

Experiencia de simulación: respuesta ante incidentes



Tiempo total
Dos horas



Cantidad máxima de
participantes
30

🎯 Público objetivo

Personal corporativo que participa en el plan de respuesta ante incidentes de su organización, independientemente de sus conocimientos técnicos o nivel de educación.

🔍 Descripción general

Un ejercicio de simulación es una recreación guiada en la cual las personas participantes interpretan diferentes situaciones. Sirve para identificar las faltas de alineación en el equipo y los puntos débiles durante los momentos de calma, lo que desarrolla la resiliencia para cuando ocurran crisis reales en las cuales la coordinación en tiempo real es fundamental. El objetivo no es lograr una ejecución perfecta, sino que el personal se prepare gracias al ensayo de situaciones.

👤 Objetivos de aprendizaje

Al final de esta experiencia, quienes participen podrán hacer lo siguiente:

- explicar la importancia que tiene un plan de respuesta ante incidentes en un entorno laboral;
- identificar las funciones y responsabilidades durante un incidente de seguridad;
- practicar la rapidez mental y la toma de decisiones eficaz durante situaciones de incidentes.

✂️ Materiales

- Listas de verificación de la respuesta ante incidentes para repartir
- Cronómetro o temporizador
- Tarjetas de participante (responsable de seguridad de TI, responsable de incidentes, responsable de comunicaciones, responsable de asesoramiento legal, representante de RR. HH. y gerente de departamento)
- Tarjetas de situación para interpretar
- Pizarra o rotafolio
- Marcadores
- Lapiceras y blocs de notas

👤 Funciones en el ejercicio de simulación

Persona facilitadora: es quien controla el ritmo del ejercicio, guía los debates, actualiza lo que ocurre en las situaciones, se asegura de que todas las personas participen y presenta la información para poner a prueba el enfoque del equipo.

Participantes: representan sus funciones durante la simulación, debaten de manera abierta sobre sus procesos de razonamiento, respaldan a los miembros del equipo y responden a las situaciones acorde a las responsabilidades de la función que cumplen.

Persona evaluadora: evalúa las fortalezas y debilidades, redacta informes luego de la acción y analiza la alineación con los procedimientos y planes existentes.

Persona observadora: brinda conocimientos expertos sobre la materia sin participar de forma directa en el ejercicio, y respalda a las personas participantes planteando preguntas relevantes y ofreciendo orientación cuando se necesite.

Persona tomadora de notas: registra todas las actividades del ejercicio, los debates, las brechas identificadas, la alineación con los procedimientos oficiales de la organización y las mejoras sugeridas.

Introducción

🕒 Duración: 10 minutos

Una respuesta ante incidentes eficaz necesita una comunicación clara, funciones definidas y adaptabilidad. Anuncie a las personas participantes que las actividades simularán situaciones y desafíos reales que les ayudarán a desarrollar las habilidades esenciales necesarias para gestionar los incidentes de seguridad. Recuerde que una respuesta ante incidentes exitosa depende de la **coordinación en equipo** y la **rapidez mental**.

Actividad 1: lista de verificación para una respuesta rápida

 Duración: 30 minutos

Materiales

- Cronómetro o temporizador
- Lapiceras y blocs de notas
- Listas de verificación de la respuesta ante incidentes para repartir (ver archivo adjunto de la Actividad 1)

Actividad

En esta actividad se pone a prueba el plan de respuesta ante incidentes de cada participante, junto con su estrategia de comunicación y su proceso para tomar decisiones.

Presente a las personas participantes la siguiente situación:

“Un servidor crítico de su organización se encuentra cifrado por ransomware, y las personas atacantes exigen una gran suma de criptomonedas a cambio de descifrar los archivos”.

