



FLORES GARIBAY®

CONSULTORÍA FISCAL, LEGAL Y DE NEGOCIOS

Certeza, crecimiento y tranquilidad

**MODELO DE GESTION DE LAS
TECNOLOGIAS DE LA INFORMACION**

FLORES GARIBAY CONSULTORES S.C.

CONFIDENCIAL

1. Historial de cambios

Revisión	Fecha	Autor	Nombre de Documento
0.01	22 Sep 2014	Ing. Oscar Vázquez del Mercado	MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION FGC.DOCX

NOTAS DE REVISIÓN

Revisión	Fecha	Autor	NOTAS

2. Contenido

1. Historial de cambios	2
2. Contenido	3
3. Introducción	4
3.1 Propósito	4
3.2 Alcance	4
6. Requisitos específicos	5

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

3. Introducción

3.1 Propósito

Describir en detalle el MODELO DE GESTIÓN de las tecnologías de la información que permite a Flores Garibay Consultores S.C. cumplir con sus objetivos.

3.2 Alcance

Este documento establece con detalle los elementos fundamentales de gestión de las tecnologías de la información en Flores Garibay Consultores S.C..

Se definen los elementos generales siguientes:

1. *POLITICA INTERNA DE GESTIÓN DE LA INFORMACION*
2. *MODELO DE CLASIFICACION DE LA INFORMACION*
3. *ANALISIS DE RIESGOS, EVALUACION Y CONTROLES*
4. *INDICADORES DE GESTION*
5. *PLAN DE RECUPERACION DE DESASTRES - DRP*
6. *ARQUITECTURA DE RED*
7. *DOMINIOS, PROCESOS Y ROLES*
8. *CUMPLIMIENTO REGULATORIO*

Se definen las categorías particulares siguientes para el tratamiento de la información:

- 1.- *DATOS DE COLABORADORES*
 - 1.1 *SOCIOS*
 - 1.2 *ASOCIADOS*
 - 1.3 *EMPLEADOS*
 - 1.4 *BECARIOS*
 - 1.5 *ASPIRANTES*
- 2.- *DATOS DE CLIENTES*
- 3.- *DATOS DE PROVEEDORES*
- 4.- *DATOS DE SOCIOS DE NEGOCIOS*
- 5.- *DATOS DE VISITANTES*



**POLITICA INTERNA DE
GESTION DE LA INFORMACION**
FLORES GARIBAY CONSULTORES S.C.

 <p>FLORES GARIBAY CONSULTORIA FISCAL, LEGAL Y DE NEGOCIOS</p>	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

1. POLITICA INTERNA DE GESTION DE LA INFORMACION

I. PRELIMINARES

Responsable: DEPARTAMENTO DE SISTEMAS

Ámbito de aplicación: El presente documento aplica para las bases de datos del grupo empresarial FLORES GARIBAY, correspondiente a información relacionada al ejercicio de la actividad de giro y a su objeto social.

FLORES GARIBAY está comprometido a proteger la veracidad, confidencialidad, transparencia, integridad y seguridad de la información personal que clientes, existentes y potenciales nos confían. Nuestra política de privacidad incluye normas y procedimientos relacionados con el uso y la divulgación de información acerca de nuestros clientes e incorpora cualquier operación o conjunto de operaciones sobre recolección, almacenamiento, uso, circulación o supresión de datos personales de los clientes de FLORES GARIBAY.

II. PROTECCIÓN DE DATOS

La LFPDPPP, conocida como Ley de Protección de Datos Personales, incluye disposiciones generales para la protección de datos personales. En cumplimiento de esta normativa, FLORES GARIBAY informa mediante un aviso de privacidad en la página web de la compañía [http:// www.floresgaribay.com.mx/](http://www.floresgaribay.com.mx/), a sus clientes que la compañía no comparte información personal con terceros, excepto en lo que atañe al correcto desarrollo de los contratos y negocios jurídicos celebrados con ellos, así como para las finalidades que autoricen y para los casos permitidos por ley. Así mismo, la compañía divulga y da a conocer en sus clientes nuestras políticas para la Protección de Datos Personales, al momento en que la relación comercial es establecida y la misma se mantiene en la página web de la compañía para libre consulta. De igual manera, se informa a los clientes al momento de establecer la relación la ubicación de las políticas y procedimientos de tratamiento de datos personales

a. Información Personal

Es definida como cualquier información respecto de una persona, que no es de público acceso o que puede obtenerse sin reserva alguna.

b. Dato personal

Se entiende como cualquier información vinculada o que pueda asociarse a una o varias personas determinadas o determinables. El hecho de ser asegurado, el número del documento de identificación, teléfonos, direcciones, información financiera y estado de salud son algunos datos personales.

c. Autorización del cliente.

Si cualquiera de los datos personales es requerido por una persona fuera del ámbito de servicio y/o comercial proporcionado o en el contrato celebrado, incluido pero no limitado a la reclamación, la autorización de servicio de salud o estudios relacionados, la compañía debe contar con la autorización

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

escrita del tomador, asegurado o intermediario, previo a la entrega de los datos. La misma autorización debe solicitarse si tratándose de un servicio prestado, el beneficiario es una persona distinta del cliente y éste no lo ha autorizado para acceder a su información personal, a excepción de que el cliente haya fallecido y así se verifique.

El formato de autorización para que el cliente permita que FLORES GARIBAY maneje sus datos personales se adjunta como parte de los formatos de control interno, listados en la estructura documental del Modelo de Gestión.

d. Limitación de acceso interno.

El contenido de los archivos relativos a los servicios, resultados, informes, etc. de FLORES GARIBAY no puede ser discutido o comentados con compañeros de trabajo o familiares o personas que no requieran esa información o no tengan derecho a conocerla.

e. Control de la reproducción y destrucción de documentos.

Los archivos que contengan datos personales de clientes, proveedores, empleados, colaboradores, socios, asociados o intermediarios que sean objeto de reproducción o impresión, deberán retirarse del lugar de reproducción de manera inmediata evitando que otras personas puedan tener acceso a ellos. Los mismos archivos en caso de tener que ser desechados, serán destruidos manual o mecánicamente de forma tal que se evite el acceso a la información que ellos contienen.

f. Política de escritorio limpio.

Los documentos que contengan datos personales solamente se colocan en los escritorios mientras el personal de la firma está trabajando en ellos; cuando el personal de la firma termine de utilizarlos, o se levante, o se retira al final del día, debe guardar los documentos que contienen datos personales en gabinete bajo llave. Cuando otra persona se acerca a hablar con el personal de la firma, se debe bloquear por cualquier medio la visibilidad de la información o cerrar el expediente.

g. Política de bloqueo de pantalla.

Cuando el personal de la firma que maneje datos personales de clientes se levante de su escritorio, alguien se acerque a su escritorio, o se retire al final del día, debe dar CTRL+ALT+DELETE y seleccionar bloquear pantalla o apagar el computador. En todo caso, transcurridos cinco (5) minutos sin actividad en el computador, se ha programado su bloqueo automático.

h. Declaración de privacidad al pie de los correos electrónicos.

Los correos electrónicos del personal de la firma FLORES GARIBAY, deben incluir una nota que aparezca automáticamente que indique que cualquier información contenida en el mismo tiene carácter privilegiado y confidencial. (Si bien este tipo de información no tiene en todos los casos protección legal, se incluye a modo preventivo).

i. Protección de información confidencial en Recepción.

Cuando se recibe información confidencial en la Recepción, se debe depositar en un sobre opaco o adjuntarle una portada, para que mientras se espera a su reparto al área encargada, tal información no pueda ser vista por personas que se acercan a Recepción.

j. Expediente de información sensible.

Los documentos que contengan datos personales deben mantenerse en un sistema interno de control

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

de operación y funciones, en una carpeta protegida a la cual solamente tengan acceso los autorizados.

k. Limitación de acceso a Intermediarios.

Los intermediarios con quienes FLORES GARIBAY tenga vínculo comercial deberán suscribir un acuerdo de confidencialidad que proteja la privacidad de los datos personales.

l. Revelación de información.

Está prohibida la revelación de datos personales para objetivos de mercadeo, excepto cuando se trata de mercadeo directo con el propietario de la información o cuando el área comercial de la compañía organice una promoción para ellos.

Así mismo, cuando alguna autoridad administrativa o judicial solicite la revelación de datos personales, el área legal de la firma deberá hacer la revisión, previo a su revelación.

m. Procedimiento para solicitar cambios, actualización o supresión de información personal.

Las personas tienen derecho a conocer sus datos personales. Para ello, pueden:

- 1) Inspeccionarlos en forma gratuita, previa solicitud en las oficinas que se mencionan o indican en la Política de Privacidad (previa validación de la identificación del solicitante),
- 2) Consultar vía telefónica o por escrito tanto el contenido de sus datos personales como evidencia de la autorización dada para su tratamiento, así como ser informado del uso que FLORES GARIBAY le ha dado a sus datos personales.

Consulta telefónica:

Se dará trámite a la solicitud de conocimiento de los datos cuando ella se reciba vía telefónica siempre que se valide la identificación de quien la solicita de acuerdo con el siguiente procedimiento de validación. Se debe verificar que la persona que está llamando es el propietario de los datos personales solicitados, a través de la formulación de preguntas de validación, como podrían ser la fecha exacta del nacimiento o la fecha de expedición del documento de identidad. Debe quedar constancia escrita de haberse adelantado este procedimiento. El hecho de contar con un servicio previamente otorgado constituye información personal que no puede ser revelada a quien esté llamando sin que previamente se verifique que se trata del propietario de los datos personales o de alguien que este haya autorizado.

Consulta presentada por escrito:

Se dará trámite a la solicitud por escrito siempre que la misma sea recibida i) directamente en oficinas de FLORES GARIBAY que se haya comunicado para atender dichas solicitudes o ii) enviada desde la dirección de correo electrónico registrada por el cliente dirigida a:

privacidad@floresgaribay.com.mx Recibida la solicitud, FLORES GARIBAY contará con diez (10) días hábiles contados desde la fecha de la petición para darle respuesta. De no ser posible, se deberá informar al solicitante las razones y se indicará que en un término máximo de cinco (5) días hábiles contados desde la fecha de vencimiento del primer término, se atenderá la consulta.

La copia de la autorización para el tratamiento de datos personales se entregará, excepto en aquellos casos en los que la ley exceptúe contar con dicha autorización como requisito para el tratamiento de los datos personales. No se requiere de autorización cuando los datos están incorporados en el registro civil de las personas, en el certificado de existencia y representación legal de la entidad, sean

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

datos públicos, datos requeridos por autoridad o entidad pública o administrativa en el ejercicio de sus funciones o por orden judicial, en casos de urgencia médica manifiesta o sanitaria o cuando los datos vayan a ser utilizados para fines estadísticos, históricos o científicos conforme la autorización legal para esos efectos.

3) Solicitar la actualización o rectificación de sus datos personales. FLORES GARIBAY contará con cinco (15) días hábiles a partir del recibo de la solicitud para realizar la actualización de datos. Si la misma requiere soportes para su cambio, por ejemplo porque se trata de información pública o contenida en documentos administrados por entidades públicas, el solicitante deberá radicar el documento correspondiente adjuntando: i) la identificación del titular (cliente, proveedor, empleado, socio, asociado, colaborador o intermediario) ii) describiendo los hechos que dan lugar al reclamo, iii) indicando su dirección, iv) entregando la documentación que quiera presentar para este trámite.

Si a juicio de FLORES GARIBAY la solicitud resulta incompleta, requerirá al interesado dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha de este requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido de este trámite.

Si FLORES GARIBAY no fuere competente para resolver la solicitud, dará traslado a quien corresponda, si lo conociere, en un término máximo de dos (10) días hábiles, informando la situación. Si no conociere quién es el competente, en el mismo término dará respuesta al solicitante.

Recibido la solicitud completa, se incluirá, en un término máximo de dos (10) días hábiles, en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo. Se debe mantener esa leyenda hasta que el reclamo sea decidido.

El término máximo para atender esta solicitud será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo completo. Cuando no fuere posible atenderla en ese plazo, se informará al solicitante el motivo y la fecha en la que se atenderá, la que en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

4) Revocar la autorización o solicitar la supresión del dato, siempre que no esté vigente la relación comercial con FLORES GARIBAY o derechos u obligaciones entre la persona y la compañía y en todo caso, la revocación o solicitud de supresión procederá siempre que no se respeten los principios, derechos y garantías constitucionales y legales. Para ello, será el IFAI quien determine que FLORES GARIBAY ha incurrido en conductas que generen la revocación o supresión del dato. Sólo se procederá a la revocación o supresión del dato, si fuere en ese sentido la decisión del IFAI.

Así mismo, las personas pueden presentar ante el IFAI quejas por infracciones a lo dispuesto en este documento y demás normas que la modifiquen, adicionen o complementen.

n. Personas que pueden solicitar cambios, actualización o supresión de información personal.

