sedian

Seguridad Digital
de Andalucía

Medidas de contención, mitigación y recuperación, así como protocolo para recolección y custodia de evidencias una vez que hemos detectado un ciberincidente

Sesión 2: 18 de marzo de 2021

Junta de Andalucía

INDICE

Medidas de contención.

Medidas de Contención

- **¿Qué es una medida de contención?**

Es una medida que impide que un incidente se extienda a otros recursos. Como consecuencia, se minimizará su **impacto (**separando equipos de la red afectada, deshabilitando cuentas comprometidas, cambiando contraseñas, etc.).

Si un incidente ha logrado comprometer un dispositivo o sistema, se debe evitar que pueda comprometer un segundo; si ha logrado extraer información o anular un servicio, la labor del equipo de respuesta, en este momento, es evitar que se extraiga más información al exterior o se anulen más servicios. La formación y experiencia del personal implicado en la gestión de incidentes será un factor determinante durante esta fase.

La máxima prioridad es contener el impacto del mismo en la organización de forma que se puedan evitar lo antes posible la propagación a otros sistemas o redes evitando un impacto mayor, y la extracción de información fuera de la organización.

La contención del incidente proporciona tiempo para desarrollar una estrategia de respuesta a medida. Una parte esencial de la contención es la toma de decisiones rápidas como puede ser cerrar un sistema, aislarlo de la red, deshabilitar ciertas funciones, etc. Estas decisiones son más fáciles de tomar si existen estrategias predeterminadas que establezcan cómo se debe gestionar cada tipo de incidente

Medidas de Contención

- **¿Qué es una medida de contención?**

Cuando ocurre un ciberincidente, esta suele ser la fase en la que se toman las decisiones de forma más rápida ya que el tiempo es un factor determinante y la reputación o la continuidad del negocio están en jaque y hay que recordar que las decisiones precipitadas son buenas aunque no siempre son acertadas.

La documentación de cada paso que se tome o cada actividad que se observe durante esta fase resulta de gran importancia para incluir en la bitácora o la herramienta de gestión de incidentes. Las decisiones se toman rápidamente y resulta extremadamente sencillo realizar alguna acción indebida, o que requiera un posterior seguimiento, que podría no ser recordada y comprometer con ello la resolución del problema, sobre todo cuando no se siguen los procedimientos existentes sobre gestión de incidentes.

Medidas de Contención

- **¿Qué es una medida de contención?**

Ésta suele ser la fase en la que se realiza el **triaje** que consiste en evaluar toda la información disponible en ese momento realizar una clasificación y priorización del ciberincidente en función del tipo y de la criticidad de la información y los sistemas afectados. Adicionalmente se identifican posibles impactos en el negocio y en función de los procedimientos se trabaja en la toma de decisiones con las unidades de negocio apropiadas y/o a los responsables de los servicios.

Durante esta fase se debe:	Registrar y monitorizar los eventos de las redes, sistemas y aplicaciones.
	Recolectar información situacional que permita detectar anomalías.
	Disponer de capacidades para descubrir ciberincidentes y comunicarlos a los contactos apropiados.
	Recopilar y almacenar de forma segura todas las evidencias.
	Compartir información con otros equipos internos y externos de forma bidireccional para mejorar las capacidades de detección.

Medidas de Contención

- **¿Qué es una medida de contención?**

Una vez que se ha comenzado a estudiar la situación, se está en disposición de proceder a la clasificación del ciberincidente, lo que permitirá determinar cómo abordarlo y revelará algunas pautas para su resolución. Una taxonomía de ciberincidente permite realizar una priorización en función del tipo de incidente y peligrosidad del mismo. El impacto producido por el ciberincidente es un tercer valor con carácter más dinámico que los anteriores y puede variar a lo largo del ciclo de vida del incidente ya que, lo que inicialmente puede parecer un problema simple relacionado con un correo electrónico podría resultar finalmente una crisis con robo de propiedad intelectual y daño de reputación.

Es una buena práctica que las empresas desarrollen políticas de actuación para la gestión de los incidentes en general y de los incidentes vinculados con datos personales en particular. La complejidad de estas políticas irá vinculada a las características, volumen y operaciones de tratamiento que se realicen sobre los datos y será conveniente llevar a cabo procesos de verificación que permitan validar el funcionamiento de las mismas.

Una correcta clasificación de los ciberincidentes permite a los equipos de respuesta asignar la prioridad adecuada a cada problema, asegurando que se tratan en primer lugar o que se asignan más recursos a aquellos casos más graves.

