

Pruebas de recuperación de servicios tecnológicos

Pruebas de recuperación de servicios tecnológicos

- Una vez realizado el análisis de capacidades de recuperación de servicios tecnológicos con la Gerencia de TI y Operaciones, a continuación se plantean las siguientes pruebas:

Prueba #1: Activación de canal secundario de acceso a internet y VPNs

Prueba #1: Activación de canal secundario de acceso a internet y VPNs

No.	Escenario de Desastre	Causas
1.	Indisponibilidad del canal principal de acceso a internet y VPNs 11-10-2024 Horario no hábil 8:00pm	• Falla en canales de comunicación: Corte de fibras. • Daño de dispositivos de comunicación. Routers. • Acceso físico no autorizado. • Errores humanos. • Amenazas naturales.

Prueba #1: Activación de canal secundario de acceso a internet y VPNs

Participantes Internos

Nombre	Cargo	Contacto
Jair Antonio Villanueva Ricardo	Gerencia de TI y Operaciones	JairVR@idea.gov.co
Alexander Restrepo Zuluaga	Dirección de TI	AlexanderRZ@idea.gov.co
Carlos Eduardo Ochoa	Profesional Universitario	carlosoa@idea.gov.co
Diego Londoño	Profesional Universitario	diegolv@idea.gov.co
Diana Sirley Ortiz Velásquez	Gerente de Riesgos	DianaOV@idea.gov.co
William René Alvarado Ordóñez	Dirección de Ciberseguridad y Seguridad de la Información	WilliamAO@idea.gov.co
Leydy Carolina Barrios Urrego	Contratista- Gerencia de Riesgos	LeydyBU@idea.gov.co

Prueba #1: Activación de canal secundario de acceso a internet y VPNs

Participantes Externos

Proveedor	Nombre y Cargo	Contacto
Tigo UNE - Canales	No se requiere en la prueba	
Core IP – Ciberseguridad – Firewall	No se requiere en la prueba	
Proveedor SOC - Olimpia	Requerido	Dirección de Ciberseguridad y Seguridad de la Información
Valor Mas – VPNs Linea 800 Mesa de Servicio	Requerido	Dirección de TI
SIIF G&G	Requerido	Dirección de TI
Conectividad Bancos	Pruebas de autenticación en portales	Gerencia de TI y Operaciones
Iseguras (Observadores)	Plinio Palomino – Consultor BCP Juan Santoyo – Consultor BCP Joaquin Afanador – Consultor BCP	plinio.palomino@iseguras.com.co juan.santoyo@iseguras.com.co joaquin.afanador@iseguras.com.co

Prueba #1: Activación de canal secundario de acceso a internet y VPNs

Alcance de la prueba

Actividad	Tiempo Estimado
1. Se dará inicio a la prueba una vez todos los participantes invitados se unan la reunión de Teams.	10 min
2. La Gerencia de TI y Operaciones simulará la falla del canal principal y verificará que el canal secundario permita la conectividad según lo esperado.	10 min
3. Una vez se verifique la operación del canal secundario se procederá con las pruebas de las siguientes VPNs:	
• VPN site to site entre IDEA y Azure	5 min
• VPN site to site entre IDEA y G&G producción	5 min
• VPN site to site entre IDEA y G&G contingencia	30 min
• VPN site to site entre IDEA y SOC	10 min
• Pruebas con portales bancarios	10 min
4. Se declara el éxito de la prueba.	5 min
5. Se identifican lecciones aprendidas.	10 min
6. Fin de la prueba.	
Tiempo estimado de la prueba	**1:35 horas**

Prueba #2: Activación contingencias de Software Gestión Documental "G+"

Prueba #2: Activación contingencias de Software Gestión Documental "G+"

No.	Escenario de Desastre	Causas
2.	Indisponibilidad del servidor principal de BD del Software Gestión Documental "G+" ubicado en Azure 16-10-2024 Horario no hábil	• Ciberataques. • Modificación no autorizada. • Errores de configuración. • Errores humanos. • Errores de actualización de parches.

Prueba #2: Activación contingencias de Software Gestión Documental "G+"

Participantes Internos

Nombre	Cargo	Contacto
Jair Antonio Villanueva Ricardo	Gerencia de TI y Operaciones	JairVR@idea.gov.co
Alexander Restrepo Zuluaga	Dirección de TI	AlexanderRZ@idea.gov.co
Carlos Eduardo Ochoa	Profesional Universitario	carlosoa@idea.gov.co
Diego Londoño	Profesional Universitario	diegolv@idea.gov.co
Diana Sirley Ortiz Velásquez	Gerente de Riesgos	DianaOV@idea.gov.co
William René Alvarado Ordóñez	Dirección de Ciberseguridad y Seguridad de la Información	WilliamAO@idea.gov.co
Leydy Carolina Barrios Urrego	Contratista- Gerencia de Riesgos	LeydyBU@idea.gov.co
Definir usuario	Centro Administración Documental	Leydy Carolina Barrios Urrego
Definir usuario	Oficina Jurídica – respuesta a derechos de petición	Leydy Carolina Barrios Urrego

Prueba #2: Activación contingencias de Software Gestión Documental "G+"

Participantes Externos

Proveedor	Nombre y Cargo	Contacto
Proveedor Software - Gestion Positiva	No se requiere en la prueba	
Iseguras (Observadores)	Plinio Palomino – Consultor BCP Juan Santoyo – Consultor BCP Joaquin Afanador – Consultor BCP	plinio.palomino@iseguras.com.co juan.santoyo@iseguras.com.co joaquin.afanador@iseguras.com.co

Prueba #2: Activación contingencias de Software Gestión Documental "G+"