Para el ejercicio de los derechos sobre los datos personales, la solicitud puede ser presentada por las siguientes personas:

1. El cliente, proveedor, empleado, socio, asociado, colaborador o intermediario (cada uno de ellos, actuando en su nombre).
2. Un apoderado especial autorizado para ello. En este caso, el poder debe contar con nota de

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

presentación personal del cliente, proveedor, empleado, socio, asociado, colaborador o intermediario. FLORES GARIBAY debe contar con un archivo de las autorizaciones firmadas por el cliente, proveedor, empleado, socio, asociado, colaborador o intermediario y revisarlo previo a revelar información personal a terceras personas.

3. Si se trata de menores de edad, la solicitud debe hacerla cualquiera de los padres del menor siempre que ambos ejerzan la patria potestad. En este caso, debe validarse la identificación del padre o madre con su cédula de ciudadanía o identificación oficial, así como con el acta de registro civil de nacimiento del menor. Ambos documentos deben ser suministrados por el solicitante. La revisión del registro civil de nacimiento permitirá igualmente verificar si sólo uno de los padres ejerce la patria potestad sobre el menor, y en ese caso sólo quien la ejerza tendrá la legitimación para realizar las solicitudes a que previamente se hizo referencia.

En el evento en el que se verifique que los padres del menor presentan solicitudes divergentes, si ambos ejercen la patria potestad se les pedirá una petición conjunta y en su defecto, la decisión de un juez que determine de qué manera se debe proceder con la solicitud.

4. Si se trata de una notificación recibida de autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal, FLORES GARIBAY insertará en la base de datos la leyenda “información en discusión judicial”.

FLORES GARIBAY se abstendrá de circular información que esté siendo controvertida por el tomador o asegurado, cuyo bloqueo haya sido ordenado por la disposición judicial o el IFAI.

o. Procedimiento ante un potencial evento de fuga de información de datos personales.

Para efectos de este documento se entenderá como un potencial evento de fuga de información como cualquier incidente de adquisición, uso o revelación de información personal de clientes, no autorizada y que comprometa la seguridad, integridad y confidencialidad de esa información, creando un riesgo para el cliente.

Por ejemplo:

- Un empleado que accede a la información de un cliente por fuera del ejercicio de sus funciones laborales.
- La pérdida o hurto de un computador que contenga información personal no encriptado.
- Información personal de clientes enviada por error a un fax o dirección de correo.

Cualquier potencial evento de fuga de información deberá ser reportado al jefe inmediato o al responsable de seguridad de la información (protección de datos) inmediatamente y en todo caso en un máximo de dos días hábiles contados desde la fecha del descubrimiento de los hechos. Si la fuga involucra una situación de pérdida o hurto de un computador, deberá igualmente ser reportada a la Dirección de la compañía o quien lo represente. A juicio del responsable, si la posible fuga de información constituye una violación a los códigos de seguridad, deberá informarlo al IFAI y a las autoridades pertinentes.

p. Capacitación del personal.

FLORES GARIBAY capacitará a su personal por lo menos una vez cada año, respecto del contenido de este documento en aras de garantizar la seguridad, confidencialidad, veracidad e integridad de los

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

datos personales de sus clientes. Cada capacitación contará con un listado de los asistentes así como del contenido programático de las mismas.

Si Usted tiene alguna pregunta o inquietud relacionada con los procedimientos para la protección de datos personales de FLORES GARIBAY, puede contactarnos a:

FLORES GARIBAY CONSULTORES S.C.

Ubicado en: Avenida de las Rosas # 210, Colonia Chapalita, Guadalajara, Jalisco, C.P. 44510.

Tel. +52 (33) 30030100

Correo Electrónico: contacto@floresgaribay.com.mx

La revisión más reciente de esta política interna de seguridad de la información se llevó a cabo el 22 de Septiembre de 2014. Nos reservamos el derecho de cambiar esta declaración en cualquier momento con el fin de cumplir con las leyes aplicables o para reflejar la actualización de nuestra práctica empresarial. Cualquier cambio en esta declaración será efectivo a partir del día en que sea publicado en nuestra página web: <http://www.floresgaribay.com.mx/>

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	



MODELO DE CLASIFICACION DE LA INFORMACION
FLORES GARIBAY CONSULTORES S.C.

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

3. Introducción

3.1 Propósito

Describir en detalle el tipo, categoría, disponibilidad y accesibilidad de la información que procesa para sus operaciones Flores Garibay Consultores S.C.

3.2 Alcance

Este documento establece con detalle la clasificación de la información que Flores Garibay Consultores S.C. define para la información que procesa.

Se definen las categorías generales siguientes para el tratamiento de la información:

- 1.- *DATOS PERSONALES GENERALES*
- 2.- *DATOS PERSONALES SENSIBLES*
- 3.- *DATOS INSTITUCIONALES PRIVADOS*
- 4.- *DATOS INSTITUCIONALES PUBLICOS*

Se definen las categorías particulares siguientes para el tratamiento de la información:

- 1.- *DATOS DE COLABORADORES*
 - 1.1 *SOCIOS*
 - 1.2 *ASOCIADOS*
 - 1.3 *EMPLEADOS*
 - 1.4 *BECARIOS*
 - 1.5 *ASPIRANTES*
- 2.- *DATOS DE CLIENTES*
- 3.- *DATOS DE PROVEEDORES*
- 4.- *DATOS DE SOCIOS DE NEGOCIOS*
- 5.- *DATOS DE VISITANTES*

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

4. CATEGORIAS GENERALES Definiciones

4.1- *DATOS PERSONALES GENERALES*

Se trata de toda aquella información general o específica que identifique o revele elementos de identificación de una persona en particular.

4.2- *DATOS PERSONALES SENSIBLES*

Se trata de toda aquella información general o específica de carácter sensible que identifique o revele elementos de la personalidad, gustos, intereses, creencias y/o situación patrimonial de una persona en particular.

4.3- *DATOS INSTITUCIONALES PRIVADOS*

Se trata de toda aquella información general o específica que identifique o revele elementos de identificación de una empresa, sociedad o grupo de personas; esta información no debe ser revelada a ningún tercero ajeno a su tratamiento.

4.4- *DATOS INSTITUCIONALES PUBLICOS*

Se trata de toda aquella información general o específica que identifique o revele elementos de identificación de una empresa, sociedad o grupo de personas; esta información ya se encuentra disponible en medios accesibles públicamente y no existe restricción alguna de ser procesada por terceros.

 FLORES GARIBAY <small>CONSULTORIA FISCAL, LEGAL Y DE NEGOCIOS</small>	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

5. CATEGORIAS PARTICULARES Definiciones

5.1- *DATOS DE COLABORADORES*

Se trata de toda aquella información general, sensible, privada o pública de las personas vinculadas a Flores Garibay Consultores S.C. mediante una incorporación formal a la sociedad en cualquiera de las siguientes modalidades:

5.1.1 *SOCIOS*

5.1.2 *ASOCIADOS*

5.1.3 *EMPLEADOS*

5.1.4 *BECARIOS*

5.1.5 *ASPIRANTES*

5.2.- *DATOS DE CLIENTES*

Se trata de toda aquella información general, sensible, privada o pública de las personas, empresas o grupos de personas que reciben servicios profesionales de Flores Garibay Consultores S.C. en calidad de Clientes.

5.3.- *DATOS DE PROVEEDORES*

Se trata de toda aquella información catalogada como datos personales generales o sensibles de las personas, empresas o grupos de personas que prestan servicios profesionales, comerciales o que suministran bienes o servicios a Flores Garibay Consultores S.C. en calidad de Proveedores.

5.4.- *DATOS DE SOCIOS DE NEGOCIOS*

Se trata de toda aquella información general, sensible, privada o pública de las personas, empresas o grupos de personas que se vinculan a Flores Garibay Consultores S.C. en calidad de socios de negocios.

5.5.- *DATOS DE VISITANTES*

Se trata de toda aquella información general, sensible, privada o pública de las personas que acuden e ingresan a las instalaciones de Flores Garibay Consultores S.C. en calidad de visitantes por cualquier motivo.

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

6. DATOS DE COLABORADORES

- 6.1. *SOCIOS*
- 6.2. *ASOCIADOS*
- 6.3. *EMPLEADOS*
- 6.4. *BECARIOS*
- 6.5. *ASPIRANTES*

Flores Garibay Consultores S. C. podrá solicitar los siguientes datos personales, generales, sensibles, privados o públicos de sus colaboradores y los gestionará mediante un sistema de cómputo que para este fin ha desarrollado e implementado:

6.1.- DATOS PERSONALES DE LOS COLABORADORES (DATOS GENERALES)

INDICE				
6.1.0	<i>IdUsuario</i>	(string:20) De sistema	requerido	
6.1.1	<i>usuario</i>	(string:10 min:8)	requerido	
6.1.2	<i>nombre(s)</i>	(string:30)	requerido	
6.1.3	<i>apellido paterno</i>	(string:50)	requerido	
6.1.4	<i>apellido materno</i>	(string:50)	opcional	
6.1.5	<i>fecha nacimiento</i>	(date:aaaammdd)	opcional	
6.1.6	<i>lugar de nacimiento</i>	(string:100)	requerido	
6.1.7	<i>tipo de sangre</i>	(string:50)	opcional	
6.1.8	<i>alergias</i>	(string:2000)	opcional	
6.1.9	<i>sexo</i>	(string:1) Masculino Femenino	opcional	

6.2.- DATOS PERSONALES DE LOS COLABORADORES (EN CASO DE EMERGENCIA AVISAR A)

INDICE				
6.2.1	<i>nombre-apat-amat</i>	(string:200)	requerido	
6.2.2	<i>telcontacto1</i>	(string:50)	requerido	
6.2.3	<i>telcontacto2</i>	(string:50)	opcional	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

6.3.- DATOS PERSONALES DE LOS COLABORADORES (DOMICILIO PARTICULAR Y DE CONTACTO)

INDICE				
6.3.1	<i>calle</i>	(string:200)	requerido	
6.3.2	<i>numero exterior</i>	(string:50)	requerido	
6.3.3	<i>numero interior</i>	(string:50)	requerido	
6.3.4	<i>colonia</i>	(string:200)	requerido	
6.3.5	<i>poblacion</i>	(string:200)	requerido	
6.3.6	<i>municipio</i>	(string:200)	requerido	
6.3.7	<i>codigo postal</i>	(string:5)	requerido	
6.3.8	<i>estado</i>	(string:200)	requerido	
6.3.9	<i>pais</i>	(string:200)	requerido	
6.3.10	<i>teléfono particular</i>	(integer:12)	opcional	
6.3.11	<i>teléfono celular</i>	(integer:12)	opcional	
6.3.2	<i>email</i>	(string:100)	requerido	
6.3.3	<i>email alternativo</i>	(string:100)	requerido	
6.3.4	<i>categoría</i>	(integer) Socio]Asociado Empleado Aspirante	requerido	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

7. DATOS DE CLIENTES

Flores Garibay Consultores S. C. podrá solicitar los siguientes datos personales, generales, sensibles, privados o públicos de sus clientes y los gestionará mediante un sistema de cómputo que para este fin ha desarrollado e implementado:

7.1.- DATOS PERSONALES DE LOS CLIENTES (DATOS GENERALES)

INDICE				
7.1.0	<i>IdUsuario</i>	(string:20) De sistema	requerido	
7.1.1	<i>usuario</i>	(string:10 min:8)	requerido	
7.1.2	<i>razón social</i>	(string:30)	requerido	
7.1.3	<i>RFC</i>	(string:50)	requerido	
7.1.4	<i>CURP</i>	(string:50)	opcional	
7.1.5	<i>fecha alta</i>	(date:aaaammdd)	opcional	
7.1.6	<i>grupo empresarial</i>	(string:100)	requerido	
7.1.7	<i>giro empresarial</i>	(string:50)	opcional	
7.1.8	<i>email</i>	(string:2000)	opcional	
7.1.9	<i>tipo persona</i>	(string:1) Fisica Moral	opcional	

7.2.- DATOS PERSONALES DE LOS CLIENTES (DOMICILIO PARTICULAR)

INDICE				
7.2.1	<i>calle</i>	(string:200)	requerido	
7.2.2	<i>numero exterior</i>	(string:50)	requerido	
7.2.3	<i>numero interior</i>	(string:50)	requerido	
7.2.4	<i>colonia</i>	(string:200)	requerido	
7.2.5	<i>poblacion</i>	(string:200)	requerido	
7.2.6	<i>municipio</i>	(string:200)	requerido	
7.2.7	<i>codigo postal</i>	(string:5)	requerido	
7.2.8	<i>estado</i>	(string:200)	requerido	
7.2.9	<i>pais</i>	(string:200)	requerido	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

