Plan de Continuidad de Negocio para Tecnologías de Información

Contenido

1. Resumen Ejecutivo

Un Plan de Continuidad de Negocio (por sus siglas en ingles BCP, Business Continuity Plan) es un plan de emergencia con el objetivo de mantener la funcionalidad de la organización a un nivel mínimo aceptable durante una contingencia. Debe contemplar las medidas preventivas y de recuperación para cuando se produzca una contingencia que afecte al negocio.

El proceso de BCP se llevará a cabo después de un evento de emergencia de tecnología, en la evaluación de daños definidos, es mandatorio bajo la naturaleza de la emergencia y la magnitud de los daños valuados como sea permitido. El área de BCP trabajará en la coordinación del plan y el resultado de los daños evaluados bajo los formatos implementados para el análisis de daños.

2. Introducción

Este documento contiene el Plan de Continuidad del Negocio para la Dirección Tecnologías de Información del Grupo Ventura. Está destinado describir las tareas y procedimientos que serían necesarios para facilitar el proceso de toma de decisiones de la administración y su respuesta oportuna a cualquier interrupción disruptiva de la infraestructura de Tecnologías de Información en el ambiente productivo.

Grupo Ventura es una empresa 100% mexicana con más de 10 años de experiencia especializada en subastas electrónicas. Vamos a la vanguardia. Utilizamos tecnología para el desarrollo de soluciones integrales automatizadas para la venta y/o compra de bienes y/o servicios.

Grupo Ventura ofrece una amplia gama de productos y servicios para la comercialización de salvamentos, autos seminuevos y autopartes a través de subastas electrónicas contando con la base más grande del país de compradores especializados.

3. Objetivo del Manual

Proporcionar el plan de Continuidad de Negocio para la Dirección de Tecnologías de Información de Grupo Ventura.

3.1. Objetivo General

El objetivo del Plan de Continuidad de Negocio (BCP), es disminuir el impacto ante cualquier incidente o fallo en los sistemas productivos alojados en la nube de Microsoft Azure, así mismo, que la Dirección de TI de Grupo Ventura esté preparada para poder responder y accionar oportunamente ante estos eventos.

3.2. Objetivos específicos

- Proporcionar un mapa de los procesos críticos para la continuidad de los sistemas de tecnologías de información productivos alojados en la nube de Microsoft Azure de Grupo Ventura.
- Determinar e identificar a los propietarios de los procesos críticos y definir claramente su responsabilidad y ámbito de acción en lo respectivo a la administración de riesgos de cada proceso.
- Establecer el marco de acción general y específico que guiará a la organización frente a la materialización de un escenario de riesgo que afecte la operación normal.
- Definir la estructura organizacional, roles y responsabilidades de los equipos que realizarán las actividades específicas necesarias para responder frente a la contingencia en sus diversas fases, esto es:
    - En el momento siguiente a su ocurrencia;
    - durante la activación y vigencia del proceso de operación alternativa y,
    - finalmente, durante la restauración a la operación normal de los procesos afectados.
- Adherencia y cumplimiento de la normativa vigente en relación a la existencia de planes de continuidad de negocio.

4. Alcance

El alcance de este plan se relaciona con los servicios relacionados a los usuarios y clientes de Grupo Ventura que utilicen los servicios de Tecnologías de Información productivos alojados en la nube de Microsoft Azure.

- VSIS
- CATALOGO
- VSAS
- PAGINA WEB

Este plan es el diseño para cubrir los siguientes riesgos y vulnerabilidades de tecnología

- Riesgos:
  - Caída del sistema
  - Configuración errónea
  - Difusión de software dañino (virus, malware, etc.)
  - Funcionamiento anómalo

- Vulnerabilidades
  - de desbordamiento de buffer
  - de error de formato de cadena (format string bugs)
  - de denegación del servicio

5. Hipótesis

El presente plan está basado en el servicio que proporcionan los activos productivos de Tecnologías de Información para Grupo Ventura, los cuales han sido identificados como críticos para su adecuada operación:

La funcionalidad adecuada del plan esta sujeta a que se presenten algún fallo de los activos previamente descritos.

6. Responsable del Documento

- Dirección de Tecnologías de Información
- Gerencia de Seguridad de TI

7. Frecuencia de Revisión

Este procedimiento se deberá modificar toda vez que por necesidad del área sea requerido o surjan adecuaciones al documento los cuales, previa validación, serán llevados a cabo con un tiempo de planeación y puesta en marcha para el uso del documento.

8. Lista de Distribución

- Dirección General de Subastas Ventura
- Dirección de Tecnologías de Información
- Gerencia de Infraestructura de TI
- Gerencia de Seguridad de TI

9. Glosario

Activo

En relación con la seguridad de la información se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Alcance

Límite que aplica a un proceso, procedimiento, certificación, contrato, etc. y que detalla las especificaciones y responsabilidades de todas las partes para la elaboración de un producto, la entrega de un servicio o un proyecto.

Amenazas

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis del impacto del negocio

Proceso del análisis de actividades y el efecto que una interrupción del negocio podría tener sobre ellas. (ISO 22301)

Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Categorías de Riesgos

Tipos de riesgo similares son agrupados bajo un título clave, también conocido como "categorías de riesgo". Estas categorías incluyen reputación, estrategia, financieros, inversiones, infraestructura operativa, negocio, cumplimiento regulatorio, subcontratación, personas, tecnología y conocimientos.

Ciberseguridad

Es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil,

Control

Es el proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo o potenciar oportunidades positivas.

Evaluación de vulnerabilidades

Revisión sistemática de un sistema de información o producto para determinar la suficiencia de las medidas de seguridad, identificar deficiencias de seguridad, proporcionar datos para predecir la eficacia de las medidas de seguridad propuestas y confirmar que tales medidas son idóneas después de la implementación.

Plan de Continuidad de Negocio

Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel pre-definido de operación debido a la interrupción. (ISO 22301).

Probabilidad

Posibilidad verosímil y fundada de que algo suceda, haya sido esto definido, medido o estimado objetiva o subjetivamente. Se pueden utilizar términos descriptivos generales (tales como "improbable", "poco probable", "probable", "casi seguro"), frecuencias o probabilidades matemáticas. Puede ser expresado cualitativa o cuantitativamente.

Recuperación

Actividades y programas diseñados para regresar las condiciones a un nivel que sea aceptable para la entidad.

Riesgo

Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos resultantes.

Riesgo inherente

Es el cálculo del daño probable a un activo de encontrarse desprotegido, sin controles.

Seguridad de la información

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Trazabilidad

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad

Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

10. Referencias

- ISO/IEC 27000, Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary
- ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements
- ISO 22301:2012, Sistemas de Gestión y Continuidad del Negocio.
- Marianne Swanson. (Mayo 2010). NIST Special Publication 800-34 Rev. 1. En Contingency Planning Guide for Federal Information Systems(149). NIST: U.S. Department of Commerce.
- ISACA Costa Rica. (2014). Introducción al ISO 22301 - Nuevo estándar de Continuidad de Negocios . 16-Oct-2015, de ISACA Costa Rica Sitio web: https://www.youtube.com/watch?v=hUdUT9OU7yc
- Contingency Planning World. (2012). Business Impact. 2015, de Contingency Planning World Sitio web: http://www.business-continuity-world.com/

11. Plan de Continuidad de Negocio para la Dirección de TI

Fases Generales del plan BCP

11.1 Conceptos de operación

Los sistemas identificados por el área de Tecnologías de Información como críticos están a cargo de las siguientes áreas de Grupo Ventura:

- Gerencia de Infraestructura de Tecnologías de Información.
- Gerencia de Desarrollo de Sistemas
- Administrador de Base de Datos

