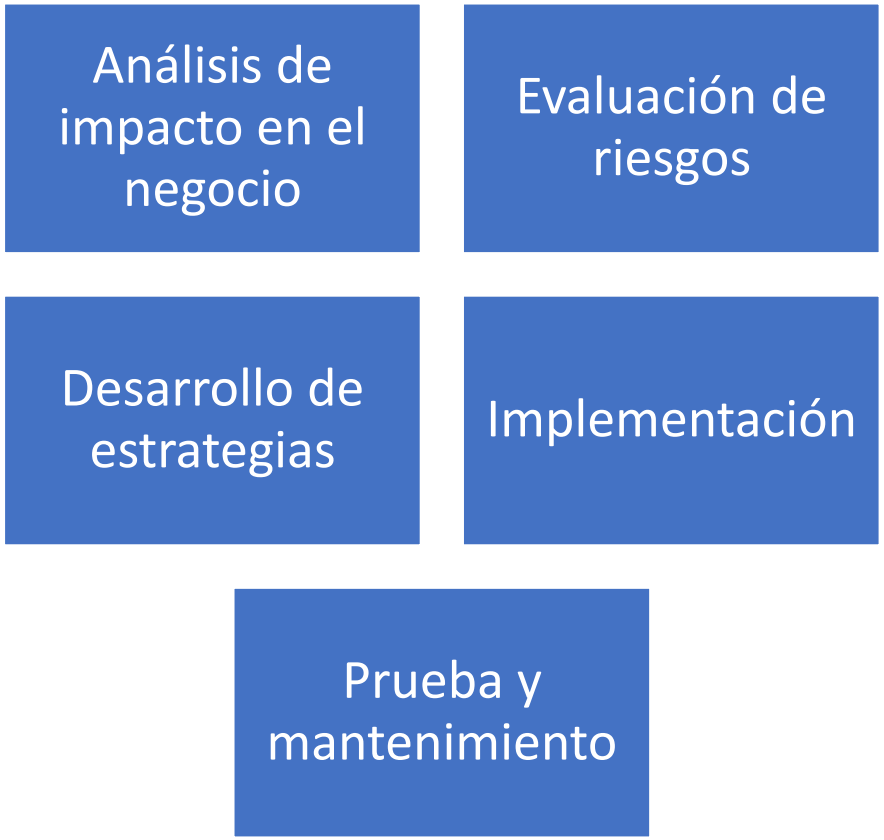
Evaluación de riesgos

- En esta fase se deben identificar las posibles amenazas y vulnerabilidades de la organización. Se deben evaluar los riesgos asociados con la ciberseguridad, como los ataques de malware, los ataques DDoS, la ingeniería social y la violación de datos.



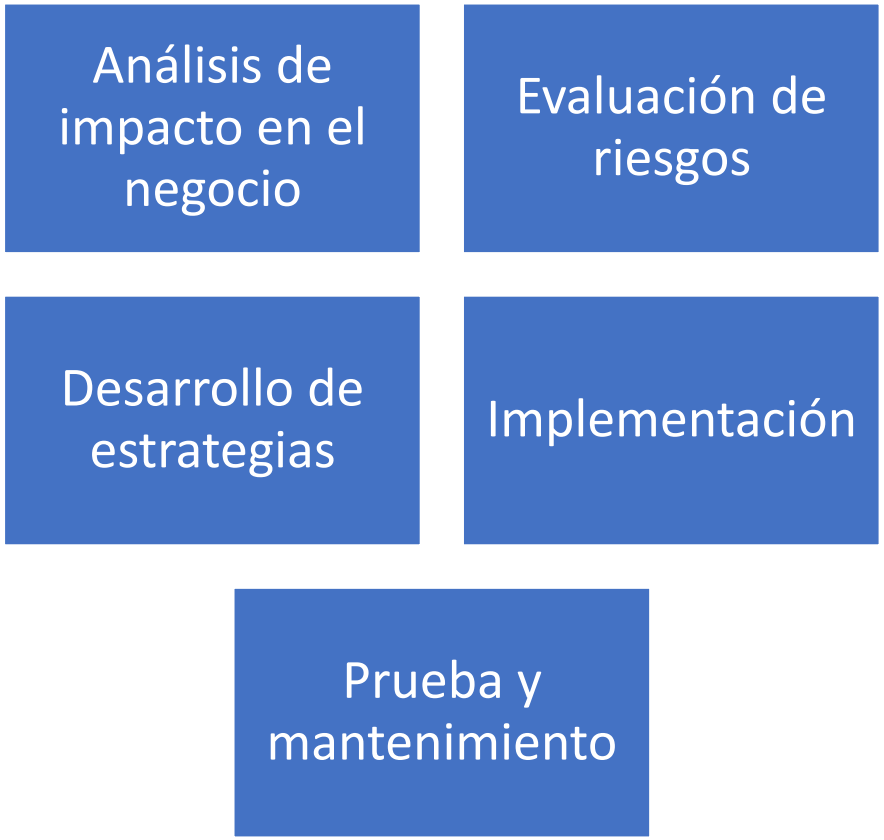
Desarrollo de estrategias

- Esta fase implica el desarrollo de estrategias de continuidad del negocio para hacer frente a los riesgos identificados. Se deben establecer planes detallados para la recuperación de sistemas y datos, la gestión de la comunicación, la continuidad de las operaciones y la gestión de crisis.



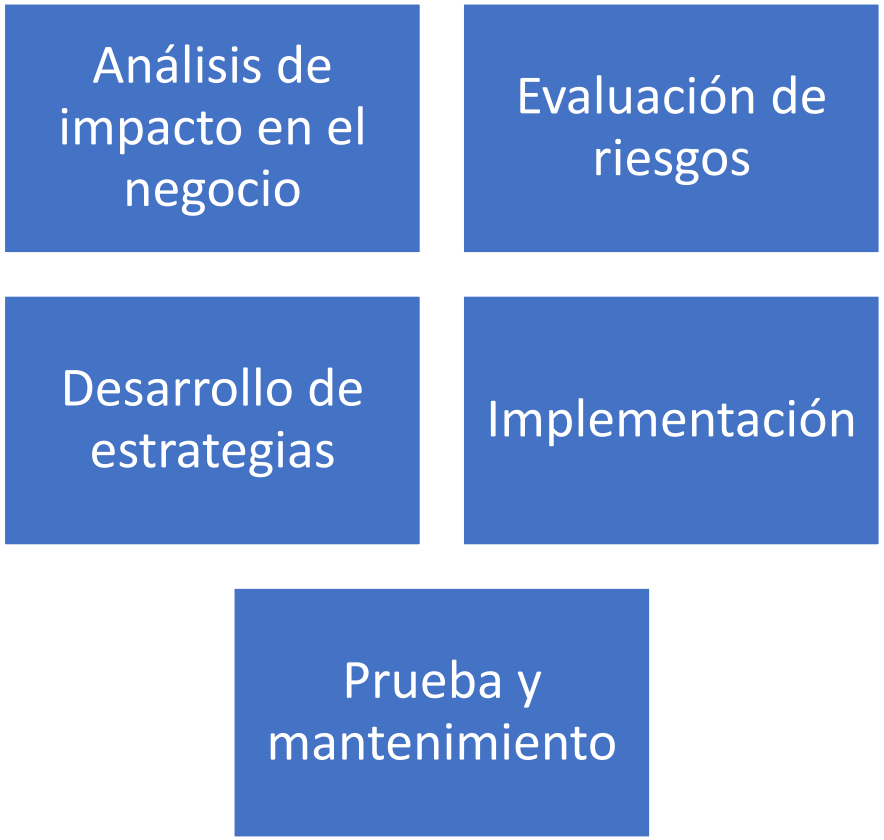
Implementación

- En esta fase se deben implementar las estrategias desarrolladas en la fase anterior. Esto puede incluir la instalación de medidas de seguridad de la información, la implementación de sistemas de recuperación de desastres y la realización de pruebas para asegurar que el plan sea efectivo.



