GOBIERNO AUTÓNOMO
DESCENTRALIZADO MUNICIPAL
DEL CANTÓN PORTOVIEJO

QUERER ES PODER

PLAN DE CONTINGENCIAS INFORMÁTICO

Revisión Preliminar	**Aprobado por:**
Dirección de Informática	**Director de Informática** **Enero de 2014**

CONTENIDO

PRESENTACIÓN

El Gobierno Autónomo Descentralizado Municipal del Cantón Portoviejo, considera que la información es el patrimonio principal de toda la institución, por lo que se deben aplicar medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

Con el propósito de que los diversos usuarios municipales protejan su información y aseguren la continuidad del procesamiento de la información necesaria para el adecuado desempeño de sus funciones Institucionales, La Dirección de Informática en cumplimiento de las Normas de Control Interno de la Contraloría General del Estado presenta el **"Plan de Contingencias Informático"**.

A medida que la tecnología ha ido evolucionando y con ella, la envergadura de los sistemas de información de las instituciones públicas y privadas, la seguridad del entorno informático (hardware, software, comunicaciones, etc.) se ha convertido en una de las grandes preocupaciones de los profesionales de esta actividad. Esta preocupación debe ser adecuadamente comprendida y compartida por los directivos, los cuales deben considerar a las inversiones en medidas de seguridad informática, como un gasto necesario, que contribuye a mantener la operatividad y rentabilidad de la Institución.

Esto implica que los responsables de la Dirección Informática, deban explicar con la suficiente claridad y con un lenguaje claro, las potenciales consecuencias de una política de seguridad insuficiente o incluso inexistente. El presente documento pretende ayudar a comprender mejor la problemática implícita de los sistemas de información soportados por computador, de las medidas de seguridad adecuadas, tanto en su número como en su rigor y nivel de aplicación; toda institución debe estar preparada para el caso de ocurrencias imprevistas que detengan el normal funcionamiento de los servicios informáticos.

La Dirección Informática con este documento, continúa contribuyendo a la modernización de la gestión de los Servicios Informáticos, poniéndola a disposición de las Autoridades, Directivos y usuarios en general.

Director de Informática Portoviejo, enero de 2014

1. PLAN DE RESPUESTA

El plan de respuesta debe nacer de un análisis de los posibles riesgos, los cuales permitirán conocer cuáles posteriormente deberían ser las acciones a tomarse en caso de que uno de ellos llegase a ocurrir.

Estos Riesgos los podríamos clasificar por su proveniencia: Endógenos (factores internos) y Exógenos (factores externos).

1.1. FACTORES ENDÓGENOS

1.1.1.Daño del cableado de red.-

Para que los equipos informáticos del GAD PORTOVIEJO se integren a una red de datos y por ende accedan a sus servicios, se usan cables de cobre, los mismos que se encuentran protegidos por canaletas plásticas (ya sea de pared o de piso) en el resto de los casos la conexión y el acceso es vía inalámbrica (wireless). La presencia de esta amenaza se circunscribe desde la inaccesibilidad a la red por parte de un equipo, pasando por la de una Dirección, todo un piso y en el caso más grave a todo el edificio municipal y locales anexos, todo ello provocado por cortes de cable, quiebres de cable, estiramientos de cable, amalgamiento con cables eléctricos y/o telefónicos, sulfatación de conectores entre otros factores; o en los casos de conexiones inalámbricas, puede ser debido a ruidos, vibraciones, interferencias, entre otros.

1.1.2. Falla de los equipos de Comunicación.-

La Red de Datos llega a todas las Direcciones del edificio del GAD PORTOVIEJO a través de los equipos de comunicación (ya sean switches o Acces Point) ubicados estratégicamente en los diferentes pisos y edificios aledaños tal como se detalla a continuación: Donde obviamente la alteración y/o inoperatividad de algunos de estos componentes se traducirían en que determinadas Direcciones no tengan acceso a los servicios que brinda la infraestructura de red de la Dirección de Informática.

1.1.3.Inoperatividad de los Servidores de comunicación del Data Center.-

Es una situación fortuita, ocasionada por fallas del hardware y/o software, que acarrea la imposibilidad de acceder a los servicios de internet tan comunes en nuestros días como: correo electrónico, navegación por páginas web, portales, transferencia de archivos (ftp), entre otros. Así mismo la imposibilidad de acceder a los servicios de la Intranet Institucional: Tesorería, Sistema de Trámites Municipales (workflow), requerimiento de bienes y servicios, requerimientos de insumos, control de vehículos, recursos humanos, sistema financiero, control de combustible, sistema de catastro, entre otros.

1.1.4.4.- Inoperatividad de Servidores de Base de Datos.-

Todos los aplicativos y sistemas de información que almacenan sus datos en este servidor estarían impedidos de acceder a su información (nivel interno), así como las aplicaciones que interactúan con el portal web institucional no podrían brindar consultas de tipo “on line” en el ambiente virtual.

1.1.5.5.- Inoperatividad del Servidor de DNS.-

Se cuenta con un servidor DNS que resuelve los nombres de dominio internos, cuya falla originaría también problemas en la red, obstaculizando el acceso a las cuentas de usuario de los empleados y por ende a los equipos y su información.

1.1.6.6.- Inconvenientes eléctricos.-

Por razones de seguridad interna la Dirección Administrativa en conjunto con la Dirección de Obras Públicas deben disponer la supervisión y mantenimiento periódico de las instalaciones, dispositivos y conexiones de la red eléctrica del Data Center y de la línea de backup eléctrica (tableros, circuitos, pozo a tierra, grupo electrógeno, entre otros).

1.1.7.7.- Pérdida de información.-

Que afectaría lo dispuesto en la ley de transparencia la cual establece la publicación de la información concerniente a la institución utilizando para ello la intranet y el portal web institucional.

Es importante señalar el almacenamiento físico de los medios donde se realizan las copias de seguridad en los servidores de Backup (storage) y en las cintas magnéticas que se almacenan en la caja de seguridad del Banco del Pichincha, medida que permite salvaguardar la información importante de la institución, los mismos medios que están a cargo de la Dirección de Informática del GAD Portoviejo.