Una vez establecido el contexto:

1. Entregue una lista de verificación de la respuesta ante incidentes a cada participante. En la lista de verificación se muestran en orden aleatorio los pasos comunes que se siguen durante una respuesta ante incidentes.
2. Otorgue 10 minutos a las personas participantes para que prioricen de manera individual los pasos de su lista de verificación en el orden que consideren más apropiado para la situación de ransomware presentada.
3. Agrupe a las personas participantes en grupos pequeños de entre 3 y 4 miembros para que debatan sobre su priorización durante 10 minutos, y asegúrese de que cada persona complete su propia lista de verificación por separado.
4. Dedique los últimos 10 minutos para analizar junto con todo el grupo las secuencias de una respuesta eficaz y converse sobre por qué algunos pasos deben ocurrir antes que otros.

Respuestas

En función de las prácticas recomendadas del sector, estos son los elementos fundamentales que debe incluir la lista de verificación:

1. Reportar el incidente de inmediato (de acuerdo con la política de escalamiento de la organización).
2. Movilizar al equipo de respuesta ante incidentes.
3. Aislar los sistemas afectados.
4. Registrar la línea temporal del incidente.
5. Evaluar el estado de las copias de seguridad de los datos.
6. Activar el plan de comunicación que tiene la organización con las partes interesadas.
7. Seguir los procedimientos de notificación establecidos para cumplir los requisitos regulatorios.
8. Buscar asesoramiento legal.
9. Ejecutar la política de respuesta ante pedidos de rescate de la organización.
10. Comunicarse con los organismos policiales (según la política de la organización).

Actividad 2: simulación de respuesta ante incidentes

 Duración: 35–60 minutos

Materiales

- Tarjetas de referencia para participantes de la organización (ver archivo adjunto de la Actividad 2).
- Tarjetas de situación con complicaciones (ver archivo adjunto de la Actividad 2).
- Cronómetro o temporizador
- Pizarra o rotafolio
- Marcadores
- Lapiceras y blocs de notas
- Plan de respuesta ante incidentes real de la organización.

Actividad

En esta actividad se ponen a prueba las capacidades de respuesta transversal utilizando las funciones reales de las personas participantes en la organización, las estrategias de comunicación interna y externa, y los procesos de toma de decisiones al enfrentar incidentes con complicaciones.

Divida a las personas participantes en grupos que representen los equipos reales de respuesta ante incidentes que tiene la organización. Cada participante debe asumir su función real durante una respuesta ante incidentes, o la función más parecida de la tarjeta de participante.

Instrucciones:

1. Entregue una tarjeta de situación a cada grupo donde se describa un incidente de seguridad con complicaciones.
2. Conceda 20 minutos para que los grupos debatan y formulen una estrategia de respuesta usando sus funciones designadas y los procedimientos de la organización.
3. Cada grupo luego debe presentar su plan (5 minutos por grupo).
4. Presente una complicación adicional para cada situación (por ejemplo, “El incidente salió en los medios porque hubo una filtración”).
5. Otorgue 10 minutos a los grupos para que ajusten sus planes en función de esta información nueva utilizando los procedimientos establecidos.
6. Los grupos deben presentar sus planes modificados y analizar cómo se adaptaron dentro de los marcos de la organización.

Instrucciones adicionales para los grupos:

- Se debe hacer referencia al plan real de respuesta ante incidentes de su organización durante los debates.
- Es bueno “pensar en voz alta” para que la toma de decisiones sea visible.
- Fomente la participación de todas las personas con base en sus responsabilidades reales.
- El foco debe estar en las medidas reales que tomaría en la realización de su función.

Debate

 Duración: 15 minutos

Preguntas

- ¿De qué manera les ayudó el ejercicio de ordenar la secuencia de la Actividad 1 como preparación para la simulación?
- ¿Qué desafíos enfrentaron al aplicar los procedimientos reales de la organización?
- ¿Qué brechas identificaron en sus procedimientos actuales de respuesta ante incidentes?
- ¿Qué tan eficaz fue la comunicación entre los departamentos durante los ejercicios?
- ¿Qué capacitaciones adicionales o recursos podrían ayudar a que sientan una mayor preparación ante esas situaciones en su función actual?