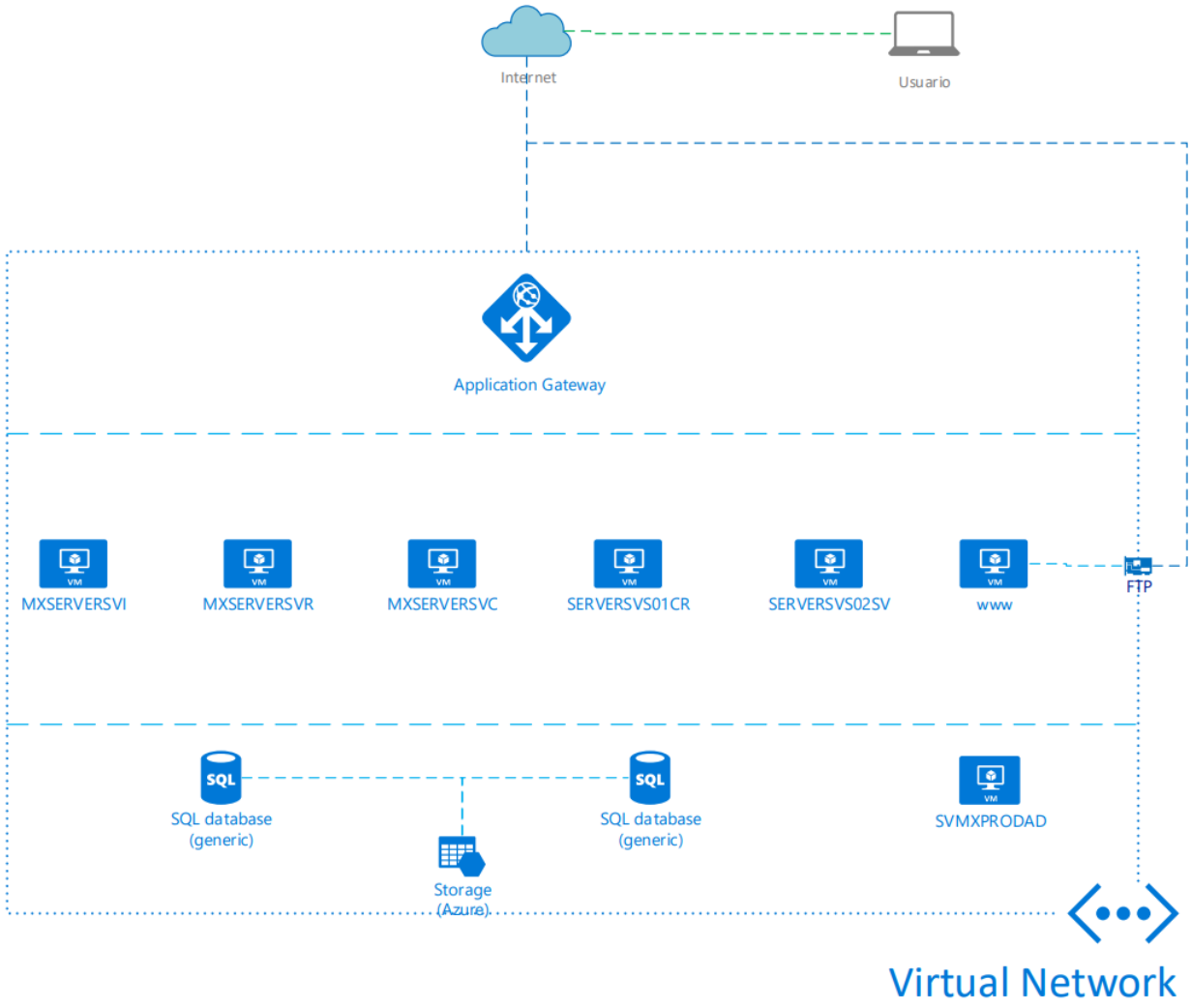
La Dirección de TI de Grupo Ventura tiene sus sistemas productivos hospedados en la nube de Microsoft Azure. A continuación se mencionan lo mas importantes:

#	Nombre del Sistema	Descripción del Sistema	Responsable
1	VSIS	Sistema Integral de Salvamentos es el sistema principal de Grupo Ventura. Principales funciones: • Administrar compradores • Inventario las subastas • Ingresos y los cierres de subastas	• GIT • DBA • GDS
2	CATALOGO	Catalogo de las subastas	• GIT • DBA • GDS
3	VSAS	Sistema administrador de las subastas	• GIT • DBA • GDS
4	PAGINA WEB	Pagina principal de todos los sistemas de Grupo Ventura	• GIT • GDS
5	APLICATIVOS	Un servidor de aplicaciones un sistema especializado cuyo software entrega servicios a otras computadoras o personas (clientes)	• GDS

11.2 Acrónimos

DTI	Dirección de Tecnologías de Información
GIT	Gerencia de Infraestructura de Tecnologías de Información
DBA	Administrador de Base de Datos
GDS	Gerencia de Desarrollo de Sistemas
GSI	Gerencia de Seguridad de la Información

11.3 Esquema de conectividad



11.4 Roles y responsabilidades

Nombre	Responsabilidad
Usuario Interno	• Notificar anomalías en caso de fallo
Dirección TI	• Toma de decisiones • Recibir notificaciones • Contratos vigentes de proveedores de internet • Autorizar la adquisición y renovación de tecnologías
Gerencia de Infraestructura de TI	• Consultoría sobre anomalías detectadas en TI • Activar Plan BCP • Escalar fallos o anomalías con proveedores • Validación continúa de equipos de cómputo, dispositivos de red y UPS.
Gerencia Seguridad Informática	• Coordinar actividades para aplicar el plan BCP • Documentación de actividades realizas previas, durante y posteriores a la ejecución del plan. • Activar Plan BCP
Proveedor Microsoft Azure	• Respetar y garantizar los niveles de servicio acordados en garantías en enlaces de internet

11.5 Fase de Activación y Notificación

Durante la contingencia o incidente, la prioridad de Grupo Ventura es proporcionar el servicio que el usuario/cliente necesita. El presente Plan de Continuidad de Negocio (BCP) se asegura de que el conjunto de procedimientos de respuesta establecidos previamente se encuentren en total disponibilidad y debidamente documentados con el fin de proporcionar un mejor control y resolución de cualquier situación de emergencia.

11.5.1 Criterios de Activación

El Plan de Continuidad debe ser accionado y empezar su operación siempre y cuando se presente cualquiera de los siguientes escenarios:

#	Componente Critico	D*	Comentarios
	Infraestructura del Servidor		
	Servicios aplicativos en línea		
	Certificado Digital Vigente		
	Codificación del sistema		
	Base de Datos		

D* = Disponibilidad del componente

11.5.2 Notificación

Si cualquiera de los escenarios mencionados anteriormente se ha materializado los pasos a seguir deben ser ejecutados por los propietarios del Componente Critico:

#	Componente Critico	GIT	DBA	GDS	GSI	DTI
	Infraestructura del Servidor	✓				
	Servicios en línea (FTP)	✓	✓	✓		
	Servicios en línea (www)	✓	✓	✓		
	Disrupción en aplicación			✓		
	Base de Datos		✓			
	Activación del BCP	✓			✓	✓

En cualquiera de los escenarios para una apropiada ejecución deberá apegarse a los lineamientos establecidos en el presente plan conforme a:

- Realizar las notificaciones correspondientes (Anexo B – Lista de Contactos)
- Ejecutar el plan conforme a las actividades y responsabilidades descritas en la Fase de Recuperación.