En estos medios de almacenamiento se guardan las copias de las bases de datos, los códigos fuentes de los programas, configuraciones de dominio y centrales telefónicas y de los archivos documentales generados por los funcionarios de las diferentes direcciones municipales.

La información almacenada en los discos duros de las computadoras de los funcionarios es de total responsabilidad del respectivo funcionario que genera dicha información documental.

1.1.8.8.- Acción de virus Informático.-

Se consideran a los virus informáticos como amenazas endógenas cuando se infiltran desde el interior de la Institución a través del uso de dispositivos de almacenamiento externo infectados por parte de los usuarios del GAD Portoviejo y como amenazas exógenas cuando se infiltran a través del correo electrónico y la navegación en internet.

1.1.9.9.- Alteración de la Información.-

Los diversos aplicativos y sistemas de información implementados en la red de datos del GAD Portoviejo son accedidos a través del software instalado en la computadora cliente, con los niveles de acceso y/o carpetas de seguridad que provee dicho software, el Motor de Base de Datos y la plataforma operativa. Hay que indicar que los usuarios que acceden a las diferentes fuentes de información son personal autorizado formalmente por su jefe inmediato o Director.

Esto garantiza el acceso a la información solo por personal autorizado, evitando la manipulación de estos por personal no autorizado que traería como consecuencia graves daños a la información.

La administración de la instalación en donde se ubican los servidores del GAD Portoviejo está a cargo de la Dirección de Informática a través del Administrador de la Red de Datos.

1.2. FACTORES EXOGENOS.

1.2.1.Corte de fluido eléctrico.-

Todos los equipos informáticos hacen uso de electricidad por lo que su ausencia conduce directamente a una inoperatividad de los mismos.

1.2.2.Desconexión del servicio de Internet.-

Se cuenta con el servicio de Internet para la transmisión y recepción de datos. Su corte temporal o definitivo aislaría tecnológicamente a la institución a nivel nacional e internacional. Mediante el servicio de Internet funcionan la plataforma de pagos en línea, control sobre el consumo de combustible, correo electrónico, enlace de datos externos, entre otros.

1.2.3.Avería de los enlaces de fibra óptica.-

Este tipo de conexión tiene un tramo físico fuera de la sede institucional susceptible de presentar averías y por ende degradación de los servicios o pérdida total del mismo. Es así que servicios como la troncal Ip, internet, enlace de datos con la Epmapap, Centro Comercial se perderían si estos enlaces se perdieran. Empresas tales como eléctrica, agua potable, cable, constructoras, entre otras podrían dañar las líneas de transmisión que se encuentran instaladas de manera aérea en los postes de alumbrado eléctrico.

1.2.4.13.- Inoperatividad del servidor de DNS externo.-

El servidor de DNS que resuelve los nombres de dominios de internet está bajo la administración de la Dirección de Informática a través del Administrador de Redes, y la inoperatividad del mismo se traduciría en la imposibilidad de acceder a Internet.

1.2.5. Acción de virus informáticos.-

Se consideran a los virus informáticos como amenazas exógenas debido a que pueden alterar el normal desenvolvimiento de las servicios que ofrecen los equipos y aplicativos puestos a disposición de la institución por la Dirección de Informática, infiltrándose desde el exterior a través del correo electrónico, archivos adjuntos infectados o con la acción de navegar en el internet. Es de suma importancia señalar que los usuarios de la red, cuentan con el servicio de actualización automática del antivirus corporativo y protección adicional a nivel del servidor de correos.

1.2.6. Incendios.-

La institución no cuenta con sistemas de detección de humo ni aspersión automática en la sala de Servidores y Comunicaciones (Data Center); existen extintores de incendios en su lugar así como en todas las oficinas del edificio municipal.

1.2.7. Sismos.-

El Edificio del GAD Portoviejo es un edificio antisísmico, sin embargo tiene más de 30 años de funcionamiento por lo que los daños que podría causar un sismo a la infraestructura tecnológica sería de moderado a grave.

1.2.8. Atentados.-

Son actos criminales efectuados por personas o grupos al margen de la ley. El GAD Portoviejo cuenta con personal de seguridad, quienes se encuentran ubicados estratégicamente en las diversas áreas y puertas de acceso de la Sede Central, para realizar labores de control y vigilancia a efectos de evitar cualquier robo o daño material.

Adicionalmente la empresa dentro de sus políticas y exigencias del contrato garantiza la honestidad y honradez de su personal de seguridad, a fin de evitar que estos resulten involucrados en acciones deshonestas.

1.2.9.Hackers.-

Se denomina Hacker al individuo que usa sus habilidades y recursos para invadir sistemas informáticos ajenos. Al tener comunicación global a través del internet estamos expuestos a este tipo de accesos que pueden ocasionar daños a la Red de Datos Municipal.

1.3. Definición de Posibles escenarios

Un escenario es la combinación de una amenaza con una actividad, y se define como la posibilidad para que una amenaza determinada se materialice como una emergencia en un sitio determinado.

La definición de escenarios para el proyecto se hará combinando las actividades y amenazas identificadas en los numerales anteriores. Los resultados de ésta combinación se presentan en la tabla 1.

TABLA Nº 1 - ESCENARIOS DE EMERGENCIA

AMENAZAS			ACTIVIDAD	
			INTERNET	BASES DE DATOS Y SISTEMAS
Endógenos	1	Daño en el cableado de red	X	X
	2	Falla de los equipos de Comunicación.-	X	X
	3	Inoperatividad de los Servidores de comunicación del Data Center.-	X	
	4	Inoperatividad de Servidores de Base de Datos.-		X
	5	Inoperatividad del Servidor de DNS.-	X	
	6	Inconvenientes eléctricos.-	X	X
	7	Pérdida de información.-		X
	8	Acción de virus Informático.-		X
	9	Alteración de la Información.-		X
Exógenos	10	Corte de fluido eléctrico.-	X	X
	11	Desconexión del servicio de Internet.-	X	
	12	Avería de los enlaces de fibra óptica.-	X	X
	13	Inoperatividad del servidor de DNS externo.-	X	
	14	Acción de virus informáticos.-		X
	15	Incendios.-	X	X
	16	Sismos.-	X	X
	17	Atentados.-	X	X
	18	Hackers.-		X

INTERNET	Acceso a herramientas: email; ftp, browser, bases de datos, intranet, pagos en línea, control de combustible.
BASES DE DATOS /SISTEMAS	Administración, desarrollo, ingreso de datos, administración de file servers.