Prueba y mantenimiento

- Esta fase implica la realización de pruebas y simulaciones regulares para asegurarse de que el BCP esté actualizado y sea efectivo. Los planes de continuidad del negocio deben ser revisados y actualizados periódicamente para adaptarse a los cambios en el entorno de seguridad de la información y a los riesgos emergentes.



Métricas para BCP

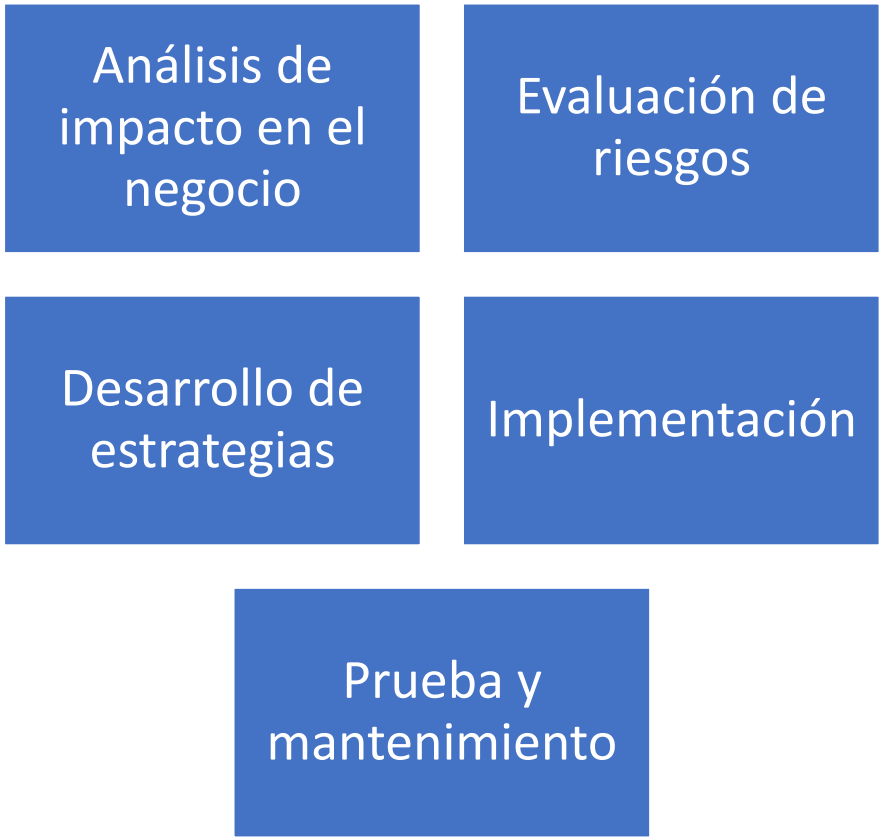
Métricas de plan de continuidad del negocio

1. **Tiempo de recuperación objetivo (RTO):** Esta métrica mide el tiempo objetivo que la organización se ha fijado para recuperar los servicios críticos del negocio después de un incidente. Un RTO más corto puede ayudar a minimizar el impacto del incidente en la continuidad del negocio.
2. **Tiempo de punto de recuperación objetivo (RPO):** Esta métrica mide el tiempo objetivo en el que la organización se ha fijado para restaurar los datos y la información crítica después de un incidente. Un RPO más corto puede ayudar a minimizar la pérdida de datos y la interrupción en el negocio.
3. **Nivel de servicio (SLA):** Esta métrica mide la calidad del servicio que la organización debe proporcionar después de un incidente y establece los objetivos de tiempo para la restauración de servicios críticos.

Ejemplo de Implementación de BCP

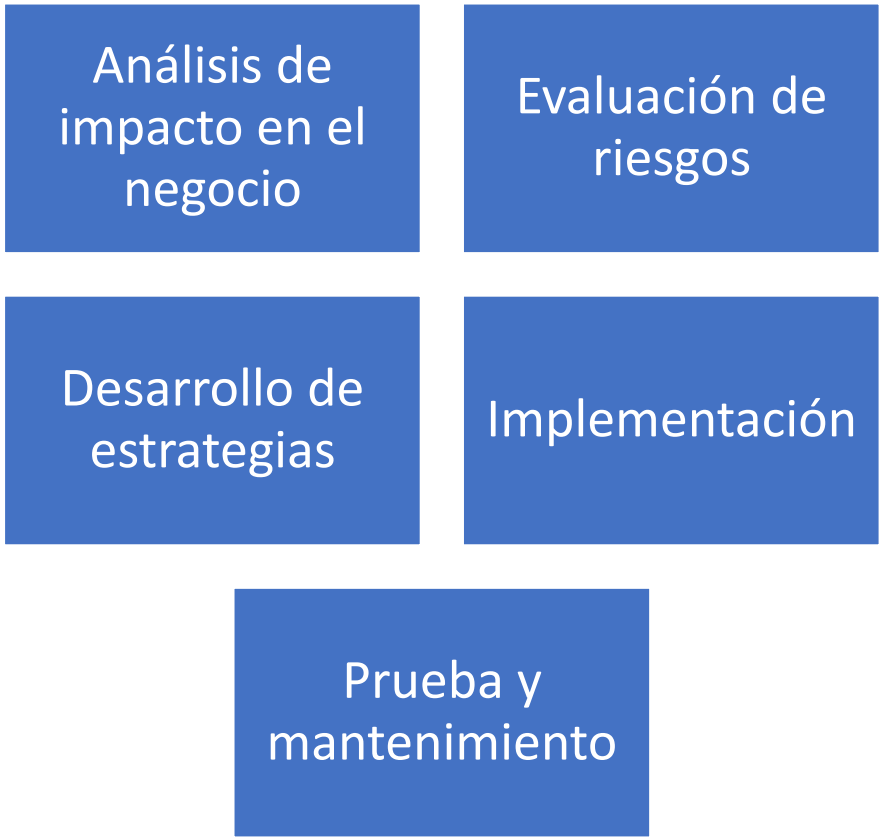
Análisis de impacto en el negocio (Ejemplo)

- Una organización de servicios financieros realiza un análisis de impacto en el negocio para identificar los procesos críticos y los recursos necesarios para mantenerlos en funcionamiento. Los procesos críticos identificados incluyen el procesamiento de transacciones de clientes y la gestión de datos financieros. Los recursos necesarios incluyen sistemas de información, personal clave y proveedores externos.