11.6 Fase de Recuperación

#	Componente Critico	Resp	Actividad		Tiempo
1	Pagina Web	GIT	PW_1	Validar comunicación	5 min
		GIT	PW_2	SI es un problema de conectividad IR a INF_1 SINO IR a PW_3	---
		GIT	PW_3	SI es un problema servicio WEB IR a PW_3 SINO IR a PW_6	---
		GIT	PW_4	Reiniciar servicio WEB	5 min
		GIT	PW_5	SI el problema esta resuelto IR a PW_F SINO IR a PW_6	---
		GIT	PW_6	Revisión de logs del servidor IR a PW_7	30 min
		GIT	PW_7	SI es un problema de configuración IR a PW_8 SINO IR a PW_11	---
		GIT	PW_8	Revisar y corregir la configuración	5 min
		GIT	PW_9	Reiniciar servicio WEB	---
		GIT	PW_10	SI el problema esta solucionado IR a PW_F SINO IR a INF_1	5 min
		GDS	PW_11	Revisar los endpoint de la aplicación	30 min
		GDS	PW_12	SI el problema es de endpoint IR a PW_13 SINO IR a INF_1	---
		GDS	PW_13	Corregir endpoint	10 min
		GDS	PW_14	Reiniciar servicio WEB ir a PW_10	5 min
		GIT	PW_F	Informar servicio restablecido	2 min

#	Componente Critico	Resp	Actividad		Tiempo
2	Servicio FTP	GIT	FTP_1	Validar comunicación	5 min
		GIT	FTP_2	SI es problema de comunicación ir a Infra_0 SINO IR a FTP_3	---
		GIT	FTP_3	SI es problema del servicio FTP ir a FTP_4 SINO IR a FTP_6	---
		GIT	FTP_4	Reiniciar servicio de FTP	5 min
		GIT	FTP_5	SI se resolvió el problema ir a FTP_F SINO IR a INF_1	---
		GIT	FTP_6	Revisión de logs del servidor y configuración del firewall	30 min
		GIT	FTP_7	SI se identifico el problema IR a FTP_8 SINO IR a INF_1	10 min
		GIT	FTP_8	Solucionar el problema	---
		GIT	FTP_9	Reiniciar el servicio	5 min
		GIT	FTP_10	SI se resolvió el problema ir a FTP_F SINO IR a INF_1	---
		GIT	FTP_F	Informar servicio restablecido	2 min

#	Componente Critico	Resp	Actividad		Tiempo
3	Infra_Servidor _Productivo	GIT	INF_1	Verificar comunicación	5 min
		GIT	INF_2	Si es problema de comunicación IR a INF_3	---
		GIT	INF_3	Entrar a la consola de Azure	1 min
		GIT	INF_4	Identificar el problema	20 min
		GIT	INF_5	Solucionar el problema	2 min
		GIT	INF_6	Si el servicio ha sido restablecido ir a INF_F SINO IR a INF_7	---
		GIT	INF_7	**ACTIVAR BCP**	1 min
		GIT	INF_8	Reiniciar servicio	5 min
		GIT	INF_9	Si es problema del servicio ir a INF_10 SINO IR INF_13	---
		GIT	INF_10	Reiniciar servicios	5 min
		GIT	INF_11	Comprobar servicios	5 min
		GIT	INF_12	Si se resolvió el problema IR a INF_6 SINO IR INF_8	---
		GIT	INF_13	Revisar los recursos	2 min
		GIT	INF_14	Si es problema de recursos IR A INF_15 SINO IR a INF_19	---
		GIT	INF_15	Modificar recurso	10 min
		GIT	INF_16	Planificar los cambios y planear el reinicio	10 min
		GIT	INF_17	Programar ventana de mantenimiento	10 min
		GIT	INF_18	Si se resolvió el problema IR a INF_6 SINO IR INF_13	---
		GIT	INF_19	Si es problema de conexión con Base de Datos IR a INF_20 SINO IR INF_22	---
		GIT	INF_20	Verificar conectividad con BD	5 min
		GIT	INF_21	Si es problema de conectividad IR a INF_! SINO IR a BD_1	---
		GIT	INF_22	Revisar disco duro	2 min
		GIT	INF_23	Si es problema con disco duro IR a INF_24 SINO IR INF_13	---
		GIT	INF_24	Corregir problema de disco duro	30 min
		GIT	INF_25	Si se resolvió el problema IR a INF_6 SINO IR a INF_1	---
		GIT	INF_F	Informar servicio restablecido	2 min

#	Componente Critico	Resp	Actividad		Tiempo
4	Base_Datos	DBA	BD_1	Verificar bloqueo de la base de datos	1 min
		DBA	BD_2	Si el problema es por bloqueo IR A BD_3 SINO IR BD_13	---
		DBA	BD_3	Verificar consulta IR A BD_4 y BD_5	10 min
		DBA	BD_4	Enviar a desarrollo	2 min
		DBA	BD_5	SI se desbloquea en 5 minutos IR A BD_9 SINO IR BD_6	---
		DBA	BD_6	Eliminar consulta	5 min
		DBA	BD_7	Analizar respuesta de desarrollo y tomar acción	10 min
		DBA	BD_8	Verificar consistencia de Base de Datos IR a BD_11	30 min
		DBA	BD_9	Desbloqueo de Base de datos de forma automática	5 min
		DBA	BD_10	Si funciona el desbloqueado y a BD_11 SINO IR a BD_1	---
		DBA	BD_11	Verificar funcionalidad	10 min
		DBA	BD_12	SI el problema se soluciono IR a BD_F SINO IR a BD_1	---
		DBA	BD_13	Verificar disponibilidad de la base de datos	10 min
		DBA	BD_14	Si es el problema es la disponibilidad IR a BD_15 SINO IR a BD_18	---
		DBA	BD_15	Esperar 25 minutos	25 min
		DBA	BD_16	Si el problema persiste IR a BD_17 SINO IR a BD_12	---
		DBA	BD_17	**Activar BCP**	1 min
		DBA	BD_18	Revisar logs de la base de datos	30 min
		DBA	BD_19	Si se ha identificado el problema IR a BD_20 SINO IR a BD_17	---
		DBA	BD_20	Si el problema es el servidor IR a INF_1 SINO IR a BD_21	---
		DBA	BD_21	Si el problema es base de datos IR BD_22 SINO IR a BD_23	---
		DBA	BD_22	Solucionar problema de base de datos IR a BD_12	10 min
		DBA	BD_23	Si el problema es Desarrollo IR a BD_24 SINO IR a BD_18	---
		DBA	BD_24	Enviar consulta a Desarrollo	5 min
		DBA	BD_25	Si el problema es la consulta IR a BD_1 SINO IR a APL_1	---
		DBA	BD_F	Informar servicio restablecido	2 min