TABLA Nº 2 - PROBABILIDAD DE LOS SINIESTROS

Probabilidad	Definicion	Ocurrencia de Eventos	Puntaje
Frecuente	De ocurrencia Alta	de 1 al mes	6
Moderado	De ocurrencia media	entre 2 y 6 meses	5
Ocasional	De ocurrencia Limitada	entre 7 y 12 meses	4
Remoto	De ocurrencia baja	entre 1 y 5 años	3
Improbable	De ocurrencia muy baja	entre 6 y 10 años	2
Imposible	Excepcional posibilidad de ocurrencia	de 10 años a mas	1

Los valores de probabilidad asignados a cada unos de los escenarios definidos se muestran en la **tabla 3**.

TABLA Nº 3 - ESTIMACIÓN DE PROBABILIDADES

		ESCENARIO (Amenaza + Actividad)	Probabilidad	Puntaje
Endógenos	1	Daño en el cableado de red en la actividad del Internet	Moderado	5
	2	Daño en el cableado de red en la actividad de las bases de datos	Moderado	5
	3	Falla de los equipos de Comunicación en la actividad del internet	Ocasional	4
	4	Falla de los equipos de Comunicación en la actividad de las bases de datos	Ocasional	4
	5	Inoperatividad de los Servidores de comunicación del Data Center en la actividad del internet	Ocasional	4
	6	Inoperatividad de Servidores de Base de Datos en la actividad de los sistemas	Ocasional	4
	7	Inoperatividad del Servidor de DNS interno en la actividad del internet	Improbable	2
	8	Inconvenientes eléctricos en la actividad del internet	Ocasional	4
	9	Inconvenientes eléctricos en la actividad de las bases de datos y los sistemas	Ocasional	4
	10	Pérdida de información en la actividad de las bases de datos	Improbable	2
	11	Acción de virus Informáticos en la actividad del Internet	Improbable	2
	12	Acción de virus Informáticos en la actividad de las bases de datos - Internet	Improbable	2
	13	Alteración de la Información en las bases de datos.	Improbable	2
Exógenos	14	Corte de fluido eléctrico en la actividad del internet	Ocasional	4
	15	Corte de fluido eléctrico en la actividad de los sistemas y las bases de datos.	Ocasional	4
	16	Corte del servicio de Internet	Improbable	2
	17	Avería de los enlaces de fibra óptica en la actividad del internet.	Improbable	2
	18	Inoperatividad del servidor de DNS externo en la actividad del internet.	Improbable	2
	19	Acción de virus informáticos en la actividad de los sistemas.	Improbable	2
	20	Incendios en las actividades del internet	Improbable	2
	21	Incendios en las actividades de las bases de datos	Improbable	2
	22	Sismos durante la actividad del internet.	Improbable	2
	23	Sismos durante la actividad de las bases de datos.	Improbable	2
	24	Atentados contra la actividad del Internet.	Improbable	2
	25	Atentados contra las acitividades de los sistemas y las bases de datos.	Improbable	2
	26	Ataque de los Hackers.	Ocasional	4

1.3.1.Definición de Factores de Vulnerabilidad.

La vulnerabilidad es el grado relativo de sensibilidad, que un sistema tienen respecto a una amenaza determinada. Los factores de vulnerabilidad dentro de un análisis de riesgo, permite determinar cuáles son los efectos negativos que sobre un escenario y

sus zonas de posible impacto pueden tener los eventos que se presente. Para efecto del análisis de riesgo, se consideran los siguientes factores de vulnerabilidad:

Victimas: se refiere al número y clase de afectados (empleados, personal de emergencia y la comunidad); considera también el tipo y la gravedad de las lesiones.

Daño ambiental: incluye los impactos sobre aire y comunidad a consecuencia de la emergencia.

Pérdidas materiales o económicas: representadas en instalaciones, equipos, productos, valor de las operaciones de emergencia, multas, indemnizaciones, y atención médica entre otros.

Imagen institucional: califica el nivel de deterioro de la imagen de la Institución como consecuencia de la emergencia.

Suspensiones: determina los efectos de la emergencia sobre el desarrollo normal de las actividades de la Institución en términos de días perdidos.

1.3.2.Estimación de Gravedad:

La gravedad de las consecuencias de un evento se evalúa sobre los factores de vulnerabilidad y se califican dentro de una escala que establece cuatro niveles. Los niveles corresponden a gravedad nivel 1 o insignificante, nivel 2 o marginal, nivel 3 o crítica y nivel 4 o catastrófica. Los criterios de calificación para los factores de vulnerabilidad se presentan en la tabla 4.

TABLA Nº 4 - CALIFICACIÓN DE GRAVEDAD

Factor de Vulnerabilidad	Calificación de Gravedad			
	Insignificante 1	Marginal 2	Crítica 3	Catastrófica 4
Víctimas	No hay lesiones o no se requiere atención hospitalaria	Lesiones leves que requieren atención	Lesiones con necesidad de hospitalización	Muertes
Daño Ambiental	No hay impactos ambientales significativos	Impactos ambientales dentro del área del escenario	Impactos en las áreas aledañas al escenario	Impactos ambientales dentro del área del escenario
Pérdidas Materiales Económicas	Menos de $ 1.000,00	entre $ 1.000,00 y $ 5.000,00	entre $ 5.000,00 y $ 10.000,00	De $ 10.000,00 a más
Imagen Institucional	Solo de conocimiento Interno	Conocimiento local	Conocimiento Nacional	Conocimiento Internacional
Suspensiones	No hay suspensión	Suspensión de 1 día	Suspensión de 2 días	Suspensión de 3 o más días

1.3.3.Cálculo de Riesgo

El riesgo es producto de la combinación de dos factores: la probabilidad de ocurrencia de una amenaza y la gravedad de las consecuencias de la misma.