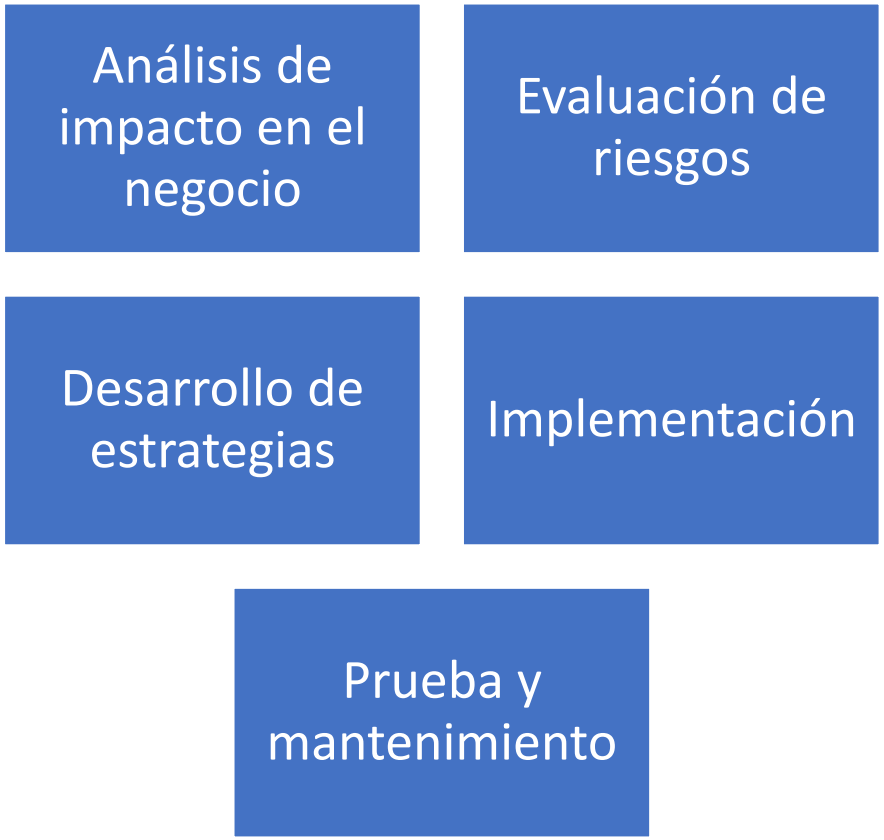
Evaluación de riesgos (Ejemplo)

- La organización realiza una evaluación de riesgos para identificar posibles amenazas y vulnerabilidades. Se identifican riesgos tales como ataques de malware, ataques de phishing y fallas en los sistemas de información.



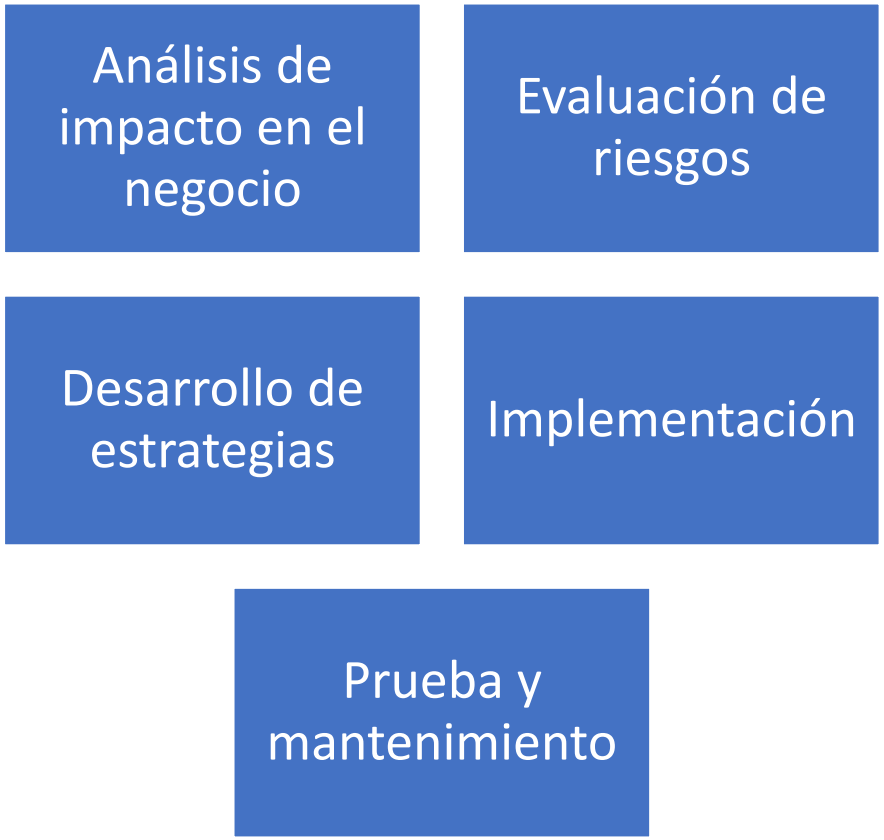
Desarrollo de estrategias (Ejemplo)

- La organización desarrolla estrategias de continuidad del negocio para hacer frente a los riesgos identificados. Se establecen planes detallados para la recuperación de sistemas y datos, la gestión de la comunicación con clientes y partes interesadas, la continuidad de las operaciones y la gestión de crisis. Se establecen procedimientos de respaldo y recuperación de desastres para asegurar que los datos estén disponibles y se restaure el servicio tan pronto como sea posible.



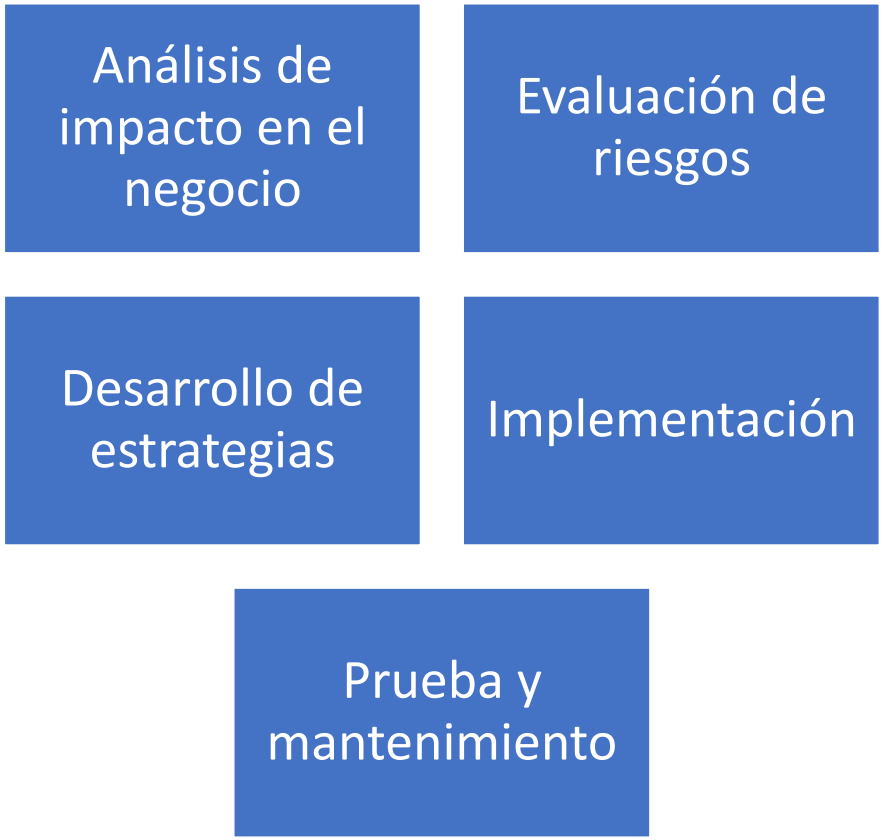
Implementación (Ejemplo)

- La organización implementa las estrategias desarrolladas en la fase anterior. Se instalan medidas de seguridad de la información, como firewalls y software antivirus, se implementan sistemas de recuperación de desastres y se realizan pruebas para asegurar que el plan sea efectivo.



Prueba y mantenimiento (Ejemplo)

- La organización realiza pruebas y simulaciones regulares para asegurarse de que el BCP esté actualizado y sea efectivo. Se revisan y actualizan los planes de continuidad del negocio periódicamente para adaptarse a los cambios en el entorno de seguridad de la información y a los riesgos emergentes.
- La organización también proporciona capacitación y concientización en seguridad de la información a todo el personal para asegurarse de que estén preparados para enfrentar cualquier evento de seguridad de la información.