#	Componente Critico	Resp	Actividad		Tiempo
5	Aplicativos	GDS	APL_1	Revisar logs/querys	2 hrs
		GDS	APL_2	SI es problema de código IR a APL_3 SINO IR a APL_9	---
		GDS	APL_3	Revisar y corregir el problema	1 – 3 hr
		GDS	APL_4	Planificar los cambios y programar el reinicio	1 – 2 hr
		GDS	APL_5	Aplicar corrección durante ventana de mantenimiento	30 min
		GDS	APL_6	Realizar comprobación	1 hr
		GDS	APL_7	SI el problema esta resuelto IR A APL_F sino IR a APL_8	---
		GDS	APL_8	Aplicar Rollback e IR a APL_3	1 - 4 hr
		GDS	APL_9	SI es problema de comunicación de Base de Datos IR a APL_10 SINO ir APL_14	---
		GDS	APL_10	Revisar conexiones existentes	10 min
		GDS	APL_11	SI las conexiones son suficientes IR a BD_1 SINO IR a APL_12	---
		GDS	APL_12	Aumentar pool de servicios	10 min
		GDS	APL_13	SI persiste el problema IR a BD_1 SINO IR a APL_4	---
		GDS	APL_14	SI es problema de memoria IR a APL_15 SINO IR APL_18	---
		GDS	APL_15	Programar ventana de mantenimiento	10 min
		GDS	APL_16	Incrementar memoria del servidor de aplicaciones	10 min
		GDS	APL_17	SI es problema de memoria RAM IR a INF_0 SINO IR APL_18	---
		GDS	APL_18	SI hay comunicación entre 2 o mas sistemas problema de memoria RAM IR a APL_19 SINO IR INF_0	---
		GDS	APL_19	Revisar y ajustar endpoint	30 min
		GDS	APL_20	SI se soluciono el problema IR a APL_F SINO IR APL_21	---
		GDS	APL_21	Revisar que 2 o mas aplicaciones no estén en el mismo puerto	30 min
		GDS	APL_22	SI se soluciono el problema IR a APL_F SINO IR APL_1	---
		GDS	APL_F	Informar servicio restablecido	2 min

#	Componente Critico	Resp	Actividad		Tiempo
6	Cert_Digita	GIT	Cert_1	Validar fecha de vigencia	1 min
		GIT	Cert_2	Si el problema es de caducidad IR a Cert_10 SINO IR a Cert_3	---
		GIT	Cert_3	Si el archivo de configuración esta dañado IR a Cert_5 SINO IR a Cert_6	---
		GIT	Cert_4	Generar archivo dañado	10 min
		GIT	Cert_5	Validar configuración archivo	5 min
		GIT	Cert_6	Programar ventana de mantenimiento	10 min
		GIT	Cert_7	Reiniciar servicios	5 min
		GIT	Cert_8	Verificar funcionalidad	10 min
		GIT	Cert_9	Si el se ha restablecido el servicio IR a Cert_F SINO IR a Cert_5	---
		GIT	Cert_10	Si el problema es del cliente IR a Cert_10 SINO IR a Cert_17	---
		GIT	Cert_11	Solicitar al cliente el nuevo certificado	5 min
		GIT	Cert_12	Esperar el nuevo certificado	Indefinido
		GIT	Cert_13	Instalar el nuevo certificado	10 min
		GIT	Cert_14	Programar ventana de mantenimiento	10 min
		GIT	Cert_15	Reiniciar servicios	5 min
		GIT	Cert_16	Si el servicio se ha restablecido IR a Cert_F SINO IR a Cert_11	---
		GIT	Cert_17	Solicitar renovación del nuevo certificado	2 min
		GIT	Cert_18	Generar archivo de configuración	5 min
		GIT	Cert_19	Solicitar el pago	5 min
		GIT	Cert_20	Esperar a que proceda el pago	Indefinido
		GIT	Cert_21	Renovar el certificado con el proveedor	5 min
		GIT	Cert_22	Esperar nuevo certificado	4 hrs
		GIT	Cert_23	Cargar/instalar certificado en webserver y en infraestructura WAF	20 min
		GIT	Cert_24	Programar ventana de mantenimiento	10 min
		GIT	Cert_25	Reiniciar servicios	5 min
		GIT	Cert_26	Si el servicio se ha restablecido IR a Cert_F SINO IR a Cert_27	---
		GIT	Cert_27	Validar configuración e IR a Cert_23	5 min
		GIT	Cert_F	Informar servicio restablecido	2 min

11.7 Fase de Reconstitución

La reconstitución es el proceso por el cual las actividades de recuperación se han completado y las operaciones normales del sistema se reanudaron. La determinación debe hacerse de si el sistema ha experimentado un cambio significativo y requerirá la reevaluación y reautorización.

11.7.1 Validación

#	Componente Critico	Resp	Actividad	D*
1	Servicio FTP	GIT	Validar conectividad a nivel de TCP/IP	
			nslookup	
			ping	
			Validar servicio FTP	
			Validar actividad de servicio FTP (modo operacional)	
			Revisar la configuración del Firewall	
			Logs activos	

#	Componente Critico	Resp	Actividad	D*
2	Pagina Web	GIT	Validar conectividad a nivel de TCP/IP	
			nslookup	
			ping	
			Validar funcionalidad del servicio WEB	
			Verificar archivos de configuración correspondientes al servicio Web	
			Logs activos	
		GDS	Validar los endpoint a la aplicación	

#	Componente Critico	Resp	Actividad	D*
3	Infra_Servidor_Prod	GIT	Validar conectividad a nivel de TCP/IP	
			nslookup	
			ping	
			Acceso a la consola de Microsoft Azure	
			Servicios habilitados	
			Recursos óptimos para Servidor	
			Memoria	
			Procesador	
			Espacio en disco	
			Conectividad con Base de Datos	

#	Componente Critico	Resp	Actividad	D*
4	Base de Datos	DBA	Base de datos disponible	
			Motor de base de datos operacional	
			Recursos óptimos para Base de Datos	
			Memoria	
			Procesador	
			Espacio en disco	
			Logs activos	

#	Componente Critico	Resp	Actividad	D*
5	Aplicativos	GDS	Revisar que los procesos estén funcionando adecuadamente	
			Código en operación	
			Validar comunicación con la base de datos	
			Recursos óptimos para Servidor de aplicaciones	
			Memoria	
			Procesador	
			Espacio en disco	
			Revisar servicios en modo operacional	

#	Componente Critico	Resp	Actividad	D*
7	Certificado Digital (cliente o Grupo Ventura)	GIT	Validar fecha de vigencia	
			Validar instalación correcta del certificado	

D* = Disponibilidad

11.7.2 Notificar a los involucrados

Cada vez que se finalice la validación correspondiente se deberá notificarse a todos los involucrados para que estén informados acerca del resultado y ejecución del plan de contingencia.

Ver Anexo B – Lista de Contactos Sistemas y Operación (Directores)

