



PLAN DE CONTINGENCIA TECNOLÓGICA

Rol	Funcionario (responsable)	Cargo (puesto)	Firma
Elaborado por:	Adrian Trejos Calderón	Equipo Infraestructura TIC	
Validado por:	Daniel Ramirez Gonzalez	Director Área de TIC	
Revisado por:	MichaelVargas Fernández	Encargado Área de Planeamiento	
Aprobado por:	Mario Redondo Poveda.	Alcalde Municipal	

Versión 3.0

Junio 2024

TABLA DE CONTENIDO

Contenido

PLAN DE CONTINGENCIA TECNOLÓGICA	1
CONTROL DE CAMBIOS.....	4
INTRODUCCIÓN.....	5
1. OBJETIVOS.....	5
2. ALCANCE	6
3. GLOSARIO DE TÉRMINOS.....	6
4. MARCO NORMATIVO	8
5. ANÁLISIS DE IMPACTO AL NEGOCIO - BIA (Business Impact Analysis)	8
5.1 Identificación de los procesos misionales y criticidad de recuperación	9
5.2 Identificación de las prioridades de recuperación de servicios y sistemas	10
6. CONTROLES PREVENTIVOS	12
6.1 Capacidad de las UPS y Planta de respaldo en Palacio Municipal.....	13
6.2 Capacidad de los sistemas de refrigeración	13
6.3 Sistema de extinción de incendio	13
6.4 Sistemas de monitoreo capacidad de los servidores	13
6.5 Sistemas de monitoreo de aplicaciones	13
6.6 Sistemas de monitoreo de bases de datos	13
6.7 Toma de copias de respaldo y periodicidad.....	14
6.8 Sistemas de almacenamiento de copias de respaldo	15
6.9 Sistemas de protección de la seguridad de la información	15
6.10 Realizar simulacros y pruebas a los backups realizados.....	16
7. ESTRATEGIAS DE CONTINGENCIA.....	16
7.1 Empresas de Servicio o Proveedores de Servicios Externos.....	16
7.2 Identificación de incidentes que se pueden presentar	16
8. MANTENIMIENTO AL PLAN	16
9. PRESENTAR EL INFORME RESULTANTE DE LAS ACCIONES LLEVADAS A CABO	19
ANEXO 1. PLAN DE ACCIÓN PARA EL SISTEMA WIZDOM	20
ANEXO 2. PLAN DE ACCIÓN MUNIRED.....	21
ANEXO 3. PLAN DE ACCIÓN SOPORTE.....	23
ANEXO 4: Plan de acción MANTENIMIENTO CORRECTIVO.....	24
ANEXO 5: PLAN DE ACCION MANTENIMIENTO PREVENTIVO.....	24
ANEXO 6 PLAN DE ACCION INTERNET	26
ANEXO 7 PLAN DE ACCION CORREO INSTITUCIONAL.....	31
ANEXO 8 PLAN DE ACCION ACTIVE DIRECTORY.....	34
ANEXO 9 PLAN DE ACCION REGISTRO EN LINEA.....	37
ANEXO 10 PLAN DE ACCION SIPORE.....	38



ANEXO 11 PLAN DE ACCION SISTEMA DE REQUERIMIENTOS AREA TIC	38
ANEXO 12 PLAN DE ACCION SISTEMA DELPHOS.....	39
ANEXO 13 PLAN DE ACCION PORTALES WEB	42
ANEXO 14 PLAN DE ACCION ESTACIONOMETROS	44
ANEXO 15 PLAN DE ACCION SISTEMA DE RECURSOS HUMANOS.....	45
ANEXO 16 PLAN DE ACCION SISTEMAS BIENES INMUEBLES	46
ANEXO 17 PLAN DE ACCION CONECTIVIDAD.....	48
ANEXO 18 PLAN DE ACCION TELEFONIA IP NUBE	50
Anexos a Plan de contingencia tecnológica 2024-2025 Municipalidad de Cartago Aplicación y cronograma .	51
Cronograma de Aplicación	52
PARCHES DE EMERGENCIA Y CIBERSEGURIDAD	52
DOCUMENTACION Y UBICACION.....	53

CONTROL DE CAMBIOS

Fecha:	Modificado por:	Sección en que se realiza el cambio	Descripción del cambio realizado
1/12/2023	Daniel Ramírez González	Se realiza la actualización de la información de acuerdo con el BIA institucional y al PCN de octubre 2023	Actualizar procesos a la actualidad de la Municipalidad de acuerdo con el plan de continuidad de negocio (BIA) y el Análisis del Impacto de negocio (PCN).
20/05/2023	Daniel Ramirez Gonzalez / Adrian Trejos	Se realiza por la actualización de la telefonía IP y nuevo licenciamiento Windows CSP para el año 2024	Actualización del documento, por cambios tecnológicos en la infraestructura municipal por modernización Telefonía IP, Pago de parquímetros, velocidad de internet y licencias Windows en nube

INTRODUCCIÓN

Para la Municipalidad de Cartago, es muy importante asegurar la operación y continuidad del negocio. Por tal motivo, ha decidido planear, implementar y mejorar un Plan de Contingencia Tecnológica, en adelante PCT, para identificarla infraestructura física, tecnológica, procesos críticos y sobre todo los riesgos de tipo catastróficos y así definir estrategias, con el fin de reducir los tiempos de recuperación, garantizando la continuidad de las operaciones y la gestión de los riesgos que pudieran afectar la continuidad de la Institución.

El PCT en la Municipalidad de Cartago permite que se realice la identificación de los riesgos que afecten la continuidad de la Institución, la priorización de procesos de acuerdo con su criticidad, la definición de estrategias de recuperación y el retorno de los procesos en el menor tiempo posible, por medio de la identificación y asignación de recursos humanos y financieros y la definición de un plan de pruebas para el mantenimiento y mejora del PCT. Al establecer las medidas de mitigación, la MC, habilita los mecanismos que le permitan cumplir con los siguientes propósitos:

- Reducir el impacto generado sobre la operación de las funciones críticas.
- Proteger la imagen, los intereses y el buen nombre de la entidad.
- Disminuir las pérdidas de información.
- Obtener formación frente a incidentes para lograr la protección de la integridad de las personas y bienes de la entidad en forma adecuada, realizando una buena administración de la crisis.

1. OBJETIVOS

1.1. Objetivo General

Proporcionar a la Municipalidad de Cartago un plan con las estrategias que permitan mitigar los riesgos, las causas y consecuencias asociadas a la infraestructura tecnológica, de manera que se pueda generar confianza a todos los interesados en cuanto al funcionamiento y rápida recuperación de los sistemas de información y servicios tecnológicos ante las posibles fallas que interrumpan la operación normal de los mismos.

1.2. Objetivos específicos

1. Ejecutar las actividades preventivas y controles necesarios que permitan mantener en correcto funcionamiento la infraestructura tecnológica de la entidad.
2. Garantizar la continuidad del negocio controlando los componentes y elementos considerados como críticos en la operación diaria.
3. Definir las acciones preventivas y correctivas, que permitan prevenir las eventualidades en las operaciones de los sistemas de información de la MC y corregir en forma oportuna cualquier anomalía que afecte su correcto funcionamiento.

4. Determinar mediante un análisis de una manera precisa cuales son los riesgos informáticos a los que se encuentra expuesto la municipalidad.
5. Reevaluar los controles existentes que sean considerados poco efectivos o no sean aplicables.
6. Presentar recomendaciones que permitan disminuir la probabilidad de ocurrencia de una eventualidad y definir los procedimientos preventivos resultantes de estas recomendaciones.
7. Listar las posibles fallas que se pueden presentar en el funcionamiento del hardware y software que conforman la plataforma estratégica de la MC.
8. Definir los lineamientos a seguir en caso de una eventual falla de la infraestructura o de los sistemas de información.

2. ALCANCE

El Plan de Contingencia de la Municipalidad de Cartago, se orienta al proceso establecido como crítico dentro de la matriz de análisis de impacto del negocio, el cual es Gestión de las Tecnologías de la Información y las Comunicaciones y sus activos de información como proceso crítico. Dicho proceso es importante para que la entidad continúe operando.

Este alcance estará sujeto a las actualizaciones requeridas por la alta dirección y actividades de la entidad.

3. GLOSARIO DE TÉRMINOS

Copias de seguridad (Backup): una copia de seguridad o backup (su nombre en inglés) en tecnología de la información o informática es una copia de seguridad - o el proceso de copia de seguridad - con el fin de que estas copias adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos.

Cliente SSH: Aplicación que implementa el protocolo SSH para realizar acceso remoto a dispositivos de cómputo que dispongan de dicho servicio.

Disco duro: en informática, un disco duro o disco rígido (en inglés *Hard Disk Drive*, HDD) es un dispositivo de almacenamiento de datos no volátil que emplea un sistema de grabación magnética para almacenar datos digitales. Se compone de uno o más platos o discos rígidos, unidos por un mismo eje que gira a gran velocidad dentro de una caja metálica sellada. Sobre cada plato se sitúa un cabezal de lectura/escritura que flota sobre una delgada lámina de aire generada por la rotación de los discos.

Sistema Core: Es un software desarrollado por Microsoft, nombrado CRM Dynamics, el cual ha sido normalizado para apoyar los procesos del área Tributaria institucional

Enrutador (router): el enrutador (del inglés *router*), direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos.

Gestión de continuidad de negocio (BCM): Proceso general de gestión holístico que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación de negocio en caso de materializarse y el cual provee un marco de trabajo para la construcción de la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de las partes

interesadas claves, reputación, marca y actividades de creación de valor.¹

Hardware: corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Hiperconvergencia: La hiperconvergencia es la combinación de componentes virtuales y físicos de una infraestructura, tales como servidores, redes y hardware de almacenamiento, resultando en un único dispositivo controlado por software. La hiperconvergencia permite simplificar las operaciones de TI desglosando los nichos tradicionales y permitiendo que el mismo hardware gestione el almacenamiento, el procesamiento, las redes y la virtualización.

Hub: Concentrador. Dispositivo capaz de enlazar físicamente varios ordenadores de forma pasiva, enviando los datos para todos los ordenadores que estén conectados, siendo éstos los encargados de discriminar la información.

Wizdom: Es un sistema integrado de gestión financiera, que ofrece funcionalidades propias financieras, desarrollado por la empresa Optec para apoyar las funciones financieras, contables y de activos municipales

LAN: (Local Area Network - Red de Área Local). Interconexión de computadoras y periféricos para formar una red dentro de una empresa u hogar, limitada generalmente a un edificio.

Máquina virtual: una máquina virtual es un software que simula un sistema de computación y puede ejecutar programas como si fuese una computadora real.

Módem: Un **módem** es un dispositivo que sirve para enviar una señal llamada *moduladora* mediante otra señal llamada *portadora*. Se han usado módems desde los años 60, principalmente debido a que la transmisión directa de las señales electrónicas inteligibles, a largas distancias, no es eficiente, por ejemplo, para transmitir señales de audio por el aire, se requerirían antenas de gran tamaño (del orden de cientos de metros) para su correcta recepción. Es habitual encontrar en muchos módems de red conmutada la facilidad de respuesta y marcación automática, que les permiten conectarse cuando reciben una llamada de la RTPC (Red Telefónica Pública Conmutada) y proceder a la marcación de cualquier número previamente grabado por el usuario. Gracias a estas funciones se pueden realizar automáticamente todas las operaciones de establecimiento de la comunicación.

Plan de Contingencia: Conjunto de estrategias, acciones, procedimientos planificados y responsabilidades definidas para minimizar el impacto de una interrupción imprevista de las funciones críticas y conseguir la restauración de estas, dentro de unos límites de tiempo establecidos. Sin que sea una regla general, se suele aplicar al plan circunscrito a las actividades de los departamentos de Sistemas de Información.

Red: Una red de computadoras, también llamada red de ordenadores o red informática es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos para compartir información y recursos. Este término también engloba aquellos medios técnicos que permiten compartir la información.

Sitio alterno: Ubicación alterna de operaciones seleccionada para ser utilizada por una organización cuando las operaciones normales no pueden llevarse a cabo utilizando las instalaciones normales después de que se ha producido una interrupción.

Software: se conoce como software al equipamiento o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos del sistema, llamados hardware.

Servidores: Un equipo informático que forma parte de una red y provee servicios a otros equipos

S.O. (Sistema Operativo): un **Sistema operativo** (SO) es un software que actúa de interfaz entre los

dispositivos de hardware y los programas de usuario o el usuario mismo para utilizar un computador. Es responsable de gestionar, coordinar las actividades y llevar a cabo el intercambio de los recursos y actúa como intermediario para las aplicaciones que se ejecutan.

Sistema de información: Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Snapshots de almacenamiento: Los Snapshots de almacenamiento son una forma cada vez más común de protegerlos archivos y los sistemas de almacenamiento. Gracias a la tecnología de los snapshots podemos crear copias de nuestros sistemas de archivos en un momento en el tiempo y en un estado concreto, los Snapshots no son un sistema de recuperación de datos en sí ya que dependen de la fuente principal para restaurar la información a un estado anterior.