Plan de Respuesta a Incidentes

Plan de Respuesta a Incidentes

- Es un conjunto de medidas y acciones destinadas a minimizar el impacto de los incidentes de ciberseguridad en una organización. El objetivo principal de este plan es garantizar una respuesta rápida y efectiva ante un incidente de seguridad informática.

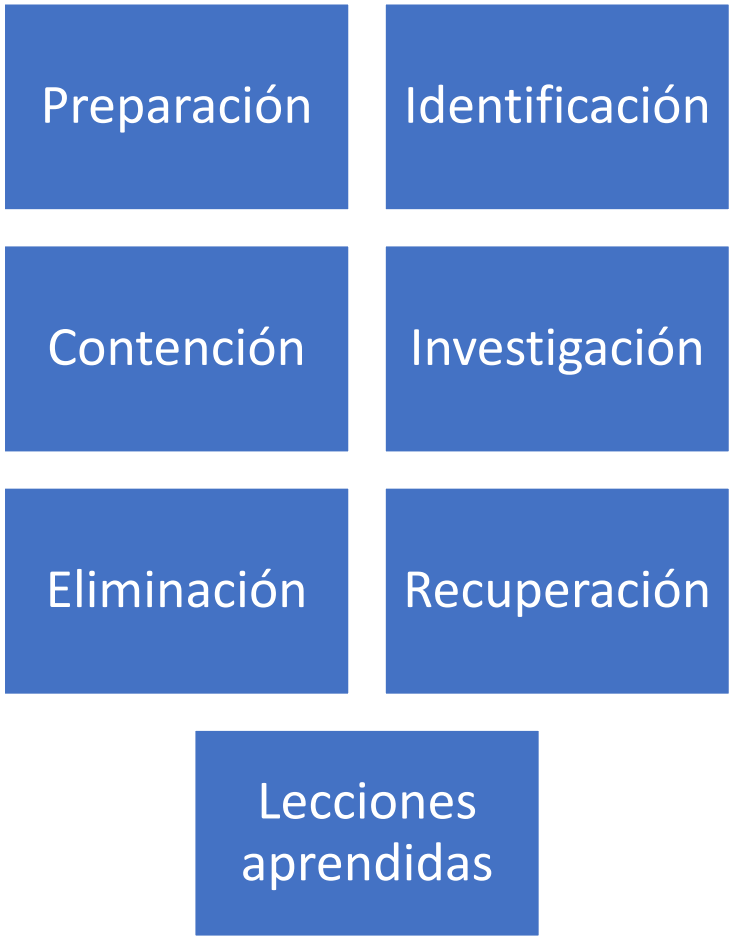
¿Qué incluye un Plan de Respuesta a Incidentes?

- El plan debe incluir
  - una estrategia general que establezca los procedimientos y protocolos para la identificación, contención, análisis, erradicación y recuperación de los incidentes de ciberseguridad.
  - la definición del equipo de respuesta a incidentes y sus responsabilidades.
  - procedimientos detallados para la recolección y preservación de evidencia digital, identificación y notificación de los afectados, y comunicación interna y externa.
  - la evaluación y el análisis de las causas y el impacto del incidente.
  - la implementación de medidas para prevenir futuros incidentes.
- Es importante que el plan **sea probado y validado regularmente** mediante ejercicios de simulación para asegurarse de que sea efectivo y esté actualizado frente a las amenazas emergentes de ciberseguridad.

Fases generales de implementación

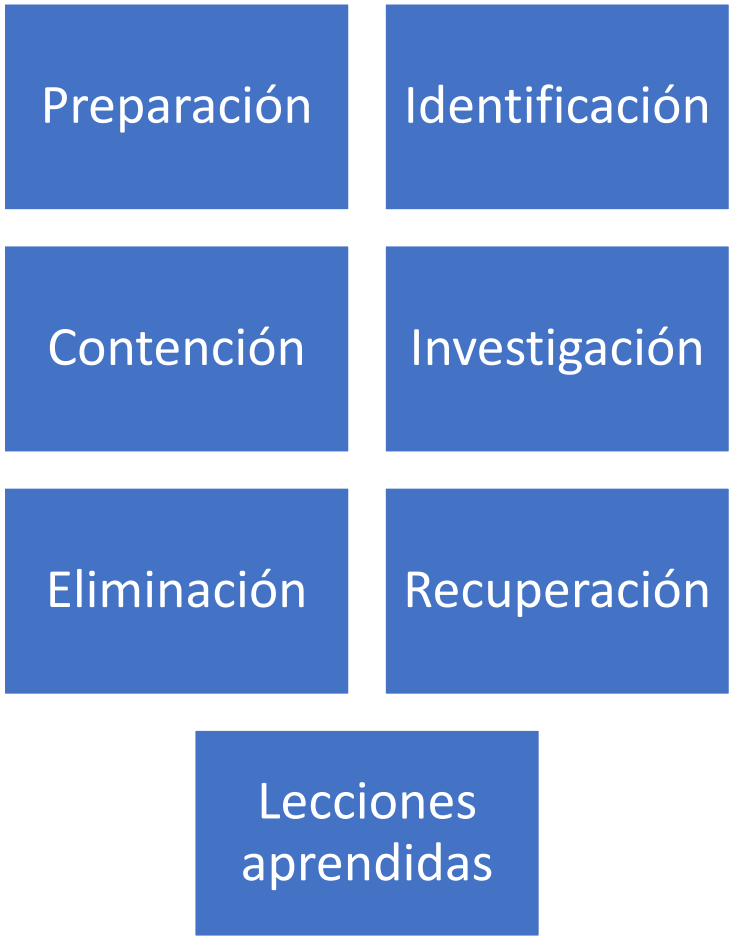
- Preparación
- Identificación
- Contención
- Investigación
- Eliminación
- Recuperación
- Lecciones aprendidas

Preparación



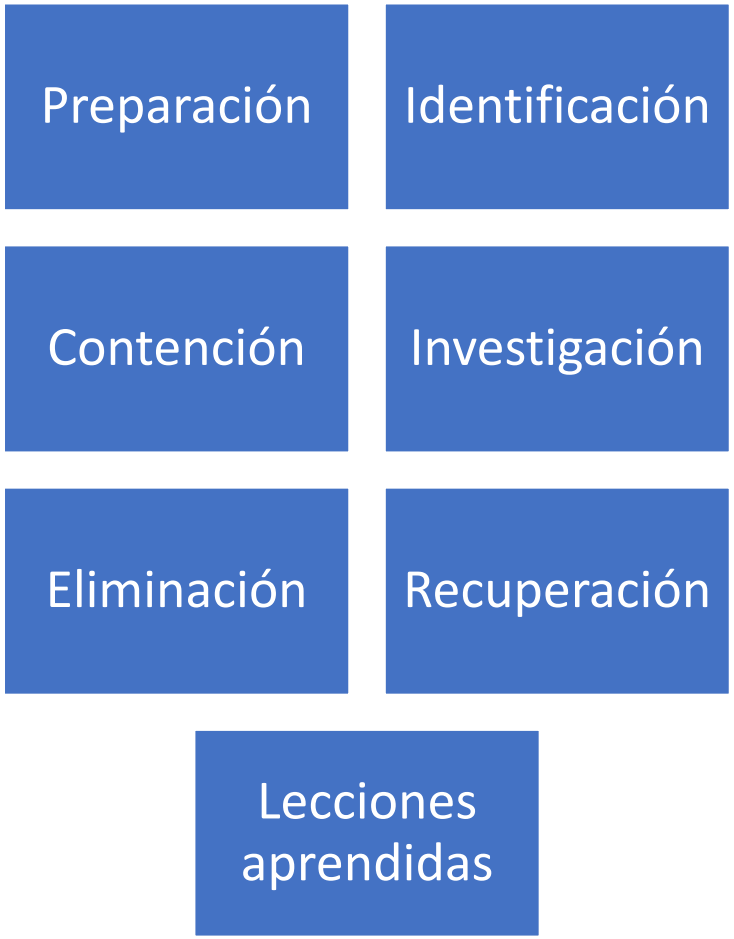
- En esta fase, se establecen los procedimientos y los recursos necesarios para responder a los incidentes de ciberseguridad. Esto incluye la identificación y el entrenamiento de un equipo de respuesta a incidentes, la implementación de herramientas y soluciones de seguridad de la información, y la creación de un plan de respuesta a incidentes.
- Se establecen también procedimientos de comunicación para informar a las partes interesadas y se establecen protocolos de notificación y escalación.