Matemáticamente el riesgo (R) puede expresarse como el producto de la probabilidad de ocurrencia (P) por la gravedad (G).

R = P x G

En la tabla 5 se presenta un resumen de la aceptabilidad de riesgos según combinación de probabilidad de ocurrencia y la gravedad de un evento.

TABLA Nº 5 - Aceptabilidad según Combinación de Probabilidad de Ocurrencia - Gravedad de un Evento

Aceptabilidad del Riesgo			Gravedad			
			Insignificante 1	Marginal 2	Crítica 3	Catastrófica 4
Probabilidades de los siniestros	1	Imposible	a	a	t	i
	2	Improbable	a	t	t	i
	3	Remoto	a	t	i	i
	4	Ocasional	t	t	i	i
	5	Moderado	t	i	i	i
	6	Frecuente	t	i	i	i

Leyenda	
Aceptable	a
Tolerable	t
Inaceptable	i

Aceptabilidad.-

En cuanto a la aceptabilidad a los riesgos, los escenarios se clasifican como:

Aceptable: Un escenario situado en esta región de la matriz significa que la combinación de probabilidad-gravedad no representa una amenaza significativa por lo que no amerita la inversión inmediata de recursos y no requiere una acción específica para la gestión sobre el factor de vulnerabilidad considerado en el escenario. Cuantitativamente representa riesgos con valores menores o iguales a tres puntos.

Tolerable: un escenario situado en esta región de la matriz significa que, aunque deben desarrollarse actividades para la gestión sobre el riesgo, estas tienen una prioridad de segundo nivel. Cuantitativamente representa riesgos con valores entre cuatro y seis puntos.
Inaceptable: Un escenario situado en esta región de la matriz significa que se requiere siempre desarrollar acciones prioritarias e inmediatas para su gestión, debido al alto impacto que tendrían sobre el sistema. Cuantitativamente representa valores de riesgo entre ocho y veinticuatro puntos.

Aceptabilidad de Riesgo		
Aceptable	**Tolerable**	**Inaceptable**

Niveles de Planeación

La aceptabilidad de riesgos está directamente relacionada con los niveles de planeación de contingencias requeridos específicamente para el GAD PORTOVIEJO, de la siguiente manera:

- **No plan.-** Un escenario situado en esta región de la matriz significa que la combinación de probabilidad-gravedad no representa una amenaza significativa; por tanto no se requiere la inversión específica de recursos especiales, ya que los mecanismos de control existentes en el GAD PORTOVIEJO contrarrestan significativamente los efectos del riesgo identificado.
- **Plan General:** Un escenario situado en esta región de la matriz significa que, aunque debe diseñarse una respuesta para dichos casos, esta debe ser solo de carácter general.
- **Plan detallado:** Un escenario situado en esta región de la matriz significa que se requiere siempre diseñar una respuesta detallada a las contingencias y que es preciso realizar inversiones particulares para cada uno de estos escenarios.

Niveles de Planeación		
No plan	**Plan General**	**Plan Detallado**

Los resultados de la estimación de gravedad para los escenarios de emergencia son

presentados en la Tabla 6A y en la Tabla 7B se presentan los resultados del cálculo de riesgo y la aceptabilidad de los riesgos.

TABLA Nº 6A - VALORES DE GRAVEDAD Y RIESGO PARA LOS DIFERENTES FACTORES DE VULNERABILIDAD

		ESCENARIO		FACTORES DE VULNERABILIDAD									
				Victimas		Daño Ambiental		Pérdidas Económicas		Imagen Institucional		Suspensión	
		AMENAZA	Proba.	G	R	G	R	G	R	G	R	G	R
Endógenos	1	Daño en el cableado de red en la actividad del Internet	5	1	5	2	10	1	5	1	5	1	5
	2	Daño en el cableado de red en la actividad de las bases de datos	5	1	5	2	10	1	5	1	5	1	5
	3	Falla de los equipos de Comunicación en la actividad del internet	4	1	4	1	4	2	8	4	16	1	4
	4	Falla de los equipos de Comunicación en la actividad de las bases de datos	4	1	4	1	4	2	8	1	4	1	4
	5	Inoperatividad de los Servidores de comunicación del Data Center en la actividad del internet	4	1	4	1	4	2	8	4	16	1	4
	6	Inoperatividad de Servidores de Base de Datos en la actividad de los sistemas	4	1	4	1	4	2	8	1	4	1	4
	7	Inoperatividad del Servidor de DNS interno en la actividad del internet	2	1	2	1	2	2	4	4	8	1	2
	8	Inconvenientes eléctricos en la actividad del internet	4	1	4	1	4	2	8	2	8	1	4
	9	Inconvenientes eléctricos en la actividad de las bases de datos y los sistemas	4	1	4	1	4	2	8	1	4	1	4
	10	Pérdida de información en la actividad de las bases de datos	2	1	2	1	2	2	4	1	2	1	2
	11	Acción de virus Informáticos en la actividad del Internet	2	1	2	1	2	2	4	1	2	1	2
	12	Acción de virus Informáticos en la actividad de las bases de datos - Internet	2	1	2	1	2	2	4	1	2	2	4
	13	Alteración de la Información en las bases de datos.	2	1	2	1	2	3	6	1	2	1	2
Exógenos	14	Corte de fluido eléctrico en la actividad del internet	4	1	4	1	4	4	16	1	4	2	8
	15	Corte de fluido eléctrico en la actividad de los sistemas y las bases de datos.	4	1	4	1	4	4	16	1	4	2	8
	16	Corte del servicio de Internet	2	1	2	1	2	2	4	4	8	1	2
	17	Avería de los enlaces de fibra óptica en la actividad del internet.	2	1	2	1	2	2	4	4	8	1	2
	18	Inoperatividad del servidor de DNS externo en la actividad del internet.	2	1	2	1	2	2	4	4	8	1	2
	19	Acción de virus informáticos en la actividad de los sistemas.	2	1	2	1	2	2	4	8	16	1	2
	20	Incendios en las actividades del internet	2	3	6	3	6	4	8	8	16	4	8
	21	Incendios en las actividades de las bases de datos	2	3	6	3	6	4	8	8	16	4	8
	22	Sismos durante la actividad del internet.	2	2	4	2	4	1	2	4	8	2	4
	23	Sismos durante la actividad de las bases de datos.	2	2	4	2	4	1	2	4	8	2	4
	24	Atentados contra la actividad del Internet.	2	4	8	4	8	4	8	4	8	4	8
	25	Atentados contra las acitividades de los sistemas y las bases de datos.	2	4	8	4	8	4	8	4	8	4	8
	26	Ataque de los Hackers.	4	1	4	1	4	2	8	1	4	1	4