11.7.3 Documentación

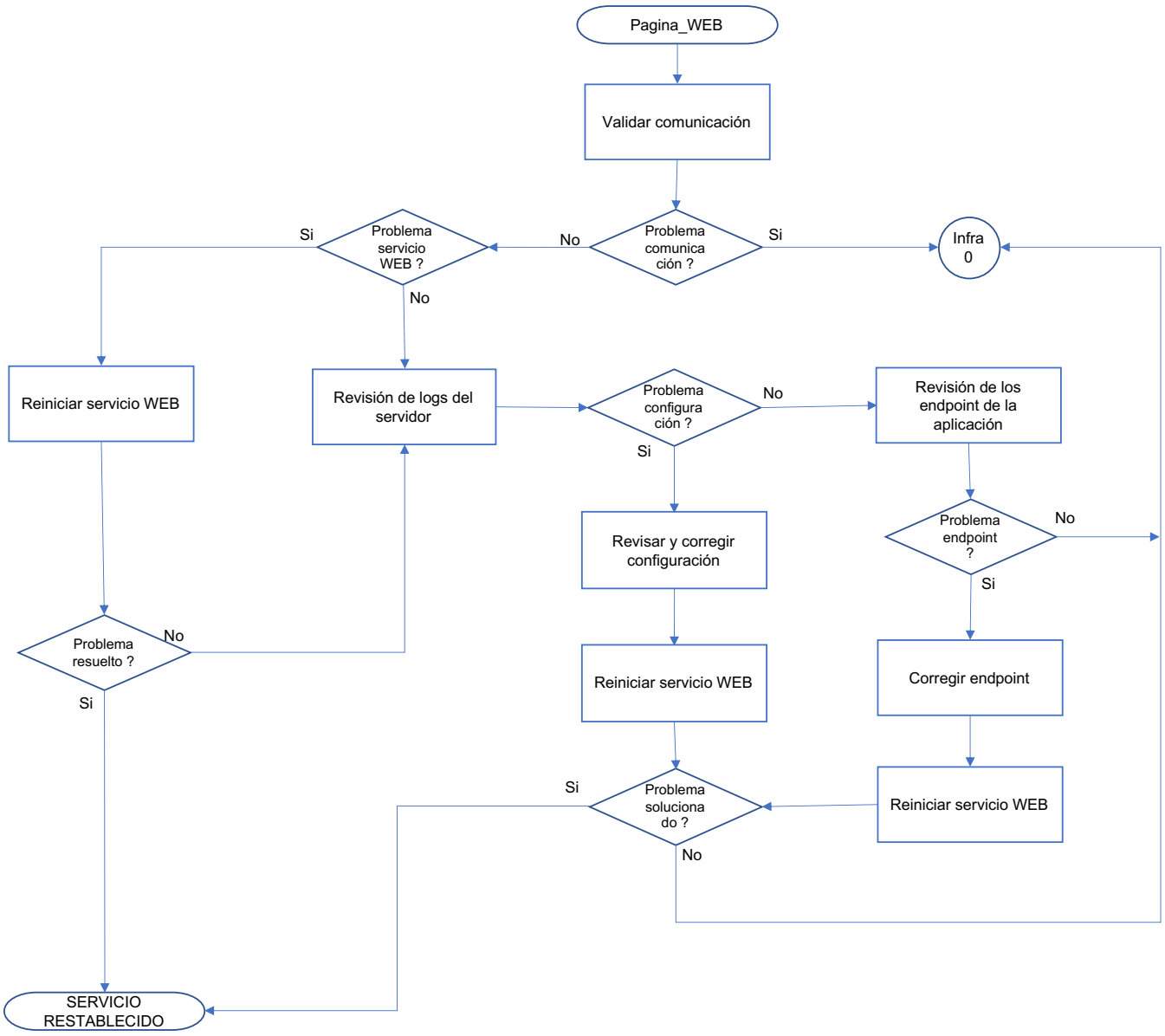
La documentación que se debe incluir dentro de esta fase debe considerar los siguientes aspectos:

- Lecciones aprendidas.
- Actividades realizadas (configuración, validación, entre otras)
- Resultado de las pruebas.

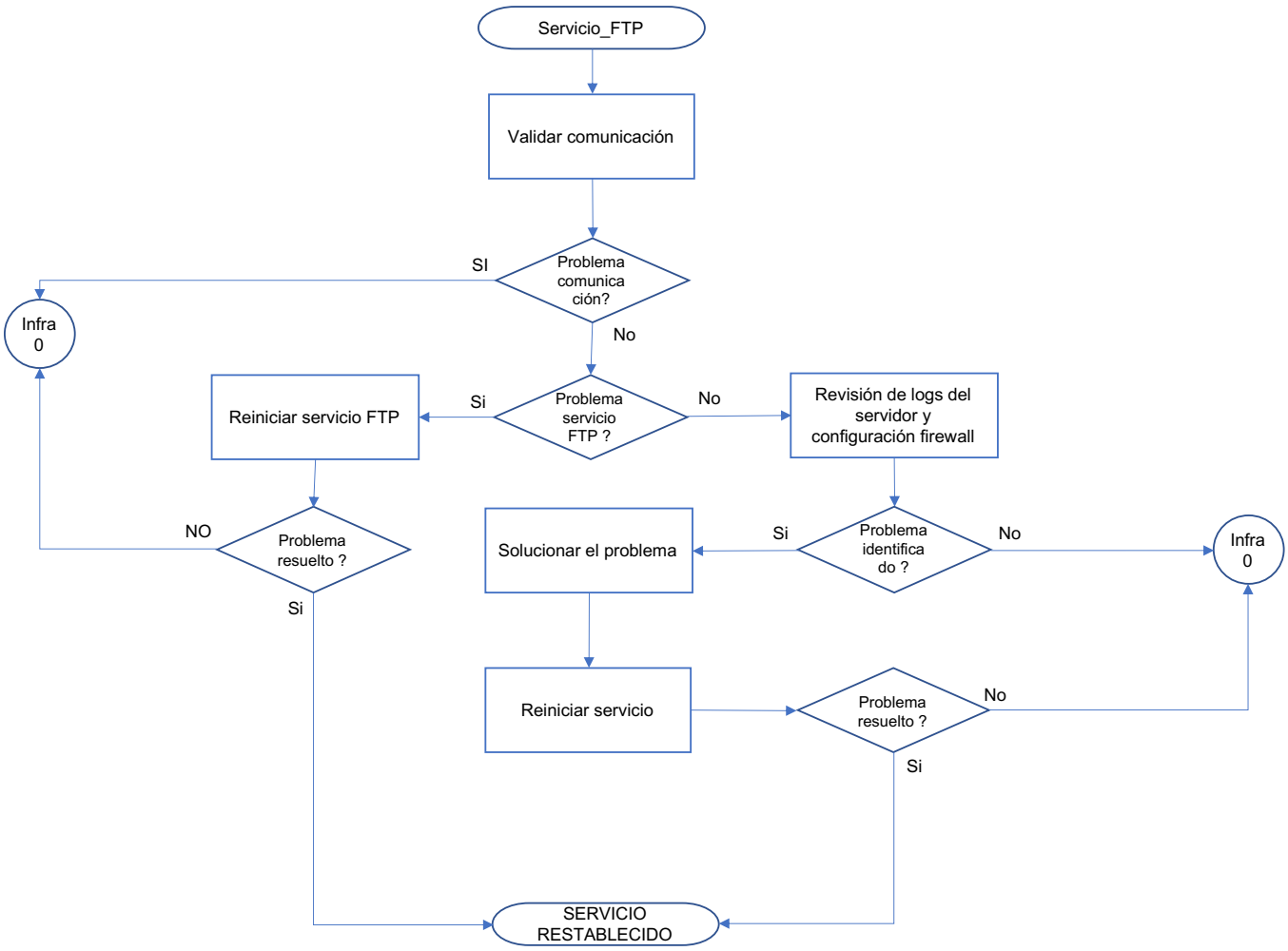
Anexo A – Lista de Contactos

Nombre	Cargo	Área	Teléfono	Correo Electrónico
Francisco González	Director de TI	Sistemas	5548513351	fgonzalez@g-ventura.com
Eloy Flores	Gerente de Infraestructura de TI	Sistemas	5512401711	eflores@g-ventura.com
Jorge Martínez	Gerente de Desarrollo	Sistemas	5564453097	jmartinez@g-ventura.com
Eloy Flores	DBA	Sistemas	5512401711	eflores@g-ventura.com
Luis Díaz	Arquitecto de Seguridad de TI	Sistemas	7221685760	ldiaz@g-ventura.com
José Luis Oceguera	Subdirector de Operaciones	Operaciones	5513206360	joceguera@g-ventura.com
Cesar Tapia	Director General	Dirección	5628322033	ctapia@g-ventura.com