Alcance de la prueba

Actividad	Tiempo Estimado
1. Se dará inicio a la prueba una vez todos los participantes invitados se unan la reunión de Teams.	10 min
2. La Gerencia de TI y Operaciones simulará la falla del servidor de BD principal del Software Gestión Documental "G+".	10 min
3. Una vez se verifique que el servidor de BD principal del Software Gestión Documental "G+“, aparece como desconectado se verificará que el servidor secundario asume la carga.	5 min
4. Cuando la Gerencia de TI y Operaciones informe que el servidor secundario se encuentra operativo, se realizarán pruebas de usuario final del Software Gestión Documental "G+“, para verificar que el sistema continua operando con normalidad y sin pérdida de información. • ***Pruebas por parte del Centro Administración Documental y Oficina Jurídica***	30 min
5. Se declara el éxito de la prueba.	5 min
6. Se identifican lecciones aprendidas.	10 min
7. Fin de la prueba.	
Tiempo estimado de la prueba	**1:10 horas**

Prueba #3: Activación ambiente de contingencia de G&G

Prueba #3: Activación ambiente de contingencia de G&G

No.	Escenario de Desastre	Causas
3.	Indisponibilidad de los servicios del SIIF desde el Datacenter de Producción de IBM Cloud ubicado en Dallas. Fecha pendiente de disponibilidad del proveedor - Dirección de TI Horario hábil	• Fallas de energía eléctrica prolongadas. • Falla en canales de comunicación: Corte de fibras. • Falla de los sistemas de aire acondicionado de precisión. • Daño de infraestructura tecnológica crítica. • Ciberataques. • Acceso físico no autorizado. • Errores humanos. • Amenazas naturales.

Prueba #3: Activación ambiente de contingencia de G&G

Participantes Internos

Nombre	Cargo	Contacto
Jair Antonio Villanueva Ricardo	Gerencia de TI y Operaciones	JairVR@idea.gov.co
Alexander Restrepo Zuluaga	Dirección de TI	AlexanderRZ@idea.gov.co
William René Alvarado Ordóñez	Dirección de Ciberseguridad y Seguridad de la Información	WilliamAO@idea.gov.co
Diana Sirley Ortiz Velásquez	Profesional Universitario - Gerencia de Riesgos	DianaOV@idea.gov.co
Leydy Carolina Barrios Urrego	Profesional Universitario - Gerencia de Riesgos	LeydyBU@idea.gov.co

Participantes Externos

Proveedor	Nombre y Cargo	Contacto
Sistemas G&G	William Martínez - Gerente de soporte	william.martinez@sistemasgyg.com.co 7446999 ext. 143
Sistemas G&G	Giovany Cadena - Director de soporte	giovany.cadena@sistemasgyg.com.co 7446999 ext. 209 ext. 1421
Iseguras (Observadores)	Plinio Palomino – Consultor BCP Juan Santoyo – Consultor BCP Joaquin Afanador – Consultor BCP	plinio.palomino@iseguras.com.co juan.santoyo@iseguras.com.co joaquin.afanador@iseguras.com.co

Actividad	Tiempo Estimado
1. Se dará inicio a la prueba una vez todos los participantes invitados se unan la reunión de Teams.	10 min
2. La Gerencia de TI y Operaciones solicitará al proveedor G&G activar el ambiente de contingencia ubicado en la nube de IBM en Washington. **Viernes**	30 min
3. Luego se solicitará la restauración de un backup completo de la BD del sistema SIIF **POS. Viernes**	
4. Se verificara la restauración del backup. **Viernes**	
5. Una vez finalizado el proceso de restauración se procederá con la verificación de que los servidores de aplicación cuenten con la última configuración. **Viernes**	30 min
6. Una vez finalizado las verificaciones de infraestrcutura se procederá con la asignación de credenciales en ambiente de contingencia. **Lunes**	30 min
Se da visto bueno para operar en contingencia durante el día **Lunes.**	
En la noche del día **Lunes** se hace backup de BD del sistema SIIF POS y se restaura en el ambiente productivo	
El día M**artes** se verifica que los datos trabajado el día lunes estén en el ambiente productivo	
8. Se declara el éxito de la prueba.	5 min
9. Se identifican lecciones aprendidas.	10 min
10. Fin de la prueba.	
Tiempo estimado de la prueba	**7:25 horas**

IDEA

Fase 2 - Pruebas BCP

Prueba #4: Gestión de Crisis

No.	Escenario de Desastre	Objetivo
4.	Interrupción de procesos o sistemas de información misionales Situaciones que no interrumpen, pero si generan impacto alto: • Fuga de Información • Incumplimiento Regulatorio 1-11-2024 Horario hábil Gerencia de Riesgos Gerencia de TI y Operaciones Oficina Comunicaciones	• Convocar al comité de continuidad o de crisis • Analizar la situación presentada • Invitar equipos de respuesta al comité: ➢ Equipo de Respuesta a Emergencias ➢ Equipo de Evaluación de Daños en Instalaciones ➢ Equipo DRP • Tomar la decisión de activar el BCP / DRP • Enviar notificaciones correspondientes

Prueba #5: Prueba Integral

No.	Escenario de Desastre	Objetivo
4.	Interrupción de procesos o sistemas de información misionales 8-11-2024 Horario no hábil	• Convocar al comité de continuidad o de crisis • Analizar la situación presentada • Invitar equipos de respuesta al comité: ➢ Equipo de Respuesta a Emergencias ➢ Equipo de Evaluación de Daños en Instalaciones ➢ Equipo DRP • Tomar la decisión de activar el BCP / DRP • **Activar estrategias para la recuperacion de procesos** • **Activar estrategias para la recuperacion de sistemas de información** • Enviar notificaciones correspondientes


IDEA