TABLA Nº 6B - VALORES DE GRAVEDAD Y RIESGO PARA LOS DIFERENTES FACTORES DE VULNERABILIDAD ASOCIADOS A NIVELES DE ACEPTABILIDAD

ESCENARIO				FACTORES DE VULNERABILIDAD									
				Victimas		Daño Ambiental		Pérdidas Económicas		Imagen Institucional		Suspensión	
		AMENAZA	Prob	G	R	G	R	G	R	G	R	G	R
Endógenos	1	Daño en el cableado de red en la actividad del Internet	5	1	5	2	10	1	5	1	5	1	5
	2	Daño en el cableado de red en la actividad de las bases de datos	5	1	5	2	10	1	5	1	5	1	5
	3	Falla de los equipos de Comunicación en la actividad del internet	4	1	4	1	4	2	8	4	16	1	4
	4	Falla de los equipos de Comunicación en la actividad de las bases de datos	4	1	4	1	4	2	8	1	4	1	4
	5	Inoperatividad de los Servidores de comunicación del Data Center en la actividad del internet	4	1	4	1	4	2	8	4	16	1	4
	6	Inoperatividad de Servidores de Base de Datos en la actividad de los sistemas	4	1	4	1	4	2	8	1	4	1	4
	7	Inoperatividad del Servidor de DNS interno en la actividad del internet	2	1	2	1	2	2	4	4	8	1	2
	8	Inconvenientes eléctricos en la actividad del internet	4	1	4	1	4	2	8	2	8	1	4
	9	Inconvenientes eléctricos en la actividad de las bases de datos y los sistemas	4	1	4	1	4	2	8	1	4	1	4
	10	Pérdida de información en la actividad de las bases de datos	2	1	2	1	2	2	4	1	2	1	2
	11	Acción de virus Informáticos en la actividad del Internet	2	1	2	1	2	2	4	1	2	1	2
	12	Acción de virus Informáticos en la actividad de las bases de datos - Internet	2	1	2	1	2	2	4	1	2	2	4
	13	Alteración de la Información en las bases de datos.	2	1	2	1	2	3	6	1	2	1	2
Exógenos	14	Corte de fluido eléctrico en la actividad del internet	4	1	4	1	4	4	16	1	4	2	8
	15	Corte de fluido eléctrico en la actividad de los sistemas y las bases de datos.	4	1	4	1	4	4	16	1	4		0
	16	Corte del servicio de Internet	2	1	2	1	2	2	4	4	8	1	2
	17	Avería de los enlaces de fibra óptica en la actividad del internet.	2	1	2	1	2	2	4	4	8	1	2
	18	Inoperatividad del servidor de DNS externo en la actividad del internet.	2	1	2	1	2	2	4	4	8	1	2
	19	Acción de virus informáticos en la actividad de los sistemas.	2	1	2	1	2	2	4	1	2	1	2
	20	Incendios en las actividades del internet	2	3	6	3	6	4	8	3	6	4	8
	21	Incendios en las actividades de las bases de datos	2	3	6	3	6	4	8	3	6	4	8
	22	Sismos durante la actividad del internet.	2	2	4	2	4	1	2	4	8	2	4
	23	Sismos durante la actividad de las bases de datos.	2	2	4	2	4	1	2	4	8	2	4
	24	Atentados contra la actividad del Internet.	2	4	8	4	8	4	8	4	8	4	8
	25	Atentados contra las acitividades de los sistemas y las bases de datos.	2	4	8	4	8	4	8	4	8	4	8
	26	Ataque de los Hackers.	4	1	4	1	4	2	8	1	4	1	4

1.3.4.Conclusiones

El análisis de riesgo realizado para el GAD PORTOVIEJO constituye un análisis inicial de los riesgos asociados al desarrollo de las actividades informáticas al interior de la Institución. Este análisis en particular permite establecer un estado inicial de referencia sobre el cual compara los riesgos en los escenarios identificados y que potencialmente pueden desarrollarse durante el quehacer diario.

Los resultados del análisis indican que los escenarios que presentan mayor riesgo del tipo exógeno son: corte de fluido eléctrico, problemas con los enlaces de fibra óptica, el Servidor DNS, los problemas naturales y de infraestructura. Los escenarios de tipo endógeno que presentan mayor riesgo son la inoperatividad de los equipos de comunicación e infraestructura.

2. PLAN DE CONTINGENCIA

La Dirección de Informática cuenta con un Plan de Evacuación, el cual permite a los funcionarios responsables conocer anticipadamente las acciones a ejecutar cuando las circunstancias lo requieran, a fin de contribuir a minimizar o neutralizar los efectos del desastre.

La Dirección de Informática cuenta con un proceso de copias de seguridad (backup) de la información clave de la institución (bases de datos, código fuente de aplicaciones, instaladores de aplicaciones, configuraciones, entre otros); dicha información se almacena en los servidores de Backup y es copiado diariamente en cintas de respaldo (tape backup) que posteriormente una vez cada 15 días se almacenan en un casillero de seguridad de un banco de la localidad.

La información de trabajo del personal administrativo (información documental como archivos de texto, hojas de cálculo, planos, fotos, videos entre otros) es almacenada bajo pedido del director de un área en carpetas compartidas con niveles de acceso por usuario.