Conviene registrar y documentar el ciberincidente con el apoyo de una herramienta de gestión de incidentes, incluyendo la información obtenida durante la fase de identificación así como los valores de clasificación, peligrosidad e impacto inicial. También es el momento de considerar la necesidad de comunicar la existencia de un incidente de seguridad a un nivel superior en la estructura organizativa de la entidad (responsables de departamentos, CISO, CIO, Comité de crisis...) en función de cómo se haya definido en los procedimientos.

Medidas de Contención

- **¿Qué es una medida de contención?**

Si no ha ocurrido ya, es muy probable que las acciones que se tomen a partir de este momento puedan afectar a la prestación de algún servicio ofrecido por la organización. Dado que no es labor del equipo de respuesta, ni éste tiene el conocimiento necesario para estimar la pérdida que puede suponer para el negocio aislar un servidor que ofrece un servicio esencial para la organización, siempre se debe obtener la autorización del área de negocio antes de iniciar acciones de contención de gran impacto. Evite siempre que el remedio sea peor que la enfermedad.

Conocida la extensión del problema a través de diagramas de red, sistemas de detección, correladores de eventos y otras tecnologías, se pueden buscar características comunes entre los activos afectados y tomar medidas de aislamiento en función de los patrones identificados.

Las medidas de contención podrán ser inmediatas o de aplicación progresiva en función del desarrollo de la resolución del incidente. Es conveniente determinar las medidas a implantar estableciendo un orden de prioridad, los responsables asignados, tiempos estimados y los efectos esperados. Algunas medidas de contención serán sencillas y las podrá iniciar el usuario, sin embargo otras medidas son más complejas y deben estar en manos de personal especializado que se encargue de la seguridad informática de la empresa

Medidas de Contención

- **¿Qué es una medida de contención?**

Las medidas de contención se pueden categorizar en dos, por el impacto que tienen sobre las operaciones de negocio de nuestra empresa:

Medidas que no afectan a la operativa normal: incluirá actividades que pueden ser realizadas de forma preventiva lo antes posible y que mitigan el riesgo de forma casi transparente.

Medidas que sí afectan a la operativa normal: se deben valorar las actividades a realizar, reconocer a qué partes del negocio impactaría y cómo. En este momento se debe involucrar a las áreas de negocio afectadas y establecer con ellos un plan de seguimiento del impacto interno

Medidas de Contención

- **¿Qué es una medida de contención?**

Es muy importante también comenzar a definir un plan, incluyendo el horizonte temporal de aplicación de dichas medidas. También se debe confirmar que la situación está bajo control. Sin esa confirmación, no podríamos asegurar en último término la correcta contención en nuestra empresa.

Se debe recordar que es posible que el incidente siga evolucionando, por lo que es necesario dedicar un equipo de trabajo a la búsqueda de nuevos indicadores de ataque y a su clasificación. Este equipo deberá trabajar de manera coordinada con el equipo de contención validando las diferentes hipótesis de ataque que se realicen.

Es necesario también implantar una adecuada monitorización y supervisión para verificar que los controles que se están llevando a cabo son eficaces.

Por último, es más que recomendable activar un equipo de recuperación lo antes posible, recurriendo a los medios con los que cuente cada empresa y que, a partir de la información disponible, active los mejores planes de vuelta a la normalidad y coordine, en caso necesario, las acciones derivadas del plan de continuidad de negocio. Es por ello también importante informar y alertar a los departamentos de negocio afectados y a los potenciales afectados en función de las medidas que la empresa decida tomar, de la posibilidad de la puesta en marcha de algún/os plan/es.

Medidas de Contención

- **¿Qué es una medida de contención?**

Algunas de las acciones que se pueden tomar en primer lugar consisten en:

Desconectar el equipo o segmento de red del resto de redes de la organización. Esto puede hacerse, si se trata de un equipo aislado, desconectando el cable de red o tirando el enlace inalámbrico si la conexión se realiza a través de Wi-Fi.

En caso de tratarse de algún equipo que desempeña una función crítica para el negocio, es posible proceder a la colocación de un firewall intermedio entre el segmento afectado y el resto de la red que permita filtrar el tráfico y permitir únicamente aquello que sea estrictamente necesario para la prestación del servicio.

Reubicación del recurso comprometido en una VLAN aislada.

Considerar la aplicación de técnicas de DNS sinkholing para controlar tráfico malicioso.