6.3.- DATOS PERSONALES DE LOS CONTACTOS – FUNCIONARIOS DEL CLIENTE

INDICE				
7.3.1	<i>nombre-apat-amat</i>	(string:200)	requerido	
7.3.2	<i>telcontacto1</i>	(string:50)	opcional	
7.3.3	<i>telcontacto2</i>	(string:50)	opcional	
7.3.4	<i>email</i>	(string:100)	opcional	
7.3.5	<i>email alternativo</i>	(string:100)	opcional	
7.3.6	<i>departamento</i>	(string:100)	opcional	
7.3.7	<i>puesto</i>	(string:100)	opcional	

7.4.- DATOS PERSONALES DE LOS COLABORADORES ASOCIADOS AL CLIENTE

INDICE				
7.4.1	<i>nombre-apat-amat</i>	(string:200)	requerido	
7.4.2	<i>fecha inicio</i>	(date)	requerido	
7.4.3	<i>Fecha fin</i>	(date)	requerido	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

8. DATOS DE PROVEEDORES

Flores Garibay Consultores S. C. podrá solicitar los siguientes datos personales, generales, sensibles, privados o públicos de sus proveedores y los gestionará mediante un sistema de cómputo que para este fin ha desarrollado e implementado:

8.1.- DATOS PERSONALES DE LOS PROVEEDORES (DATOS GENERALES)

INDICE				
8.1.0	<i>IdUsuario</i>	(string:20) De sistema	requerido	
8.1.1	<i>usuario</i>	(string:10 min:8)	requerido	
8.1.2	<i>razón social</i>	(string:30)	requerido	
8.1.3	<i>RFC</i>	(string:50)	requerido	
8.1.5	<i>fecha alta</i>	(date:aaaammdd)	opcional	

8.2.- DATOS PERSONALES DE LOS PROVEEDORES (DOMICILIO PARTICULAR)

INDICE				
8.2.1	<i>calle</i>	(string:200)	requerido	
8.2.2	<i>numero exterior</i>	(string:50)	requerido	
8.2.3	<i>numero interior</i>	(string:50)	requerido	
8.2.4	<i>colonia</i>	(string:200)	requerido	
8.2.5	<i>poblacion</i>	(string:200)	requerido	
8.2.6	<i>municipio</i>	(string:200)	requerido	
8.2.7	<i>codigo postal</i>	(string:5)	requerido	
8.2.8	<i>estado</i>	(string:200)	requerido	
8.2.9	<i>pais</i>	(string:200)	requerido	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

9. DATOS DE SOCIOS DE NEGOCIOS

Flores Garibay Consultores S. C. podrá solicitar los siguientes datos personales, generales, sensibles, privados o públicos de sus socios de negocios y los gestionará mediante un sistema de cómputo que para este fin ha desarrollado e implementado:

9.1.- DATOS PERSONALES DE LOS SOCIOS DE NEGOCIOS (DATOS GENERALES)

INDICE				
9.1.0	<i>IdUsuario</i>	(string:20) De sistema	requerido	
9.1.1	<i>usuario</i>	(string:10 min:8)	requerido	
9.1.2	<i>razón social</i>	(string:30)	requerido	
9.1.3	<i>RFC</i>	(string:50)	requerido	
9.1.5	<i>fecha alta</i>	(date:aaaammdd)	opcional	

9.1.- DATOS PERSONALES DE LOS CONTACTOS – SOCIOS DE NEGOCIOS

INDICE				
9.1.1	<i>nombre-apat-amat</i>	(string:200)	requerido	
9.1.2	<i>telcontacto1</i>	(string:50)	opcional	
9.1.3	<i>telcontacto2</i>	(string:50)	opcional	
9.1.4	<i>email</i>	(string:100)	opcional	
9.1.5	<i>email alternativo</i>	(string:100)	opcional	
9.1.6	<i>departamento</i>	(string:100)	opcional	
9.1.7	<i>puesto</i>	(string:100)	opcional	

9.2.- DATOS PERSONALES DE LOS SOCIOS DE NEGOCIOS (DOMICILIO PARTICULAR)

INDICE				
9.2.1	<i>calle</i>	(string:200)	requerido	
9.2.2	<i>numero exterior</i>	(string:50)	requerido	
9.2.3	<i>numero interior</i>	(string:50)	requerido	
9.2.4	<i>colonia</i>	(string:200)	requerido	
9.2.5	<i>poblacion</i>	(string:200)	requerido	
9.2.6	<i>municipio</i>	(string:200)	requerido	
9.2.7	<i>codigo postal</i>	(string:5)	requerido	
9.2.8	<i>estado</i>	(string:200)	requerido	
9.2.9	<i>pais</i>	(string:200)	requerido	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

10. DATOS DE VISITANTES

Flores Garibay Consultores S. C. podrá solicitar los siguientes datos personales, generales, sensibles, privados o públicos de los visitantes a sus oficinas y los gestionará mediante un sistema de cómputo que para este fin ha desarrollado e implementado:

10.1.- DATOS PERSONALES DE LOS VISITANTES (DATOS GENERALES)

INDICE				
10.1.1	<i>nombre-apat-amat</i>	(string:200)	requerido	
10.1.2	<i>fecha ingreso</i>	(date)	opcional	
10.1.3	<i>hora de ingreso</i>	(time)	opcional	
10.1.4	<i>hora de salida</i>	(time)	opcional	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

10. SISTEMAS DE REGISTRO

Flores Garibay Consultores S. C. cuenta con un conjunto de sistemas y/o formularios electrónicos y/o expedientes físicos que permitirán la gestión correcta y segura de los datos personales e institucionales.

No.	TIPO DE INFORMACION	SISTEMA DE REGISTRO	TIPO DE SISTEMA	ESTATUS
1	COLABORADORES	CATALOGO DE COLABORADORES	BD MSQL	Vigente
2	CLIENTES	CATALOGO DE CLIENTES – PryCobranza	BD MSQL	Vigente
3	PROVEEDORES	CONTROL DE GASTOS Y CONTABILIDAD	BD MSQL	Vigente
4	SOCIOS DE NEGOCIOS	DIRECTORIOS	MANUAL	Vigente
5	VISITANTES	LIBRETA DE REGISTRO	MANUAL	No Vigente



**ANALISIS DE RIESGOS
EVALUACION Y CONTROLES
TECNOLOGIAS DE LA INFORMACION**
FLORES GARIBAY CONSULTORES S.C.

 <p>FLORES GARIBAY CONSULTORÍA FISCAL, LEGAL Y DE NEGOCIOS</p>	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

4. ANALISIS DE RIESGOS

4.1- ANALISIS DE RIESGOS

Se trata de toda aquella información general o específica que identifique o revele elementos de identificación de una persona en particular.

RIESGO	CATEGORIA	IMPACTO
Pérdida o corrupción parcial o total de información almacenada en los sistemas de misión crítica	CRITICO	Pérdida de fuente de ingresos, grave responsabilidad civil
Sustracción no autorizada de información almacenada en los sistemas de misión crítica	CRITICO	Pérdida de confianza, grave responsabilidad civil
Exposición no autorizada de información almacenada en los sistemas de misión crítica	CRITICO	Pérdida de confianza, grave responsabilidad civil
Daño parcial o total de los sistemas de misión crítica	SEVERO	Activación de plan de recuperación de desastres, pérdida de tiempo – productividad
Exposición de daño severo por condiciones metereológicas, terremoto, incendio o asalto con violencia	SEVERO	Activación manual del botón de paro de emergencia del Centro de Datos
Fraude, abuso de confianza, corrupción	SEVERO	Pérdida de ingresos

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

4.2- *CONTROLES DE RIESGOS*

Se trata de todo aquel mecanismo, política, procedimiento, software, o instrumento manual, automático o semiautomático que evita o minimiza un riesgo.

RIESGO	CONTROLES
Pérdida o corrupción parcial o total de información almacenada en los sistemas de misión crítica	POLITICA DE RESPALDO DE INFORMACION, PLAN DE RECUPERACION DE DESASTRES DRP.
Sustracción no autorizada de información almacenada en los sistemas de misión crítica	POLITICA INTERNA DE GESTIÓN DE INFORMACIÓN, CONTROL DE ACCESO
Exposición no autorizada de información almacenada en los sistemas de misión crítica	POLITICA INTERNA DE GESTIÓN DE INFORMACIÓN, CONTROL DE ACCESO
Daño parcial o total de los sistemas de misión crítica	POLIZAS DE SEGURO, GARANTIAS, PROGRAMA DE MANTENIMIENTO / PLAN DE RECUPERACION DE DESASTRES DRP.
Exposición de daño severo por condiciones metereológicas, terremoto, incendio o asalto con violencia	BOTON DE PARO DE EMERGENCIA, SISTEMA CONTRA-INCENDIO
Fraude, abuso de confianza, corrupción	ACUERDOS DE CONFIDENCIALIDAD, POLITICAS DE GESTION DE ACTIVOS DE TI

 FLORES GARIBAY <small>CONSULTORIA FISCAL, LEGAL Y DE NEGOCIOS</small>	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

POLITICA DE RESPALDO DE INFORMACION

Objetivo:

Garantizar la disponibilidad de la información contenida en los sistemas de misión crítica de FLORES GARIBAY, almacenándolos en una caja de seguridad fuera del centro de datos de FLORES GARIBAY.

Definiciones:

Los sistemas de misión crítica de FLORES GARIBAY son identificados y listados en el DRP y como parte de los inventarios tecnológicos y de infraestructura de FLORES GARIBAY.

Los respaldos de información se harán de la base de datos de los sistemas de misión crítica bajo las modalidades de:

Respaldo incremental, el cual contempla solamente las actualizaciones de transacciones que fueron modificadas por el(los) sistema(s).

Respaldo total, el cual contempla una copia completa de la información al momento en la base de datos.

POLITICA:

La Gerencia de Sistemas deberá contar con una caja de seguridad resistente al fuego fuera del Centro de Datos para almacenar las copias de los respaldos a las bases de datos generadas por los sistemas de misión crítica de la compañía. Esta política aplica por igual a toda la información en formato original o copias controladas de ellos que permitan la regeneración del ambiente productivo de los servidores (sistema operativo, utilerías, parches, etc.).

De manera adicional, se podrá contar con una caja de seguridad externa (de preferencia en un banco) en donde se puedan almacenar copias complementarias de los respaldos de la base de datos de los sistemas de misión crítica.

PROCEDIMIENTO:

Definición inicial

Se configura en los servidores de los sistemas de misión crítica el horario en el cual se deberá de efectuar un respaldo incremental, en el caso del respaldo total se arrancará el proceso de respaldo desde la consola del servidor por el especialista de Informática. La colocación de las cintas y/o unidades de respaldo se hará en forma manual todos los días (de Lunes a Viernes) por la tarde, en caso de realizarlo de manera automática, se deberá supervisar el proceso por el responsable de Sistemas.

Respaldo e identificación

El especialista responsable verifica el estado lógico y físico de las unidades de respaldo de la información de la base de datos. Identifica y controla de manera comprensible para identificación, indica si el respaldo es

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Incremental o Total, se registra la fecha y hora de generación del respaldo.

Actualiza su bitácora de control de unidades de respaldo para determinar las que serán almacenadas en la caja de seguridad y las que deberán ser llevadas a la caja de seguridad FLORES GARIBAY (en caso de que aplica).

Instala y/o prepara una nueva unidad del servidor para que se efectúe el respaldo del siguiente día.

Almacenamiento

El especialista lleva todos los días el respaldo generado con la información más actualizada a la caja de seguridad ubicada al otro lado del edificio, lo deposita en la caja de seguridad y extrae de ella las unidades para ser los procesos de respaldo, una vez cubierta las condiciones de vigencia y retención de la información. En caso de contar con una caja de seguridad bancaria hará una rotación de las unidades (al menos una vez cada año) para ser garantizados en el proceso de respaldo y para mantener una copia complementaria en FLORES GARIBAY.

Tipos de respaldos y tiempos de retención en la caja de seguridad local

FRECUENCIA DE RESPALDO	TIPO DE RESPALDO	LATENCIA (RESGUARDO)
Diario	Incremental	8 días de respaldo
Semanal	Total	2 semanas de respaldo con las copias de los lunes y los viernes
Mensual	Total	3 meses de respaldo

Tiempos de respaldo en la caja de seguridad bancaria

FRECUENCIA DE RESPALDO	TIPO DE RESPALDO	LATENCIA (RESGUARDO)
Diario	Incremental	Los últimos 21 días
Semanal	Total	Las últimas 4 semanas
Mensual	Total	Los últimos 13 meses

Programación de respaldos

DIA	FRECUENCIA DE RESPALDO	TIPO DE RESPALDO
SABADO (por la noche)	Semanal	Total
Lunes - Viernes	Diario	Incremental
Días 1 (Fin de Mes anterior)	Mensual Total	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

POLITICA DE CONTROL DE ACCESO - CREACION DE CUENTAS DE USUARIO

Objetivo:

Establecer un mecanismo formal de asignación de cuentas de usuario para los diferentes sistemas y aplicaciones de FLORES GARIBAY, incluyendo el acceso a la red vía Windows.