Identificación



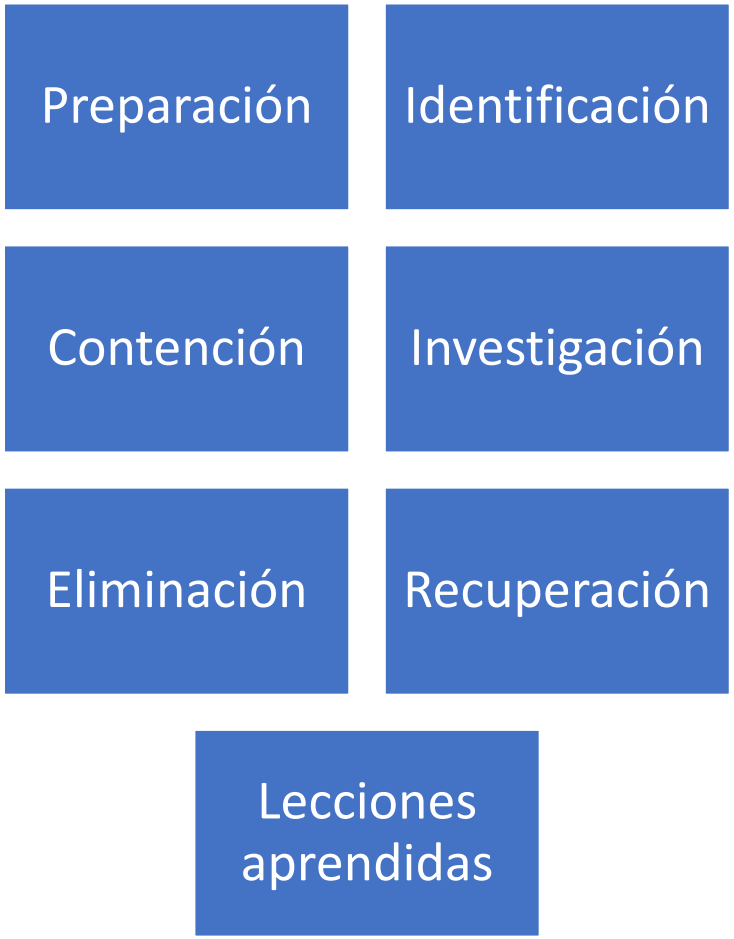
- En esta fase, se detecta y se confirma la existencia de un incidente de seguridad de la información. Esto puede incluir la identificación de un ataque, una violación de datos o una pérdida de información.

Contención



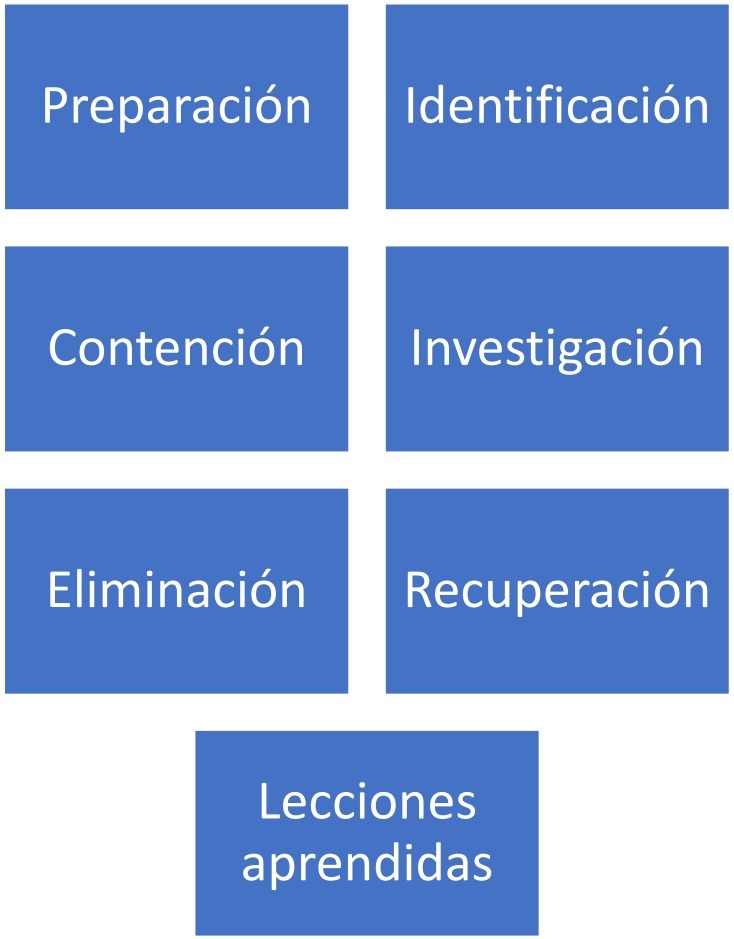
- En esta fase, se toman medidas para contener el incidente de seguridad de la información. Esto puede incluir el aislamiento de sistemas y redes afectadas, la eliminación de software malicioso y la restricción del acceso a la información.

Investigación



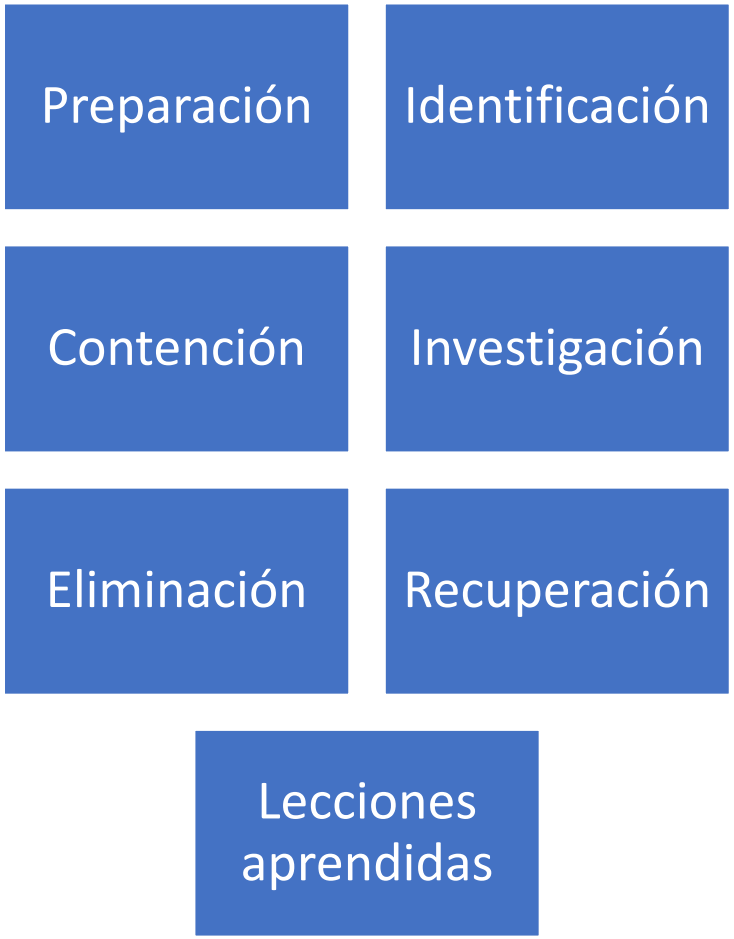
- En esta fase, se investiga la causa y el alcance del incidente de seguridad de la información. Esto puede incluir la identificación del tipo de ataque, la evaluación del daño causado, la recopilación de información de registro y la identificación de los sistemas afectados.