SSH: (o Secure Shell) es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada. Además de la conexión a otros dispositivos, SSH permite copiar datos de forma segura (tanto archivos sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir contraseñas al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH y también puede redirigir el tráfico del (Sistema de Ventanas X) para poder ejecutar programas gráficos remotamente. El puerto TCP asignado es el 22.

Telecomunicaciones: es una técnica consistente en transmitir un mensaje desde un punto a otro, normalmente con el atributo típico adicional de ser bidireccional. El término *telecomunicación* cubre todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de computadoras a nivel de enlace.

VPN: por las siglas en inglés de Virtual Private Network, o red privada virtual, es un túnel seguro entre su dispositivo y la internet. Las VPN protegen su tráfico en línea contra espías, interferencias y censura.

4. MARCO NORMATIVO

- ✓ Código Municipal.
- ✓ Ley 7202 del Sistema Nacional de Archivos.
- ✓ Ley 8292 Ley General de Control Interno
- ✓ Reglamento autónomo interno de trabajo, Municipalidad de Cartago.
- ✓ Convención colectiva de trabajo de la Municipalidad de Cartago.
- ✓ Normativa técnica de las TIC, emitida por el MICITT
- ✓ Plan de continuidad de Negocio Municipalidad de Cartago
- ✓ Resoluciones Comisión Nacional de Selección y Eliminación de Documentos.
- ✓ Declaratoria General de documentos con valor científico cultural para el sector Municipal.
- ✓ Plan Estratégico de Tecnologías de la Información y comunicación PETIC

5. ANÁLISIS DE IMPACTO AL NEGOCIO - BIA (Business Impact Analysis)

La fase de Análisis de Impacto del Negocio BIA (Business Impact Analysis) por sus siglas en inglés), permite identificar los procesos misionales y analizar el nivel de impacto que traería sobre estos las fallas que puedan presentarse en los servicios y sistemas de información que lo soportan.

Propósito del Análisis BIA:

A. Identificar los procesos misionales y criticidad de recuperación:

Se identifican los sistemas y servicios más importantes y los cuales deben ser recuperados con prioridad sobre los demás. El plan de contingencia contempla la recuperación de los sistemas y servicios de criticidad alta.

B. Identificar los requerimientos de recursos

La identificación de los esfuerzos necesarios para recuperar los sistemas implica una evaluación detallada de los recursos necesarios para reactivar los procesos misionales y la identificación de las interdependencias entre recursos y sistemas. Algunos de los elementos que se deben considerar incluyen: talento humano, instalaciones, equipos, software, archivos de datos y componentes de los sistemas.

C. Identificar las prioridades de recuperación de servicios y sistemas de información

Se identifican los sistemas y servicios que sean prioritarios de recuperar ante eventuales fallas.

5.1 Identificación de los procesos misionales y criticidad de recuperación

Para formular el BIA la MC realizó un inventario de activos de información donde se clasificaron los sistemas y servicios como críticos.

ACTIVIDAD O PROCESO	AREA O DEPARTAMENTO	DESCRIPCIÓN DEL PROCESO	ENTRADAS SALIDAS
Sistema de Gestión Tributaria	Módulo de Plataforma de servicio	Módulo utilizado como ventanilla única para todos los trámites municipales	Procedimiento 01: Módulo de Plataforma
Sistema de Gestión Tributaria	Módulo de Plataforma de servicio	Modulo para la actualización del registro único de los contribuyentes	Procedimiento 02: Módulo de RUC
Sistema de Gestión Tributaria	Módulo de Permisos de construcción	Módulo de permisos de construcción	Procedimiento 03: Módulo de Permisos de Construcción
Sistema de Gestión Tributaria	Modulo Comercial	Módulo de trámites de comercial incluye agua y otros tributos	Procedimiento 04: Módulo de Comercial
Sistema de Gestión Tributaria	Modulo Patentes	<i>Módulo de patente comercial</i>	Procedimiento 05: Módulo de Patentes
Sistema de Gestión Tributaria	Modulo Comercial	<i>Módulo de Plataforma de cobro</i>	Procedimiento 06: Módulo de Cobro
Sistema de Gestión Tributaria	Modulo Comercial	<i>Módulo de administración de mercado municipal</i>	Procedimiento 07: Módulo de Mercado
Sistema de Bienes Inmuebles	Modulo Consultas Generales / Reportes / Estadísticas	<i>Módulo de reportes y consultas de Bienes Inmuebles</i>	Procedimiento PR 01: Consulta de bienes inmuebles
Sistema de Bienes Inmuebles	Módulo de Cobro de Impuestos	<i>Módulo de declaración de Bienes Inmuebles</i>	Procedimiento PR 02: Presentación de la declaración

ACTIVIDAD O PROCESO	AREA O DEPARTAMENTO	DESCRIPCIÓN DEL PROCESO	ENTRADAS SALIDAS
Sistema de Bienes Inmuebles	Módulo de Cobro de Impuestos	<i>Módulo de cobro de Bienes Inmuebles</i>	Procedimiento PR 03: Modificación a las bases de datos RUC-BIENES
Sistema de Gestión Financiera	Módulo de presupuesto (Proceso presupuesto)	<i>Elaboración y modificación del presupuesto institucional</i>	Procedimiento PR 01: Registro y consultas de presupuesto sistema Wizdom
Sistema de Gestión Financiera	Módulo de contratación pública (Proceso Proveeduría):	<i>Procesa la gestión de las contrataciones y adquisiciones</i>	Procedimiento PR 02: Realización de compras sin sistema interno
Sistema de Gestión Financiera	Módulo de Inventario (Proceso Almacén Municipal):	Gestión de inventarios y abastecimiento, custodia y administración de materiales en las bodegas de suministros	Procedimientos PR 03: Recepción de inventarios a proveedores y entrega de inventarios a clientes internos.
Sistema de Gestión Financiera	Módulo de activos (proceso Activos): se	Verificación de las entradas y salidas de activos, así como el levantamiento en las distintas oficinas	Procedimiento PR 04: Registro de entradas y salidas en el sistema.
Sistema de Gestión Financiera	Módulo de Recursos Humanos (proceso Recursos Humanos):	El procedimiento de planillas, en el cual se envía la documentación necesaria al departamento de Tesorería	Procedimientos PR 05: Elaboración de planillas.
Sistema de Gestión Financiera	Módulo de cuentas por pagar y cobro de tributos (proceso Tesorería).	Administrado por el Área Tributaria, y el procedimiento de cuentas por pagar, llevado a cabo en el sistema SIAF administrado por el Área Administración Financiera.	Procedimientos PR 06: Cobro de tributos y realización de pagos urgentes.
Sistema de Gestión Financiera	Módulo de contabilidad (proceso Contabilidad):	El procedimiento contable se integra mediante el SIAF con los demás procesos,	Procedimientos PR 07: Registros contables y presupuestarios. Emisión de estados financieros y cuadros de ejecución presupuestaria.

5.2 Identificación de las prioridades de recuperación de servicios y sistemas

Ante las fallas de los sistemas de información y/o servicios tecnológicos que se prestan a los usuarios de la MC, se priorizan de acuerdo con el impacto que la caída de estos pueda generar en la operación diaria

de la Municipalidad detallados en la siguiente tabla.:

RECURSOS HERRAMIENTAS	MÁXIMO HORAS INTERRUPCIÓN MTD	PROCESOS DE SINCRONIZACIÓN	REQUISITOS NEGOCIO		CAPACIDAD SISTEMAS	
			RTO	RPO	RTO	RPO
Sistema Core Tributario / Red interna / recursos humanos	8	Si con Tribunal supremo de elecciones, Registro de la propiedad, web services de personas	1	3	1	3
Sistema Core Tributario / Red interna / recursos humanos	8	Si con Tribunal supremo de elecciones, Registro de la propiedad, web services de personas	1	3	1	3
Sistema Core Tributario / Red interna / recursos humanos	24	Si con Tribunal supremo de elecciones, Registro de la propiedad, Colegio de ingenieros y Arquitectos CFIA	2	2	2	3
Sistema Core Tributario / Red interna / recursos humanos	24	Si con Tribunal supremo de elecciones, Registro de la propiedad, web services de personas	2	2	2	2
Sistema Core Tributario / Red interna / recursos humanos	8	Si con Tribunal supremo de elecciones, Registro de la propiedad, web services de personas	3	5	3	4
Sistema Core Tributario / Red interna / recursos humanos	NO puede estar sin funcionar	Si con Tribunal supremo de elecciones, Registro de la propiedad, web services de personas	1	1	1	1
Sistema Bienes Inmuebles / Red interna / Personal	72	Si con Tribunal supremo de elecciones, Registro de la propiedad, web services de personas	5	1	1	5
Sistema Bienes Inmuebles / Red interna / Personal	8	Si con Tribunal supremo de elecciones, Registro de la propiedad, web services de personas	1	4	1	3
Sistema Bienes Inmuebles / Red interna / Personal	8	Si con Tribunal supremo de elecciones, Registro de la propiedad, web services de personas	1	2	1	2

RECURSOS HERRAMIENTAS	MÁXIMO HORAS INTERRUPCIÓN MTD	PROCESOS DE SINCRONIZACIÓN	REQUISITOS NEGOCIO		CAPACIDAD SISTEMAS	
			RTO	RPO	RTO	RPO
Sistema Bienes Inmuebles / Red interna / Personal	NO puede estar sin funcionar	Si con Tribunal supremo de elecciones, Registro de la propiedad, web services de personas	1	1	1	1
Sistema SIAF / Red interna / Personal	NO puede estar sin funcionar	Con Contraloría General de la República	2	1	2	1
Sistema SIAF / Red interna / Personal	24	Con Contraloría General de la República /SICOP	3	3	3	3
Sistema SIAF / Red interna / Personal	72	Con Contraloría General de la República /SICOP	4	5	4	5
Sistema SIAF / Red interna / Personal	72	NO	4	5	4	5
Sistema SIAF / Red interna / Personal	NO puede estar sin funcionar	Bancos, cooperativas, CCSS, Ministerio de hacienda	1	1	1	1
Sistema SIAF / Red interna / Personal	NO puede estar sin funcionar	Bancos, Cooperativas, Epark, conectividad pagos	1	1	1	1
Sistema SIAF / Red interna / Personal	8	Contraloría General de la República, Contabilidad Nacional	2	2	2	1

6. CONTROLES PREVENTIVOS

Esta sección identifica y detalla los controles preventivos que se realizan como parte de las actividades de los planes de seguridad y privacidad de la información, plan de tratamiento de riesgos y plan de mantenimiento y monitoreo que tienen como propósito la realización de tareas y el establecimiento de controles tanto preventivos como correctivos para evitar las fallas de los sistemas de información y de los servicios informáticos.

6.1 Capacidad de las UPS y Planta de respaldo en Palacio Municipal

Ups destinada para equipos crítico como el Data Center del Palacio, UPS en Museo Municipal y Plantel Municipal, además de Plantas de respaldo en Palacio y Plantel Municipal destinadas y administradas por el departamento de Servicios Generales.

El tiempo máximo a full carga según el fabricante es de 10 min, hay que tener en cuenta que las UPS están diseñadas para dar el tiempo suficiente para la transferencia de ups a planta de forma controlada en los equipos de computación (PCs y Servidores) y equipos de comunicaciones.

6.2 Capacidad de los sistemas de refrigeración

La unidad de Aire Acondicionado principal es de presión es de 24000 BTU suficiente para mover y refrigerar el Data Center del palacio, además se cuenta con aire de confort de respaldo en caso de falla en el datacenter más crítico.

6.3 Sistema de extinción de incendio

La MC está protegida con un extintor clase C (equipos eléctricos energizados) para el datacenter, así mismo se suspendieron los aspersores en este sitio ya que se cuenta con un sensor de humo.

6.4 Sistemas de monitoreo capacidad de los servidores

Los servidores se monitorean directamente y se revisan los logs generados para validar las situaciones que se están presentando y tomar acciones correctivas y preventivas. Cada 3 meses como máximo se valida si existen actualizaciones del sistema operativo para realizarlas y los cambios críticos o recomendados se aplican de inmediato.

6.5 Sistemas de monitoreo de aplicaciones

Los sistemas de información Municipales se monitorean a diario en horario laboral con el fin de determinar que se encuentran en funcionamiento correcto

El funcionamiento de la página web se realiza diariamente, por medio de mensajes automatizados y se realiza una copia de seguridad y se actualiza el sistema alterno de contingencia, esta actividad es realizada todos los días.

El sistema de hiperconvergencia Nimble que aloja las aplicaciones municipales es monitoreado a diario para validar el estado de este y los servidores físicos y virtuales.

La MC cuenta con herramientas de monitoreo por lo tanto estas actividades se realizan de forma directa sobre las máquinas a través de los sistemas propios por medio de la consola de antivirus.

Las temperaturas y emisión de humo son monitoreados en tiempo real y envían alarmas correctivas en caso de ser necesario.