POLITICA:

Las cuentas de usuario para los sistemas de FLORES GARIBAY, deberán ser únicas para evitar confusiones en el acceso a las aplicaciones y deberán ser personalizadas para identificar claramente al usuario y su función dentro de los sistemas de la compañía. Solamente en contadas excepciones se proporcionará una cuenta de acceso genérica la cual será compartida por personal específico del departamento que la solicita.

Queda estrictamente prohibido prestar la cuenta de acceso a cualquier persona, sin excepción, esto constituye una violación grave a las políticas de operación en la firma y por lo tanto el usuario que sea sorprendido prestando su cuenta de acceso podrá ser sujeto a las sanciones que la empresa determine.

La Gerencia de Sistemas está comprometida a proporcionar una cuenta de acceso a aquellos usuarios que hayan sido autorizados por sus superiores (Socios y Gerentes) para utilizar los recursos informáticos de la firma.

PROCEDIMIENTO:

Los Superiores (Socios o Gerentes) entregarán formalmente el formulario de datos personales de la persona que desean autorizar para el acceso a los sistemas de la firma, a fin de que sea creada una cuenta de usuario para un sistema determinado proporcionando para ello además el perfil que utilizará en cada aplicación, es práctica común solicitar que se asigne un perfil de usuario ya existente en el mismo departamento.

La Gerencia de Sistemas recibe el requerimiento, elabora el ticket y el formato correspondiente en dónde recopilará la autorización de dicha solicitud. Una vez autorizada el personal de Sistemas procederá a la creación de la cuenta de usuario en el sistema o aplicación específica (Sistema, Correo, Internet, etc.)

Las cuentas de usuario se crearán utilizando la siguiente convención:

1. Considerar el Registro Federal de Contribuyentes, tomar las primeras 4 cuatro letras del RFC y concatenar a la derecha la homoclave.
2. En caso de que la persona no cuente con homoclave se utilizará los últimos 3 dígitos de la fecha de nacimiento, 1 dígito para el mes y dos para el año.
3. En el remoto caso en que se repita la cuenta, se asignará un número consecutivo al final de la cuenta creada si no cumple con las condiciones de los puntos 1 y 2.

Una vez creada la cuenta se le asignará una contraseña (password) la cual el usuario tendrá la opción de cambiar en su siguiente entrada (en el caso de Windows) o bien se negociará con el usuario el password de aplicación que utilizará para trabajar.

La Gerencia de Sistemas notifica al usuario de manera personal su nueva cuenta de acceso, cierra el ticket y el formato, con ello da por terminado el proceso de la creación de la cuenta del usuario.

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

POLITICA DE CONTROL DE ACCESO - MANTENIMIENTO DE CUENTAS DE USUARIO

MODIFICACION DE DATOS DE LA CUENTA DE USUARIO

POLITICA:

Las cuentas de usuario solo podrán ser modificadas a petición explícita del usuario propietario de la cuenta, con excepción única ante la baja temporal o permanente del personal de la firma.

La solicitud de modificación deberá realizarse personalmente ante la Gerencia de Sistemas.

BAJA DE LA CUENTA DE USUARIO

POLITICA:

Las cuentas de usuario podrán ser dadas de baja de los sistemas de la firma a petición explícita del usuario propietario de la cuenta con autorización de su superior.

La baja en todos los casos será solo administrativa, esto significa que no serán eliminados de los sistemas las cuentas de usuario dadas de baja, solo aplicará un efecto de desactivación y será totalmente restringida su utilización en los sistemas de la firma.

ELIMINACION DE LA CUENTA DE USUARIO

POLITICA:

Las cuentas de usuario no se podrán eliminar de los sistemas de FLORES GARIBAY, a excepción única mediante solicitud por escrito de la Junta de Socios de la firma o de la Dirección General.

ENMASCARAMIENTO DE LOS DATOS PERSONALES ASOCIADOS A LA CUENTA DE USUARIO

POLITICA:

Los datos personales asociados a las cuentas de usuario que se han dado de baja podrán ser “desasociados” o “enmascarados”, pasados 12 meses desde su desactivación o marcado como baja, de tal manera que se eliminará de las bases de datos de FLORES GARIBAY solo los datos personales, sin embargo los datos generales se conservarán, lo cual ya no permitirá la identificación de la persona asociada a la cuenta de usuario.

Solo podrán ser enmascarados datos personales de las cuentas de usuario de quienes estén ya etiquetados en estatus de “baja”.

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	



**INDICADORES DE GESTION
TECNOLOGIAS DE LA INFORMACION**
FLORES GARIBAY CONSULTORES S.C.

 <p>FLORES GARIBAY CONSULTORÍA FISCAL, LEGAL Y DE NEGOCIOS</p>	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

INDICADORES DE GESTION

INDICADOR 1.- Plan de mantenimiento preventivo de equipos de cómputo y Telefonía

Se documentará el plan de mantenimiento así como las fechas a realizar, los insumos necesarios, se implantará un medio electrónico para llevar bitácora de mantenimientos

Planes de mantenimiento

1. Se realizarán 4 mantenimientos preventivos al año a los equipos de cómputo
2. El mantenimiento a los servidores se realizará 1 al año
3. En los conmutadores se realizará 1 al año y este se ejecutara antes de temporada de lluvias
4. Se entregara un informe a la dirección de la condición de los equipos para en su caso su sustitución ya que su vida útil ya caduco

INDICADOR 2.- % Disponibilidad de los servicios críticos de la Compañía

En el proceso ITIL llamado Gestión de la Continuidad de los servicios ITSCM, el cual nos ayudara a documentar el plan de contingencia para los servicios críticos paso a paso.

Las principales actividades de la Gestión de la Continuidad de los Servicios TI se resumen en:

- a. Establecer las políticas y alcance de la ITSCM.
- b. Evaluar el impacto en el negocio de una interrupción de los servicios TI.
- c. Analizar y prever los riesgos a los que está expuesto la infraestructura TI.
- d. Establecer las estrategias de continuidad del servicio TI.
- e. Adoptar medidas proactivas de prevención del riesgo.
- f. Desarrollar los planes de contingencia.
- g. Poner a prueba dichos planes.
- h. Formar al personal sobre los procedimientos necesarios para la pronta recuperación del servicio.
- i. Revisar periódicamente los planes para adaptarlos a las necesidades reales del negocio

 FLORES GARIBAY CONSULTORIA FISCAL, LEGAL Y DE NEGOCIOS	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Organización y Planificación

1. Plan de prevención de riesgos.
2. Plan de gestión de emergencias.
3. Plan de recuperación.

1. Plan de prevención de riesgos

- a. Almacenamiento de datos distribuidos.
- b. Sistemas de alimentación eléctrica de soporte.
- c. Políticas de back-ups.
- d. Duplicación de sistemas críticos.
- e. Sistemas de seguridad pasivos

2. Plan de gestión de emergencias

- a. Evaluación del impacto de la contingencia en la infraestructura TI.
- b. Asignación de funciones de emergencia al personal del servicio TI.
- c. Comunicación a los usuarios y clientes de una grave interrupción o degradación del servicio.
- d. Procedimientos de contacto y colaboración con los proveedores involucrados.
- e. Protocolos para la puesta en marcha del plan de recuperación correspondiente.

3. Plan de recuperación

- a. Reorganizar al personal involucrado.
- b. Restablecer los sistemas de hardware y software necesarios.
- c. Recuperar los datos y reiniciar el servicio TI.

INDICADOR 3.- Gestión de controles de Seguridad

1. Documentación de controles de acceso de modo eficiente para cumplir la metas de los procesos
2. En conjunto con los directores y jefes departamentales documentar los perfiles de acceso de todos los usuarios para realizar sus funciones de acuerdo al puesto
3. Autorización vía correo electrónico de las altas de los nuevos usuarios así como las bajas o cambios

 FLORES GARIBAY CONSULTORIA FISCAL, LEGAL Y DE NEGOCIOS	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

4. Se realizara una impresión de los usuarios activos en los sistemas para cortejar con el departamento de RH. Y en caso de existir una discrepancia corregirla inmediatamente.
5. En el recorrido de colaboradores de baja, el personal de sistema firmara el documento donde entregan equipo cómputo y en ese momento se desactiva las contraseñas a los sistemas,

INDICADOR 4.- Presupuestos

Se realiza un levantamiento de necesidades con las diferentes áreas en los 3 hoteles previo a la presentación de presupuestos para elaborar un plan de inversión ya sea actualización de software o implementación de nuevo software que lleve al cumplimiento de los objetivos del Grupo FLORES GARIBAY

El presupuesto a presentar debe cumplir lo siguiente:

1. Total de la inversión y los alcances que se pretende
2. Fechas en que se ejercerá el proyecto
3. Actualizaciones necesarias del software para el cumplimiento de reformas fiscales
4. Sustitución de equipo obsoleto que entorpece las labores de los usuarios
5. La implantación de nuevo software que lleve a los objetivos de la empresa con menos procesos y sea veras, cumpliendo las normas de proceso d instalación d un software

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	



**PLAN DE RECUPERACION DE DESASTRES
“DRP”
TECNOLOGIAS DE LA INFORMACION**

 FLORES GARIBAY <small>CONSULTORIA FISCAL, LEGAL Y DE NEGOCIOS</small>	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

FLORES GARIBAY CONSULTORES S.C.

VERSIÓN 1.0

PLAN DE RECUPERACIÓN DE DESASTRES Y CONTINGENCIAS

0. Enmiendas (control de cambios y autorización de versión)

Descripción Fecha Emite Autoriza

Ejemplos:

Se realiza un plan detallado de cada una de las áreas de negocio de la empresa.

Se incluyen plan de distribución y plan de simulacros del plan DRP

1. ORGANIZACIÓN DE ESTE DOCUMENTO

El presente Plan de Recuperación de Desastres y Contingencias está estructurado como sigue:

CAPITULO 1: OBJETIVOS Y CONSIDERACIONES PRELIMINARES

Explica los objetivos del Plan de Recuperación de Desastres y Contingencias, instrucciones de uso y distribución, junto con una visión de las acciones a realizar.

Se incluyen las direcciones y teléfonos de contacto de los miembros de los equipos, proveedores, organizaciones y entidades oficiales y personas clave que pueda ser preciso contactar durante la recuperación.

CAPITULO 2: EQUIPOS DEL PLAN DE RECUPERACIÓN

Describe la organización en Equipos de responsabilidad concreta de las personas claves para las tareas de recuperación. Describe la composición y responsabilidades de cada equipo.

CAPITULO 3: CRITERIO PARA ACTIVAR EL PLAN DE RECUPERACIÓN DE DESASTRES Y CONTINGENCIAS

Especifica el criterio a seguir para poner en marcha el Plan de Recuperación de Desastres y Contingencias.

CAPITULO 4: PLAN DE ACCIONES PARA HABILITAR APLICACIONES CRÍTICAS

Detalla el plan de acciones a realizar por los componentes de los equipos durante el desarrollo del Plan, organizados en FASES ACTIVIDADES y TAREAS, para la habilitación de las aplicaciones críticas de FLORES GARIBAY.

CAPITULO 5: CRITERIO PARA REGRESAR A OPERACIÓN NORMAL

Especifica el criterio a seguir para regresar a la operación normal una vez recuperadas las aplicaciones críticas.

CAPITULO 6: PLAN DE ACCIONES PARA REGRESAR A OPERACIÓN NORMAL

Detalla el plan de acciones a realizar por los componentes de los equipos, organizados en FASES ACTIVIDADES y

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

TAREAS, para regresar a la operación normal una vez superado el desastre o contingencia.

CAPITULO 7: PRUEBAS DEL PLAN

Recoge sintéticamente de cada prueba del Plan que se haya realizado: los objetivos, alcance, registro del seguimiento de actividades, asuntos a tener en cuenta, resultados e incidencias.

CAPITULO 8: MANTENIMIENTO DEL PLAN

Detalla el plan de acciones a realizar por los componentes de los equipos, organizados en FASES ACTIVIDADES y TAREAS, para realizar el mantenimiento del plan.

CAPITULO 9: ANEXOS

Información relacionada con el Plan de Recuperación de Desastres y Contingencias a tener en consideración.

CAPITULO 10: LISTA DE PRECIOS

Información relacionada con precios de mano de obra y refacciones de los equipos de cómputo del Plan de Recuperación de Desastres y Contingencias.

2. OBJETIVOS Y CONSIDERACIONES PRELIMINARES

2.1. Objetivos del Plan

El objetivo general del presente Plan de Recuperación de Desastres y Contingencias es la protección de las aplicaciones críticas de FLORES GARIBAY y su información para salvaguardar los registros vitales de la organización y para asegurar la disponibilidad de las mismas en el caso de un desastre o contingencia que afecte su funcionalidad normal. La principal función del plan es documentar las acciones de respuesta, recuperación, habilitación de las aplicaciones críticas y el regreso a la operación normal.