La información del usuario que está almacenada en el disco duro de la computadora bajo su cargo, cuenta de correo electrónico, u cualquier otros dispositivo de almacenamiento o unidad de trabajo diferente a lo indicado en el párrafo anterior, es de total responsabilidad del usuario, NO ES responsabilidad de la Dirección de Informática.

2.1. Actividades previas al desastre.

Son todas las actividades de planeamiento, preparación, entrenamiento, mantenimiento preventivo y correctivo del parque informático y ejecución de las actividades de resguardo de la información e identificación de las prioridades de restauración de los sistemas informáticos, que nos aseguren un tiempo de respuesta aceptable y óptimo que implique el menor costo posible a nuestra institución.

2.1.1.Establecimiento del Plan de Acción

Se han establecido los procedimientos relativos al mantenimiento de equipos, impresoras y servidores, copia de respaldo (backups) e instalación/actualización de software antivirus.

Para poder efectuar en forma óptima y en el menor tiempo posible las actividades descritas anteriormente se debe conocer lo siguiente:

Reconocer el ambiente donde se encuentran los Servidores del GAD PORTOVIEJO, y saber identificar a cada uno de ellos. Para ello en el anexo 01 adjunto al presente plan se detalla la estructura de la “Data Center”, donde se muestra la distribución de equipos informáticos y de los equipos de comunicación.

Conocer los procedimientos a realizar para ofrecer los servicios críticos del GAD PORTOVIEJO a través de la Dirección de Informática.

Gestionar adecuadamente los activos de software para contar con un Inventario de Software por cada computadora de los usuarios, que facilite una rápida identificación y restauración de las aplicaciones instaladas.

A continuación se detallan los mantenimientos preventivos por equipo informático realizados en el GAD PORTOVIEJO.

Mantenimiento Preventivo por Equipo Informático		
Equipo	**Acción Preventiva / correctiva**	**Responsable**
Computadores Personales	Revisión, limpieza interna y externa de todos los componentes. Revisión de virus	Dirección de Informática, terceros (si equipo tiene garantía)
Impresoras	Limpieza interna	Dirección de Informática, terceros (si equipo tiene garantía)
Servidores	Se realiza un monitoreo a través de acciones manuales en la consola del servidor. Limpieza interna. Dos mantenimientos generales al año.	Dirección de Informática, terceros (si equipo tiene garantía). Terceros contratados para el efecto.

a. Sistemas de Información.

Se detalla la relación de los niveles de prioridad con el puntaje que se aplicará a los Sistemas de Información desarrollados por la Dirección de Informática o por terceros.

Niveles de Prioridad de Sistemas de Información

Prioridad	Puntaje
Baja	1
Media	2
Alta	3

A continuación se muestra la lista de los Sistemas de Información ordenados por prioridad de restauración (desde la máxima prioridad hasta la más baja), que son necesarios para garantizar una continuidad de la operatividad y servicios que ofrece la Dirección de Informática ante un desastre o siniestro.

SISTEMAS DE INFORMACIÓN / SERVICIOS IMPLEMENTADOS					
APLICATIVO	PROVEEDOR	PLATAFORMA	LENGUAJE DE PROGRAMACIÓN	USUARIOS	PRIORIDAD
Procesos administrativos municipales	Desarrollo propio	SQL, bajo Windows	.NET	Todas las Direcciones	3
Ordenanzas y documentos digitales	Desarrollo propio	SQL, bajo Windows	.NET	Secretaría General; Dirección Administrativa.	1
Catastros / GIS	Desarrollo propio; software libre	SQL, bajo Windows; PostGres	.NET;	Dirección de Catastro; Gestión de Riesgo; Planificación; Comisaría Municipla; Higiene; Coactivas	3
Recursos Humanos	Desarrollo propio	SQL, bajo Windows	.NET	Dirección de Desarrollo Institucional y Humano.	2
Coactivas	Desarrollo propio	SQL, bajo Windows	.NET	Tesorería - Coactivas	2
Requerimiento de materiales a Bodega	Desarrollo propio	SQL, bajo Windows	.NET	Directores y Jefes Departamentales	1
Pagos y consultas en línea	Desarrollo propio	SQL, IIS	ASP .NET	Recaudadores en vía pública (inactivo)	1
Portal Web transaccional	Desarrollo propio	SQL, IIS	ASP .NET	Ciudadanía en General que poseá tarjeta Dinners.	1
Sistema de localización de flota vehicular	TRACKLINK	-	-	Dirección Administrativa.	1
Sistema de control de combustible con acceso biométrico	Desarrollo propio	SQL, bajo Windows	.NET	Dirección Administrativa. Proveeduría	3
Sistema de adquicisión de Bienes y Servicios	Desarrollo propio	SQL, bajo Windows	.NET	Directores y Jefes Departamentales	2
Control de Garantías	Desarrollo propio	SQL, bajo Windows	.NET	Tesorería.	2
Seguimiento y control de obras publicas municipales.	Desarrollo propio	SQL, bajo Windows	.NET	Obras Públicas; Jurídico; Planificación, Alcaldía.	1
Sistema de análisis de Precios unitarios.	Desarrollo propio	SQL, bajo Windows	.NET	Planificación; Obras Públicas	1
Seguimiento y registro de informes de auditoría	Desarrollo propio	SQL, bajo Windows	.NET	Unidad de Seguimiento y Control de Recomendaciones de Contraloría.	1
Quantum Gis	software libre	windows	.NET	Catastro, Planificación, Obras Públicas	3
Financiero Contable Olympo	PROTELCOTELSA	SQL, bajo Windows	.NET	Dirección Financiera; Bodega; Dirección de Desarrollo Institucional y Humano.	3
Autocad 2010	AUTODESK	SQL, bajo Windows	-	Obras Públicas; Planificación.	2

La Dirección de Informática mantiene un inventario de los equipos informáticos; estos conforman el parque informático del GAD PORTOVIEJO. A continuación se mostrará una serie de gráficos con información sobre el parque informático.

Obtención y almacenamiento de los respaldos de información.

La Dirección de Informática mantiene realiza copias de respaldo de lo siguiente:

SOFTWARE:

Bases de Datos
De aplicativos y programas
De archivos de trabajo ubicados en los repositorios compartidos de las Direcciones.