Posibles respuestas u orientaciones

- Desafíos: coordinación entre los departamentos, acceder a la información real de contacto, aclarar quién es la autoridad real y quién tiene poder para la toma de decisiones.
- Brechas: vías de escalamiento poco claras, información de contacto desactualizada, autoridades indefinidas para la toma de decisiones, plantillas de notificación faltantes.
- Mejoras: capacitación regular entre departamentos, listas de contactos actualizadas, esquemas de toma de decisiones más claros, guías de referencia rápida específicas para cada función.
- Recursos: tarjetas de respuesta específicas para cada función, simulacros regulares con los miembros reales del equipo, capacitación actualizada del plan de respuesta ante incidentes.

Conclusión

 Duración: 5 minutos

Resuma los aportes clave de ambos ejercicios:

- El ejercicio de secuencia mejoró la comprensión sobre los procedimientos de respuesta ante incidentes de la organización, mientras que la simulación enfatizó los retos de la coordinación en una situación real.
- Para que la respuesta ante incidentes sea eficaz, son fundamentales tanto la preparación individual como la respuesta coordinada en equipo basada en sus atribuciones reales.
- Siempre habrá complicaciones. El éxito depende de la adaptabilidad dentro de los marcos establecidos.

Próximos pasos

- Actualice el plan de respuesta ante incidentes de su organización a partir de las brechas identificadas.
- Actualice las listas de contactos y los protocolos de comunicación.
- Subsane todas las ambigüedades que se hayan detectado en la definición de funciones o la autoridad para la toma de decisiones.
- Programe ejercicios de simulación regulares con los miembros reales del equipo de respuesta ante incidentes para lograr una mejora continua.

Archivo adjunto de la Actividad 1: listas de verificación de la respuesta ante incidentes para repartir

Imprima una copia de esta página cada seis participantes. Corte por las líneas marcadas para crear tarjetas individuales y entregue una tarjeta a cada participante. Para una mayor durabilidad, realice la impresión sobre una cartulina o un papel de alto gramaje.



Lista de verificación para una respuesta rápida ☐ Aislar los sistemas afectados. ☐ Reportar el incidente de inmediato (de acuerdo con la política de escalamiento de la organización). ☐ Evaluar el estado de las copias de seguridad de los datos. ☐ Comunicarse con los organismos policiales (según la política de la organización). ☐ Buscar asesoramiento legal. ☐ Ejecutar la política de respuesta ante pedidos de rescate de la organización (se requiere consultar). ☐ Activar el plan de comunicación que tiene la organización con las partes interesadas. ☐ Registrar la línea temporal del incidente. ☐ Seguir los procedimientos de notificación establecidos para cumplir los requisitos regulatorios. ☐ Movilizar al equipo de respuesta ante incidentes.

Tarjeta de participante Responsable de seguridad de TI Está a cargo del análisis y la contención de los incidentes técnicos. Evalúa el alcance y la naturaleza de la violación de seguridad. Implementa medidas de contención inmediatas. Dirige las actividades de análisis forense. Realiza la coordinación con proveedores de seguridad externos.	Tarjeta de participante Responsable de incidentes Es responsable general de la respuesta ante incidentes y quien toma las decisiones. Coordina todas las actividades del equipo de respuesta. Toma las decisiones estratégicas críticas. Informa al liderazgo ejecutivo. Asigna recursos y prioridades.	Tarjeta de participante Responsable de comunicaciones Gestiona toda la mensajería interna y externa. Ejecuta los planes de comunicación existentes. Redacta las notificaciones a las partes interesadas. Realiza la coordinación con los medios y el equipo de Relaciones Públicas. Supervisa las redes sociales y las noticias.
Tarjeta de participante Responsable de asesoramiento legal Asesora sobre las implicaciones legales y el cumplimiento regulatorio. Garantiza el cumplimiento de las leyes de notificación de violaciones de seguridad. Asesora sobre la preservación de pruebas. Revisa todas las comunicaciones externas. Realiza la coordinación con los organismos policiales en caso de ser necesario.	Tarjeta de participante Representante de RR. HH. Maneja los aspectos relacionados con el personal de la respuesta ante incidentes. Gestiona las comunicaciones internas entre el personal. Se encarga de las investigaciones de amenazas internas. Coordina los servicios de soporte al personal. Aborda las necesidades de continuidad de la fuerza laboral.	Tarjeta de participante Gerente del departamento Representa las operaciones de la unidad comercial afectada. Evalúa el impacto comercial del departamento. Implementa las medidas de continuidad del negocio. Realiza la coordinación con la gerencia de otros departamentos. Informa sobre el estado operativo a la persona responsable de incidentes.
Situación Ataque de ransomware con robo de datos “Cifraron mediante ransomware los servidores de archivos de su organización. Las personas atacantes además se robaron los datos financieros de la clientela y amenazan con publicarlos si no se paga un rescate en un plazo de 24 horas. Complicación: el sistema de copias de seguridad muestra señales de haber sido vulnerado desde hace dos semanas”	Situación Correos electrónicos corporativos comprometidos “Se expuso la cuenta de correo electrónico de la persona a cargo del departamento financiero y se utilizó para autorizar una transferencia bancaria de \$500 000 a una cuenta desconocida. La transferencia se realizó esta mañana. Complicación: se enviaron correos electrónicos fraudulentos similares a tres clientes importantes solicitando ‘información de pagos actualizada’”	Situación Robo interno de datos “Un empleado que estaba abandonando el departamento de TI fue atrapado copiando registros delicados de la clientela en una unidad personal de almacenamiento USB. El personal de seguridad lo detiene a la salida, pero el empleado afirma que los datos ‘solamente son archivos personales del trabajo’. Complicación: el empleado ya publicó mensajes enigmáticos en LinkedIn con afirmaciones como ‘me llevo una experiencia valiosa a mi puesto nuevo’”