6.6 Sistemas de monitoreo de bases de datos

La base de datos SQL server, es validada y documentada por uno de los funcionarios de infraestructura, según lo establece la política de configuración de administración de base de datos

 MUNICIPALIDAD CARTAGO	SISTEMA DE GESTIÓN MUNICIPAL		Código:	ATIC-PO-01
	DEPENDENCIA: AREA DE TECNOLOGIA DE INFORMACION Y COMUNICACIÓN		No. Versión:	V.01
	Política Configuración de Administración de Base de Datos		Fecha vigencia R:	31/03/2023

Rol	Nombre (responsable)	Cargo (puesto)	Firma
Elaborado por:	Ing. Juan Arias Artavia	Subencargado Área Tecnología de información	JUAN DIDIER ARIAS ARTAVIA (FIRMA) Firmado digitalmente por JUAN DIDIER ARIAS ARTAVIA (FIRMA) Fecha: 2023.03.31 15:04:47 -0500'
Validado por:	Ing. Daniel Ramírez González.	Encargado Área Tecnología de información	DANIEL RAMIREZ GONZALEZ (FIRMA) Firmado digitalmente por DANIEL RAMIREZ GONZALEZ (FIRMA) Fecha: 2023.03.31 15:05:18 -0500'
Revisado por:	Ing. Stephanie Arias Arroyo.	Equipo Técnico de Procesos	STEPHANIE MARIA ARIAS ARROYO (FIRMA) Firmado digitalmente por STEPHANIE MARIA ARIAS ARROYO (FIRMA) Fecha: 2023.03.31 15:07:21 -0500'
Aprobado por:	Lic. Mario Redondo Poveda.	Alcalde Municipal	MARIO REDONDO POVEDA (FIRMA) Firmado digitalmente por MARIO REDONDO POVEDA (FIRMA) Fecha: 2023.03.31 15:08:50 -0500'

A. Presentación (antecedentes):

La gestión de la configuración es un proceso que busca mantener los sistemas informáticos, los servidores y el software en un estado deseado y uniforme. Permite garantizar que un sistema funcione como se espera a medida que se realizan cambios. Para gestionar la configuración de un sistema de TI es necesario definir el estado deseado, como los ajustes del servidor, y luego diseñar y mantener el sistema. Es un área muy relacionada con la evaluación de la configuración y el análisis de los ajustes, ya que utiliza ambos para identificar los sistemas que requieren actualizaciones, reconfiguraciones o ejecuciones de parches.

6.7 Toma de copias de respaldo y periodicidad

Los respaldos se generan de forma automatizada por medio del sistema destinado para este fin, que se encarga del proceso de las copias de seguridad de los servidores que se encuentran en producción en el datacenter de la MC, esta actividad se realiza con el objetivo de contar con los respaldos necesarios en caso de presentarse una emergencia; esto incluye las bases de datos de cada uno de los sistemas existentes y las carpetas TRD como parte del proceso de contingencia tecnológico aplicado. Los ingenieros del Área de TIC validan Backups diarios a los registros de las bases de datos con los que funcionan los diferentes aplicativos con los que cuenta la MC (Base de datos SQL, Página Web, entre otros) de todos los sistemas municipales. Los servidores de Página Web cuentan con scripts que realizan las copias de respaldo de las aplicaciones, archivos instalados en estos servidores, así como las bases de datos que los soportan.

Los backups realizados se registran por medio del reporte diario de respaldos de servidores, si se requiere información adicional puede validarse el proceso de respaldos del área de TIC, detallado en Munired.

Listado de backups que se realizan con periodicidad para atender las posibles contingencias que se pudieran presentar

Proceso	Subproceso	Procedimiento
Sistema de Gestión Tributaria	Módulo de Plataforma de servicio	Procedimiento 01: Módulo de Plataforma
Sistema de Gestión Tributaria	Módulo de Plataforma de servicio	Procedimiento 02: Módulo de RUC

Proceso	Subproceso	Procedimiento
Sistema de Gestión Tributaria	Módulo de Permisos de construcción	Procedimiento 03: Módulo de Permisos de Construcción
Sistema de Gestión Tributaria	Modulo Comercial	Procedimiento 04: Módulo de Comercial
Sistema de Gestión Tributaria	Modulo Patentes	Procedimiento 05: Módulo de Patentes
Sistema de Gestión Tributaria	Modulo Comercial	Procedimiento 06: Módulo de Cobro
Sistema de Gestión Tributaria	Modulo Comercial	Procedimiento 07: Módulo de Mercado
Sistema de Bienes Inmuebles	Modulo Consultas Generales / Reportería/ estadísticas	Procedimiento PR 01: Consulta de bienes inmuebles
Sistema de Bienes Inmuebles	Módulo de Cobro de Impuestos	Procedimiento PR 02: Presentación de la declaración
Sistema de Bienes Inmuebles	Módulo de Cobro de Impuestos	Procedimiento PR 03: Modificación a las bases de datos RUC-BIENES
Sistema de Gestión Financiera	Módulo de presupuesto (Proceso presupuesto)	Procedimiento PR 01: Registro y consultas de presupuesto sistema Wizdom
Sistema de Gestión Financiera	Módulo de contratación pública (Proceso Proveeduría):	Procedimiento PR 02: Realización de compras sin sistema interno
Sistema de Gestión Financiera	Módulo de Inventario (Proceso Almacén Municipal):	Procedimientos PR 03: Recepción de inventarios a proveedores y entrega de inventarios a clientes internos.
Sistema de Gestión Financiera	Módulo de activos (proceso Activos):	Procedimiento PR 04: Registro de entradas y salidas en el sistema.
Sistema de Gestión Financiera	Módulo de Recursos Humanos (proceso Recursos Humanos):	Procedimientos PR 05: Elaboración de planillas.
Sistema de Gestión Financiera	Módulo de cuentas por pagar y cobro de tributos (proceso Tesorería).	Procedimientos PR 06: Cobro de tributos y realización de pagos urgentes.
Sistema de Gestión Financiera	Módulo de contabilidad (proceso Contabilidad):	Procedimientos PR: Registros contables y presupuestarios. Emisión de estados financieros y cuadros de ejecución presupuestaria.

6.8 Sistemas de almacenamiento de copias de respaldo

Se almacenan semanalmente los backups (copias de respaldo o de seguridad) en una storage que queda ubicado en el datacenter, de allí se generan las copias de respaldo. Los respaldos realizados también se trasladan a un lugar externo dedicado para su conservación.

6.9 Sistemas de protección de la seguridad de la información

La información de las tablas TRD (datos, dbf) está protegida a través de las reglas del Directorio Activo que restringen los accesos a las carpetas de cada una de las oficinas. Así mismo estas carpetas solo pueden accederse con una conexión autorizada a la red de la MC a través del usuario y clave asignados. Si se realiza por conexión remota esta es validada y asignada a través del usuario y clave proporcionado para el uso de la VPN y controlado a su vez por el firewall de la municipalidad.

Se cuenta además con el software antivirus instalado en todas las máquinas de la MC.

Las bases de datos de los sistemas de información se encuentran protegidas en servidores a los

cuales únicamente se tiene acceso por parte del grupo de Ingenieros del área. Se cuenta con grupos en el directorio activo y reglas que restringen los accesos por lo que solo las personas autorizadas podrán tener acceso a los servidores que alojan las bases de datos.

Las IPS de los servidores que alojan las bases de datos y las claves de acceso directo a las mismas solo son conocidas por los Ingenieros del área y solo se puedan acceder a través de los usuarios autenticados.

6.10 Realizar simulacros y pruebas a los backups realizados

Se realizó el simulacro según se detalla en la normativa técnica de las técnicas de las TIC, y según lo indicado en el proceso de respaldos según las recomendaciones detalladas en el correo del MICITT

7. ESTRATEGIAS DE CONTINGENCIA

Para que exista continuidad del negocio en la MC, se deben tener presentes los planes de contingencia definidos con cada uno de los proveedores de servicios como también las estrategias definidas al interior de la entidad.

7.1 Empresas de Servicio o Proveedores de Servicios Externos

La MC actualmente cuenta con el respaldo de los Terceros que proveen el soporte a los sistemas de información y Humano con quienes se tienen acuerdos para brindar el soporte que se requiera a los planes de contingencia en la MC. Se cuenta con el contrato de mantenimiento a la infraestructura lógica de la MC mediante el cual se tiene previsto tener disponibilidad el apoyo técnico de Ingenieros y expertos en los diversos temas y plataformas que maneja la entidad a fin de brindar el soporte requerido en caso de contingencia. Si se requieren detalles adicionales se cuenta con una herramienta de seguimiento.

7.2 Identificación de incidentes que se pueden presentar

- Para incidentes que se presenten en relación de operadores de servicios públicos como luz, agua, internet y otros, que afecten la operación de la municipalidad.
- Cualquier incidente interno que pudiera potencialmente causar o afectar la interrupción de las operaciones de los sistemas de información, como son la falla en los servidores o puntos de conexión.
- Cualquier incidente o incorrecta manipulación de los sistemas de información que ocasionen desviaciones o pérdida de información.
- Inundación del datacenter.
- Apagado de los servidores por una descarga eléctrica.
- Fallas en el sistema de aire acondicionado que genere recalentamiento en los equipos del Data Center.
- Interrupción total de las operaciones del Centro de Cómputo debido a daños en hardware y/o software de los equipos servidores o pérdida de conectividad.

8. MANTENIMIENTO AL PLAN

8.1 Revisión y actualización del plan

Se tiene previsto realizar una revisión y actualización al plan de contingencia al menos una vez al año. La revisión del plan de contingencia es una de las actividades que se debe incluir en la revisión del Sistema Integrado de gestión de la MC.

Los aspectos que se deben tener en cuenta para realizar las actualizaciones al plan son las siguientes:

- Resultados de auditorías al cumplimiento del plan de contingencia.
- Retroalimentación de partes interesadas como proveedores relacionados con el plan de contingencia, oficina de control interno entre otros.

8.2 Fases del plan para los Sistemas de información

Un Plan de Contingencia consiste en restar el impacto financiero que puede acusar un «incidente» inesperado en la organización dentro del marco de los procedimientos habituales, este plan trabaja para recuperar a la institución de los imprevistos especiales que se puedan dar, y que por su causa interrumpen la operación de los servicios.

Un Plan de Continuidad está enfocado a asegurar la continuidad, cuando de repente ocurre un incidente inesperado. Este plan lo que intenta es no detener la productividad de la organización, e intentar que la situación que ha sucedido en ese momento nos afecte lo menos posible

Muchas veces estos dos conceptos no se pueden desligar, un plan de contingencia puede estar dentro de un Plan de Continuidad, ya que lo que se busca con estas medidas es una rápida recuperación ante los desastres, para reanudar lo antes posible los servicios de la municipalidad.

8.3 Notificación del incidente

Los usuarios de los diferentes sistemas de información deben informar formalmente de la pérdida total o parcial de la disponibilidad, integridad o autenticidad. Esto se debe realizar por medio del sistema de incidentes, seleccionando el sistema de información o servicio que presenta la falla.

8.4 Evaluación del Incidente

Los Ingenieros a cargo del área de Sistemas evalúan el incidente teniendo en cuenta los aspectos a continuación:

Los incidentes ocurridos en los sistemas de información y/o servicios son escalados a través del centro de servicio y clasificados de acuerdo con los Ingenieros asignados como soporte de primer nivel. En este caso la persona a cargo evalúa el incidente y determina el tipo de incidente.

En caso de que el incidente sea de un sistema de información para el cual se cuenta con servicio de soporte por parte del fabricante o desarrollador, se contactará el proveedor a fin de determinar el origen de este y determinar el impacto, tiempos y la solución.

En caso de que el incidente se trate de una falla técnica que deja sin funcionamiento una parte del hardware se contactará el proveedor del servicio de mantenimiento de la infraestructura de la MC a fin de recibir el soporte requerido y el reemplazo o arreglo de las piezas que fallan.

Los Ingenieros a cargo del área de TI evalúan la situación y determinan si es necesario activar o

no el plan de contingencia. Se notifica al proveedor del sistema o servicio sobre la falla y al encargado de área de TI para que en conjunto se determine la activación del plan de contingencia.

Posterior a la evaluación se notifica a través de correo electrónico a las partes interesadas de los tiempos estimados en la recuperación del sistema o servicio.

8.5 Establecer el origen de la falla y la posible solución

En esta fase se determina que originó la falla y cuál es la solución recomendada para restablecer el servicio. Así mismo es necesario determinar los recursos, impactos y tiempos para restablecer el servicio. Se debe especificar los recursos humanos que intervienen en la solución y el rol que tiene cada uno frente a la solución que se dará.

Solo en caso de que la falla deje en indisponibilidad uno de los servicios críticos en horas laborales y que se determine que se tomará más de 4 horas en el restablecimiento de este se activará el plan de contingencia detallado en los anexos de este documento.

8.6 Activar el plan de contingencia y notificar

En esta fase se activa el plan de contingencia y se informa a los interesados el tiempo que tomará en restablecerse el servicio.