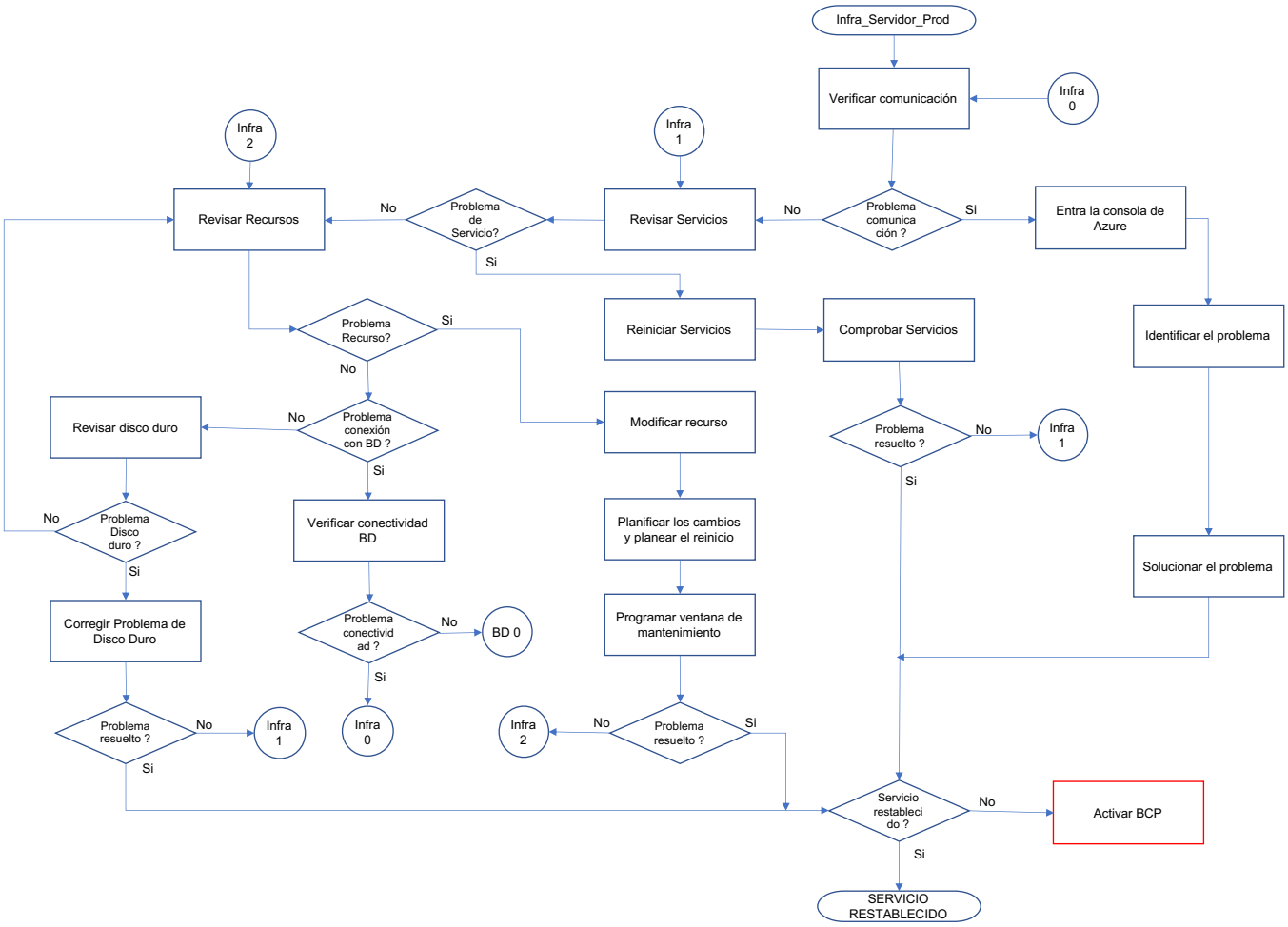
Anexo B – Diagramas de Activación – Pagina WEB