Eliminación



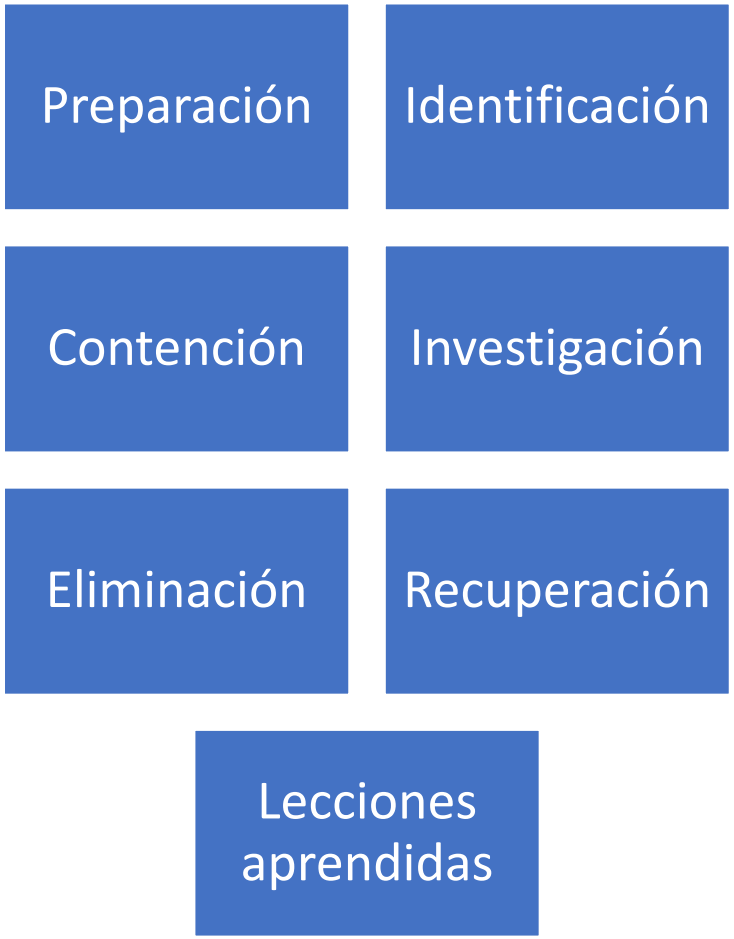
- En esta fase, se eliminan los efectos del incidente de seguridad de la información. Esto puede incluir la restauración de datos y sistemas afectados, la reparación de los sistemas afectados y la eliminación de cualquier malware o software malicioso.

Recuperación



- En esta fase, se restauran los sistemas y servicios a su estado normal. Esto puede incluir la restauración de datos y sistemas, la restauración de la funcionalidad de la red y la reintegración de los sistemas afectados a la infraestructura de la organización.

Lecciones aprendidas



- En esta fase, se realiza una evaluación del incidente de seguridad de la información y se documentan las lecciones aprendidas. Esto puede incluir la identificación de los errores cometidos, las mejoras necesarias y la actualización del plan de respuesta a incidentes.

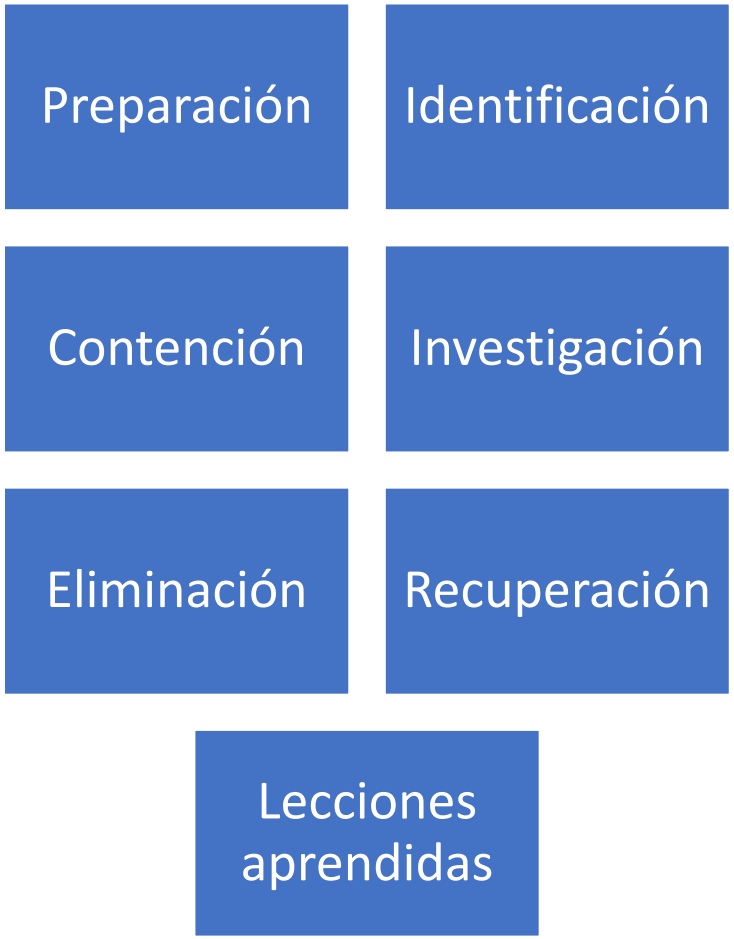
Métricas para Plan de Respuesta a Incidentes

Métricas de plan de respuesta a incidentes

1. **Tiempo de detección del incidente**: Esta métrica mide el tiempo transcurrido entre la ocurrencia de un incidente y su detección. Un tiempo de detección más corto puede ayudar a minimizar el impacto del incidente.
2. **Tiempo de respuesta:** Esta métrica mide el tiempo transcurrido desde la detección del incidente hasta el inicio de la respuesta. Un tiempo de respuesta más corto puede ayudar a minimizar el daño causado por el incidente.
3. **Tiempo de recuperación:** Esta métrica mide el tiempo transcurrido desde la ocurrencia del incidente hasta la recuperación completa del sistema afectado. Un tiempo de recuperación más corto puede ayudar a minimizar el impacto del incidente en la continuidad del negocio.