HARDWARE:

No se cuenta en la actualidad con respaldo de equipos Servidores ubicados en el Data Center de los siguientes servicios: Bases de datos, Intranet, correo, DNS, y demás servicios, sin embargo a fin de cumplir con las normas de control interno en las cuales se recomienda la utilización de centros de datos alternos, se ha colocado en el plan operativo de este año la actividad para la contratación o implementación de dicha alternativa.

Políticas (Normas y Procedimientos de backups).

La Dirección de Informática es la responsable del monitoreo Informático, tiene establecido procedimientos para obtener copias de seguridad de Base de Datos, aplicativos y Archivos de trabajo de las diferentes direcciones, tal como se estipula en el **"Instructivo para la Administración y Uso de los Recursos Tecnológicos del GAD Portoviejo"**.

2.1.2.Formación de Equipos Operativos

En cada unidad operativa de la Institución, que almacene información y sirva para la operatividad Institucional, se deberá designar a un responsable de la seguridad de la Información de su unidad, pudiendo ser éste el jefe de dicha Área Operativa.

Sus labores serán:

- ✓ Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
- ✓ Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
- ✓ Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas.

- ✓ Supervisar procedimientos de respaldo y restauración.
- ✓ Supervisar la carga de archivos de datos de las aplicaciones, y la creación de los respaldos increméntales.
- ✓ Coordinar líneas, terminales, modem, otros aditamentos para comunicaciones.
- ✓ Establecer procedimientos de seguridad en los sitios de recuperación.
- ✓ Organizar la prueba de hardware y software.
- ✓ Ejecutar trabajos de recuperación.
- ✓ Cargar y probar archivos del sistema operativo y otros sistemas almacenados en un lugar externo a la institución.
- ✓ Realizar procedimientos de control de inventario y seguridad del almacenamiento en el local alternante.
- ✓ Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
- ✓ Participar en las pruebas y simulacros de desastres.

Para cumplir con sus labores es necesario definir las responsabilidades de los funcionarios claramente, a continuación se detalla la responsabilidad de cada uno de ellos y su ámbito de acción.

Responsabilidades asignadas a los miembros del equipo		
Contacto	**Cargo**	**Responsabilidad**
Pedro Moreno Intriago	Director de Informática	Coordinar con los responsables de cada una de las áreas la puesta en marcha de las operaciones en caso de desastre
Betty Moreira Pico	Soporte y Helpdesk	matenimiento y/o reparación de los equipos informáticos. Instalación de aplicaciones, programas, etc. Instalación de impresoras, respaldos (de tenerse alguno) en los equipos clientes, instalación de puntos de red.
Gustavo Donoso Lange	Administrador de Base de Datos	Crear los respaldos de las bases de datos, verificar la validez de los respaldos y el estado de las cintas de backup. Levantar los respaldos de las bases de datos en cualquier circunstancia.
Javier Cedeño Rodríguez	Administrador de aplicaciones	Crear respaldos de las aplicaciones y códigos fuentes de aplicaciones creadas. Recuperar los respaldos de las aplicaciones y sus códigos fuentes.

Boris Mero Casanova	Administrador de Redes y Comunicaciones	Establecer los enlaces y las comunicaciones para el funcionamiento de la Red de voz datos y video; crear respaldos de dominio y sus configuraciones, centrales telefónicas y equipos de video; recuperar los respaldos del dominio y sus configuraciones, centrales telefónicas y equipos de video. Levantar los servidores.
Enrique Zambrano Espinoza	Soporte y Helpdesk	matenimiento y/o reparación de los equipos informáticos. Instalación de aplicaciones, programas, etc. Instalación de impresoras, respaldos (de tenerse alguno) en los equipos clientes, instalación de puntos de red.
José Hernández Chilan	Administrador de Proyectos	Trasladar los respaldos del Data Center a la bóveda externa. Recuperar los respaldos de la Bóveda externa. Contactar a los proveedores externos de aplicaciones y equipos para mantenimientos y/o cobertura de garantías.

2.1.3.Formación de Equipos de Evaluación.

Esta función debe ser realizada de preferencia por personal de la Auditoría Interna, de no ser posible, la realizará el personal del área de Informática, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:

- ✓ Revisar que las Normas y procedimientos con respecto a Backups y seguridad de equipos y data se cumpla.
- ✓ Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
- ✓ Revisar la correlación entre la relación de Sistemas e Información necesaria para la buena marcha de la Institución y los backups realizados.
- ✓ Informar de los cumplimientos e incumplimientos de las Normas, para las acciones de corrección respectivas.

2.2. Actividades durante el Desastre.

2.2.1.Plan de emergencias.

La Dirección de informática pondrá en ejecución el Plan de Evacuación cuando se produzcan desastres de diversos tipos, y en esto, los brigadistas juegan un rol importante; por su parte el personal de Informática actuará paralelamente en los rubros inherentes a su actividad.

Al respecto la Dirección de Informática proporciona una relación de su personal, la misma que será utilizada en caso de producirse algún incidente informático. Esta lista debe estar en poder del personal de seguridad y vigilancia del GAD PORTOVIEJO para los casos de horarios de fines de semana y/o feriados si se diere el caso.

Procedimiento en caso de emergencia

El siguiente procedimiento de acción detalla los pasos que se deberán seguir en casos de emergencia. Este procedimiento podrá ser modificado para incorporar información adicional que sea pertinente.

a. Determinar la ubicación del incidente, estimar el tamaño y el tipo de incidente.
b. Llevar a cabo acciones específicas para controlar la anomalía informática.
c. Notificar la ocurrencia a los responsables de la Dirección de Informática.
d. Modificar las operaciones para evitar la re-ocurrencia potencial del incidente.
e. Documentar el incidente.

A continuación se muestra un cuadro resumen de procedimientos durante la emergencia:

Procedimientos durante la Emergencia		
Horario	**Ocurrencia**	**Acción a Seguir**
Laboral	Problemas en funcionamiento de computador personal	Avisar a la Dirección de Informática via correo electrónico, informe, personalmente.
Laboral	Problemas en el Portal, correo, Internet y comunicaciones.	Avisar a la Dirección de Informática via correo electrónico, informe, personalmente.