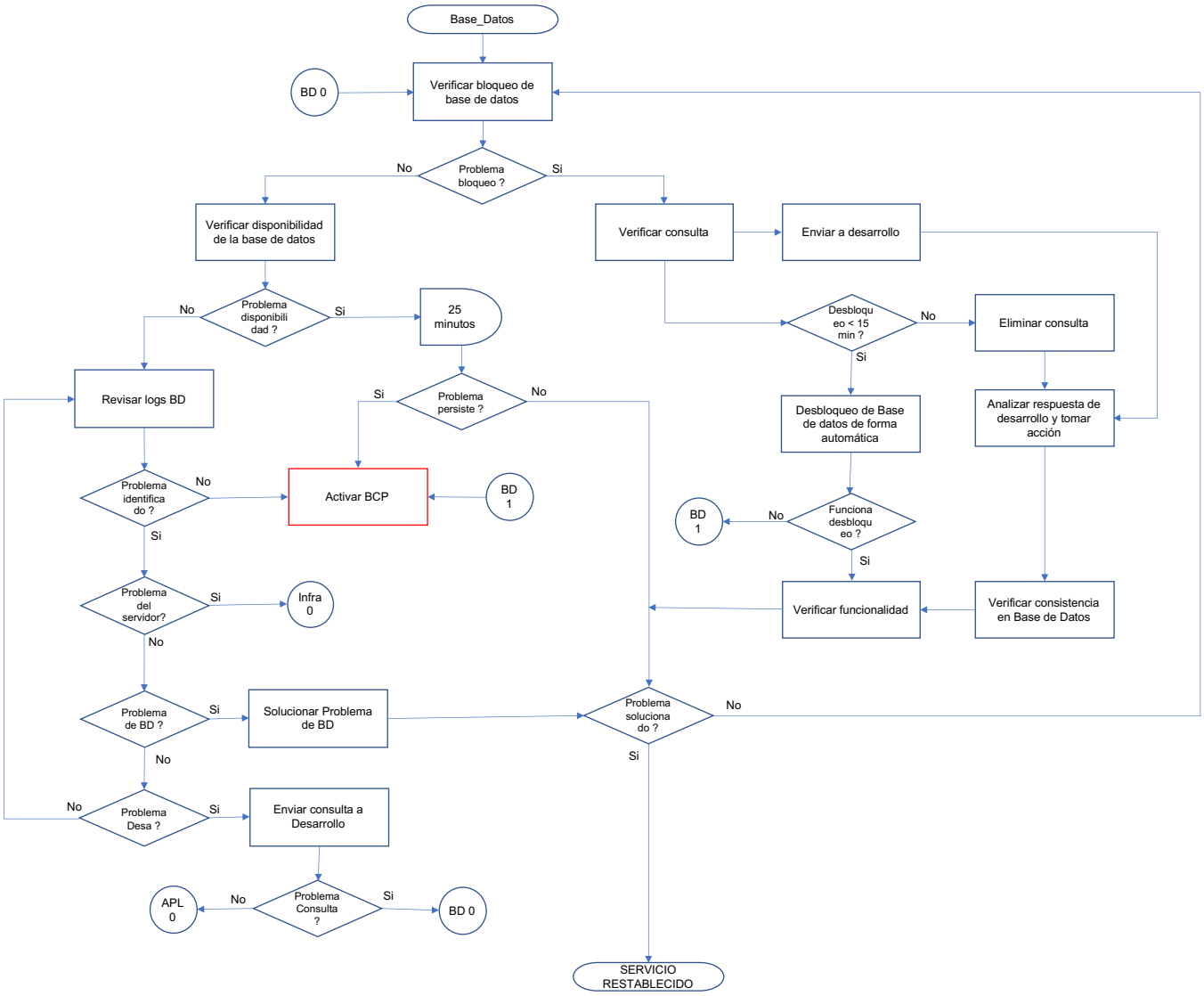
Diagramas de Activación – Servicio FTP



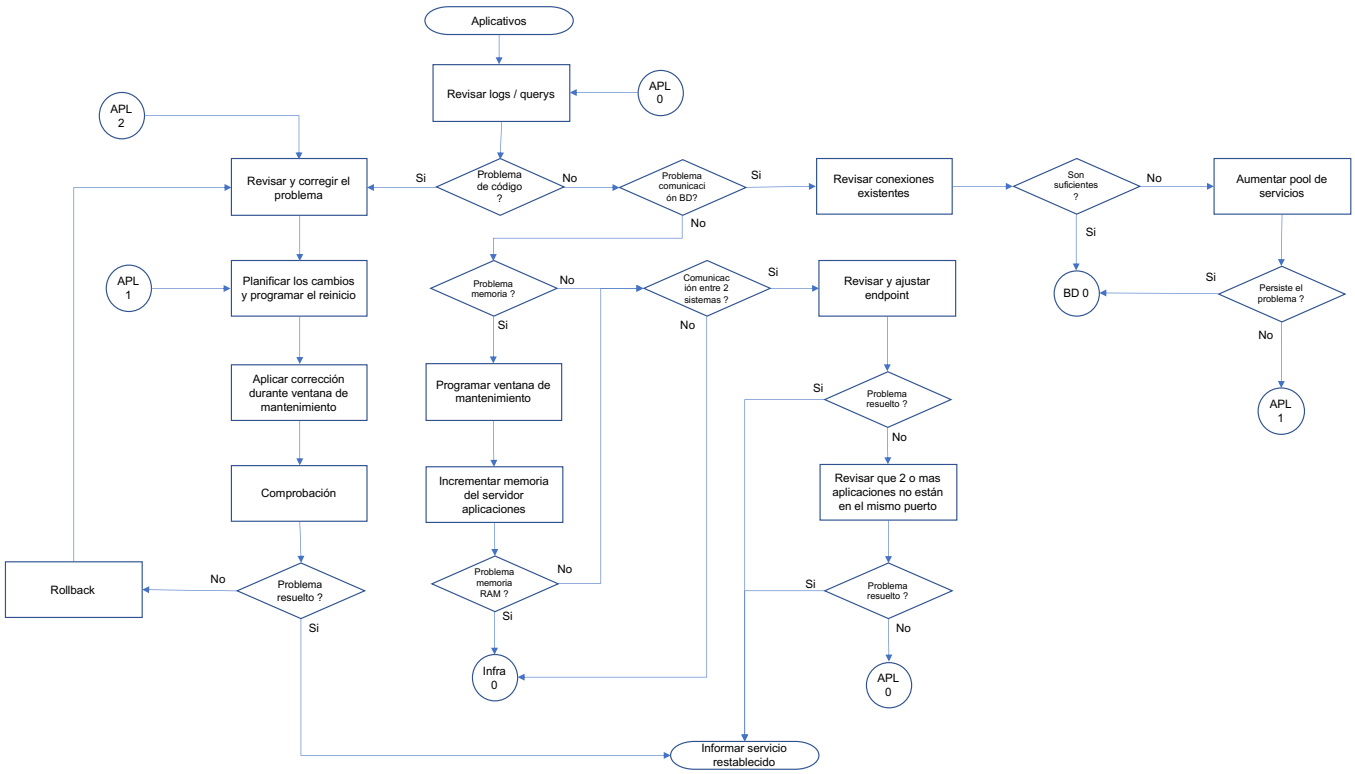
Diagramas de Activación – Infraestructura Servidor Productivo