8.7 Llevar a cabo las acciones para restablecer el servicio

En esta fase se llevan a cabo las actividades planteadas en los anexos de este documento para cada sistema o servicio que presente la falla.

8.8 Validar el resultado de las acciones realizadas

Una vez se surten las actividades definidas en cada uno de los planes individuales de acuerdo con la contingencia

8.8.1 Notificación del incidente

Los usuarios de los diferentes sistemas de información deben informar formalmente de la pérdida total o parcial de disponibilidad, integridad o autenticidad. Esto se debe realizar por medio del sistema de incidentes, seleccionado el sistema de información o servicio que presenta la falla.

8.8.2 Evaluación del Incidente

Los Ingenieros a cargo del área de Sistemas evalúan el incidente teniendo en cuenta los aspectos a continuación:

Los incidentes ocurridos en los sistemas de información y/o servicios son escalados a través del centro de servicio y clasificados de acuerdo con los Ingenieros asignados como soporte de primer nivel. En este caso la persona a cargo evalúa el incidente y determina el tipo de incidente.

En caso de que el incidente sea de un sistema de información para el cual se cuenta con servicio de soporte por parte del fabricante o desarrollador, se contactará el proveedor a fin de determinar el origen de este y determinar el impacto, tiempos y la solución.

En caso de que el incidente se trate de una falla técnica que deja sin funcionamiento una parte del hardware se contactará el proveedor del servicio de mantenimiento de la infraestructura de la MC a fin de recibir el soporte requerido y el reemplazo o arreglo de

las piezas que fallan.

Los Ingenieros a cargo del área de TI evalúan la situación y determinan si es necesario activar o no el plan de contingencia. Se notifica al proveedor del sistema o servicio sobre la falla y al encargado de área de TI para que en conjunto se determine la activación del plan de contingencia.

Posterior a la evaluación se notifica a través de correo electrónico a las partes interesadas de los tiempos estimados en la recuperación del sistema o servicio.

8.8.3 Establecer el origen de la falla y la posible solución

En esta fase se determina que originó la falla y cuál es la solución por brindar para restablecer el servicio. Así mismo es necesario determinar los recursos, impactos y tiempos para restablecer el servicio. Se debe especificar los recursos humanos que intervienen en la solución y el rol que tiene cada uno frente a la solución que se dará.

Solo en caso de que la falla deje en indisponibilidad uno de los servicios críticos en horas laborales y que se determine que se tomará más de 4 horas en el restablecimiento de este se activará el plan de contingencia detallado en los anexos de este documento.

8.8.4 Activar el plan de contingencia y notificar

En esta fase se activa el plan de contingencia y se informa a los interesados el tiempo que tomará en restablecerse el servicio.

8.8.5 Llevar a cabo las acciones para restablecer el servicio

En esta fase se llevan a cabo las actividades planteadas en los anexos de este documento para cada sistema o servicio que presente la falla.

8.8.6 Validar el resultado de las acciones realizadas

Una vez se surten las actividades definidas en cada uno de los planes individuales de acuerdo con la contingencia presentada, es necesario realizar las validaciones para verificar el estado de estas acciones. Así mismo después de que la contingencia sea superada es necesario realizar el respectivo seguimiento por un lapso de tiempo para poder determinar que la contingencia ha sido superada con éxito.

9. PRESENTAR EL INFORME RESULTANTE DE LAS ACCIONES LLEVADAS A CABO

Toda vez que finalicen las actividades de los planes y una vez superada la contingencia es necesario presentar el respectivo informe que contenga la información suficiente para permitir tomar acciones correctivas o preventivas a fin de que esta no vuelva a ocurrir. Por lo tanto, se debe contar con datos como

9.1 Origen de la contingencia - Qué provocó la falla.

9.2 Actividades realizadas para corregir la falla.

ANEXO 1. PLAN DE ACCIÓN PARA EL SISTEMA WIZDOM

Objetivo General

- Reestablecer el funcionamiento del Sistema Integrado del Área Financiera, para continuar con la actividadde compras y abastecimiento de la institución.

Objetivos Específicos

- Establecer un plan, para en caso de una eventualidad restaurar el sistema y continuar con la operatividadinstitucional
- Comprobar el correcto funcionamiento de cada uno de los módulos del sistema Wizdom (Presupuesto,Compras, Almacén, Tesorería y Contabilidad).
- Inicializar el proceso de compras, adjudicaciones, recepciones y pagos; para permitir el abastecimiento delas diferentes necesidades institucionales.

Alcance

- El alcance de este plan se aplica para la restauración del Sistema Integrado del Área Financiera (Wizdom).

Plan de acción

A continuación, se describen las actividades, responsables y tiempos estimados para la realización del plan de contingencia en caso de una eventualidad.

Actividad	Responsable	Tiempo Estimado
Configurar un servidor de aplicaciones (Sistema Operativo Windows Server)	Integrante de Infraestructura del Área de TICS de la Municipalidad deCartago, en conjunto con funcionario de la empresa OPTEC	2 horas
Configuración de los Web Services para el correcto funcionamiento de la Base de Datos	Integrante deInfraestructura del Área de TICS de la Municipalidad deCartago, en conjunto con funcionario de la empresa OPTEC	1,5 horas
Configuración del APPEON SERVER, para el respectivo acceso vía Web	Integrante deInfraestructura del Área de TICS de la Municipalidad de Cartago, en conjunto con funcionario de la empresa OPTEC	2 horas
Configuración de las reglas del negocio, para brindar la seguridad y correcto uso del sistema.	Integrante de Infraestructura del Área de TICS de la Municipalidad deCartago, en conjunto con funcionario de la empresa OPTEC	1,5 horas
Configuración del puerto 80, para permitir las correspondientes transacciones a través del firewall corporativo.	Integrante de Infraestructura del Área de TICS de la Municipalidad deCartago, en conjunto con funcionario de la empresa OPTEC	45 minutos

Actividad	Responsable	Tiempo Estimado
Configurar un servidor de Bases de Datos (Sistema Operativo Windows Server)	Integrante de Infraestructura del Área de TICS de la Municipalidad de Cartago, en conjunto con funcionario de la empresa OPTEC	2 horas
Crear las respectivas estructuras (tablas requeridas por el sistema).	Integrante de Infraestructura del Área de TICS de la Municipalidad de Cartago, en conjunto con funcionario de la empresa OPTEC	2 horas
Restaurar la Base de Datos anterior al incidente	Responsables de las Base de Datos, deben verificar y restaurar el respaldo en el servidor respectivo.	1 hora
Crear y configurar los perfiles de usuario para las respectivas transacciones en el sistema.	Integrante de Infraestructura del Área de TICS de la Municipalidad de Cartago, en conjunto con funcionario de la empresa OPTEC	2 horas

ANEXO 2. PLAN DE ACCIÓN MUNIRED

Objetivo General

El objetivo de este plan es el de brindar contingencia servicio del sistema Munired, el cual consiste una la herramienta de Microsoft Sharepoint, en el cual se gestiona la documentación digital de la Municipalidad, este plan nos permitirá dar continuidad a las operaciones y en caso de que se materialice un riesgo poder seguir brindando el servicio que depende de esta herramienta, en un grado aceptable.

Objetivos Específicos

1. Contar con un plan para que, en caso de fallas en sistema de Munired, los servicios que dependen de estopuedan seguir funcionando.
2. Contar con un plan, para que en caso de que falle el sistema de Munired, tener una guía que nos ayude a resolver el incidente.
3. Brindar continuidad a los servicios que dependen del sistema de Munired.

Plan de acción

Actividad	Responsable	Tiempo Estimado
En caso de tener un plan emergente, se realiza un respaldo diario en el Data Center externo, este proceso incluye realizar el respaldo de la VM de aplicación de SharePoint, el cual tienen la IP 192.168.0.147 con nombre de SVCAPMR01, además se realiza respaldos al servidor de base de datos el cual tiene la IP 192.168.0.149 con nombre SVCDBMR01, el respaldo a estos datos se realiza todos los días en horas de la noche, según documento de programación de respaldos 7F80. En caso de falla en el sistema se debe realizar análisis del problema, el cual podría ser ocasionado por la caída de algún servicio de SharePoint, alguna actualización de Microsoft, problemas con el motor de la Base de datos, problema de comunicación entre los servidores de aplicación y Base de Datos, problema con los nodos donde se encuentra hospedadas las máquinas virtuales, para lo que se debe tratar de reestablecer el servicio ejecutando las tareas de mantenimiento de los servidores, asignando los recursos necesarios para que la aplicación y base de datos corra adecuadamente, tomando en cuenta espacio en discos, memoria RAM, procesadores y ancho de banda en la red. Si el problema no puede ser solucionado por el personal de infraestructura tecnológica del área de TIC de la Municipalidad, se debe contactar al proveedor contratado para brindarle soporte al sistema, el cual deberá realizar el diagnóstico de la falla, en caso de que al	DIRECCION Y SUB-DIRECCION DE TIC INFRAESTRUCTURA TIC. PROVEEDOR DE SERVICIO DE RESPALDOS PROVEEDOR DE SOPORTE AL SISTEMA DE MUNIRED	5 HORAS

Actividad	Responsable	Tiempo Estimado
validad la falla esta requiera realizar un gran esfuerzo para reestablecer el sistema, se valida la opción de restaurar los ambientes tanto de aplicación como de base de datos, los cuales están respaldados. Para lo cual se contacta al proveedor de los respaldos y se realiza la solicitud de restaurar la información necesaria, se valida la información restaurada, se realizan las configuraciones respectivas, se realizan las pruebas correspondientes y se activa nuevamente en producción el sistema.		

ANEXO 3. PLAN DE ACCIÓN SOPORTE

Objetivo general

Mantener la operatividad del equipo informático corrigiendo y manteniendo, preventivamente fallos en los equipos de cómputo del parque tecnológico de la institución, para asegurar su correcta operación.

Objetivos específicos

1. Mantener de forma operativa los equipos de cómputo de la institución disminuyendo los costos de reemplazo y reparación.
2. Garantizar la continuidad de las labores de los usuarios de TI.
3. Evaluar las condiciones actuales de los equipos de cómputo.
4. Proyectar necesidades presentes y futuras, operacionales y de hardware y software de la institución.

Alcance

Acciones de mantenimiento correctivas enfocadas en la localización de una falla en un dispositivo que ha dejado defuncionar de forma normal durante un periodo determinado (por afectaciones en el hardware o software), con el fin de corregirle lo más pronto posible.

El mantenimiento preventivo se basa en inspecciones regulares programadas, las cuales se realizan a los dispositivos con el fin de detectar daños o desgastes que puedan llegar a provocar una falla imprevista. A diferencia del mantenimiento correctivo, el mantenimiento preventivo trata de evitar que el equipo falle por medio del cambio (deser necesario) de accesorios y partes, antes de que se dañen; a su vez, también determinar las mejoras que se le pueden hacer al equipo de manera que mejore su rendimiento y se actualice a las necesidades del usuario o del software instalado, como, por ejemplo: aumento de memoria RAM.

ANEXO 4: Plan de acción MANTENIMIENTO CORRECTIVO.

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
Notificación de la Incidencia a través del Software de Atención de Requerimientos de TI	Centro de servicio	De 1 a 30 minutos.
Evaluación de la Incidencia.	Técnico asignado a la Incidencia.	De 5 a 15 minutos.
Establecer el origen de la falla y la posible solución.	Técnico de TI	De 5 a 15 minutos, según el tipo de falla.
Activar el plan de contingencia y notificar	Técnico de TI.	Dependiendo de la prioridad de la incidencia.
Llevar a cabo las acciones para restablecer el servicio.	Técnico de TI.	De 5 minutos a 2 horas.
Validar el resultado de las acciones realizadas. (pruebas de acceso)	Técnico de TI.	De 5 a 15 minutos.
Presentar el informe resultado de las acciones realizadas.	Técnico de TI.	De 5 a 15 minutos.

ANEXO 5: PLAN DE ACCION MANTENIMIENTO PREVENTIVO.

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
Programar y ejecutar el mantenimiento preventivo.	Técnicos de TI.	Una vez por semestre.
Determinar y velar por el cumplimiento de Contratos de Mantenimiento y/o tiempos de garantía del Equipo.	Técnicos de TI.	Durante el año laboral.
Determinar las necesidades de equipo y software del parte tecnológico de la institución.	Técnicos de TI.	Durante el año laboral.
Realizar las cotizaciones y licitaciones, para la compra de equipo y software, según las necesidades determinadas.	Técnicos de TI.	Durante el año laboral.
Dar seguimiento a las compras y entrada de equipo y suministros	Técnicos de TI.	Durante el año laboral.
Determinar la obsolescencia y reciclaje del equipo de cómputo.	Técnicos de TI.	Durante el año laboral.

Activar el plan de contingencia y notificar

➤ **Si la computadora es nueva o necesita formateo.** Definir particiones del disco duro. (al

menos dos de usuario) Formatear las particiones creadas.