Si se conocen los detalles técnicos del tipo de ciberincidente se pueden aplicar medidas de contención más ajustadas a cada situación (bloqueo de determinados correos electrónicos, aplicación de reglas en los cortafuegos, bloqueo de acceso a unidades compartidas, etc.).

Contactar con terceras entidades que pueden ofrecer ayuda en la contención. Los proveedores de servicio de Internet pueden aplicar filtros o activar medidas de protección e INCIBE-CERT puede ofrecer información adicional y coordinación a nivel nacional e internacional con otros posibles implicados en el incidente.

Medidas de Contención

- **¿Qué es una medida de contención?**

Algunas de las acciones que se pueden tomar en primer lugar consisten en:

impedir el acceso al origen de la divulgación: dominios, puertos, servidores, la fuente o los destinatarios de la divulgación. Dependiendo del vector de ataque, impedir el acceso al origen: dominios, conexiones, equipos informáticos o conexiones remotas, puertos, parches, actualización del software de detección (antivirus, IDS, etc.) bloqueo de tráfico, deshabilitar dispositivos, servidores, etc.

Suspender las credenciales lógicas y físicas con acceso a información privilegiada. Cambiar todas las contraseñas de usuarios privilegiados o hacer que los usuarios lo hagan de manera segura.

Hacer una copia del sistema (clonado), hacer una copia bit a bit del disco duro que contiene el sistema, y luego analizar la copia utilizando herramientas forenses.

Aislar el sistema utilizado para revelar los datos con el fin de realizar un análisis forense más tarde.

Si los datos han sido enviados a servidores públicos, solicitar al propietario (o webmaster) que elimine los datos divulgados.

Si no es posible eliminar los datos divulgados, proporcionar un análisis completo al departamento correspondiente (Legal, Compliance, RRHH, etc.) o a quien ejerza dichas funciones en la empresa.·

Vigilar la difusión de los documentos/datos filtrados en los diferentes sitios web y redes sociales (FB, Twitter, etc.) así como los comentarios y reacciones de los usuarios de Internet

Medidas de Contención

- **¿Qué es una medida de contención?**

Una vez que se han tomado las medidas iniciales para contener el problema, cuidando de no destruir información valiosa, es momento de comenzar con los procedimientos de toma y preservación de evidencias. Este paso resulta importante, tanto por si finalmente es necesario judicializar el incidente, como para poder analizar correctamente el origen y determinar el impacto real del problema.

Los datos volátiles almacenados en la memoria del equipo pueden resultar muy importantes para el proceso de análisis en casos de programas maliciosos o de intrusiones y éstos se perderían si se apagara el equipo, por lo que en caso de considerarlo relevante se han de aplicar técnicas para su adquisición antes del apagado de los equipos. Para la adquisición de memoria volátil se pueden utilizar herramientas forenses (tanto hardware como software), procurando en todo momento no alterar el sistema ni los datos del mismo ya que podrían modificarse o perderse evidencias importantes. En sistemas virtualizados la memoria RAM está disponible como un fichero; en el caso de VirtualBoxéste tiene la extensión ".sav" y ".vmem" en VMWare.

Medidas de Contención

- **¿Qué es una medida de contención?**

Una vez completado el proceso de adquisición de datos volátiles de la memoria ya se podría proceder al apagado del sistema. Para ello, y con el fin de evitar algún comportamiento desconocido de un posible programa malicioso presente en el equipo comprometido, lo más recomendable es proceder a un corte de energía repentino del sistema, desconectando el cable de corriente o retirando la batería del equipo.

Para los datos no volátiles se deben realizar copias exactas (bit a bit) de los datos originales. Esto se puede realizar a través de diferentes utilidades o herramientas o mediante dispositivos físicos conocidos comúnmente con el nombre de clonadoras. Siempre que se realice una copia de un medio de almacenamiento conviene verificar que el medio original no sufrirá ninguna alteración, por lo que se recomienda emplear Procedimiento de gestión de ciberincidentes para el sector privado y la ciudadanía15elementos que bloqueen la escritura en ellos (write-block) mientras se realiza el clonado.

Medidas de Contención

- **¿Qué es una medida de contención?**

La información copiada se debe almacenar en dispositivos sobre los que se hayan aplicado previamente técnicas de borrado seguro para garantizar que no contengan ninguna información anterior que pudiera contaminar los nuevos datos. Conviene que los medios de destino tengan un tamaño ligeramente superior al medio de origen. Es posible que, en algunos casos, no sea posible realizar una copia completa del sistema ni de la memoria; en estos casos se pueden evaluar alternativas como realizar un análisis forense en vivo.