No laboral	Problemas en el Portal, correo, Internet y comunicaciones.	Avisar al guardia de seguridad encargado del piso o puerta, quien notificará al personal de la lista de números telefónicos de emergencia.
Laboral	Siniestro	Avisar a la Dirección de Informática via correo electrónico, informe, personalmente.
No laboral	Siniestro	Avisar al guardia de seguridad más cercano quien notificará al personal de la Lista de números telefónicos de emergencia.

Números telefónicos en caso de incidentes informáticos				
Contacto	**Cargo**	**Teléfonos**		
		Oficina	**Extensión**	**Celular**
Pedro Moreno Intriago	Director de Informática	3700250	200	0985771465; 0995983967
Betty Moreira Pico	Soporte y Helpdesk	3700250	2000	998519726
Gustavo Donoso Lange	Administrador de Base de Datos	3700250	2009	991320877
Javier Cedeño Rodríguez	Administrador de aplicaciones	3700250	2004	984070271
Boris Mero Casanova	Administrador de Redes y Comunicaciones	3700250	2015	967585803
Enrique Zambrano Espinoza	Soporte y Helpdesk	3700250	2005	997287179
José Hernández Chilan	Administrador de Proyectos	3700250	2007	986513778

2.2.2.Formación de Equipos Operativos

La Dirección de Informática a través del Comité de Defensa Civil del GAD PORTOVIEJO (en caso de existir), deberá contar con brigadistas que deben ser designados por los Directores de las diferentes áreas, jefaturas o Direcciones, quienes actuarán inmediatamente en la lucha contra incendios, evacuación y primeros auxilios, así mismo, harán uso de extintores contra incendios y por su parte, personal de la Dirección de Informática se encargará del aspecto referente a los Recursos

Informáticos de acuerdo a la clasificación de prioridades.

Equipo Mínimo de Respuesta	
Equipos	**Cantidad**
Servidores de Base de Datos y Aplicativos	2
Computadores Personales	10
Extintores de incendio	5
Switches	5
Patch cords	20
Switches wireless	3
Herramientas y otros	varios
Rollos de cable	2

2.3. Actividades después del desastre

2.3.1.Evaluación de Daños

Inmediatamente después que el siniestro haya concluido, los brigadistas y el personal de la Dirección de Informática realizarán en primer caso una evaluación de los bienes materiales, equipos y sistemas de Información que se hayan visto afectados por el siniestro, indicando cuales pueden ser recuperados en cuanto tiempo.

2.3.2.Priorización de actividades del Plan de Acción.

Las oficinas involucradas en el Plan de Contingencia de acuerdo al ámbito de su competencia, previa evaluación de los siniestros priorizan las actividades correspondientes, a fin de habilitar los ambientes y poner en funcionamiento en el término perentorio los equipos, sistemas operativos y sistemas de aplicación de la institución. En materia de informática se dará prioridad a las actividades estratégicas y urgentes, las cuales pueden ser:

- ✓ Habilitación de servidores si fuera el caso que estén dañados.
- ✓ Restauración del último backup de datos de los sistemas en producción.
- ✓ Reinstalación de los sistemas de información de acuerdo al cuadro de prioridades en las PCs clientes.
- ✓ Reinstalación de sistemas operativos y software de base en los terminales que se encuentren operativos en ese momento, si es que presentasen problemas.
- ✓ Puesta en marcha del Centro de datos Alterno (si se tuviere).

Mantenimiento Preventivo por Equipo Informático			
Equipo Informático afectado	**Acción correctiva**	**Tiempo estimado**	**Dependencia/ area responsable**
Equipos de Red: Switch, routers.	Se reemplaza con switch, router inalámbrico del stock de equipos informáticos (si hubiere)	60 minutos	Dirección de Informática
Impresoras matriciales, inyección de tinta, laser, otras	Se reemplaza por una impresora del mismo tipo si hay disponibilidad en stock de equipos informáticos. Caso contrario se utilizará impresora de re de la misma área o de otra área.	20 minutos	Dirección de Informática
Equipos de comunicación	Cambiar con uno nuevo si hubiere en el stock de equipos informáticos	7-8 horas	Dirección de Informática
Computadores personales	Se reemplaza con equipos disponibles en el stock de equipos informáticos. Si el equipo tiene garantía y presenta fallas se acude al fabricante o vendedor.	40 minutos. No determinado	Dirección de Informática
Servidor del Portal, Servidor intranet, Servidor de Base de Datos, Servidor de Correo			Dirección de Informática

Servidor del Portal, Servidor intranet, Servidor de Base de Datos, Servidor de Correo.	Se reemplaza con servidor de backup de Portal, servidor de backup de bases de datos, servidor de backup de intranet, servidor de backup de correo ubicados en el local institucional.	8 horas	Dirección de Informática
Servidor File Server.	Se realizan acciones de reinstalación y configuración.	No determinado	
Servidor DNS	Se reinstala y reconfigura el servidor DNS en la sala de servidores.	8 horas	

2.3.3.Ejecución de Actividades

Los brigadistas (en caso de presentarse) en forma coordinada con los responsables de la Dirección de Informática actuarán en forma conjunta con el comité responsable del Plan de Contingencias General del Edificio Municipal del GAD PORTOVIEJO (de existir dicho Comité), para la ejecución de las tareas específicas para casos de emergencia.

2.3.4.Retroalimentación del Plan de Acción

El Plan de Contingencias es un documento de gestión de la Dirección de Informática, teniendo como característica particular que cambia en el tiempo, es decir, debe adaptarse de acuerdo a las emergencias que se pudiesen suscitar, y con los cambios tecnológicos de los equipos informáticos; esta información tendrá que incorporarse al documento en el marco de una retroalimentación constante, garantizando la vigencia y utilidad de este Plan.

En pos de mantener actualizado este importante documento, se establece como política de la Dirección de Informática la revisión y actualización del Plan de Contingencias dos veces al año de la siguiente manera:

- ✓ Primera actualización en el mes uno del año en curso.
- ✓ Segunda actualización en el mes seis del año en curso.