- Instalar el sistema operativo: Windows 10.
- Instalar programas determinados por TI:
- Office 2016 u Office 365
- Google Chrome.
- Teams.
- Actualización Windows 10, versión 21H2
- Compresor de archivos: Winrar.
- Firma Digital - sfd_Windows_rev_58
- Antivirus Kaspersky 11.7.0.669 o la determinada por TI.
- Adobe Reader (readerdc64_es_xa_crd_mdr_install)
- FortiClientVPNOnlineInstaller_7.0 (si el usuario usa portátil y hace teletrabajo)
 - o Configurar la VPN.
- Cisco Jabber Setup (si el usuario usa portátil y hace teletrabajo)
- Marca de Teletrabajo. (Cuando hace teletrabajo)

Es importante reseñar que es ideal que se pueda tener una o dos computadoras de escritorio completas, o dos computadoras portátiles en bodega, listas para sustituir una computadora que presente un fallo grave y necesite reparación que lleve días, o bien, que necesite reemplazar temporal o permanentemente. O bien, por uso temporal, o persona que ingrese nuevo y necesite equipo.

- **Para usuarios de Sistema Integrado, Bienes Inmuebles, Gestión de Cobro, se debe instalar lo siguiente:**

Configurarles la unidad I:\, de la siguiente manera:

Clic en Equipo, click en pestaña PC, click en ícono Conectar a unidad de red, seleccionar en Unidad, la I; en Carpetadigitar: [\\guess\\sistema](#), luego Finalizar.

Luego en la unidad C:\, copiar de la unidad I: las carpetas: COBRO, COBRORUC y UNICO (esta última está en la unidad I:\ACCESO

Copiar de I:\ACCESO, la carpeta OCX, en el Escritorio y luego el contenido de la carpeta pegada en el Escritorio, pegarlo en C:\WINDOWS\SYSTEM.

Ejecutar como administrador el archivo ACTIVA.OCX y seguir las instrucciones.

Poner los Accesos directos en el Escritorio: Sistema Integrado, Gestión de Cobro, Bienes Inmuebles.

- **Para usuarios del CORE**

En la unidad I:\COR, copiar la carpeta PROSOFT en el Escritorio y del Escritorio, copiar a C:\ A esta carpeta (C:\PROSOFT) dar Clic Derecho, Propiedades, Seguridad, Editar, Agregar, Todos o Everyone, Permitir, Agregar, Aceptar.

Si la conexión del escáner es USB, copiar la carpeta PS_Scanner_PP a C:\, dentro de esta carpeta hay dos archivos tipo aplicación, se deben ejecutar.

Si la conexión del Escáner es en RED, copiar la carpeta PS_Scanner_Red a C:\, dentro de esta carpeta hay cuatro archivos tipo aplicación que se deben ejecutar.

En I:\COR, abrir el archivo DLL.txt, copiar el contenido, pegar y ejecutar en Windows POWER

SHELL. En I:\COR, ejecutar el Sql_serverReportingServices

Poner predeterminado el explorador Microsoft Edge

En Panel de Control, Programas, Activar o desactivar características de Windows, marcar Windows IdentityFoundation 3.5, Aceptar...

Copiar el ícono del CORE en el Escritorio.

Cuando se ejecuta y se ingresa, le pide instalar el APPEON MULTI-BROWSER.

➤ **Para usuarios del GIS**

En la carpeta I:\GIS\ARC GIS-EJECUTALES\ARGIS-10.8.1

Ejecutar el archivo (si es consulta): **ArcReader_Windows_1081_español**
y ejecutar los pasos.

Si es edición, ejecutar el archivo: **ArcGIS_Desktop_1081**, o el archivo:
ArcGIS_DesktopLP_only_1081_español
y ejecutar los pasos.

Luego de la instalación, ejecutar el archivo: **SQL_Client**

Por último, desde I:\GIS poner el acceso directo en el Escritorio: **GIS-CARTAGO.pmf**

➤ **Impresoras**

Las contingencias por impresoras van desde atascos, reconfiguraciones y fallas mayores.

Es importante reseñar que es ideal que se pueda tener una o dos impresoras en bodega, listas para sustituir una impresora que presente un fallo grave y necesite reparación que lleve días, o bien, que necesite reemplazar temporal o permanentemente.

Atascos: Verificar el mensaje para determinar dónde está el atasco, apagar la impresora, abrir la puerta indicada, remover el atasco con el cuidado y herramienta apropiada. (de ser necesario, limpiar o soplar el área afecta para quitar residuos)

Configuraciones: En ocasiones, en ciertas impresoras, se pierde la IP determinada. Se debe verificar IP, y volver a asignar el puerto con esa IP a la impresora, o bien, volver a Agregar la Impresora.

Fallas mayores: Dependiendo del tipo de fallo, se debe valorar y verificar, si la impresora está en contrato de mantenimiento, reportar el fallo a la empresa encargada del soporte. Sino está en contrato de mantenimiento, cotizarla reparación o bien, determinar si se debe discontinuar o reciclar.

ANEXO 6 PLAN DE ACCION INTERNET

Objetivo general

El objetivo de este plan es el de brindar contingencia servicio de internet de la Municipalidad, lo cual nos permitirá dar continuidad a las operaciones y en caso de que se materialice un riesgo poder seguir brindando el servicio que depende de esta herramienta, en un grado aceptable.

Para proporcionar el servicio de conexión a Internet se cuenta con dos canales principales, ambos configurados en el Firewall para que, en caso de caída de uno, el otro continúe proporcionando el servicio.

Objetivos específicos

1. Contar con un plan para que, en caso de fallas en el enlace de internet, los servicios que dependen de estos puedan seguir funcionando.
2. Contar con un plan, para que en caso de que falle el enlace de internet, tener una guía que nos ayude a resolver el incidente.
3. Brindar continuidad a los servicios que dependen del internet.

Alcance:

Se contemplan los enlaces de comunicación permitidos que se utilizan desde la Municipalidad y con acceso a internet, además de los accesos permitidos hacia la red de la institución que viene desde el internet.

FASES DEL PLAN DE CONTINGENCIA SOPORTE AL INTERNET:**➤ Fase de Notificación del incidente**

En caso de que se active alguna falla en los enlaces de internet se debe notificar a las partes interesadas, las cuales serán afectadas por la degradación del servicio de internet, para lo que se debe realizar la siguiente acción:

El encargado de gestionar los convenios con entidades recaudadoras envía correo electrónico o llamada telefónica a los entes recaudadores indicando que se activó una falla en el enlace de internet y que podría causar una degradación en el servicio de conectividad.

El centro de servicios del área de TIC enviar un correo o llamada telefónica al personal de la Municipalidad indicando que se ha generado una falla en el enlace de internet, lo cual podría generar degradación del servicio que depende de la comunicación hacia y desde el internet.

➤ Fase Evaluación del Incidente

Los Ingenieros a cargo evalúan el incidente teniendo en cuenta los aspectos a continuación:

1. Si el problema ocasiona una falla parcial o total.
2. Si el problema es ocasionado por falla con el proveedor del servicio, se contacta al administrador de la cuenta de la Municipalidad, para reportar el incidente.
3. Si la falla es ocasionada por falla en el dispositivo de seguridad perimetral, se contacta al proveedor de soporte a los equipos de seguridad perimetral.

Se debe determinar el impacto y tiempo aproximado para dar solución al incidente.

Los Ingenieros a cargo del área de infraestructura tecnológica evalúan la situación y determinan si es necesario activar o no el plan de contingencia. Se notifica al proveedor del sistema o servicio sobre la falla y al director del área de TIC para que en conjunto se determine la activación del plan de contingencia.

Como parte del plan de continuidad, la Municipalidad cuenta con los siguientes elementos:

Dos enlaces de internet, con proveedores distintos, los cuales se encuentran activos y configurados en SD-WAN, para que en caso de que falle uno de los enlaces el otro pueda seguir soportando el servicio de una forma aceptable en la que los usuarios puedan seguir navegando, aunque sea de una forma más lenta.

Dos equipos de seguridad perimetral, los cuales son el punto donde llegan los enlaces de internet, estos se encuentran configurados Activo / pasivo, lo cual significa que en caso de que el equipo que se encuentra activo falle, el equipo que se encuentra pasivo se activa y toma el rol principal. Se debe hacer un cambio de algunos cables de datos para que el equipo cubra el 100% del rol que tenía el equipo principal.

Posterior a la evaluación se notifica a través de correo electrónico o llamada telefónica a las partes interesadas de los tiempos estimados en la recuperación del sistema o servicio.

➤ **Establecer el origen de la falla y la posible solución**

Los ingenieros a cargo de atender el incidente realizan un análisis con el fin de determinar que originó la falla y cuáles la posible solución para reestablecer el servicio.

Se determinan los recursos necesarios para atender el incidente, se valora el impacto que se está ocasionando y se calcula el tiempo que se podría tardar para reestablecer el servicio.

Responsable	ROL en el proceso
Daniel Ramirez Gonzalez	Director del Área de TIC
Juan Arias Artavia	Sub-Director del Área de TIC
Francisco Monge Pacheco	Infraestructura TIC

En esta fase se determina que originó la falla y cuál es la solución para brindar para restablecer el servicio. Así mismo es necesario determinar los recursos, impactos y tiempos para restablecer el servicio. Se debe especificar los recursos humanos que intervienen en la solución y el rol que tiene cada uno frente a la solución que se dará.

Solo en caso de que la falla deje en indisponibilidad uno de los servicios críticos en horas laborales y que se determine que se tomará más de 4 horas en el restablecimiento de este se activará el plan de contingencia detallado en los anexos de este documento.

➤ **Activar el plan de contingencia y notificar**

En esta fase se activa el plan de contingencia y se informa a los interesados el tiempo que tomará en restablecerse el servicio.

➤ **Llevar a cabo las acciones para restablecer el servicio**

En esta fase se llevan a cabo las actividades planteadas en los anexos de este documento para cada sistema o servicio que presente la falla.

➤ **Validar el resultado de las acciones realizadas**

Una vez se surten las actividades definidas en cada uno de los planes individuales de acuerdo con la contingencia presentada, es necesario realizar las validaciones para verificar el estado de estas acciones. Así mismo después de que la contingencia sea superada es necesario realizar el respectivo seguimiento por un lapso de tiempo para poder determinar que la contingencia ha sido superada con éxito.

➤ **Presentar el informe resultado de las acciones realizadas**

Toda vez que finalicen las actividades de los planes y una vez superada la contingencia es necesario

presentar el respectivo informe que contenga la información suficiente para permitir tomar acciones correctivas o preventivas a fin de que esta no vuelva a ocurrir. Por lo tanto, se debe contar con datos como:

1. Origen de la contingencia - Qué provocó la falla.
2. Actividades realizadas para corregir la falla.
3. Actividades realizadas para atender la contingencia y dar continuidad al negocio.

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
Actualmente la Municipalidad cuenta con enlaces de internet, con los cuales se realiza la comunicación entre la red externa (internet) y las redes internas de la institución, es el medio de comunicación por el cual se prestan servicios tales como: • Conectividad con entidades recaudadoras. • Conexión por medio de VPN con personal que realiza teletrabajo. • Conexión por medio de VPN con personal que brinda soporte técnico. • Se publican servicios web a los ciudadanos, tales como el portal Municipal. • Se publican trámites en línea no presenciales y semipresenciales. • Navegación hacia internet de los usuarios. Los cuales podrían verse afectados por fallas en los enlaces de internet. Para lo que se debe seguir los siguientes pasos: • Los Ingenieros a cargo evalúa el incidente teniendo en cuenta los aspectos a continuación: • Si el problema ocasiona una falla parcial o total. • Si el problema es ocasionado por falla con el proveedor del servicio, se contacta al administrador de la cuenta de la Municipalidad, para reportar el incidente al número telefónico que se indica, según el proveedor del servicio: • ICE: 800 SOPORTE línea de internet 17314490	Infraestructura tecnológica	4 horas



DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
• JASEC: 2553-2684 • Si la falla es ocasionada por falla en el dispositivo de seguridad perimetral, se contacta al proveedor de soporte a los equipos de seguridad perimetral. • Enviando un correo electrónico a la dirección soporte@sefisa.com y Bernardo García Chaverri • bgarcia@sefisa.com • Si la falla está ocasionando problemas críticos, se debe contactar a don Bernardo al número: 8301 7643 • Se debe determinar el impacto y tiempo aproximado para dar solución al incidente. • Los Ingenieros a cargo del área infraestructura tecnológica evalúan la situación y determinan si es necesario activar o no el plan de contingencia. Se notifica al proveedor del sistema o servicio sobre la falla y al director del área de TIC para que en conjunto se determine la activación del plan de contingencia. • Como parte del plan de continuidad, la Municipalidad cuenta con los siguientes elementos: • Dos enlaces de internet, con proveedores distintos, los cuales se encuentran activos y configurados en SD-WAN, para que en caso de que falle uno de los enlaces el otro pueda seguir soportando el servicio de una forma aceptable en la que los usuarios puedan seguir navegando, aunque sea de una forma más lenta, pero aceptable. • Dos equipos de seguridad perimetral, los cuales son el punto donde llegan los enlaces de internet, estos se encuentran configurados activo / pasivo, lo cual significa que en caso de que el equipo que se encuentra activo falle, el equipo que		

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
está pasivo se activa y toma el rol principal. Se debe hacer un cambio de algunos cables de datos para el equipo cubra el 100% de del rol que tenía el equipo principal. • Se deben tomar fotografías para tener como respaldo de la colocación de los cables. • Posterior a la evaluación se notifica a través de correo electrónico o llamada telefónica a las partes interesadas de los tiempos estimados en la recuperación del sistema o servicio.		