Una vez extraídos los datos se deben aplicar técnicas adicionales que garanticen la integridad de los mismos; esto se consigue a través de la aplicación de funciones criptográficas o hash. La mayoría de los sistemas actuales permiten realizar funciones de tipo MD5 y SHA1, en algunos casos también existirá la opción de aplicar funciones de la familia SHA2, siendo preferibles estas últimas. Estas funciones se deben aplicar tanto en los datos de origen como en los datos de destino, verificando que el valor obtenido en ambos casos es el mismo. Esto permite comprobar de forma sencilla que los datos copiados sean idénticos a los originales.

Medidas de mitigación.

Medidas de Mitigación

- **¿Qué es una medida de mitigación?**

El objetivo principal de esta medida de seguridad es la eliminación del ciberincidente de nuestros sistemas, hasta donde sea posible y conozcamos, o bien garantizar que se está realizando en los sistemas donde nuestra información esté almacenada.

La naturaleza de esta etapa conlleva una serie de actividades que se ejecutan en algunos casos **de forma inmediata** (desconexiones, controles de acceso, revisiones…) y en otros, **con posterioridad** (infraestructuras no críticas, gestión de parches y vulnerabilidades, restructuraciones y cambios en infraestructuras…).

Deben establecerse de forma clara, entre ambas partes, cuáles van a ser los criterios y requisitos que determinen que el incidente estará efectivamente erradicado para poder proceder a la recuperación de la normalidad.

Las medidas de mitigación dependerán **del tipo de ciberincidente**, así, en casos de denegaciones de servicio distribuidas (DDoS) puede ser necesario solicitar asistencia de entidades externas, como proveedores de servicios de mitigación de este tipo de ataques o un CSIRT nacional como el CCN-CERT o INCIBE-CERT, que puedan apoyar en el análisis y definición de la estrategia de mitigación.

Medidas de Mitigación

- **¿Qué es una medida de mitigación?**

En algunos casos, la eliminación automática a través de herramientas no es posible, principalmente cuando se trata de algún tipo de rootkit o amenazas más avanzadas. En estos casos será necesario proceder a un borrado seguro del medio de almacenamiento y a una reinstalación completa del sistema operativo y aplicaciones. Si existen copias de seguridad y se conoce con exactitud la fecha de compromiso, es posible proceder a una restauración del sistema con una copia de seguridad anterior al comienzo del incidente.

Si se realiza una instalación nueva, como si se restaura una copia de seguridad previa al ciberincidente, es necesario aplicar las medidas de seguridad necesarias en el sistema; esto incluye actualizaciones tanto del sistema operativo como del resto de aplicaciones. También es necesario realizar un análisis sobre el grado de exposición del activo, ya que en muchos casos el compromiso tiene su origen en servicios expuestos mal configurados que no deberían estar activos o que, si son necesarios, deberían haber estado correctamente protegidos (telnet, ssh, rdp, etc.).

Cuando no existan copias de seguridad disponibles y se haya realizado una reinstalación completa del sistema, la información debe ser extraída manualmente del equipo previamente comprometido y transferida al nuevo sistema, con la correspondiente cautela de no transmitir junto con ella la infección.

Medidas de Mitigación

- **Estrategias para mitigar el riesgo de un ciberataque**

Existen varias estrategias de mitigación que pueden reducir considerablemente los riesgos y medidas adicionales para disminuir el impacto de un ciberataque que logre penetrar en el sistema.

Mejorar la visibilidad:	• Todos los organismos deben contar con un inventario actualizado de sus activos de la información, a fin de lograr esta visibilidad. La mayoría de los sistemas conectados en red han ido creciendo orgánicamente con el tiempo.
Proteger la red:	• Es preciso crear una red de tecnología de operaciones adecuada para el propósito con el que fue implementada.
Mantener la seguridad:	• Estar protegido hoy no significa que mañana también se esté protegido. Se deben poner en marcha procesos sencillos de gestión para mantener al día las revisiones, verificar los elementos que se agregan a la red o se retiran de ella, y evaluar con regularidad las vulnerabilidades, deben convertirse en procedimientos habituales en una empresa para que la ciberseguridad siga siendo sólida.