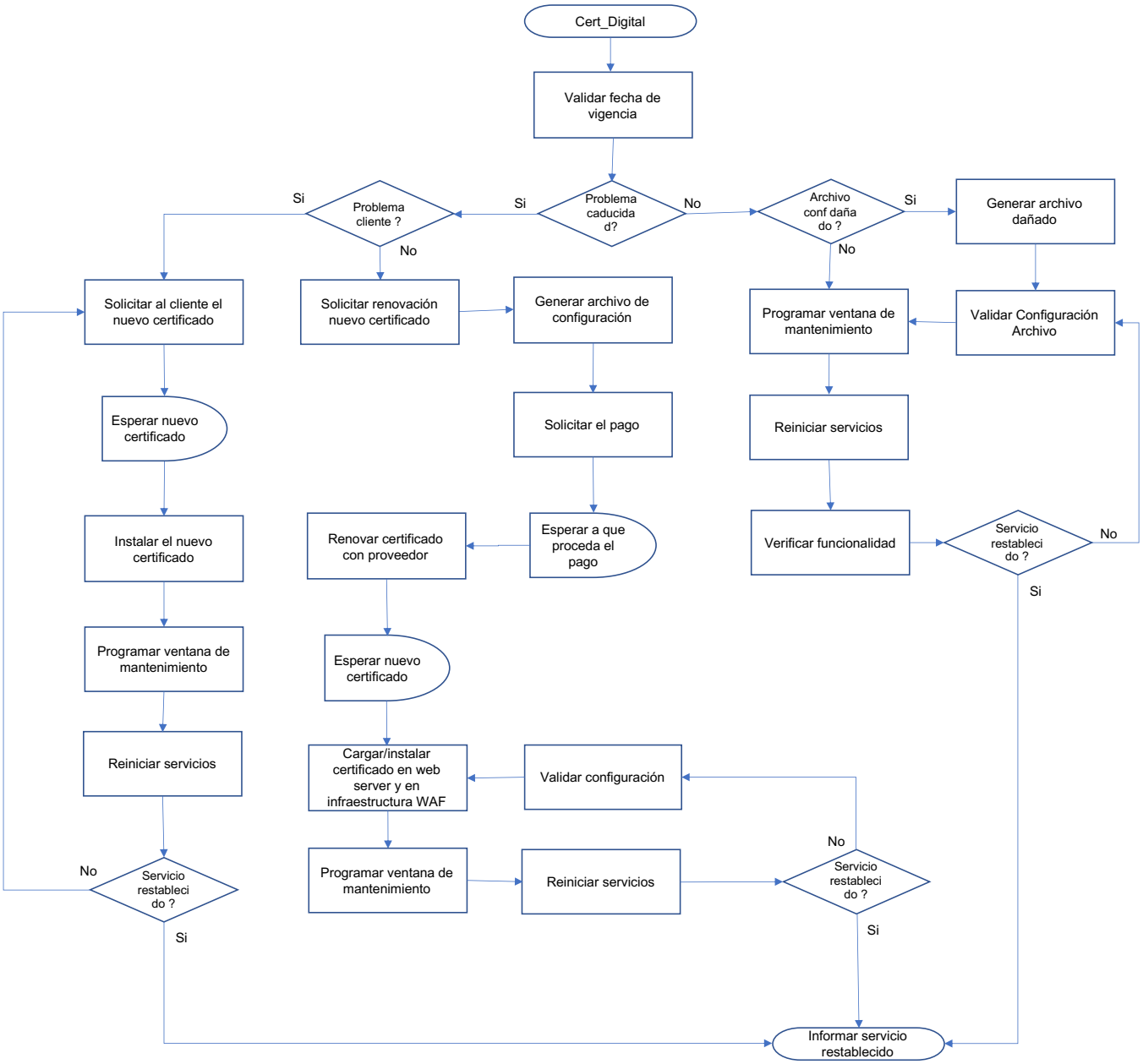
Diagramas de Activación – Base de Datos



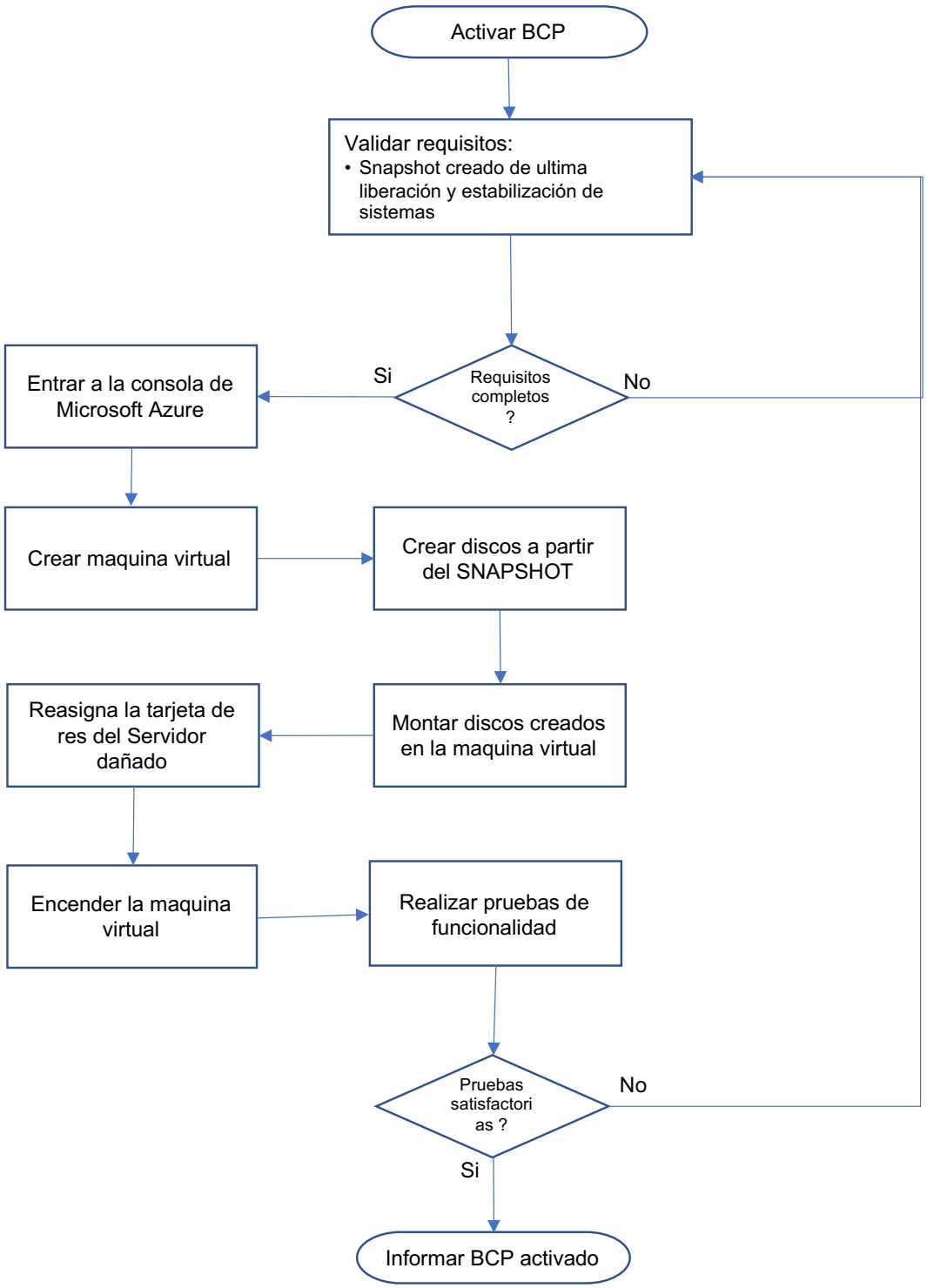
Diagramas de Activación – Aplicativos



Diagramas de Activación – Certificados Digitales



Diagramas de Activación – BCP



12. Control de Cambios

Elaboró	Comentarios	Fecha
Eloy Flores Luis M Díaz	Sesión con Gerencia de Infraestructura de Tecnologías de Información para definir el alcance 1.	27-Abr-20
Luis M Díaz	Creación de primera versión (alcance 1) del presente documento	27-Abr-20
Luis M Díaz	Avance del 30% del total de documento	30-Abr-20
Luis M Díaz	Avance del 60% del total de documento	06-May-20
Luis M Díaz	Avance del 90% del total de documento	09-May-20
Luis M Díaz	Avance del 90% del total de documento	09-May-20
Francisco González Eloy Flores Luis M Díaz	Sesión con Dirección de TI y Gerencia de Infraestructura de Tecnologías de Información para definir el alcance 2.	12-May-20
Eloy Flores Luis M Díaz	Sesión con Gerencia de Infraestructura de Tecnologías de Información para revisión general y explicar la infra hospedada en Microsoft Azure	19-May-20
Francisco González Eloy Flores Luis M Díaz	Sesión con Gerencia de Infraestructura de Tecnologías de Información para revisión general.	20-May-20
Francisco González Luis M Díaz	Revisión de BCP de otras áreas de Ventura Estandarizar formato	22-May-20 - 26-May-20
Francisco González Eloy Flores Luis M Díaz	Adecuaciones al documento Definir alcance 3. Avance 15%	31-Jul-20
Luis M Díaz	Avance 20% del total de documento	03-Ago-20
Luis M Díaz	Avance 35% del total de documento	04-Ago-20
Eloy Flores Luis M Díaz	Sesión de revisión con Gerencia de Infraestructura de Tecnologías de Información	04-Ago-20
Luis M Díaz	Avance 50% del total de documento	05-Ago-20
Luis M Díaz	Avance 60% del total de documento	06-Ago-20
Luis M Díaz	Avance 90% del total de documento	07-Ago-20
Luis M Díaz	Documento finalizado. Pendiente de revisión	10-Ago-20
Eloy Flores Luis M Díaz	Sesión de revisión con Gerencia de Infraestructura de Tecnologías de Información	13-Ago-20 25-31 Ago-20 02-Sept-20
Eloy Flores Luis M Díaz	Sesión de revisión con Gerencia de Infraestructura de Tecnologías de Información y Dirección de TI	11-Ago-20 18-Ago-20 21-Ago-20 24-Ago-20 28-Ago-20 01-Sept-20 03-Sept-20
Luis M Díaz	Documento finalizado.	04-Sept-20
Luis M Díaz	Actualización del árbol de llamadas	30-Ago-21

13. Autorizaciones

Ciudad de México, Mayo 2021.

Tomando como base y consideración que el presente Plan de Continuidad de Negocio (BCP) es un plan de emergencia con el objetivo de mantener la funcionalidad de la organización a un nivel mínimo aceptable durante una contingencia con un nivel de riesgo aceptado por la Dirección de Tecnología de Información de Grupo Ventura.

El Plan de Continuidad de Negocio contempla las medidas preventivas y de recuperación para cuando se presente una contingencia que afecte al negocio.

El alcance ha sido elaborado, revisado y aprobado por la Dirección de TI conforme los requerimientos establecidos e identificados con el personal de TI. La planificación, presupuesto y evaluación de riesgos han sido gestionados, adquiridos y autorizados previamente a la realización del presente documento.

La Dirección de TI se ha comprometido a publicar, difundir, concientizar y ejecutar lo dispuesto en la presente resolución.

De conformidad la Dirección de Tecnología de Información de Grupo Ventura aprueba el presente Plan de Continuidad de Negocio 2020 (basado en el témplate del estándar NIST Special Publication 800-34 Rev. 1), de acuerdo con lo estipulado en cada una de las fases descritas del presente documento.

Elaboró	Revisó	Autorizó
_____ Luis Manuel Díaz Cerda Arquitecto de Seguridad de TI	_____ Eloy Flores Galicia Gerente de Infraestructura TI	_____ Francisco Javier González Blancas Director Tecnología de Información