El Plan es una guía sistemática de los pasos a seguir desde que se genera un desastre o contingencia hasta la recuperación de las aplicaciones críticas en operación normal. El enfoque básico, premisas generales y secuencia de acciones que necesitan ser seguidos, se especificarán claramente en la documentación contenida en el presente Plan. Mientras esté siendo utilizado durante un desastre o contingencia, habrá situaciones que no se tengan contempladas, por lo que se tendrá que llevar un registro de dichas actividades. Todas las acciones alternativas deberían ser documentadas tan pronto como el Plan sea ejecutado y las revisiones al mismo tengan lugar. El Plan deberá ser distribuido al personal clave y ellos deberán recibir todas las actualizaciones. Esto significa que deberá de ser funcional independientemente del tipo de desastre o contingencia que ocurra.

Un desastre, para efectos de este Plan lo designaremos como desastre a la ocurrencia de cualquier evento fortuito que cause una interrupción en las aplicaciones críticas de FLORES GARIBAY tal que sea necesaria la recuperación de las mismas en un CPD (Centro de Procesamiento de Datos) alternativo.

Una contingencia, para efectos de este Plan lo designaremos como contingencia a la ocurrencia de cualquier evento fortuito que cause una interrupción en las aplicaciones críticas de FLORES GARIBAY sin que llegue al extremo de ser necesario recuperarlas en un CPD alternativo.

2.2. Premisas del Plan

La recuperación de cualquier evento, que no sea una total destrucción, será llevada a cabo utilizando el Plan.

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Normalmente los miembros disponibles del equipo pueden convertirse en indisponibles a causa del desastre o pueden no ser capaces de participar en la recuperación.

Los procedimientos son lo suficientemente detallados para que cualquier persona, además del responsable principal, pueda seguirlos.

La recuperación de las aplicaciones críticas permitirá a FLORES GARIBAY continuar con las operaciones críticas adecuadamente.

Un desastre o contingencia puede requerir que los usuarios trabajen con un soporte automatizado limitado y alguna degradación en el servicio hasta que sea realizada completamente la recuperación.

Los usuarios pueden requerir recapturar información perdida desde la realización del último respaldo hasta la recuperación de las aplicaciones críticas.

2.3. Estrategia General

La estrategia general que se seguirá para lograr los objetivos propuestos en el Plan será, para el caso general de un evento calificado como Desastre, la de contar con un CPD Alternativo pasivo, disponible para este propósito en caso de ser necesario, y levantando en él las aplicaciones críticas de FLORES GARIBAY, utilizando los respaldos de las aplicaciones y su información inmediatamente después de ocurrido el evento.

Se denomina CPD Alternativo pasivo debido a que sólo en el evento calificado como Desastre se procederá a levantar las aplicaciones críticas de FLORES GARIBAY en él, permaneciendo sin operación el resto del tiempo.

Un CPD Alternativo activo, a diferencia del CPD Alternativo pasivo, es aquel en el que se tienen instaladas las aplicaciones y existe siempre una replicación de la información de las mismas para que en el caso de un Desastre este CPD continúe en operación sin tener tiempos de interrupción. La inversión del CPD Activo en Hardware es muy elevada en comparación con la inversión requerida para un CPD Pasivo, ya que es necesario tener los equipos en Cluster (Replicación de la información).

La elección del CPD Alternativo pasivo se justifica por el costo económico y logístico que implicaría para FLORES GARIBAY mantener la replicación de la información de sus oficinas, instalaciones, unidades de negocio y/o sucursales en línea en el CPD Alternativo en uno o más equipos. Por otro lado, la probabilidad de que ocurra un desastre simultáneamente en todas las instalaciones y/o unidades es siempre menor a que ocurra en una sola unidad de negocio y/u oficina.

Los requerimientos para esta estrategia se resumen en los siguientes puntos:

1. RESPALDO EXTERNO DE DATOS Y SOFTWARE

El respaldo de seguridad consta de:

Una copia Semanal de todos los discos de la instalación, excepto los temporales y de trabajo. Esta copia respalda todo el Software de la instalación, Sistema, Productos, aplicaciones, fuentes y objetos de producción.

Una copia Diaria de los datos de las aplicaciones críticas, Bases de Datos y Ficheros. Permite recuperar los datos de las aplicaciones críticas con menos de 24 horas de proceso perdido.

Estas copias de seguridad se deben trasladar todos los días a un armario ignífugo situado en el exterior del edificio del CPD (para ver detalle del almacenamiento consultar el inventario y/o bitácora correspondiente de FLORES GARIBAY), ya que de ellas depende la recuperación de las aplicaciones críticas, objeto de este Plan.

2. CPD ALTERNATIVO

FLORES GARIBAY dispondrá, en caso de desastre, de los recursos necesarios para la recuperación en un CPD alternativo.

Siempre y cuando la magnitud del desastre permita el traslado de los equipos portátiles, para levantar el

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

servidor o los servicios afectados por el desastre, ya que se cuenta con equipo móviles (PC portátil) y se tiene la factibilidad de crear una nueva (s) partición (es) dentro de los servidores con los que cuenta FLORES GARIBAY, para mantener las operaciones críticas de FLORES GARIBAY en funcionamiento.

SERVICIO RESTRINGIDO EN EL CPD ALTERNATIVO

Como ya se ha establecido en los objetivos se recuperarán sólo las aplicaciones críticas de FLORES GARIBAY. Por lo tanto la producción en el CPD alternativo no deberá tener necesariamente las mismas características que en situación normal.

Se dispondrán de dos equipos portátiles, uno para cada aplicación, configurados de tal manera que en caso de Contingencia o Desastre la operación de los sistemas críticos, se pueda seguir desarrollando, una vez recuperados los respaldos de la bases de datos, sin necesidad de contar con el servidor de aplicación.

Los equipos portátiles destinados a estas aplicaciones deberán tener preinstalado las aplicaciones correspondientes para su correcto funcionamiento.

RESPALDO DE COMUNICACIONES

EL CPD alternativo dispondrá de las líneas de comunicaciones necesarias para el funcionamiento de las aplicaciones críticas de FLORES GARIBAY. Los controladores de comunicaciones remotos que integran la red actual dispondrán de conexión alternativa para enlazar con el sistema en el CPD alternativo. Las oficinas que dependen de los controladores del CPD principal dispondrán de línea alternativa para enlazar directamente con el controlador del CPD alternativo.

2.4. Instrucciones de Uso, Guía Rápida y Directorio Telefónico

INSTRUCCIONES DE USO

El Plan será efectivo desde el momento de declararse la situación de desastre o contingencia. La declaración de dicha situación la realizará, como se detalla en el plan de acciones, el equipo del Plan (EDP) teniendo en cuenta el informe y recomendaciones que el Equipo de Emergencia del Plan (EEP) hará después de la primera inspección y evaluación de daños.

Tan pronto como se declare la situación de emergencia el plan se activará contactando con los miembros de los Equipos y siguiendo las actividades marcadas en el plan de acciones.

El plan continuará en efecto hasta que las operaciones normales puedan ser reanudadas en el CPD reconstruido y el control devuelto a la dirección funcional habitual.

La estrategia general del Plan consiste en contar con un CPD Alterno pasivo para ser utilizado en el caso de un evento calificado como desastre (ver capítulo 1.3. Estrategia General). Este CPD Alterno será pasivo hasta declararse la situación de desastre y se pongan en marcha las acciones para levantar las aplicaciones críticas en él. A partir de este momento pasará de ser pasivo a ser activo.

El CPD Alterno continuará activo hasta que las operaciones normales puedan ser reanudadas en el CPD reconstruido y el control devuelto a la dirección funcional habitual, momento en el que pasará a ser nuevamente CPD Alterno pasivo (este momento también marca el fin del alcance del Plan).

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

GUIA RÁPIDA

Guía rápida del Plan de Recuperación en caso de Desastre.

PASO ACTIVIDADES RESPONSABLES

PASO	ACTIVIDADES	RESPONSABLES

DIRECTORIO TELEFÓNICO

Equipo Director (EDP):

Función	Nombre	Teléfono 1	Teléfono 2
Responsable			
Suplente del Responsable			
Miembro Equipo			

Equipo de Emergencia (EEP):

Función	Nombre	Teléfono 1	Teléfono 2
Responsable			
Suplente del Responsable			
Miembro Equipo			

Equipo del Centro Alternativo (ECA):

Función	Nombre	Teléfono 1	Teléfono 2
Responsable			
Suplente del Responsable			
Miembro Equipo			
Miembro Equipo			

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Equipo de Soporte a Aplicaciones (ESA):

Función	Nombre	Teléfono 1	Teléfono 2
Responsable			
Suplente del Responsable			
Miembro Equipo			
Miembro Equipo			
Miembro Equipo			

Equipo de Soporte a Usuarios (ESU):

Función	Nombre	Teléfono 1	Teléfono 2
Responsable			
Suplente del Responsable			
Miembro Equipo			

Equipo del Mantenimiento del Plan (EMP):

Función	Nombre	Teléfono 1	Teléfono 2
Responsable			
Suplente del Responsable			
Miembro Equipo			

3. EQUIPOS DEL PLAN DE RECUPERACIÓN

3.1. Introducción

El Plan establece una serie de equipos para dirigir, gestionar, controlar y mantener el mismo, cada uno de los cuales es responsable de una serie de actividades. Estas actividades y las responsabilidades consiguientes se definen claramente en este capítulo, para cada uno de los equipos contemplados.

Cada equipo está compuesto por varios miembros con un coordinador que es el máximo responsable del equipo. Su principal función es asignar el trabajo a los miembros de su equipo y controlar que las tareas de cada uno son realizadas adecuadamente.

Para el caso de que el responsable del equipo no esté presente en el momento preciso, se define la figura del coordinador suplente, quien, además de las actividades que tenga asignadas, cubrirá el puesto del coordinador durante el tiempo necesario.

La composición de cada equipo ha de considerarse flexible, debiéndose ajustar el número de personas de cada equipo dependiendo de la magnitud de la contingencia y de cada situación concreta.

La estructura organizativa del presente Plan de recuperación incluye los siguientes equipos:

- Equipo Director del Plan (EDP)
- Equipo de Emergencia del Plan (EEP)
- Equipo de Centro Alternativo (ECA)

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

- Equipo de Soporte a Aplicaciones (ESA)
- Equipo de Soporte a Usuarios (ESU)
- Equipo de Mantenimiento del Plan (EMP)

3.2. Equipo Director del Plan (EDP)

Es el máximo responsable del Plan tanto a nivel de la gestión y control del mismo como de su puesta en funcionamiento en caso de emergencia.

Las principales funciones a desempeñar por el equipo son las siguientes:

Ajuste del Plan a las directrices básicas de la empresa y definición de estrategias en relación con el Plan.

Responsable de la inclusión en el Plan de la política de seguridad corporativa, tanto a nivel general (procedimientos internos) como en relación con el entorno específico del edificio a proteger.

Decisión de activar el Plan.

Notificación a los usuarios de la situación de emergencia.

Notificación al centro alternativo de la ocurrencia de la contingencia.

Responsable directo de la prioridad de las aplicaciones.

En caso necesario, definición de los acuerdos con empresas de respaldo.

Coordinación del resto de los equipos del Plan.

Composición del Equipo Director del Plan (EDP):

- Coordinador de Organización y Sistemas (Responsable).
- Gerente de Sistemas y Telecomunicaciones (Suplente del Responsable)
- Jefe de Sistemas
- Jefe de Telecomunicaciones
- Responsable Funcional Sistemas

3.3. Equipo de Emergencia del Plan (EEP)

Es el máximo responsable del Plan una vez que el Equipo Director del Plan (EDP) ha decidido su entrada en funcionamiento.

Las principales funciones a realizar por el Equipo de Emergencia del Plan (EEP) son las siguientes:

Evaluación de daños producidos como consecuencia de la contingencia.

Decisión de la acción alternativa específica a tomar en base a la magnitud del desastre.

Decidir cuándo la situación de emergencia ha sido superada y debe retornarse a la operación normal.

Responsable de decidir en base a la prioridad de aplicaciones qué sistemas / subsistemas deben ser procesados.

Responsable de toda la actividad informática durante el tiempo que dure la contingencia.

Responsable del diseño, configuración y mantenimiento de las comunicaciones en situaciones de emergencia.

Responsable de que las medidas de seguridad física y lógica son adecuadas durante el periodo de emergencia.

Coordinación con los responsables de los Departamentos usuarios implicados.

Responsable de la aplicación puntual de las pautas contenidas en el Plan y de su control y seguimiento.