ANEXO 7 PLAN DE ACCION CORREO INSTITUCIONAL

Objetivo general

El objetivo de este plan es el de brindar contingencia al servicio de correo electrónico de la Municipalidad, lo cual nos permitirá dar continuidad a las operaciones y en caso de que se materialice un riesgo poder seguir brindando el servicio que depende de esta herramienta, en un grado aceptable.

Objetivos específicos

1. Contar con un plan para que, en caso de fallas en el servicio de correo electrónico, los servicios que dependen de esto puedan seguir funcionando.
2. Contar con un plan, para que en caso de que falle en el servicio de correo electrónico, tener una guía que nos ayude a resolver el incidente.
3. Brindar continuidad a los servicios que dependen del servicio de correo electrónico.

Alcance

Este plan contempla la contingencia al servicio de correo electrónico tanto de Microsoft Office 365 como el que se encuentra en el servidor de Exchange institucional on premise.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
El servicio de correo electrónico es utilizado en varios procesos, en los cuales se tiene comunicación entre el remitente y destinatario. Como parte de manejo de riesgo y con el fin de contar con plan de contingenciase debe mantener contratos de soporte yrespaldos de información y del servidorde correos electrónico interno, para que, en caso de materializarse alguna falla, se pueda contactar a la parte experta eneste tema para que ayude a solucionar elproblema. En caso de que se presenten fallas en elservicio se deben realizar las siguientes tareas: Se debe determinar la afectación de losservicios, identificando el incidente, tomando en cuenta: ✓ Si es a una sola cuenta. ✓ Varias cuentas. ✓ Cuentas de correo que están enel servidor de Exchange. ✓ Cuentas de servicio de Office365. La Municipalidad cuenta con una arquitectura hibrida en el servicio de correo electrónico, lo cual significa que algunas cuentas se encuentran en Microsoft Office 365 y otras en el servidor de Microsoft Exchange (on premise) Al identificar la afectación se deben tomar acciones, según corresponda: Si es una sola cuenta, el incidente lo atiende personal de soporte, en el cual valida si se venció la contraseña o si es necesario brindar mantenimientopreventivo al equipo. Si son varias cuentas, se debe	- Infraestructura Tecnológica -Soporte técnico -Proveedor del servicio de Correo	2 horas

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
determinar si estos buzones están en O365 o en Exchange local. Si están en Exchange local, se debe revisar el servidor, que este cuente con suficientes recursos tanto en disco, memoria y procesamiento para poder brindar el servicio de forma eficiente, además se debe verificar que los servicios relacionados al Microsoft Exchange estén en estado corriendo. En última instancia se debe reiniciar el servidor y al iniciar hay que verificar que los servicios de Microsoft Exchange estén en estado corriendo. Si son varias cuentas y se determina que los buzones están en Office 365, se debe revisar los Comunicados de Microsoft para ver si algo indica el por qué hay pérdida del servicio de correo, si no existe comunicado, se debe contactar a la empresa contratada para brindar el soporte. Si el servicio de office 365 está suspendido por falta de contrato (pago), se debe migrar las principales cuentas de correo electrónico al servidor de correo interno Exchange, mientras se soluciona el problema de suspensión de la cuenta. Se debe tener presente que el contrato del servicio de Office 365 se debe renovar en el mes de abril, por lo que el proceso de contratación se debe iniciar con un tiempo prudencial para que dé tiempo de tener el contrato listo antes que venza el contrato actual. Luego de haber identificado la causa, se debe enviar un comunicado a los usuarios internos, indicando que hay problemas con el servicio de correo electrónico y cuanto es el tiempo estimado de		

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
solución del problema. Luego de haber solucionado el incidente, se debe: ✓ Documentar la solución Enviar comunicado del restablecimiento del servicio		

ANEXO 8 PLAN DE ACCION ACTIVE DIRECTORY

Objetivo general

El objetivo de este plan es el de brindar contingencia al directorio activo de la Municipalidad, lo cual nos permitirá dar continuidad a las operaciones y en caso de que se materialice un riesgo poder seguir brindando el servicio que depende de esta herramienta, en un grado aceptable.

Objetivos específicos

1. Contar con un plan para que, en caso de fallas en el sistema de Active Directory, los servicios que depende esto puedan seguir funcionando.
2. Contar con un plan, para que en caso de que falle en el sistema de Active Directory, tener una guía que nos ayude a resolver el incidente.
3. Brindar continuidad a los servicios que dependen del sistema de Active Directory.

Alcance

Este plan contempla la contingencia a la herramienta de Active Directory, incluye los elementos que se deben tomar en cuenta para que, en caso de falla en el sistema, poder contar con la redundancia necesaria para que esta no afecte los demás servicios.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.



DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
La Municipalidad cuenta con un dominiolocal con el nombre muni-Cartago. local. El controlador de dominio y Directorio Activo (Active Directory) está instalado en varios servidores, esto para tener plan de contingencia, para que en caso de que uno de los servidores falle, los otros puedan soportar el servicio. Se debe contar con contratos de soporte especializado, para que, en caso de falla, poder escalar el incidente se puedaescalar el caso. Estos se encuentran instalados en los siguientes servidores. SERVIDOR: SVCADTI01 DIRECCION IP: 192.168.0.41TIPO EQUIPO: VIRTUAL UBICACIÓN: RED LOCAL/DC PALACIO SERVIDOR: SFCADTI01 DIRECCION IP: 192.168.0.42TIPO EQUIPO: FISICO UBICACIÓN: RED LOCAL/DC PALACIO SERVIDOR: SFCADTI02 DIRECCION IP: 192.168.0.43TIPO EQUIPO: FISICO UBICACIÓN: RED LOCAL/DC PALACIO SERVIDOR: SACADTI01 DIRECCION IP: 172.20.0.41TIPO EQUIPO: VIRTUAL UBICACIÓN: AZURE	Infraestructur a Tecnológica Francisco Mong ePacheco Dirección / Sub-Dirección del áreade TIC Daniel Ramire zGonzalez. Juan Arias Artavia	4 horas
SERVIDOR: SACADTI02 DIRECCION IP: 172.20.0.42TIPO EQUIPO: VIRTUAL UBICACIÓN: AZURE		

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
Estos servicios se encuentran configurados tanto en servidores físicos como virtuales, así como ubicados físicamente en el Data Center principal dela Municipalidad como en el Tenant de Microsoft Azure, la distribución porubicación es la siguiente: Servidor físico localizado en el Data Center del Palacio Municipal. 1 SFCADTI0 2 Servidor virtual localizado en el Data Center del Palacio Municipal. SVCADTI01 Servidor virtual localizado en el Tenant de Microsoft Azure. SACADTI02 Estos servidores se encuentran siempre activos y con los servicios corriendo en línea, por lo que si algo le pasa a alguno de los servidores los otros equipos soportarían el proceso y no habría afectación. Aunque existan varios servidores corriendo este servicio, en caso de algunafalla en uno de los servidores, se debe reestablecer el servidor lo antes posible para evitar que se vea afectado el serviciopor la activación de fallas en los otros servidores. En caso de que el servicio no pueda ser reestablecido por el personal interno acargo, se debe escalar el caso a la empresacontratada para brindar soporte a este servicio.		

ANEXO 9 PLAN DE ACCION REGISTRO EN LINEA

Objetivo general: Registro en línea para el control de participantes o ciudadanos en cursos, actividades o talleres municipales.

Objetivos específicos: Registro en línea para el control de datos y participación del ciudadano cartaginés en las actividades, cursos o talleres que brinda las diferentes dependencias del municipio.

Alcance: El alcance de este plan contempla dar continuidad al aplicativo o sistema de Registro en línea en caso de falla y que se necesite restituir el servicio.

Plan de acción

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
192.168.0.222: Ubicación Websites\reglinea.muni- carta.go.cr (Publicación del Sitio a lo externo de la institución: http://reglinea.muni-carta.go.cr / Descripción del Sitio: Sitio de registro del ciudadano para participar en las Actividades creadas por las dependencias municipales.	Empresa Proveedora encargada de Respaldos Infraestructura	Tiempo estimado para obtener la información de respaldo: 3Hrs. Tiempo estimado para publicar el sitio de forma externa en nuestros servidores: 2H.
192.168.0.16: Ubicación Websites\reglineaadmin.muni- carta.go.cr (Publicación del Sitio a lo externo de la institución: http://regadmin.muni- carta.go.cr / Descripción del Sitio: 1- Sitio para la administración de los datos registrados por los participantes o ciudadanos en actividades municipales. 2- Además de la creación de los Cursos, talleres o actividades que se van a visualizar en el formulario de registro del ciudadano. 3- Generación o envío de campañas masivas de Correo Electrónico a las personas registradas en todos los cursos generados por el municipio.	Empresa Proveedora encargada de Respaldos Infraestructura	Tiempo estimado para obtener la información de respaldo: 3 Hrs. Tiempo estimado para publicar el sitio de forma externa en nuestros servidores: 2H.
192.168.0.166: Ubicación Base de Datos: reglinea.muni-carta.go.cr	Empresa Proveedora encargada de Respaldos	Tiempo estimado para obtener la información de respaldo: 2Hrs.
	Encargado Base de Datos	Tiempo estimado para publicar el sitio de forma externa en nuestros servidores: 1H.

ANEXO 10 PLAN DE ACCION SIPORE

Objetivo general: Sistema desarrollado para el control de Informes Policiales (Área de Seguridad)

Objetivos específicos: Sistema desarrollado para el control de registro y estadístico:

1. Informes policiales
2. Registro de actuaciones policiales
3. Actas de Observación
4. Actas de Prevención

Alcance

El alcance de este plan contempla dar continuidad al aplicativo o sistema policial de reportes (SIPORE) encaso de falla y que se necesite restituir el servicio.

Plan de acción

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
192.168.0.222: Ubicación Websites\aseguridad.muni- carta.go.cr (Publicación del Sitio a lo interno de la institución: http://aseguridad.muni-carta.go.cr Nota: Su funcionalidad depende del funcionamiento de la Base de Datosreglinea.muni-carta.go.cr, ya que en esta se encuentra la tabla del Padrón Nacional para la validación de números de Identificación.	Empresa Proveedora encargada de Respaldos Infraestructura	Tiempo estimado para obtener la información de respaldo: 3 Hrs. Tiempo estimado para publicar el sitio de forma interna en nuestros servidores: 2H.
192.168.0.166: Ubicación Base de Datos: seguridad.muni-carta.go.cr	Empresa Proveedora encargada de Respaldos Encargado Base de Datos	Tiempo estimado para obtener la información de respaldo: 2 Hrs. Tiempo estimado para publicar el sitio de forma externa en nuestros servidores: 1H.

ANEXO 11 PLAN DE ACCION SISTEMA DE REQUERIMIENTOS AREA TIC

Objetivo general: Sistema para el control de los requerimientos de las dependencias municipales.

Objetivos específicos: Sistema para el control de requerimientos del usuario interno de las diferentes

dependencias municipales por medio de los diferentes contratos de servicio de las diferentes áreas de TI (Soporte, Infraestructura, Desarrollo)

Alcance

El alcance de este plan contempla dar continuidad al aplicativo o sistema de Control de Requerimientos Municipales en caso de falla y que se necesite restituir el servicio.

Plan de acción

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
192.168.0.222: Ubicación Websites\supportadmin.muni- carta.go.cr (Publicación del Sitio a lo interno de la institución: <a href="http://supportadmin.muni-
carta.go.cr">http://supportadmin.muni- carta.go.cr Descripción: Sitio Web para la Administración de los requerimientos presentados por los usuarios municipales.	Empresa Proveedora encargada de Respallos Infraestructura	Tiempo estimado para obtener la información de respaldo: 3 Hrs. Tiempo estimado para publicar el sitio de forma externa en nuestros servidores: 2H.
192.168.0.16: Ubicación Websites\supportuser.muni- carta.go.cr (Publicación del Sitio a lo interno de la institución: <a href="http://supportuser.muni-
carta.go.cr">http://supportuser.muni- carta.go.cr Descripción: Sitio Web para la creación o ingreso de requerimientos del usuario municipal.	Empresa Proveedora encargada de Respallos Infraestructura	Tiempo estimado para obtener la información de respaldo: 3 Hrs. Tiempo estimado para publicar el sitio de forma externa en nuestros servidores: 2H.
192.168.0.166: Ubicación Base de Datos: supportuser.muni- carta.go.cr	Empresa Proveedora encargada de Respallos Encargado Base de Datos	Tiempo estimado para obtener la información de respaldo: 2 Hrs. Tiempo estimado para publicar el sitio de forma externa en nuestros servidores: 1H.