Archivo adjunto de la Actividad 2: tarjetas de situación y tarjetas de complicaciones adicionales

Imprima este archivo adjunto y corte por las líneas marcadas para separar las tarjetas que se muestran en esta página.
Para una mayor durabilidad, realice la impresión sobre una cartulina o un papel de alto gramaje.



Situación Vulneración de la cadena de suministro “ El proveedor principal de software de su organización informa que se puso en riesgo su servidor de actualizaciones y que puede que se haya enviado código malicioso a la clientela. Sus sistemas se actualizaron ayer. Complicación: el proveedor se niega a brindar detalles técnicos y dice que conducirá su propia investigación ”	Situación Violación de seguridad física “ Se encontró una persona no autorizada en la sala de servidores después del horario de oficina con una computadora portátil conectada a la red. El personal de seguridad la escoltó fuera del edificio, pero esta persona afirma ser miembro del ‘soporte de TI’. Complicación: varios miembros del personal informaron que sus registros de acceso con insignias muestran una actividad inusual que no realizaron fuera del horario de oficina ”	Situación Vulneración del servicio en la nube “ Su proveedor de servicios de almacenamiento en la nube informa que hubo un acceso no autorizado al repositorio de datos de su organización, que contiene secretos comerciales e información de la clientela. Es posible que esta violación de seguridad exista hace varias semanas. Complicación: la comunicación inicial del proveedor de servicios en la nube contiene información contradictoria sobre el alcance y la cronología del incidente ”
Complicaciones adicionales “ Alerta en los medios: un blog de tecnología publicó un artículo sobre el incidente de seguridad de su organización con detalles específicos que todavía no se habían publicado ”	Complicaciones adicionales “ Aviso regulatorio: el ente regulador de su sector se comunicó para pedirle información de inmediato acerca del incidente y cuáles son sus medidas de respuesta ”	Complicaciones adicionales “ Crisis con un cliente: su cliente más importante pidió una reunión de emergencia para hablar sobre la seguridad de sus datos y amenaza con rescindir el contrato ”
Complicaciones adicionales “ Filtración interna: el personal debate sobre los detalles del incidente a través de los sistemas de mensajería interna, y algunos datos son imprecisos ”	Complicaciones adicionales “ Falla del sistema: durante las tareas de respuesta, un sistema comercial crítico queda fuera de servicio, posiblemente a raíz de las medidas de contención aplicadas ”	Complicaciones adicionales “ Amenaza legal: recibe una carta de un estudio de abogados que representa a la clientela afectada, donde se le pide información detallada sobre la filtración y las medidas de seguridad que se están tomando ”