Poner todos los medios técnicos necesarios para llevar a cabo la explotación de las aplicaciones críticas (configuración del sistema, herramientas de ayuda, recuperación y / o reconstrucción desde copias de seguridad de ficheros, bases de datos, programas y procedimientos de control, etc.).

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Recabar a la Dirección de OROBOLEADO los recursos humanos necesarios para tareas auxiliares pero que pueden convertirse en críticas (secretarías, conductores, personal de mantenimiento, etc.).

Asegurar el adecuado traslado y retorno de todos los activos necesarios al centro alternativo.

Suministrar todos los formularios necesarios para la explotación en el centro alternativo.

Registrar todas las incidencias que se produzcan en cualquiera de las actividades emprendidas en el periodo de emergencia, reportándolas al Equipo del Plan (EDP) con el fin de optimizar el Plan.

Asesoramiento al Equipo Director del Plan (EDP).

Composición del Equipo de Emergencia del Plan (EEP):

- Gerente de Sistemas y Telecomunicaciones (Responsable)
- Jefe de Sistemas (Suplente del Responsable)
- Jefe de Telecomunicaciones
- Responsable de Sistemas

3.4. Equipo del Centro Alternativo (ECA)

Responsable de preparar los recursos y configuración previstos en el Plan en el Centro Alternativo y de dar soporte técnico a los profesionales de FLORES GARIBAY para la restauración de su sistema y posterior explotación, tanto en las pruebas periódicas del Plan como en caso de una contingencia real.

Las principales funciones contempladas son:

Preparar la configuración HW necesaria para la restauración de las aplicaciones críticas de OROBOLEADO según los requisitos especificados.

Preparar sitio de trabajo para los técnicos y operadores de FLORES GARIBAY que deban desplazarse al Centro Alternativo para la restauración y explotación.

Gestionar autorización de acceso al Centro Alternativo a dicho personal.

Proporcionar el soporte técnico necesario, facilitar la restauración y explotación en dicho centro alternativo

Composición del Equipo del Centro Alternativo (ECA):

- Jefe de Telecomunicaciones (Responsable)
- Enlace Informático (Suplente del Responsable)
- Responsable de Sistemas

3.5. Equipo de Soporte a Aplicaciones (ESA)

Responsable de dar soporte técnico ante cualquier problema específico de una aplicación que pudiera surgir durante la restauración o explotación en el Centro Alternativo.

Las principales funciones contempladas son:

Estar disponibles durante el periodo de explotación en el Centro Alternativo, en especial durante la restauración del servicio.

Soporte técnico para la resolución de problemas específicos de cada aplicación.

Verificar, junto a los responsables de usuarios, el correcto funcionamiento de la aplicación después de la restauración

Fijar, junto a los responsables de usuarios, los criterios de pruebas y verificación de la aplicación durante las pruebas del Plan.

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Composición del Equipo de Soporte a Aplicaciones (ESA):

- Jefe de Sistemas (Responsable)
- Responsable Soporte Técnico
- Responsable de Sistemas

3.6. Equipo de Soporte a Usuarios (ESU)

Responsable de coordinar con los usuarios de las aplicaciones la explotación en condiciones de emergencia.

Las principales funciones contempladas son:

Definir los requerimientos de servicio mínimo de los usuarios, pantallas críticas y horario.

Notificar al EMP cualquier cambio en los requerimientos anteriores o en otras circunstancias de los usuarios que puedan afectar al Plan de Recuperación.

Prever los procedimientos alternativos de los usuarios durante el periodo de restauración del servicio.

Definir las prioridades en las funciones de usuarios para la explotación con servicio restringido

Coordinar los problemas y peticiones de usuarios durante el servicio restringido y notificarlos al Equipo Director del Plan (EDP).

Composición del Equipo de Soporte a usuarios (ESU):

- Responsable Funcional de Sistemas (Responsable 1)
- Responsable Funcional de Sistemas (Responsable 1)

3.7. Equipo de Mantenimiento del Plan (EMP)

Responsable, en condiciones normales de actividad, de actualizar y revisar el Plan en base a las modificaciones que se vayan produciendo.

Las principales funciones contempladas son:

Realizar la actualización puntual del Plan en base a los cambios en los diferentes aspectos que lo componen.

Adecuación del Plan a los procedimientos existentes en OroBoleado.

Comprobar que la configuración del centro alternativo es compatible con los procesos a realizar.

Dirigir y fomentar las pruebas del Plan, organizando simulacros de contingencias.

Garantizar que el personal involucrado en el Plan conoce el mismo y está suficientemente entrenado.

Registrar todo tipo de incidencias y resultados de las diferentes pruebas del Plan con objeto de optimizar el mismo.

Composición del Equipo de Mantenimiento del Plan (EMP):

- Gerente de Sistemas y Telecomunicaciones (Responsable).
- Coordinador de Organización y Sistemas (Suplente del Responsable).
- Responsable Funcional de Sistemas
- Jefe de Sistemas
- Jefe de Telecomunicaciones

4. CRITERIO PARA ACTIVAR EL PLAN DE RECUPERACIÓN DE DESASTRES Y CONTINGENCIAS

La detección de cualquier evento que pueda resultar en desastre o contingencia y que afecte las instalaciones de FLORES GARIBAY y sus diferentes sistemas, es responsabilidad de todo el personal de FLORES GARIBAY, de quien primero descubra o reciba información acerca de una situación de emergencia.

Tan pronto como una situación que pueda ocasionar la interrupción de aplicaciones ocurra, el personal deberá contactar a las autoridades de emergencia apropiadas y tomar las medidas necesarias para minimizar los daños

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

o lesiones al personal en su vecindad.

El siguiente personal y organismos deben ser notificados:

Operaciones de ORO BOLEADO

Encargados de los edificios

Policía, bomberos, cruz roja, etc. (en los casos de contingencias mayores)

Responsable del Equipo Director del Plan (EDP)

El responsable del Equipo Director del Plan (EDP) contactará al Equipo de Emergencia del Plan (EEP).

El Equipo de Emergencia del Plan (EEP) realizará una visita al sitio, hará una evaluación inicial de la extensión del daño y determinará en nivel de desastre o contingencia en función de evaluación de daños.

Basado en su asesoría se deberá decidir si es iniciado todo o parte del Plan de Recuperación de Desastres y Contingencias con su plan de acción correspondiente.

El Equipo de Emergencia del Plan (EEP) deberá decidir:

Si la operación normal en el sitio puede continuar y las reparaciones pueden ser iniciadas inmediatamente.

El daño es menor. Las operaciones pueden ser reiniciadas en corto tiempo con ninguna llamada especial a los equipos del Plan.

El tiempo previsto sin servicio es menor a un día.

Si la operación normal puede continuar o ser restaurada con la asistencia de solo ciertos equipos del Plan.

El daño es medio. Los equipos seleccionados serán llamados para una recuperación directa de las operaciones normales en el mismo CPD.

El tiempo anticipado sin servicio es de dos a seis días.

Si la operación puede continuar de manera limitada en el mismo CPD y se debe iniciar plan para reparar o reemplazar equipo dañado.

El daño es mayor. Los equipos seleccionados serán llamados para una recuperación directa de las operaciones normales en el mismo CPD.

El tiempo anticipado sin servicio es mayor a seis días.

Si el CPD ha sido destruido o el daño es de tal magnitud que debe ser utilizado el CPD alternativo.

La recuperación tomará más de una semana.

Todos los responsables de los equipos del Plan deberán ser llamados para iniciar una total implementación del Plan de Recuperación de Desastres y Contingencias.

El Equipo de Emergencia del Plan (EEP) decidirá el plan de acción y entonces lo notificará al EDP.

Si dicho plan de acción requiere la asistencia de otros equipos del Plan, esos equipos deberán ser notificados.

A continuación se presentan tres matrices que permitirán, a partir de una contingencia o desastre, determinar las acciones a seguir. Estas tres matrices componen el cubo Tipo de instalaciones – Contingencias – Aplicaciones Críticas – Acciones.

Matriz 1: Localidades por tipo de instalaciones. Define las localidades y el tipo que les corresponde, así como el lugar físico del equipo funcional alterno.

Matriz 2: Niveles de Desastre o Contingencia por Contingencia, Aplicación Crítica y Tipo de instalaciones. Relaciona, por cada posible contingencia, el nivel de desastre o contingencia que le corresponde en función a las aplicaciones críticas y el tipo de instalaciones.

Matriz 3: Fases, Actividades y Tareas, por Tipo de instalaciones y Nivel de Desastre o Contingencia. Define por cada tipo de instalaciones y cada nivel de desastre o contingencia, las fases, actividades y tareas a seguir correspondientes al PLAN DE ACCIONES PARA HABILITAR APLICACIONES CRÍTICAS.

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Los niveles de contingencia y desastre se definen como sigue:

CONTINGENCIA

Menor (Tiempo estimado sin servicio < 1 día, mismo CPD)

Media (2 días <= Tiempo estimado sin servicio <= 6 días, mismo CPD)

Mayor (Tiempo estimado sin servicio > 6 días, mismo CPD)

DESASTRE

Tiempo estimado sin servicio > 6 días, CPD Alterno

Matriz 1: Localidades por Tipo de Instalaciones

TIPO DE INSTALACIONES	LOCALIDAD	EQUIPO DE EMERGENCIA FUNCIONAL

Matriz 2: Niveles de Desastre o Contingencia por Contingencia, Aplicación Crítica y Tipo de instalaciones

CONTINGENCIA	SISTEMA 1			SISTEMA 2		
EQUIPO DE COMPUTO: SERVIDOR						
Motherboard Dañada	Menor	Menor	Media	Desastre	Desastre	Media
Procesador Dañado	Menor	Menor	Media	Desastre	Desastre	Media
Memoria Dañada	Menor	Menor	Media	Desastre	Desastre	Media
Disco Duro Dañado	Menor	Menor	Media	Desastre	Desastre	Media
Ventilador Dañado	Menor	Menor	Media	Desastre	Desastre	Media
Fuente de Poder Dañada	Menor	Menor	Media	Desastre	Desastre	Media
Unidad de Cinta Dañada	Media	Media	Media	Media	Media	Media
Daño del Rack de Computo	Desastre	Desastre	Media	Desastre	Desastre	Media
Daño del rack de Comunicaciones	Desastre	Desastre	Media	Desastre	Desastre	Media
Tarjeta de red Dañada	Desastre	Desastre	Media	Desastre	Desastre	Media
Tarjeta de Comunicación Dañada	Desastre	Desastre	Media	Desastre	Desastre	Media
Bios Dañado	Menor	Menor	Menor	n/a	n/a	n/a
Sistema Operativo Dañado	Menor	Menor	Menor	Menor	Menor	Menor
Instalación Service Pack	Menor	Menor	Menor	Menor	Menor	Menor
Base de Datos Dañada	Menor	Menor	Menor	Menor	Menor	Menor
Instalación Nueva Versión de Sw	Menor	Menor	Menor	Media	Media	Media
Virus en Sw de Aplicativo	Desastre	Desastre	Media	n/a	n/a	n/a
Aplicación Falla Cliente	Menor	Menor	Menor	Menor	Menor	Menor

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

EQUIPO DE TELECOMUNICACIONES						
Switch Dañado	Menor	Menor	Menor	Menor	Menor	Menor
Ruteador Dañado	Media	Media	Media	Media	Media	Media
NTU Dañado	Media	Media	Media	Media	Media	Media
E1 Dañado	Menor	Menor	Menor	Menor	Menor	Menor
Daño de descanalizador						
Daño del MODEM de ISDN España	Menor	Menor	Menor	Menor	Menor	Menor
Daño de Tarjeta de Router Principal						

ENERGÍA						
Daño de Regulador principal	Menor	Menor	Menor	Menor	Menor	Menor
Daño de No Brake	Menor	Menor	Menor	Desastre	Desastre	Media
Caida de Energía Eléctrica	Menor	Menor	Menor	Desastre	Desastre	Media
Problema con Planta Eléctrica	Desastre	Desastre	Media	Desastre	Desastre	Media
Corte de Energía Eléctrica Provocado	Desastre	Desastre	Media	Desastre	Desastre	Media

NATURALES O PROBLEMAS NO TECNICOS						
Huracán	Menor	Menor	Menor	Menor	Menor	Menor
Temblor	Desastre	Desastre	Desastre	Desastre	Desastre	Desastre
Terremoto	Desastre	Desastre	Desastre	Desastre	Desastre	Desastre
Corto en el Edificio	Desastre	Desastre	Desastre	Desastre	Desastre	Desastre
Derrumbe del Site	Desastre	Desastre	Desastre	Desastre	Desastre	Desastre
Daño en la estructura del Edificio	Desastre	Desastre	Desastre	Desastre	Desastre	Desastre

Matriz 3: Fases, Actividades y Tareas, por Tipo de instalaciones y Nivel de Desastre o Contingencia

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

TIPO DE INSTALACIONES	NIVEL	FASE – ACTIVIDAD – TAREA	EQUIPO RESPONSABLE
Sistema 1	Contingencia Menor	FASE 1 FASE 2 Las que apliquen FASE_3 Todas	Quien identifica la contingencia Equipo Director del Plan (EDP) Equipo Director del Plan (EDP) Equipo de Emergencia del Plan (EEP) Equipo de Centro Alternativo (ECA) Equipo de Emergencia del Plan (EEP) Equipo de Emergencia del Plan (EEP) Equipo de Emergencia del Plan (EEP) Equipo Director del Plan (EDP) Equipo de Emergencia del Plan (EEP) Equipo de Soporte a usuarios (ESU) Equipo de Soporte a aplicaciones (ESA) Equipo de Emergencia del Plan (EEP) Equipo de Soporte a usuarios (ESU) Equipo de Soporte a aplicaciones (ESA) Equipo de Emergencia del Plan (EEP)

5. PLAN DE ACCIONES PARA HABILITAR APLICACIONES CRÍTICAS

Las Fases del Plan pueden encuadrarse en dos grupos:
 RESPUESTA ANTE LA EMERGENCIA (CAPITULOS 4. Y 6.)