ANEXO 12 PLAN DE ACCION SISTEMA DELPHOS

Objetivo general

El objetivo de este plan es el de brindar contingencia al Sistema Delphos de la Municipalidad, lo cual permitirá dar continuidad a los modelos de gestión por resultados que se administran en este sistema, en caso de que se materialice un riesgo, que afecte el sistema, poder seguir brindando el servicio a los colaboradores de forma aceptable.

Objetivos específicos

Contar con un plan para que, en caso de alguna eventual falla en el sistema Delphos, los servicios que dependen de este puedan seguir funcionando, mientras se resuelve el problema que afecte al sistema.

Alcance

Dar continuidad a los modelos de gestión por resultados que se administran en este sistema.

Plan de acción

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
Para el sistema Delphos, se cuenta con una contratación de soporte por un año, con la empresa DEINSA, la cual desarrolló el sistema, dicha contratación contempla.	Funcionario del Área TIC's. responsable de las Bases de Datos.	Emergencia Notificación de interrupción del servicio TIEMPO DE RESPUESTA INICIAL 10 minutos TIEMPO DE RESOLUCION 4 horas
El mantenimiento preventivo y correctivo para el sistema. Garantizar la continuidad del servicio de este sistema.	Funcionario de la <u>Oficina</u> de Control Interno administrador del Sistema.	Crítico El problema está causando un impacto significativo en la productividad TIEMPO DE RESPUESTA INICIAL < 1 horas TIEMPO DE RESOLUCION 8 horas
Mantener y ejecutar las últimas actualizaciones del sistema.	Funcionario de la empresa DEINSA encargado del soporte técnico.	Urgente El problema está causando un impacto parcial en la productividad TIEMPO DE RESPUESTA INICIAL < 3 horas TIEMPO DE RESOLUCION 12 horas
Atención y soporte técnico en caso de fallas del sistema.		Importante
El servicio de soporte y actualización deberá cubrir las siguientes versiones		
✓ Delphos Continuum		
✓ Delphos.Net		

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
		Se sufre interrupciones parciales, pero existe una solución temporal aceptable
		TIEMPO DE RESPUESTA INICIAL
		6 horas
		TIEMPO DE RESOLUCION
		24 horas
		Programado Se programa la solución o mejora del servicio Tiempo Resolución Programado.
Contingencia en caso de falla <i>Sistema Delphos.</i> El Área de Planeamiento desarrolló una serie de herramientas en formato Excel con las cuales se determina la información primordial para iniciar cada uno de los modelos. Sistema Delphos Net 6F10 Matriz de vinculación PAO-Presupuesto. Y PLAN DE TRABAJO ANUAL (PTA) Sistema Delphos Continuum. Modelo SEVRI 6F28, Acción Aplicada. 6F29, Administración de riesgos. 6F31 Registro y Control Plan de Acción. 6F32, Carta de Riesgos Priorizados. Modelo Autoevaluación de Control Interno.		

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
Cuestionario de autoevaluación, este se renueva año con año. 6F34 Carta de compromiso de Autoevaluación Control Interno. 6F35 Registro y Control Planes de Acción Autoevaluación.		
Plan de recuperación del Sistema Delphos. El Área de TIC's cuenta con un centro de datos principal, en el cual se encuentran los equipos que contienen los diferentes servidores de aplicación y de bases de datos, que para el caso del sistema Delphos, la aplicación se encuentra instalada en un servidor virtual, en el caso de la base de datos esta se encuentra en un servidor virtual dedicado exclusivo para tal fin, por lo que en caso de falla de alguno de los servidores no se verá afectada su contraparte.	Funcionario del Área TIC's. responsable de las Bases de Datos. Funcionario del Área TIC's. responsable de la Infraestructura.	Emergencia Notificación de interrupción del servicio TIEMPO DE RESPUESTA INICIAL 10 minutos TIEMPO DE RESOLUCION 4 horas Crítico

ANEXO 13 PLAN DE ACCION PORTALES WEB

Objetivo general

Recuperar la funcionalidad del portal web de la Municipalidad de Cartago, en caso de que se afecte la producción de este.

Objetivos específicos

1. Determinar la causa o motivo por el cual los portales están fuera de línea.
2. Definir las etapas de la recuperación de acuerdo al plan indicado en este documento técnico
3. Coordinar en caso de ser necesario con el proveedor, en caso de que sea necesario escalar el incidente.
4. Realizar pruebas necesarias de validación de acceso y carga del portal web

Alcance

El alcance de este plan se aplica para la restauración en línea de los portales web de la Municipalidad de Cartago el cual es de uso únicamente del Área de TIC.

Plan de acción

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
Validar los servidores que contienen los portales web municipales 192.168.0.155 (aplicación), 192.168.0.152 (web services) y 192.168.0.156 (base de datos SQLSERVER 2016).	Infraestructura	30 min
Verificación o cambio de certificados web en servidor vencen el 28 de enero de cada año	infraestructura	3 horas
WordPress: Revisar la versión que tiene el portal y comparar con la última versión oficial, en caso de ser diferente, actualizar: plugins, certificados de confianza, Se actualiza WordPress a la versión XXX o Versión actual: X.X:X o Versión anterior: X.X:X • Actualizar los siguientes plugins: o Google Language Translator o reCAPTCHA by BestWebSoft o WP Maintenance Mode & Coming Soon o WP Super Cache	Infraestructura en conjunto con proveedor	5-6 Horas
Verificación de espacios en disco en todos los casos debe ser mayor a un 10% de la totalidad del espacio total de cada uno	Infraestructura	1 hora – 2 horas
Portales BackEnd Servicio encargado del pago y consultas de convenio. Validar autenticación a la base de datos crid.muni-cartago.cr.	Infraestructura en conjunto con empresa proveedora.	4 horas.
Problemas de internet verificar servicios de proveedores externos JASEC e ICE para verificar el acceso desde fuera de la municipalidad	Infraestructura en conjunto con empresa proveedora.	4 horas
Respallos de portales web deben realizarse dos veces al día con el fin de evitar pérdidas de información.	Infraestructura en conjunto con empresa proveedora.	6 horas

Es importante resaltar que la municipalidad de Cartago cuenta con un contrato de soporte preventivo y correctivo para los portales web, sus servicios y respaldos externos, los contactos y responsables y datos

de contactos se describen a continuación:

Nombre Contacto	Empresa correo y celular
Carlos José Fernández Montero	Prides s.a < cjfernandez@prides.net > Teléfono 2528-59-09 contrato página web
David Castros Bustamante	Kmsolutions david.castro@kmsolutions.co.cr Teléfono. 7010-7571 Contrato respaldos
Infraestructura	Municipalidad de Cartago, Infraestructura@muni-carta.go.cr 2550-4496

ANEXO 14 PLAN DE ACCION ESTACIONOMETROS

Objetivo general

Recuperar la funcionalidad del sistema de Estacionómetros y terminales de la Municipalidad de Cartago

Objetivos específicos

1. Determinar la causa o motivo por el cual el sistema web de Estacionómetros está fuera de línea.
2. Definir las etapas de la recuperación de acuerdo plan indicado en este documento técnico
3. Realizar pruebas necesarias en el sistema, la aplicación móvil de Estacionómetros, o el sistema de pagos de infracciones

Alcance

El alcance de este plan se aplica para la restauración del sistema de Estacionómetros web, pagos y móvil de laMunicipalidad de Cartago el cual es de uso únicamente del Área de TIC.

Diagrama de arquitectura parquímetros EPARK



Plan de acción

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
Validar que la aplicación E park este activa y funcionando	Epark	30 minutos
El sistema no funciona notificar a la empresa y dueños del proceso	Infraestructura	1 hora
El sistema no transfiere las boletas a las bases de datos municipales desde Epark	Infraestructura-Epark	3 horas
El sistema web no tiene conexión en la red validar la conexión de red inalámbrica o alámbrica conectado a la red LAN municipal	Infraestructura	1 hora

ANEXO 15 PLAN DE ACCION SISTEMA DE RECURSOS HUMANOS**Objetivo general**

Recuperar la continuidad de las operaciones del Sistema de Recursos Humanos de la Municipalidad de Cartago en caso de ocurrir algún evento disruptivo de manera que se pueda seguir trabajando con normalidad en ese departamento.

Los objetivos y actividades de este plan están enfocados en tener la capacidad de poner en operación el sistema que se tiene respaldado en sitio externo a la municipalidad en caso de suceder algún desastre que afecte las funciones normales del departamento lo más pronto posible para darle continuidad a esa parte del negocio.

Objetivos específicos

1. Definir las etapas del plan a seguir para la restauración del sistema.
2. Coordinar con el proveedor que nos brinda el servicio de respaldo para restablecer la aplicación.
3. Llevar a cabo las actividades que se describen en el plan para restablecer el servicio.
4. Realizar pruebas de la integridad y autenticidad de la información recuperada de los respaldos del proveedor del servicio externo el cual realiza cada hora según los cambios que se den en los diferentes componentes del sistema.

Alcance

El alcance de este plan se aplica para la restauración del Sistema de Recursos Humanos de la Municipalidad de Cartago el cual es de uso únicamente en ese departamento.

Plan de acción

Se presentan a continuación las diferentes actividades con sus responsables y tiempo estimado del desarrollo de cada una de ellas.

El sistema de Recursos Humanos está diseñado para funcionar en una plataforma Cliente-Servidor multiusuario y puede instalarse inclusive en una máquina individual aislado de la red si fuera necesario

en ambiente monousuario. El sistema se encuentra ubicado en el volumen [\\SVCVFTI03](#) mapeado con la letra "Y"

Actividades del plan de acción

Restauración del Sistema de Recursos Humanos

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
Activar un servidor para alojar el sistema, crear la unidad \\SVCVFTI03 y mapearla con la letra "Y"	Infraestructura Área TIC	2 horas
Obtener los respaldos completos del sistema que para tal efecto se llevan en sitio externo a la municipalidad	Empresa encargada de los respaldos municipales.	2 horas
Copiar los respaldos en la unidad \\SVCVFTI03 en la carpeta RECURSOH	Desarrollo Área TIC	30 minutos
Crear la carpeta temporal: c:\temppersonal en cada computadora que se vaya a instalar el sistema y copiar en ella los archivos que se encuentran en \\SVCVFTI03 \archivos locales"	Desarrollo Área TIC	5 minutos
Crear el acceso directo a los usuarios de Recursos Humanos del archivo \\SVCVFTI03\recursoh\personal.exe en su respectivo escritorio.	Desarrollo Área TIC	10 minutos por usuario
En caso de que la emergencia sea tan grande que no permita recuperar el ambiente de red, el sistema se puede instalar local (stand alone) en una computadora. Para eso se crea en la unidad C una carpeta llamada RECURSOH y ahí se copia el respaldo. Instalar el Visual Fox Pro para tener acceso a la tabla c:\recursoh\bd\camino y cambiar la ruta por "c:\recursoh" Crear en el escritorio el acceso directo al archivo c:\recursoh\personal.exe	Desarrollo Área TIC	2 horas

ANEXO 16 PLAN DE ACCION SISTEMAS BIENES INMUEBLES

Objetivo general

Mantener la continuidad de las operaciones realizadas por el Área Tributaria, Tesorería y Contabilidad en

cuanto a las transacciones que estén vinculadas al impuesto sobre Bienes Inmuebles.

Los objetivos y actividades de este plan están enfocados en restaurar la funcionalidad de todos los aplicativos que tiene que ver con el impuesto sobre Bienes Inmuebles en caso de ocurrir algún evento disruptivo que pueda afectar el funcionamiento del Área de TIC y recuperar de esta manera lo más pronto posible la normalidad de las operaciones.

Objetivos específicos

1. Definir las etapas del plan a seguir para la restauración de las aplicaciones relacionadas con Bienes Inmuebles.
2. Coordinar con el proveedor externo que tiene a cargo el servicio de respaldo para obtenerlos y poder descargarlos de acuerdo con la ubicación correspondiente.
3. Llevar a cabo la ejecución de cada una de las actividades descritas en el plan definido a continuación.
4. Tomar las acciones respectivas para realizar las pruebas de integridad y autenticidad de la información descargada de los respaldos del servicio externo y obtener así el visto bueno por parte de los usuarios respectivos.

Alcance

Este plan de acción comprende la restauración de la funcionalidad de todos los aplicativos desarrollados en la municipalidad que tengan que ver con el impuesto sobre Bienes Inmuebles.

Toda la información relacionada con el impuesto de Bienes Inmuebles se encuentra alojada en el volumen [\\guess\soft](#) en la carpeta RUC.

Las aplicaciones de Bienes Inmuebles pueden funcionar en una plataforma Cliente-Servidor multiusuario y también en una máquina individual aislada de la red si fuera necesario en ambiente stand alone.

