Crear un **Plan de Respuesta a Incidentes (PRI)** es fundamental para gestionar y mitigar los efectos de incidentes de seguridad de la información de manera efectiva. Este plan proporciona un conjunto de directrices y procedimientos que permiten a una organización responder rápida y eficazmente cuando ocurre un incidente.

A continuación, te presento los pasos para crear un Plan de Respuesta a Incidentes, especialmente aplicable a un entorno de TI en la industria hotelera, pero es adaptable a cualquier organización.

**Pasos para Crear un Plan de Respuesta a Incidentes**

**1. Definir los Objetivos y Alcance del Plan**

* Establecer el propósito del plan, que es minimizar el impacto de los incidentes de seguridad y restablecer la operación normal lo más rápido posible.
* Delimitar el alcance del plan, especificando qué sistemas, datos y servicios están cubiertos por el PRI (por ejemplo, sistemas de reservas, redes Wi-Fi, datos de huéspedes, etc.).

**2. Crear un Equipo de Respuesta a Incidentes (ERI)**

* Formar un equipo con roles y responsabilidades claramente definidos. El ERI podría incluir:
  + **Coordinador de Respuesta a Incidentes**: Supervisa y coordina la respuesta.
  + **Analistas de Seguridad**: Realizan la investigación técnica.
  + **Especialistas en TI**: Ayudan a contener y erradicar el incidente.
  + **Representante de Comunicación**: Maneja la comunicación interna y externa.
  + **Equipo Legal y de Cumplimiento**: Asegura el cumplimiento legal y regulatorio.

**3. Identificar Tipos de Incidentes y Clasificación**

* Establecer una lista de posibles incidentes que podrían ocurrir en el entorno hotelero (por ejemplo, ataques de phishing, malware, pérdida de dispositivos, accesos no autorizados).
* Clasificar los incidentes por su nivel de gravedad y urgencia:
  + **Nivel 1**: Baja severidad (incidentes menores sin impacto significativo).
  + **Nivel 2**: Media severidad (afecta a un área del negocio, pero no es crítica).
  + **Nivel 3**: Alta severidad (incidentes críticos que afectan la operación del hotel).

**4. Desarrollar Procedimientos de Respuesta a Incidentes**

* Definir los pasos detallados a seguir para cada fase de un incidente:

**a. Identificación**:

* Monitorear y detectar incidentes a través de sistemas de seguridad, alertas y reportes de empleados.
* Crear un procedimiento para que los empleados informen rápidamente cualquier sospecha de incidente.

**b. Contención**:

* Implementar acciones inmediatas para evitar que el incidente se propague (por ejemplo, aislar sistemas infectados por malware).
* Establecer procedimientos de contención a corto plazo (aislar el sistema) y a largo plazo (realizar análisis forense).

**c. Erradicación**:

* Eliminar la causa raíz del incidente (por ejemplo, eliminar el malware, cambiar contraseñas comprometidas).

**d. Recuperación**:

* Restaurar los sistemas y datos afectados asegurando que sean seguros antes de reactivar su operación.
* Realizar pruebas de funcionalidad para verificar que el incidente se haya resuelto.

**e. Análisis Posterior y Mejora Continua**:

* Evaluar el incidente y la respuesta para identificar mejoras en el proceso.
* Actualizar el plan de respuesta y la capacitación del personal en base a lo aprendido.

**5. Definir la Comunicación y Escalación de Incidentes**

* Establecer un proceso de comunicación interna y externa, incluyendo:
  + Quién debe ser notificado en caso de un incidente (alta dirección, clientes, proveedores, autoridades, etc.).
  + Cómo y cuándo se debe comunicar la información.

**6. Proporcionar Herramientas y Recursos Necesarios**

* Asegurarse de que el ERI tenga acceso a herramientas de monitoreo, análisis de incidentes, registros de eventos, y software para la gestión de incidentes.

**7. Capacitar al Personal y Realizar Simulacros**

* Realizar simulacros de respuesta a incidentes para que el equipo se familiarice con el plan y pueda reaccionar adecuadamente ante un evento real.
* Capacitar regularmente a los empleados sobre cómo identificar y reportar incidentes.

**8. Mantener y Actualizar el Plan**

* Revisar y actualizar el PRI al menos una vez al año o después de cada incidente importante.
* Asegurarse de que el plan refleje cambios en la infraestructura, personal y amenazas emergentes.

**Ejemplo de Tabla de Plan de Respuesta a Incidentes**

| **Fase** | **Acciones** | **Responsable** | **Herramientas** |
| --- | --- | --- | --- |
| Identificación | Monitorear alertas de seguridad, reportes de empleados | Analista de Seguridad | SIEM, Correo Electrónico |
| Contención | Aislar el dispositivo afectado, bloquear cuentas comprometidas | Administrador de TI | Firewall, Consola de Gestión de Usuarios |
| Erradicación | Eliminar malware, corregir configuración, actualizar contraseñas | Analista de Seguridad | Antivirus, Herramientas de Análisis |
| Recuperación | Restaurar sistemas desde copias de seguridad, verificar integridad | Administrador de Sistemas | Herramientas de Backup |
| Análisis Posterior | Revisar el incidente y mejorar procedimientos | Coordinador de Respuesta | Reportes de Incidentes |

Este plan asegura que la organización esté preparada para identificar, responder y recuperarse de cualquier incidente de seguridad de manera organizada y efectiva, minimizando el impacto en la operación del negocio y protegiendo los datos de los huéspedes y la reputación del hotel.