- FASE_1 ACTIVACION DEL PLAN
- FASE_2 EVALUACION DE DAÑOS
- FASE_3 TRASLADO AL CPD ALTERNATIVO
- FASE_4 RESTAURACION SISTEMA
- FASE_5 RESTAURACION COMUNICACIONES
- FASE_6 RESTAURACION APLICACIONES
- FASE_7 EXPLOTACIÓN RESTRINGIDA
- FASE_8 RECONSTRUCCION CPD
- FASE_9 REGRESO AL CPD
- FASE_10 EVALUACION POSTERIOR

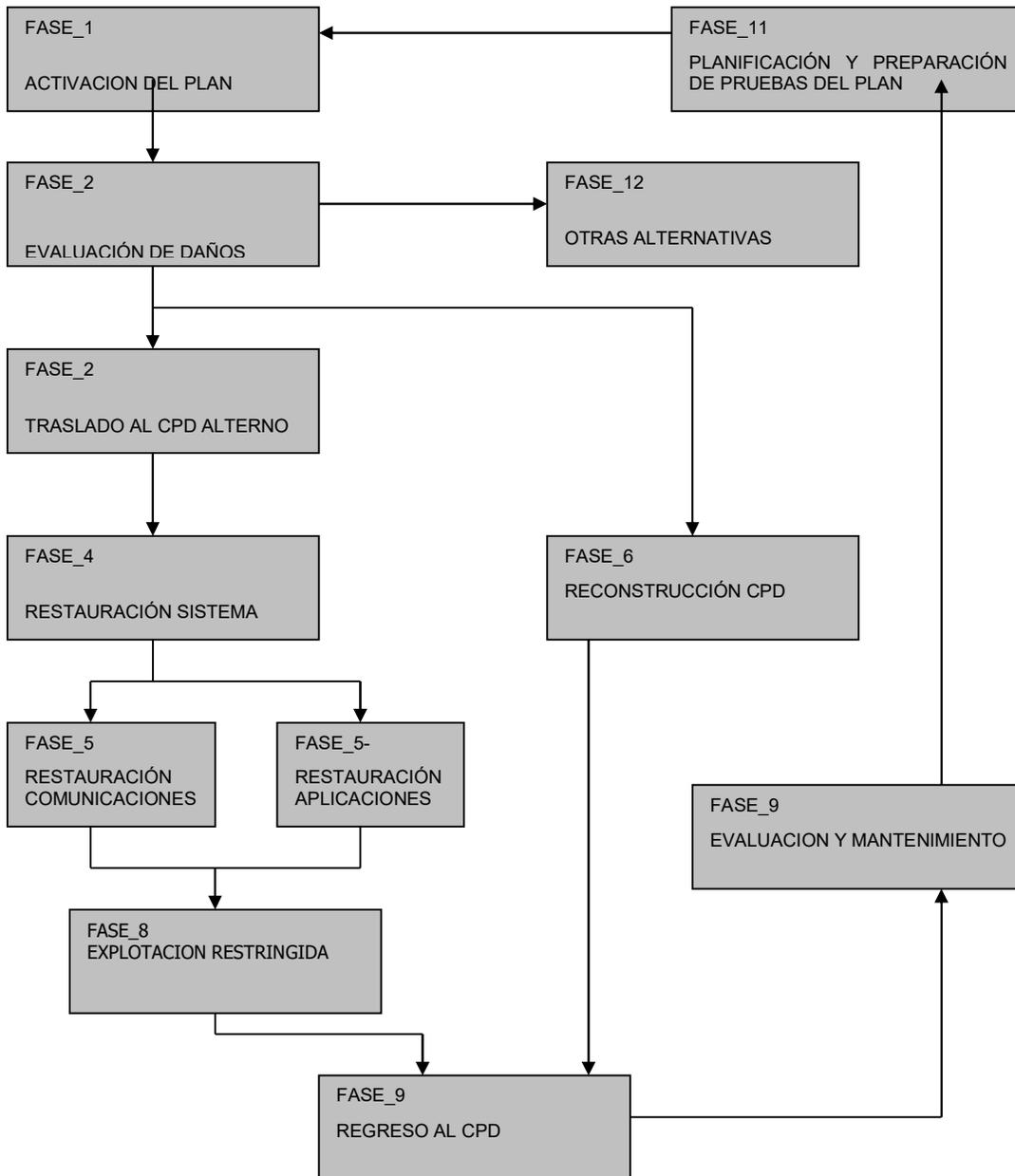
MANTENIMIENTO DEL PLAN (CAPITULOS 7. Y 8.)

- FASE_11 PLANIFICACION Y PREPARACION DE PRUEBAS DEL PLAN
- FASE_12 EVALUACION Y MANTENIMIENTO

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

La secuencia de Fases se refleja en el esquema siguiente:



MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Fase FASE_1

Actividad 31-010 AVISAR RESPONSABLES EQUIPOS EDP, EEP, ECA, ESA, ESU, EMP

Id TareaTarea Duración Responsable

=====

31010	Avisar al responsable del Equipo del Plan (EDP) x	hora(s)	Quien	identifica
	la contingencia			
31015	Avisar responsables de los otros equipos: x	hora(s)	Emergencia, Centro	Alternativo,
	Soporte a Aplicaciones, Soporte a Usuarios			

Fase FASE_2

Actividad 320 FORMAR EQUIPOS

Id TareaTarea Duración Responsable

=====

32010	Acudir a los lugares de encuentro convenidos x	hora		
32015	Ponerse en contacto con el responsable del equipo al que se x	horas		
32025	Ponerse en contacto con el responsable del Equipo de x	horas	Emergencia del Plan	

Fase FASE_3

Actividad 330 NOTIFICAR LA CONTINGENCIA

Id TareaTarea Duración Responsable

=====

33010	Notificar al Equipo del Centro Alternativo (ECA) x	hora(s)		
-------	--	---------	--	--

Fase FASE_4

Actividad 340 EVALUACION DE DAÑOS

Id TareaTarea Duración Responsable

=====

34010	Inspeccionar daños ocasionados x	hora(s)		
34015	Relacionar daños en obra e instalaciones x	hora(s)		
34020	Relación de equipo dañado y perdido x	hora(s)		
34025	Evaluar posibilidad y plazo de recuperación x	hora(s)		
34030	Informar al Equipo del Plan (EDP) x	hora(s)		

Fase FASE_5

Actividad 345 DECISION DE ALTERNATIVA

Id TareaTarea Duración Responsable

=====

34510	Decidir si se traslada la explotación al Centro Alternativo (CA) x	hora(s)		
34515	Decidir si se espera la recuperación del CPD x	hora(s)		
34520	Notificar a los otros equipos: Emergencia (EEP), Mantenimientox	hora(s)		
	(EMP), Centro Alternativo (ECA), Sporte Aplicaciones (ESA), Soporte Usuarios (ESU)			

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Fase FASE_6

Actividad 350 PREPARAR CONFIGURACION

Id TareaTarea Duración Responsable

```

=====
35010 Preparar bienes informáticos x hora(s)
35015 Preparar configuración de discos según relación requerida x hora(s)
35020 Preparar otros periféricos requeridos x hora(s)
35025 Preparar líneas comunicacionesx hora(s)
35030 Probar configuración y sus elementos x hora(s)
    
```

Fase FASE_7

Actividad 360 TRASLADO DE COPIAS DE SEGURIDAD

Id TareaTarea Duración Responsable

```

=====
36010 Reunir cintas del último backup semanal x hora(s)
36015 Reunir cintas del último backup diario x hora(s)
36020 Traslado de cintas a armario del CPD Alternativo (CA) x hora(s)
    
```

Fase FASE_8

Actividad 370 PETICIONES DE SUMINISTROS

Id TareaTarea Duración Responsable

```

=====
37010 Realización de formularios y otros recursos adicionales para x hora(s) los proveedores
37015 Petición de servicios de impresión x hora(s)
    
```

Fase FASE_9

Actividad 380 ORGANIZACION DE TURNOS

Id TareaTarea Duración Responsable

```

=====
38010 Organizar turnos de operación en el CPD actual o en CPD x horas alternativo (CA)
38015 Coordinación con los operadores propios del CPD actual o x horas CPD alternativo
38020 Organizar turnos de soporte técnico ininterrumpido durante x horas restauración en el CPD
actual o en el CPD alternativo (CA)
38025 Organizar medios de traslado del personal al Centro x horas
Alternativo (CA)
    
```

Fase FASE_9

Actividad 390 ADMISION PERSONAL EN CENTRO ALTERNATIVO (CA)

Id TareaTarea Duración Responsable

```

=====
39010 Identificación del personal de equipos de la empresa x minuto(s) ECA
    
```

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

39015 Autorizaciones de acceso x minuto(s) ECA
 39020 Informar sobre normas de seguridad del CPD Alternativo (CA) x minuto(s) ECA
 39025 Informar sobre servicios (manutención y otros) x minuto(s) ECA

Fase FASE_9

Actividad 410 RESTAURAR ULTIMO BACKUP SEMANAL

Id TareaTarea Duración Responsable

=====
 41010 Restaurar volúmenes de producción del último backup x hora(s) semanal

Fase FASE_9

Actividad 420 ACTIVACION COMUNICACIONES ALTERNATIVAS

Id TareaTarea Duración Responsable

=====
 42010 Activar RUTAS y CONFIGURACIONES alternativas x minuto(s)

Fase FASE_9

Actividad 425 RESTAURAR DATOS APLICACIONES

Id TareaTarea Duración Responsable

=====
 42510 Restaurar las Bases de Datos con el último backup diario x hora(s) anterior al desastre
 42520 Restaurar posibles ficheros de trabajo de las aplicaciones x hora(s)
 42530 Restaurar aplicaciones considerando: x hora(s)
 - Criticidad
 - Fechas críticas
 42540 Trasladar Backup de seguridad al armario ignifugo exterior x hora(s)

Fase FASE_9

Actividad 430 COMPROBAR APLICACIONES

Id TareaTarea Duración Responsable

=====
 43010 Revisar coherencia de datos y correcto funcionamiento de x hora(s) las aplicaciones

Fase FASE_9

Actividad 435 BACKUP DE SEGURIDAD

Id TareaTarea Duración Responsable

=====
 43510 Realizar Backup de seguridad antes de comenzar la x hora(s) explotación, en función del día de la semana

Fase FASE_8

Actividad 450 PLAN DE EXPLOTACION REGULAR

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Id Tarea	Tarea	Duración	Responsable
45010	Planificar explotación para recuperar el tiempo perdido	x	hora(s)
45040	Planificar explotación regular una vez el trabajo este al día	x	hora(s)

Fase FASE_8

Actividad 470 REGISTRO DE INCIDENCIAS

Id Tarea	Tarea	Duración	Responsable
47010	Registro de todas las incidencias que se detecten en todas las	x día(s)	FASES anteriores

6. CRITERIO PARA REGRESAR A OPERACIÓN NORMAL

Se deberá de seguir el plan de acciones para regresar a operación normal después del evento suscitado.