Medidas de Mitigación

- **Plan de gestión de incidentes y Plan de continuidad de negocio**

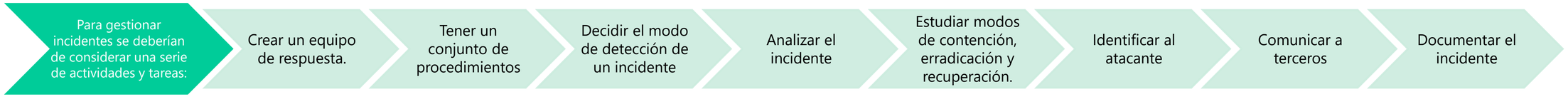
Aunque hemos enumerado, un conjunto de estrategias, la mejor manera de mitigar un incidente es contar con un plan de gestión de incidentes y un plan de continuidad de negocio.

Plan de gestión de incidentes:	Restablecer el servicio acordado lo antes posible y con el mínimo impacto.
	Garantizar el más alto nivel de calidad y disponibilidad del servicio.
	Implementar los acuerdos de nivel de servicio (SLA) que aún no están definidos.
	Registrar en forma permanente los incidentes (trazabilidad).
	Identificar proactivamente las mejoras del servicio.
	Definir las bases para la generación de la gestión de la configuración de base de datos (CMDB, por sus siglas en inglés) de acuerdo a las buenas prácticas.
	Minimizar el riesgo de incidentes perdidos.
	Recolectar datos relacionados a la gestión.
Plan de continuidad de negocio:	Plan de recuperación de desastres.
	Plan de emergencia.
	Plan de pruebas
	Lecciones aprendidas

Medidas de Mitigación

- **Plan de gestión de incidentes**

Es un documento dónde se enumeran los distintos tipos de incidentes y como reducir o mitigar su efecto



Medidas de Mitigación

- **Plan de gestión de incidentes**

Equipo de respuesta:

Debe estar constituido por personas que cuenten con la experiencia y la formación necesaria para poder actuar ante incidencias y desastres.

Las empresas deben mantener actualizada una lista de direcciones y contactos para emergencias.

En nuestro caso algún especialista en ciberseguridad, responsables técnicos, CCN, INCBE, etc.

Procedimientos y actividades a realizar:

El organismo debe definir y desarrollar un conjunto de procedimientos sencillos, claros, detallados y prácticos para restauración rápida y segura de los servicios/procesos afectados por la incidencia.

Este conjunto de procedimientos debe ir creciendo poco a poco, nuevos tipos de incidencias nuevos procedimientos.

El objetivo de esta documentación es conseguir una respuesta sistemática ante los incidentes de seguridad realizando los pasos adecuados y definidos para evitar posibles errores.

Un buen cuerpo procedimental permitirá minimizar el impacto de una incidencia.

Medidas de Mitigación

- **Plan de gestión de incidentes**

Equipo de respuesta:

- Debe estar constituido por personas que cuenten con la experiencia y la formación necesaria para poder actuar ante incidencias y desastres.
- Las empresas deben mantener actualizada una lista de direcciones y contactos para emergencias.
- En nuestro caso algún especialista en ciberseguridad, responsables técnicos, CCN, INCBE, etc.

Procedimientos y actividades a realizar:

- El organismo debe definir y desarrollar un conjunto de procedimientos sencillos, claros, detallados y prácticos para restauración rápida y segura de los servicios/procesos afectados por la incidencia.
  - Este conjunto de procedimientos debe ir creciendo poco a poco, nuevos tipos de incidencias nuevos procedimientos.
  - El objetivo de esta documentación es conseguir una respuesta sistemática ante los incidentes de seguridad realizando los pasos adecuados y definidos para evitar posibles errores.
  - Un buen cuerpo procedimental permitirá minimizar el impacto de una incidencia.

Medidas de Mitigación

- **Plan de gestión de incidentes**

Detección de un incidente:

- Debemos definir cuáles son las fuentes de entrada de la información para notificarnos un incidente y asegurarnos que no se notifique varias veces por error.

Análisis de un incidente

- Debe incluir como proceder al análisis de del mismo.
- En primer lugar debería determinarse lo más automáticamente posible:
- ¿Qué sistemas se han podido ver afectados? ¿Se ha podido comprometer información confidencial?¿Ha podido afectar a terceros?
- Seguidamente el equipo de respuesta debe determinar el origen del incidente: interno, externo, tipo de ataque de informático (o tipo de incidente definido en los procedimientos).

Medidas de Mitigación

- **Plan de gestión de incidentes**

Contención:

- Lo antes posible.
- Retrasar la contención

Erradicación

- Debe contemplar todas las actividades necesarias para eliminar los agentes causantes, secuelas. A través de antivirus, estudio de logs, actualizaciones, etc.