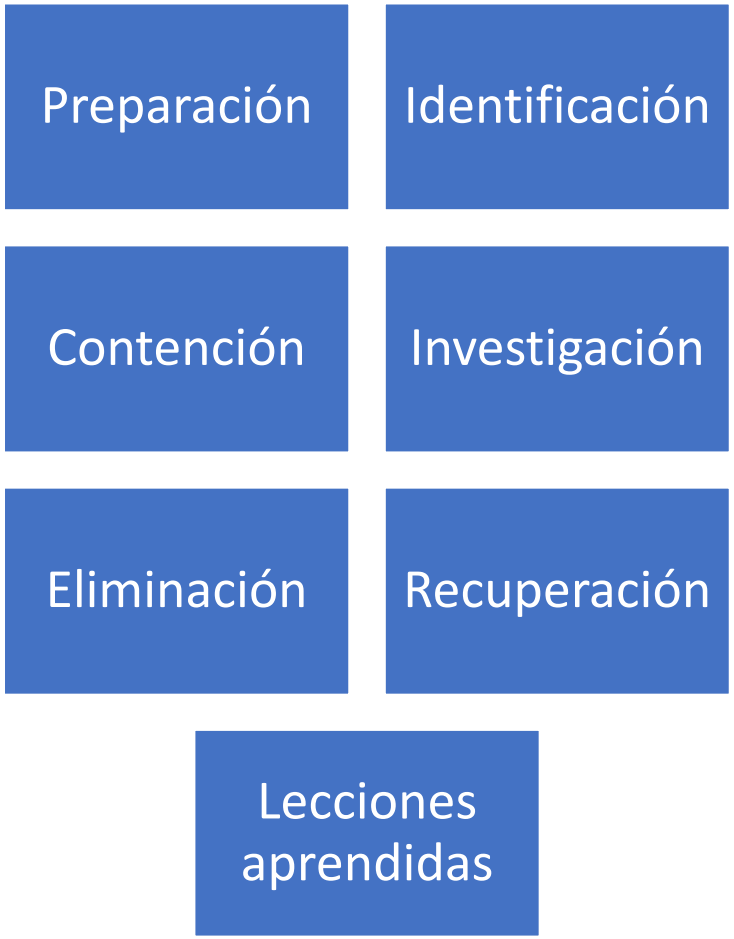
Ejemplo de implementación de un Plan de Respuesta a Incidentes

Preparación (Ejemplo)



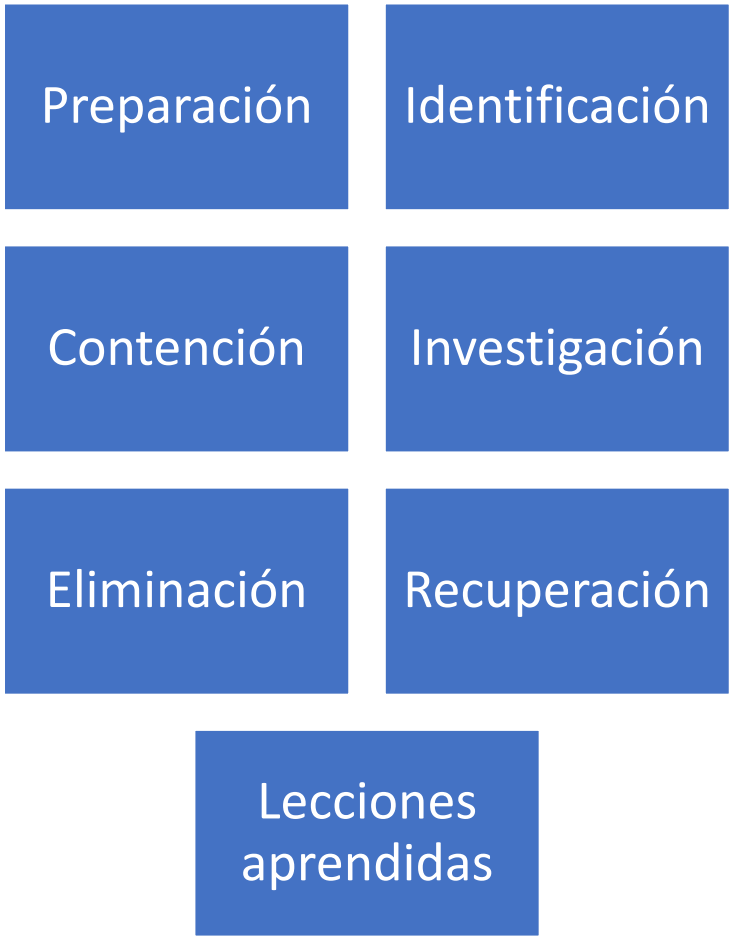
- Una empresa ha establecido un equipo de respuesta a incidentes y ha entrenado a su personal para detectar y responder a posibles incidentes de ciberseguridad. También ha implementado herramientas de seguridad de la información, como firewalls y sistemas de detección de intrusiones.

Identificación (Ejemplo)



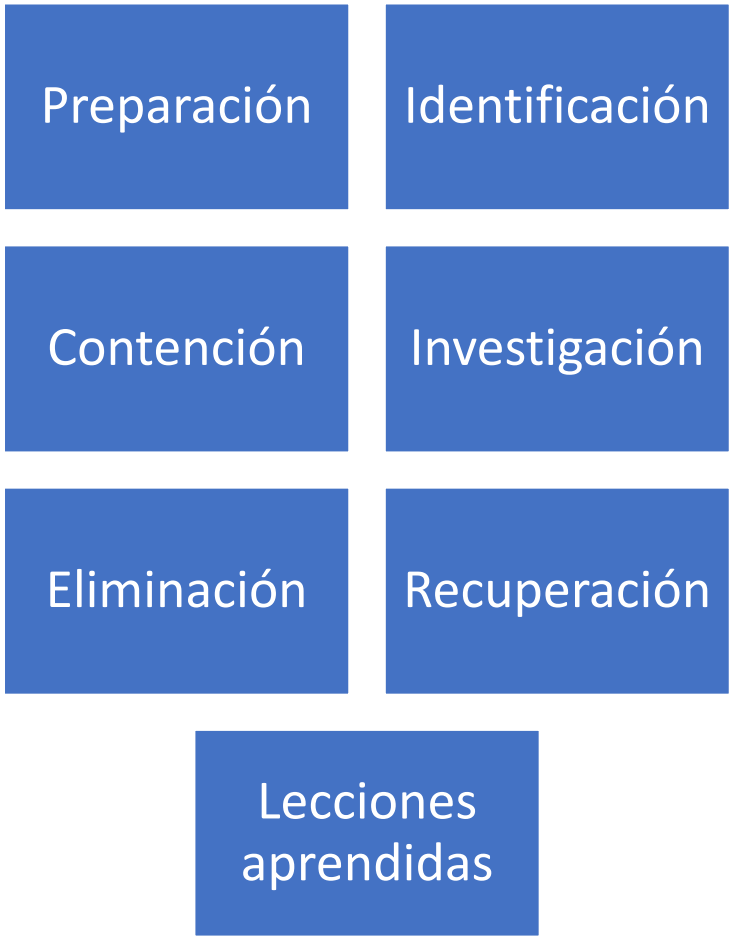
- Un empleado informa al equipo de respuesta a incidentes de que su computadora ha sido comprometida y está mostrando comportamientos extraños.

Contención (Ejemplo)



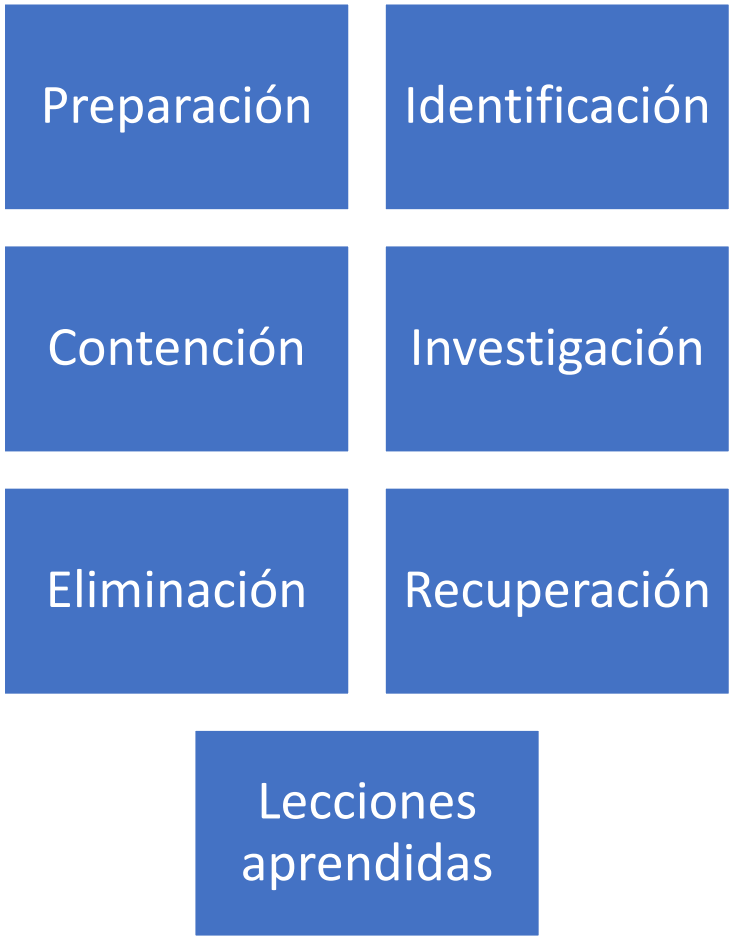
- El equipo de respuesta a incidentes aísla la computadora comprometida y comienza a investigar el incidente.