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

6.1. PLAN DE ACCIONES PARA REGRESAR A OPERACIÓN NORMAL

Fase FASE_10
 Actividad 620 RECUPERACION EQUIPOS INFORMATICOS
 Id TareaTarea Duración Responsable
 =====
 62010 Inventario de equipos informáticos en condiciones de uso y x día(s) reparables
 62020 Necesidades de equipo informático nuevo x día(s) EEP

Fase FASE_10
 Actividad 630 ACONDICIONAMIENTO NUEVO CPD
 Id TareaTarea Duración Responsable
 =====
 63010 Acondicionamiento local x día(s)
 63020 Instalaciones eléctricas, aire, agua, etc. x día(s)
 63030 Instalaciones equipo salvado, reparación y revisión x día(s)
 63040 Instalación equipo nuevo x día(s)
 63050 Acondicionamiento espacio de trabajo x día(s)
 63060 Instalación de líneas de comunicaciones x día(s)
 63070 Pruebas de toda la instalación x día(s)

Fase FASE_10
 Actividad 640 EVALUACION DE PÉRDIDAS
 Id TareaTarea Duración Responsable
 =====
 64010 Cálculo de pérdidas económicas debidas a los diversos x día(s) conceptos del desastre
 64020 Reclamaciones a compañías de SEGUROS x día(s)

Fase FASE_10
 Actividad 710 BACKUP DE PRODUCCION EN EL CPD ALTERNATIVO
 Id TareaTarea Duración Responsable
 =====
 71010 Realizar copia de seguridad de todos los discos de la x hora(s) instalación del CPD alternativo (CA)
 71020 Traslado al nuevo CPD de la empresa x día(s)

Fase FASE_10
 Actividad 720 RESTAURACION DEL BACKUP EN EL NUEVO CPD
 Id TareaTarea Duración Responsable
 =====
 72010 Restaurar copia de seguridad de todos los discos de la x hora(s) instalación en el nuevo CPD de la empresa

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Fase FASE_11

Actividad 730 PRUEBAS

Id TareaTarea Duración Responsable

=====

73010	Probar sistema, comunicaciones	x	hora(s)
-------	--------------------------------	---	---------

73020	Pruebas de aplicaciones	x	hora(s)
-------	-------------------------	---	---------

Fase FASE_11

Actividad 740 EXPLOTACION NORMAL

Id TareaTarea Duración Responsable

=====

74010	Restablecer la explotación normal	x	hora(s)
-------	-----------------------------------	---	---------

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Fase FASE_11

Actividad 810 EVALUACIÓN DEL PLAN

Id TareaTarea Duración Responsable

81010 Evaluación de los registros de Bitácora de incidencias x día(s)
81020 Estudio de problemas y soluciones x día(s)

Fase FASE_11

Actividad 820 ACTUALIZACION DEL PLAN

Id TareaTarea Duración Responsable

82010 Modificación del Plan según las experiencias adquiridas x día(s)
82020 Divulgación del Plan y modificaciones x día(s)

6.2. PRUEBAS DEL PLAN

Fase FASE_10

Actividad 110 PREPARACION CALENDARIO DE PRUEBAS Y SIMULACROS

Id TareaTarea Duración Responsable

11010 Concretar la fecha y duración de las pruebas en coordinación x día(s) con el Centro Alternativo.

Fase FASE_9

Actividad 120 DEFINICION DE PRUEBAS Y SIMULACROS

Id TareaTarea Duración Responsable

12010 Planificar los objetivos de la prueba x día(s)
12020 Planificar el alcance de la prueba x día(s)
12030 Seleccionar el método de la prueba x día(s)
12040 Planificar las actividades/tareas/recursos de la prueba x día(s)
12050 Definir los resultados esperados de la prueba x día(s)

Fase FASE_10

Actividad 130 PREPARACION Y REALIZACION DE PRUEBAS Y SIMULACROS

Id TareaTarea Duración Responsable

13010 Tareas específicas de preparación de la prueba x día(s)
13020 Proporcionar al Centro Alternativo: x día(s) La configuración actualizada de la máquina de prueba, lista del personal autorizado que participará.
13030 Solicitar al Centro Alternativo: x día(s) Los números de serie de las CPU's de la máquina donde

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

se realizaran las pruebas.

13040 Obtener los passwords correspondientes a x día(s) los números de serie de las CPU's de la máquina donde se realizaran las pruebas.

13050 Realizar las actividades seleccionadas siguiendo en detalle el x día(s) Plan con énfasis en el registro detallado de las incidencias.

7. MANTENIMIENTO DEL PLAN

El aseguramiento de que el Plan refleja los cambios suscitados en el transcurso del tiempo es crucial. El mantenimiento consiste en la revisión y actualización del Plan para la incorporación de los cambios, probar el Plan actualizado y comunicar los cambios al personal involucrado. El Equipo de Mantenimiento del Plan (EMP) es el responsable de realizar esta importante tarea.

Es recomendable que el Equipo de Mantenimiento del Plan (EMP) lleve a cabo revisiones al Plan cada 12 meses para asegurar que los cambios surgidos en el periodo hayan sido reflejados o cuando se haya suscitado un evento por lo que se tuvo que aplicar el plan de contingencia.

Así mismo se recomienda que con periodicidad anual el Equipo Director del Plan (EDP) lleve a cabo una revisión completa del Plan que involucre una revisión mayor de este documento.

Las nuevas versiones del Plan deberán ser distribuidas al personal involucrado quien deberá sustituir el anterior por el nuevo y revisado.

Adicionalmente a los periodos de revisión recomendados, el mantenimiento al Plan deberá ser realizado si ocurren cambios en el ambiente operativo tales como:

Cambios al CPD

Cambios en los equipos informáticos que soportan las aplicaciones críticas

Cambios mayores en las aplicaciones críticas

Cambios en las localidades de almacenamiento externo de respaldos

Actualización o instalación de nuevo software

Cambios en los procedimientos de respaldos

Cambios de personal en los equipos del Plan

Fase FASE_10

Actividad 150 EVALUACIÓN DEL PLAN

Id TareaTarea Duración Responsable

=====

15010 Evaluación de los registros de incidencias x día(s)

15020 Estudio de problemas y soluciones x día(s)

Fase FASE_10

Actividad 170 ACTUALIZACION DEL PLAN

Id TareaTarea Duración Responsable

=====

17010 Modificación del Plan conforme a la actualización de alguno x día(s) de los sistemas críticos

17020 Divulgación del Plan y modificaciones x día(s)

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

8. ANEXOS

8.1. Criticidad de Aplicaciones FLORES GARIBAY

En este anexo se detalla el análisis de la criticidad de las Funciones y Aplicaciones Informáticas de FLORES GARIBAY. La resultante es la evaluación del nivel de criticidad de las distintas áreas ante una contingencia o desastre y para el caso de aquellas aplicaciones que no se consideraron críticas se detalla el método alternativo de operación.

En base en las necesidades de las operaciones se determina la criticidad de los Sistemas para el área de Operaciones de FLORES GARIBAY, se ha determinado que es crítico en virtud de que para los procesos de operación tienen que estar en constante operación y en caso de contingencia o desastre la operativa sin él afectaría la continuidad de operación del negocio. Por tanto sí será integrado dentro del Plan de Desastres y Contingencias.

Operaciones

Localidad	Sistema / Aplicación	Evaluación

Facturación

Localidad	Sistema / Aplicación	Evaluación

Cobranza y Tesorería

Localidad	Sistema / Aplicación	Evaluación

En caso de contingencia o desastre que impidan contar con los sistemas de Cobranza y Tesorería, se debe

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

contar con métodos alternos para continuar la operación de estos procesos, para ellos es necesario que las áreas involucradas cuenten con dos computadoras portátiles con la aplicación de banca electrónica instalada, con Excel de Microsoft y la capacidad suficiente para soportar transacciones vía electrónica.

En caso de no contar con la información de los pagos por parte de clientes, las facturas se encuentran físicamente en cada una de las oficinas, unidades de negocio y/o sucursales, lo cual podría significar una forma alterna de consulta. Para emitir nuevas facturas estas podrían realizarse desde las Oficinas Centrales de FLORES GARIBAY.

Con estas herramientas se podría continuar con el desarrollo de las funciones de las áreas involucradas y una vez reestablecido el sistema ingresar los movimientos requeridos.

En base a las necesidades funcionales para evaluar la criticidad de Cobranza y Tesorería, se ha determinado que en caso de contingencia o desastre que impida seguir la operación sin estos sistemas, se cuenta con métodos alternos de operación que permiten darle continuidad al negocio.

Impuestos

Localidad	Sistema / Aplicación	Evaluación
		Critico
		Deseable

En caso de contingencia o desastre que impidan contar con la información de requiere el área de impuestos, se cuentan con métodos alternos para continuar la operación de estos procesos, para ellos es necesario que se cuente con una computadora portátil con la aplicaciones del Sistema de Administración Tributaria de Declaración Anual y Declaraciones Electrónicas, así como los sistemas relacionados, con Excel de Microsoft y la capacidad suficiente para soportar transacciones vía electrónica. Además será necesario contar con una estrategia de respaldo del equipo de finanzas cada 15 días, con el fin de asegurar la disponibilidad de la información.

En caso de no contar con la información que el sistema proporciona, se solicitara a Contabilidad las Balanzas de Comprobación, a Crédito y Cobranza los reportes de IVA y a Facturación el Reporte Acumulado de Facturación. En caso de un siniestro que no permitiera realizar los cálculos a la fecha de pago de las contribuciones, una alternativa sería realizar un pago provisional con el importe del periodo inmediato anterior y presentar declaración complementaria, esto sin descontar la posible generación de recargos y / o saldos a favor.

Con estas herramientas se podría continuar con el desarrollo de las funciones de las áreas involucradas.

En base a la criticidad del área de Impuestos, se ha determinado que en caso de contingencia o desastre que impida seguir la operativa sin el sistema, se cuentan con métodos alternos de operación que permiten darle continuidad al negocio. Por tanto Impuestos no serán integrados dentro del Plan de Recuperación de Desastres y Contingencias.

Contabilidad:

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Localidad	Sistema / Aplicación	Evaluación
		Crítico
		Deseable

En caso de contingencia o desastre que impidan contar con los sistemas de Contabilidad, se cuentan con métodos alternos para continuar la operación de estos procesos, para ellos es necesario que las áreas involucradas cuenten con dos computadoras portátiles con la aplicación de banca electrónica instalada, con Excel de Microsoft y la capacidad suficiente para soportar transacciones vía electrónica.

Con estas herramientas se podría continuar con el desarrollo de las funciones de las áreas involucradas y una vez reestablecido el sistema ingresar los movimientos requeridos.

En base a la criticidad de los sistema de contabilidad, se ha determinado que en caso de contingencia o desastre que impida seguir la operativa sin el sistema, se cuenta con métodos alternos de operación que permiten darle continuidad al negocio. Por tanto los sistemas de Contabilidad no serán integrados dentro del Plan de Recuperación de Desastres y Contingencias.

Comercial:

Recursos Humanos:

Localidad	Sistema / Aplicación	Evaluación
		Crítico
		Esencial

Telecomunicaciones

8.2. Matriz de Distribución del Plan

El plan de distribución se dará de acuerdo al siguiente plan, en cada uno de las oficinas y/o unidades de negocio de FLORES GARIBAY:

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

Plan de Divulgación	Duración	Fecha Comienzo	Fecha Fin
Informar vía correo electrónico del DRP	1 día	PSD	PSD
Realizar junta de información con Dirección	1 día	PSD	PSD
Realizar junta de Información con Gerencia de Operaciones	5 días	PSD	PSD
Realizar Junta de Información con Gerencia de Finanzas	3 días	PSD	PSD
Realizar junta de Información con Gerencia de Mantenimiento	1 día	PSD	PSD
Realizar Junta de Información con CREI	2 día	PSD	PSD
Validación de Divulgación de plan por todas las áreas afectadas	1 día	PSD	PSD

8.3. Plan de Simulacros

El plan de simulacros se dará de acuerdo al siguiente plan, en cada uno de las oficinas y/o unidades de negocio de FLORES GARIBAY, este plan se deberá efectuar una vez , cada nueva versión que se tenga del plan:

Plan de Divulgación	Duración	Fecha Comienzo	Fecha Fin
Revisar DRP	3 días	PSD	PSD
Elegir Plan de simulacros (elegir aplicación)	1 día	PSD	PSD
Elaborar plan de simulacros	3 días	PSD	PSD
Fijar Fechas para el simulacro	1 día	PSD	PSD
Asignación de puestos del simulacro	2 días	PSD	PSD
Emular simulacro	.5 días	PSD	PSD
Elaboración de Minuta de Simulacro	.5 días	PSD	PSD
Enviar resumen de simulacro a todas las áreas involucradas	2 días	PSD	PSD
Proyecto Simulación		PSD	PSD

9. Lista de Precios

9.1. Lista de Precios

Debido a se cuenta con un contrato de mantenimiento correctivo y preventivo, el cual incluye piezas y mano de obra de todos los equipos de cómputo, no será necesario tener una evaluación de los costos de los daños (piezas o mano de obra), ya que cada una de las empresas cuenta con este contrato y servicio de atención en escenarios de desastre y/o contingencia, contemplados contractualmente.

	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	

MODELO DE GESTION DE LAS TECNOLOGIAS DE LA INFORMACION

 FLORES GARIBAY <small>CONSULTORIA FISCAL, LEGAL Y DE NEGOCIOS</small>	Autor: Ing. Oscar Vázquez del Mercado	Modelo de Clasificación de la Información en Flores Garibay Consultores S.C.
	Revisión: 22 Septiembre 2019	