	<b>Procedimiento de pruebas al plan de respuesta a incidentes</b>	<b>Código: 24-OP-01-11</b>
		<b>Versión: 02</b>
		<b>Página 1 de 3</b>

<b>Procesos Operativos</b>	
<b>Procedimiento:</b>	Procedimiento de pruebas al plan de respuesta a incidentes
<b>Responsables:</b>	<ul style="list-style-type: none"> <li>● Coordinador</li> <li>● Administrador</li> <li>● Asistente</li> <li>● Vendedores</li> <li>● Contabilidad tarjetas</li> <li>● Ingeniero Desarrollo 2</li> <li>● Ingeniero Ciberseguridad Senior</li> <li>● Ingeniero Ciberseguridad Junior</li> </ul>

## Objetivo

Simular los diferentes incidentes establecidos en el procedimiento del plan de respuesta a incidentes, para identificar las falencias, oportunidades de mejora y toma de decisiones en lo relacionado con la certificación PCI DSS.

## Selección de participantes

Se identifican a los miembros del equipo de respuesta a incidentes que participarán en las pruebas, teniendo en cuenta que debe haber un rol por cada incidente. Para ello se hace la prueba en una estación de servicio.


## Diseño de Escenarios de Prueba

Se determinan los siguientes incidentes como escenarios de prueba realistas que abordan diversas amenazas y situaciones que podrían afectar la seguridad de los datos de tarjetas de pago. Incluye situaciones como pérdida de datos, acceso no autorizado, malware, etc.

- Abandono de tarjeta de pago en el comercio.
- Doble transacción, transacción fallida o transacción por valor errado.
- Reclamaciones por sospechas de fraude.
- Pérdida o robo del dispositivo (datáfono).
- Daño del dispositivo.
- Alteración del dispositivo.
- Casos de falla en la conexión.
- Casos de falla en la conexión WiFi – Servidor - Redes.

## Notificación y Simulación

Se notifica a los participantes sobre el inicio de las pruebas y se simula un incidente de seguridad según los escenarios diseñados. Para ello estará el guía de la prueba, con la matriz

 Pruebas procedimiento de incidentes donde se verificará el paso a paso de cada incidente y si se cumple con el procedimiento para cada caso.


### **Evaluación de Respuesta**


Se evalúa la respuesta del equipo a cada escenario de prueba. Se examina la efectividad de las medidas tomadas para contener, mitigar y resolver el incidente. Se verifica la aplicación adecuada de controles de seguridad y procedimientos establecidos en el plan de respuesta a incidentes.

### **Documentación**

Se documenta en la guía en el campo de observaciones, cada paso tomado durante las pruebas, incluyendo observaciones, resultados y lecciones aprendidas. Adicionalmente cada participante firma en constancia de realización de la misma. Este documento se carga en la carpeta “17. DATAFONOS” de la estación donde se realizó la prueba.

### **Revisión Posterior**

Realiza una revisión posterior de las pruebas con el administrador y personal con el que se realizaron dichas pruebas de respuesta a incidentes con base en la matriz  Pruebas procedimiento de incidentes

Se discuten los resultados, se identifican áreas de fortaleza y debilidad, y se proponen mejoras al plan con el equipo de trabajo los cuales quedan registrados en el campo de “Conclusiones y Comentarios de las pruebas”  Pruebas procedimiento de incidentes

### **Actualización del Plan**

Están directamente relacionadas con los nuevos requerimientos que presente la norma PCI-DSS, las nuevas prácticas que surjan para mejorar la seguridad de la información y los resultados que arrojen las pruebas de procedimiento de incidentes mencionadas en el punto anterior.

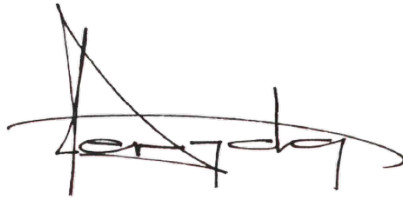
### **Repetición Periódica**

Programa pruebas con periodicidad semestral para mantener el plan de respuesta a incidentes actualizado y asegurar la efectividad continua.

### **Sanción**

Por incumplimiento de las funciones y procedimientos del cargo conforme a la circular normativa, manual de funciones y procedimientos, código de conducta y reglamento interno de trabajo dependiente del impacto económico, operación y de imagen y de acuerdo a la gravedad del incumplimiento; el jefe inmediato aplicará los correctivos y medidas correspondientes de acuerdo al reglamento interno de trabajo.

**Aprobación**



**Cesar Ayala Pizano**  
**DIRECTOR OPERATIVO**

**Control de cambios**

CONTROL DE CAMBIOS		
Versión	Fecha	Justificación de la versión
1	16/01/2024	Creación
2	25/01/2024	Actualización Procedimiento plan de respuestas a incidentes