Actividades del plan de acción

Restauración de los aplicativos de Bienes Inmuebles

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
Coordinar la activación de un servidor para alojar el respaldo, debe tener el volumen \\guess\soft , mapearlo con la letra "Z".	Infraestructura Área TIC	2 horas
Obtener los respaldos completos del sistema que para tal efecto se llevan en sitio externo a la municipalidad	Empresa encargada de los respaldos municipales	4 horas
Copiar los respaldos en el volumen \\guess\soft en la carpeta RUC.	Desarrollo Área TIC	4 horas
Crear las carpetas temporales: cobro ruc, cobro y único en la unidad "C" de cada computadora donde se vaya a instalar el acceso directo a los sistemas. "Esto se realiza solo en caso de que haya afectación en las computadoras y se tengan que formatear" de otra manera los archivos locales permanecen ahí con toda la funcionalidad.	Desarrollo Área TIC	10 minutos por usuario

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
Crear los accesos directos a los sistemas: Consulta de Bienes inmuebles: \\guess\soft\ruc\bienes\biengrafruc.exe Este acceso se les instala a todos los funcionarios que realicen consultas del IBI.	Desarrollo Área TIC Encargados de Soporte	10 minutos por usuario
Cobro de Bienes Inmuebles: \\guess\soft\ruc\bienes\cobrobiegrafruc.exe Se les instala únicamente a los cajeros del departamento de Tesorería. Exoneraciones (no afectación por inmuebleúnico) de Bienes Inmuebles: \\guess\soft\ruc\bienes\oficiosexon.exe Se les instala a los funcionarios de BienesInmuebles y a los plataformistas. Gestión de Cobro Administrativo: \\guess\soft\ruc\bienes\bienesruccobroa.d.exe Se les instala únicamente a los funcionarios del departamento de Cobro Administrativo. Prevención de avalúos: \\guess\soft\ruc\bienes\avaluos\avaluos.exe. Se les instala a los funcionarios del departamento de Valoración. Modificación a las bases de datos: \\guess\soft\ruc\bienes\ruc.exe. Se les instala a los funcionarios de Bienes Inmuebles y Valoración que están autorizados para llevar a cabo modificaciones a las bases de datos.		

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
Migración BI-Core: \\guess\soft\ruc\bienes\migraciónparcial.exe. Se debe crear una tarea programada en Windows que ejecute esa aplicación para que se haga de manera automática todas las noches a las 11:00 p.m.	Desarrollo Área TIC	

ANEXO 17 PLAN DE ACCION CONECTIVIDAD

Objetivo general

Describir los detalles del plan de acción para la conectividad de tributos municipales a través de las

plataformas bancarias y no bancarias.

Objetivos específicos

1. Establecer los mecanismos que permitan mantener los distintos elementos involucrados en la conectividad en adecuado funcionamiento.
2. Permitir brindar la documentación necesaria para orientar al personal de TIC en caso de alguna falla que se genere en la conectividad.

Alcance

El alcance de este plan se aplica para la restauración del sistema de conectividad de la Municipalidad de Cartago.

Plan de acción

Se presentan a continuación las diferentes actividades con sus responsables y tiempo estimado del desarrollo de cada una de ellas.

El sistema de conectividad está diseñado para funcionar en una plataforma Cliente-Servidor multiusuario y puede instalarse en una máquina virtual que permita el adecuado funcionamiento del sistema.

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
En caso de identificarse un fallo en la Conectividad se debe seguir los siguientes pasos: En el servidor VSRV-MCSOCK-01 (192.168.0.9) se encuentra el primer servicio de socket el cual está instalado mediante un servicio de Windows. Este socket es el que permite el enlace entre las entidades recaudadoras y la plataforma interna municipal. Este socket administra los tributos de servicios municipales, patentes municipales, mercado municipal y permisos de construcción. En el caso de infracciones por estacionamiento y bienes inmuebles solo pasan a través de este socket y se dirigen al socket ubicado en server SVCSKTP01 (192.168.0.206) que se detalla más adelante. Ir a los servicios de Windows y buscar el servicio llamado Socket producción Prosoft, y verificar que el servicio está con estado ejecución.	Infraestructura Área TIC	60 minutos o menos
Para verificar el socket que administra los tributos de infracciones por estacionamiento y Bienes Inmuebles usar escritorio remoto en el servidor SVCSKTP01 (192.168.0.206) se debe ingresar con el usuario municipal\administrator y debe estar activa la	Infraestructura Área TIC	60 minutos o menos

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
siguiente pantalla activa y abierta del aplicativo llamado AsyncServer.exe  En caso de no estar activa o presentar algún error se debe cerrar la ventana y abrir en la carpeta C:\socket\25-02-08\ el archivo llamado conecta.bat, el cual activará la pantalla del socket y se procederá a abrir la ventana respectiva, quedando habilitado el socket. En caso de que el socket AsyncServer.exe falle se deberá revisar las bases de datos llamada socket y BDInteres que esté disponible como activa en el servidor VSRV-MC SOCK-01 (192.168.0.9).		

ANEXO 18 PLAN DE ACCION TELEFONIA IP NUBE

Objetivo general

Describir los detalles del plan de acción para la conectividad de tributos municipales a través de las plataformas bancarias y no bancarias.

Objetivos específicos

1. Identificar los elementos involucrados en la plataforma de telefonía.
2. Describir los elementos que componen la telefonía IP.
3. Lograr el adecuado funcionamiento de la telefonía.

Alcance

El alcance de este plan se aplica para la restauración del sistema de telefonía IP de la Municipalidad de Cartago, que permite la comunicación telefónica en los distintos edificios municipales que posean acceso a la red local.

Plan de acción

Este plan de acción comprende la restauración de la funcionalidad del sistema de telefonía IP usada en los distintos edificios que tienen comunicación con la red local municipal.

La plataforma de telefonía IP debe instalarse en un servidor físico que permita el adecuado funcionamiento. Se cuenta con un contrato que cubre el hardware, soporte y licenciamiento para el sistema de telefonía IP.

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
El sistema de telefonía IP se encuentra ubicado en la nube de Cisco los servidores se encuentran en alta disponibilidad lo cual, ante un fallo de uno de los servidores, el otro servidor tomaría el rol y permitiría continuar el funcionamiento del sistema de la telefonía.	Infraestructura Área TIC	60 minutos
Adicionalmente se cuenta para el sistema de telefonía IP con un contrato el cual asegura la garantía sobre los equipos de hardware, licenciamiento y soporte de horas, ante un fallo, se coordina con el proveedor para el reemplazo de los servidores y la respectiva configuración.	Infraestructura Área TIC	8 a 24 horas

Anexos a Plan de contingencia tecnológica 2024-2025 Municipalidad de Cartago Aplicación y cronograma

Para la Municipalidad de Cartago, es muy importante asegurar la operación y continuidad del negocio. Por tal motivo, ha decidido planear, implementar y mejorar un Plan De Contingencia Tecnológica, en adelante PCT, para identificar la infraestructura física, tecnológica, procesos críticos y sobre todo los riesgos de tipo catastróficos y así definir estrategias, con el fin de reducir los tiempos de recuperación, garantizando la continuidad de las operaciones y la gestión de los riesgos que pudieran afectar la continuidad de la Institución para esta tarea se definió un Plan de continuidad tecnológica formalizado por el señor Alcalde en el mes de diciembre del 2023, a partir de ese plan se realiza el siguiente detalle de aplicación para el año 2024.

Plantilla de documentación : Evidencia Continuidad tecnológica

La misma debe incluir al menos :

- A. PRESENTACIÓN (ANTECEDENTES): Cuales y porque se realizan las tareas.
- B. DESCRIPCIÓN: del proceso que se va a realizar.
- C. OBJETIVOS: Que se espera alcanzar con la tareas a desarrollar.
- D. ALCANCE: Hasta , donde se espera llegar con este proceso, que abarca , requiere ventanas de tiempo.
- E. INVOLUCRADOS: Quienes son los actores claves, funcionarios, aprobadores.
- F. GLOSARIO DE DEFINICIONES Y/O ABREVIATURAS IMPORTANTES: De terminos utilizados.
- G. LINEAMIENTOS: Permisos , reglas, comunicaciones previas, confidencialidad.
- H. DESARROLLO: Imágenes del proceso y resultados.
- I. ANEXOS: Documentación llena de cada etapa firmada por cada uno de los integrantes del proceso.

Cronograma de Aplicación

Según lo detallado en el Plan de contingencia tecnológica se deben llevar a cabo simulacro y pruebas como mínimo cada 6 meses, con el fin de aplicar el mismo y atender las recomendaciones del CSIRT, se realiza el siguiente cronograma para aplicarlo cada 3 meses como mínimo durante este año 2024.

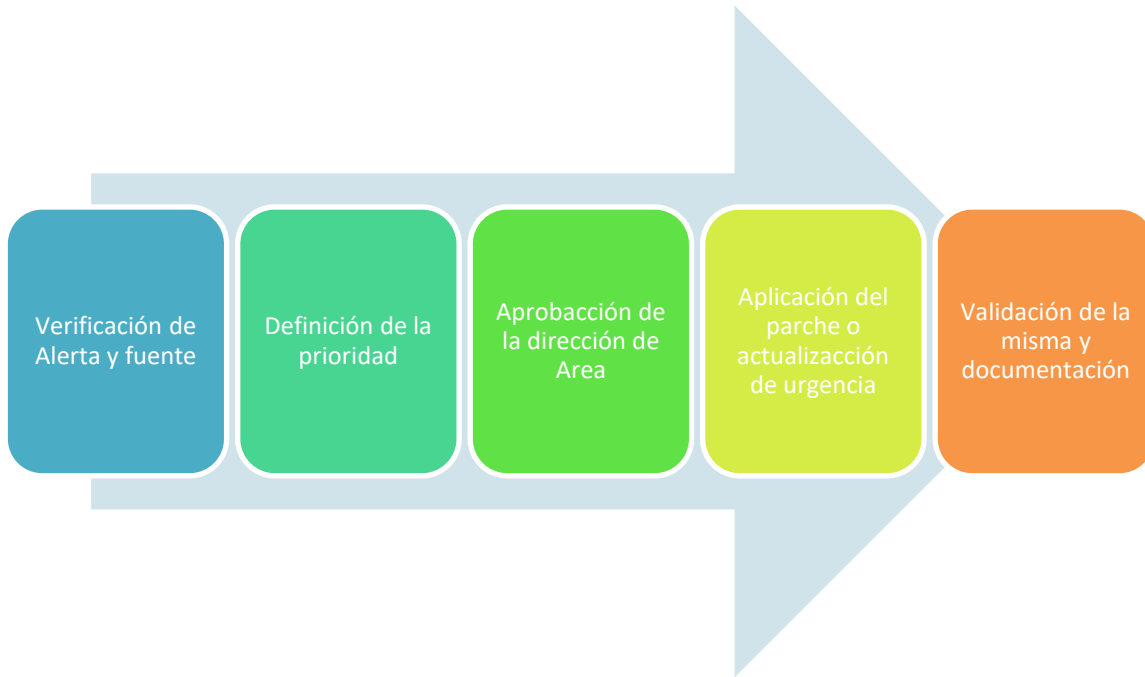
Cronograma de Aplicación Plan de contingencia tecnológica 2024 Municipalidad de Cartago			
Mes de Aplicación	Alcance	Funcionarios	Aprobador
Marzo 2024 Marzo 2025	Actualización de la plataforma tecnológica municipal y aplicación de parches	Funcionarios Area de TIC	Encargado de Area de TIC
Julio 2024 Julio 2025	Actualización de la plataforma tecnológica municipal y aplicación de parches	Funcionarios Area de TIC	Encargado de Area de TIC
Setiembre 2024 Setiembre 2025	Actualización de la plataforma tecnológica municipal y aplicación de parches	Funcionarios Area de TIC	Encargado de Area de TIC
Diciembre 2024 Setiembre 2025	Actualización de la plataforma tecnológica municipal y aplicación de parches	Funcionarios Area de TIC	Encargado de Area de TIC

PARCHES DE EMERGENCIA Y CIBERSEGURIDAD

El Plan de ciberseguridad toma como base el marco de referencia COBIT 2019 y el NIST estos se complementan de varias maneras para proporcionar una estructura completa y efectiva para gestionar la ciberseguridad.

- Garantizar la seguridad de todos los activos digitales, incluyendo datos sensibles, sistemas críticos y redes.
- Identificar y evaluar continuamente los riesgos cibernéticos para implementar medidas proporcionadas de mitigación.
- Asegurar el cumplimiento de todas las normativas y regulaciones relevantes que apliquen a la Municipalidad de Cartago en materia de ciberseguridad.
- Desarrollar capacidades de respuesta efectivas para minimizar el impacto de posibles incidentes y garantizar la continuidad del negocio.
- Fomentar una cultura de ciberseguridad mediante programas de formación y concientización para todo el personal

En el caso de aplicación de temas de urgencia a nivel de ciberseguridad se seguirá el siguiente diagrama



DOCUMENTACION Y UBICACION

Todo el proceso de documentación debe estar disponible en la intranet municipal, bajo los estándares de seguridad definidos en las políticas aplicadas en el Área de TIC, específicamente en la sección de infraestructura, la información almacenada allí tiene carácter confidencial