Recuperación

- Proceso por el que se inicia la recuperación de los sistemas, reinstalaciones, recuperación y pruebas.
- En esta parte del proceso entran en juego los planes de recuperación de desastres.

Medidas de Mitigación

- **Plan de gestión de incidentes**

Identificación del atacante

- Es factor muy importante para emprender acciones contra el atacante.
- Dependiendo del tipo de incidente la labor de identificar al atacante pueda conllevar una inversión de recursos (DDoS, Phishing…) que puede que no facilite este dato. Por otro lado para otros incidentes como la fuga de información, el uso de recursos de la empresa con fines fraudulentos, etc; es información relativamente más accesible y útil.

Comunicación a terceros

- Proveedores.
- CCN-CERT
- AEPD

Documentación del incidente

- El proceso de gestión del incidente debe documentarse de manera clara y sencilla tanto para su posterior estudio como para el aprendizaje en la gestión de tipos de incidentes concretos.

Medidas de Mitigación

- **Plan de continuidad de negocio**

Consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos .

Plan de recuperación ante desastres (DRP).	Identificarán la mejor manera de recuperarse en caso de desastre y proveerá una guía para el desarrollo de los procedimientos de recuperación de desastres. Para ello como mínimo se deberán estudiar previamente:	Umbrales de recuperación (RTO y RPO).
		Coste de la recuperación.
		Requisitos mínimos aceptables para la recuperación.
		Listado de los procedimientos de recuperación.

Medidas de Mitigación

- **Plan de continuidad de negocio**

Planes de emergencia	Se identificarán los procedimientos aplicados por los servicios de emergencia. Para alcanzar este objetivo se debería contactar a estos servicios con antelación suficiente para recoger información útil relacionada con las labores de asistencia en el caso de incidente.	Recomendaciones para establecer los puntos de encuentro y rutas de evacuación. Información de riesgos específicos por actividades (p.ej. empresas de sectores relacionados con química o sustancias peligrosas) o afectaciones (p.ej. zonas de inundación) en las inmediaciones. Conocer la posición de posibles conflictos por tráfico rodado. Acuerdos para mejorar el acceso a las instalaciones y a recursos relevantes (p.ej. bocas de suministro). Participación en simulacros de forma conjunta.

Medidas de Mitigación

- **Plan de continuidad de negocio**

Plan de pruebas	La efectividad del DRP se puede valorar si existe un plan de pruebas que se lleve a cabo en condiciones reales. La fase de prueba debe contener las actividades más importantes que requieran comprobación y certeza en su funcionamiento futuro. Se debe probar dentro de un ambiente que simule las condiciones que serían aplicables a una situación real. Es importante que las pruebas se lleven a cabo por las personas que serían responsables en condiciones reales.	Desarrollo de los objetivos y alcance de la prueba Configuración del ambiente de prueba Preparación de los datos de la prueba Identificación de quién dirigirá la prueba Identificación de quién controla y supervisa la prueba Preparación de cuestionarios de evaluación Preparación de presupuesto para la fase de prueba Entrenamiento a los grupos de prueba de las unidades de negocio

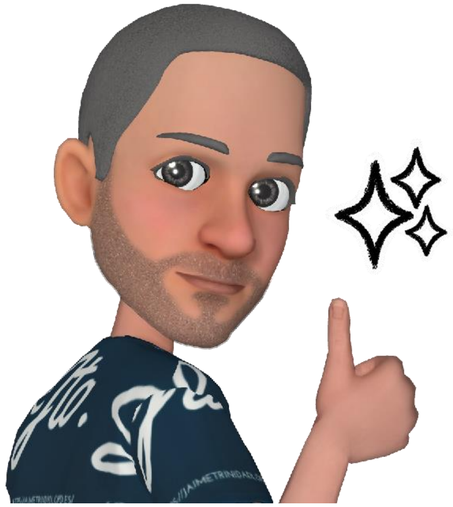
Medidas de Mitigación

- **Plan de continuidad de negocio**

Lecciones aprendidas

- Todo plan o procedimiento tiene que llevar un registro de los resultados obtenidos de las pruebas o situaciones reales para analizar posteriormente y proponer mejoras en los sistemas.

EL PRÓXIMA DÍA, Medidas de recuperación
Ciclo de vida de un incidente de ciberseguridad



https://jaimetrinidadlopd.es/

Jaime T. Ortiz

CONSULTOR DE SEGURIDAD DE LA INFORMACION

HTTPS://JAIMETRINIDADLOPD.ES/

sedian Seguridad Digital de Andalucía