Investigación (Ejemplo)



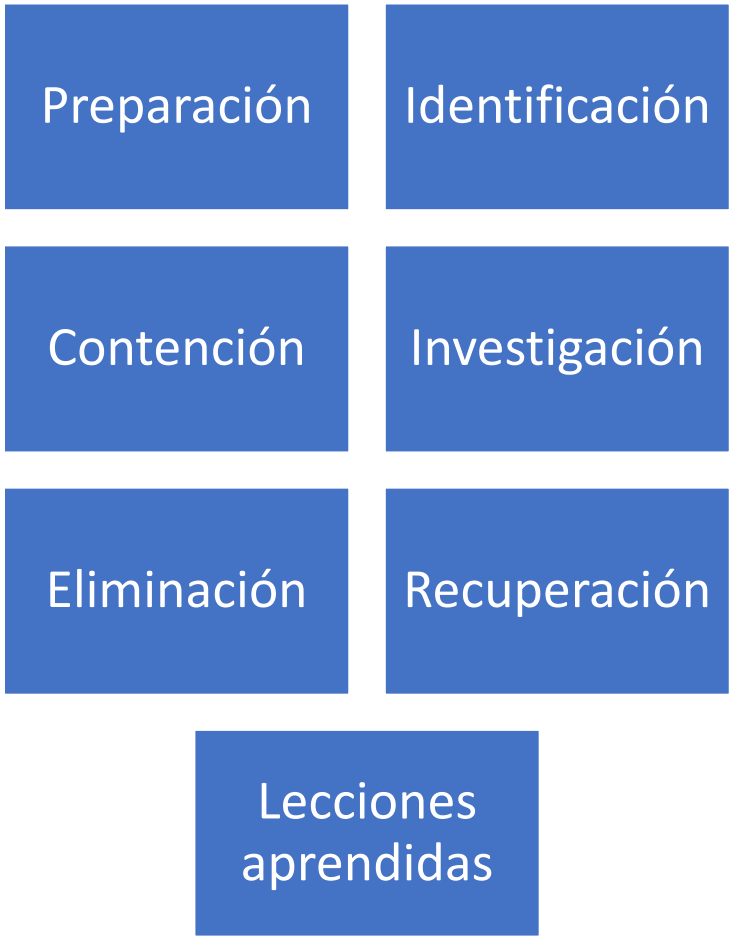
- El equipo de respuesta a incidentes identifica que un atacante ha ganado acceso a la red de la empresa a través de una vulnerabilidad en un servidor de correo electrónico. El equipo investiga el alcance del ataque y determina que se ha comprometido la información de los clientes.

Eliminación (Ejemplo)



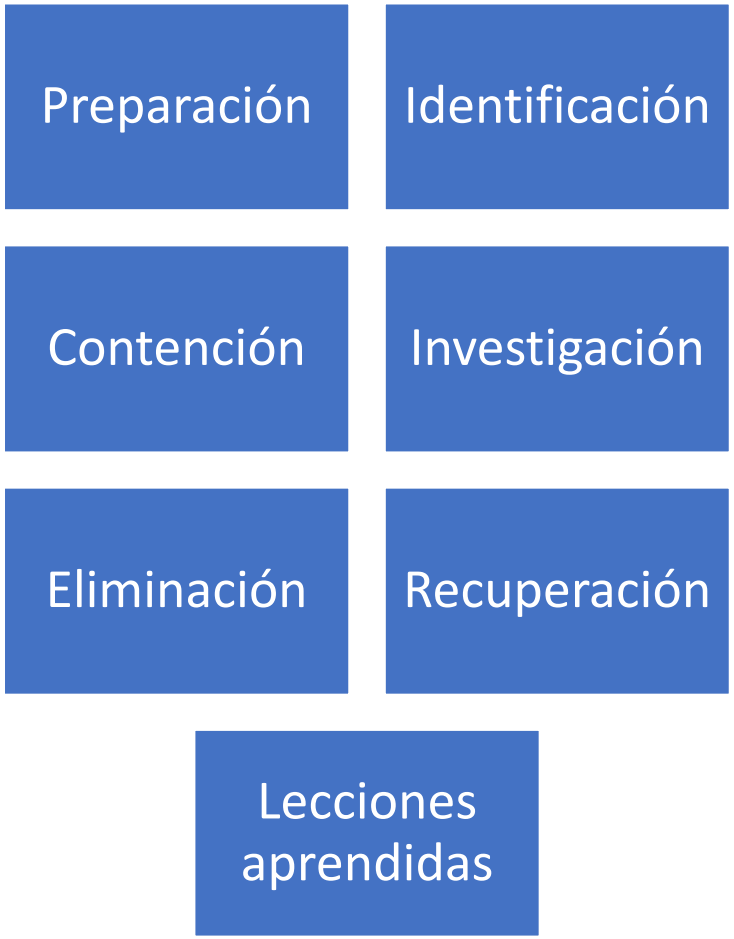
- El equipo de respuesta a incidentes trabaja para eliminar los efectos del ataque, incluyendo la eliminación del malware y la corrección de la vulnerabilidad en el servidor de correo electrónico.

Recuperación (Ejemplo)



- La empresa trabaja para restaurar los sistemas y servicios afectados a su estado normal. Se restauran los sistemas comprometidos, se restaura la funcionalidad de la red y se reintegran los sistemas afectados a la infraestructura de la organización.

Lecciones aprendidas (Ejemplo)



- El equipo de respuesta a incidentes documenta las lecciones aprendidas y actualiza el plan de respuesta a incidentes de la empresa. La empresa también realiza una revisión de sus políticas y procedimientos de seguridad de la información para identificar y abordar posibles vulnerabilidades y mejorar su postura de seguridad.

¿Plan de Continuidad del Negocio o Plan de Respuesta a Incidentes?

¿Por cual empezar?

- Se recomienda implementar primero el plan de continuidad del negocio y luego el plan de respuesta a incidentes. Esto se debe a que el plan de continuidad del negocio aborda los riesgos y amenazas a largo plazo que pueden afectar la continuidad de las operaciones de la organización, mientras que el plan de respuesta a incidentes aborda los riesgos y amenazas a corto plazo que pueden interrumpir las operaciones de la organización.

Resumen

- El plan de continuidad del negocio debe implementarse primero para garantizar la continuidad de las operaciones de la organización en *situaciones de crisis*, mientras que el plan de respuesta a incidentes debe implementarse posteriormente para *proteger la información y los sistemas críticos* de la organización en caso de un incidente de seguridad de la información.