CONCEJO MUNICIPAL DE CARTAGO – VALLE DEL CAUCA

PLAN CONTINUIDAD DIGITAL DEL CONCEJO MUNICIPAL DE CARTAGO

Cartago, Vigencia 2024

INTRODUCCION

En la era digital actual, las fallas y eventos tecnológicos son inevitables y forman parte integral de la realidad operativa de las organizaciones. El Concejo Municipal de Cartago, como entidad clave en la administración local, no es una excepción a esta regla. Las interrupciones en los sistemas tecnológicos pueden derivarse de múltiples fuentes, como fallos de hardware, ataques cibernéticos, desastres naturales o errores humanos. Estos eventos tienen el potencial de afectar gravemente la capacidad del Concejo para ofrecer servicios esenciales a la comunidad y mantener la continuidad de sus operaciones.

Reconociendo la importancia crítica de mantener la operatividad en todo momento, el Concejo Municipal de Cartago se compromete a implementar un Plan de Continuidad Tecnológica. Este plan tiene como objetivo principal garantizar que, ante cualquier evento disruptivo, la organización pueda recuperar sus servicios tecnológicos de manera rápida y efectiva, volviendo a la normalidad en el menor tiempo posible.

El Plan de Continuidad Tecnológica del Concejo Municipal de Cartago se ha diseñado para abordar y mitigar los impactos de las interrupciones tecnológicas mediante la implementación de estrategias claras y bien definidas. Este plan no solo busca asegurar la recuperación de los sistemas afectados, sino también mantener la confianza de la comunidad al garantizar que los servicios públicos esenciales continúen funcionando sin interrupciones prolongadas.

A través de la identificación de riesgos potenciales, el establecimiento de procedimientos de respaldo y recuperación, y la capacitación continua del personal, el Concejo Municipal de Cartago se prepara para enfrentar cualquier desafío tecnológico con un enfoque proactivo. Este plan integral proporciona un marco para la recuperación efectiva, minimizando el tiempo de inactividad y asegurando que los recursos tecnológicos de la organización estén protegidos y disponibles cuando más se necesiten.

PLAN CONTINUIDAD DIGITAL DEL CONCEJO MUNICIPAL DE CARTAGO

1. OBJETIVO:

El objetivo del Plan de Continuidad Tecnológica del Concejo Municipal de Cartago es asegurar la capacidad de la Corporación para mantener y recuperar sus operaciones tecnológicas esenciales ante cualquier interrupción o evento disruptivo. Este objetivo se desglosa en los siguientes propósitos específicos:

- Garantizar la Disponibilidad de Servicios Críticos: Asegurar que los servicios tecnológicos fundamentales para la administración y operación del Concejo Municipal, tales como sistemas de gestión de documentos, plataformas de comunicación, y aplicaciones de gestión pública, permanezcan disponibles o se restauren rápidamente en caso de fallo.

- Minimizar el Tiempo de Inactividad: Reducir al máximo el tiempo de inactividad de los sistemas y servicios tecnológicos para minimizar el impacto en la operatividad del Concejo Municipal y garantizar que los servicios a la ciudadanía no se vean interrumpidos por períodos prolongados.

- Proteger la Integridad y Confidencialidad de la Información: Implementar medidas para asegurar que la información crítica y sensible, incluyendo datos personales y registros administrativos, esté protegida durante y después de cualquier evento disruptivo, garantizando su integridad y confidencialidad.

- Establecer Procedimientos Claros de Recuperación: Definir y documentar procedimientos detallados y eficientes para la recuperación de sistemas y datos, asegurando una respuesta coordinada y efectiva en caso de incidentes tecnológicos.

- Fortalecer la Capacidad de Respuesta y Recuperación: Desarrollar la capacidad del personal para gestionar incidentes tecnológicos mediante capacitación continua, simulacros regulares y el mantenimiento de un plan de continuidad actualizado y accesible.

- Asegurar la Comunicación Efectiva durante Incidentes: Implementar un sistema de comunicación claro y efectivo para mantener informados a todos los stakeholders (empleados, ciudadanos y otras partes interesadas) sobre el estado de los sistemas y los pasos que se están tomando para la recuperación.

Al alcanzar estos objetivos, el Concejo Municipal de Cartago estará mejor preparado para enfrentar y superar cualquier desafío tecnológico, manteniendo la confianza pública y asegurando la continuidad y eficiencia en la prestación de servicios a la comunidad.

2. ALCANCE

El **alcance del Plan de Continuidad Tecnológica del Concejo Municipal de Cartago** incluye la protección y recuperación de sistemas críticos como gestión de documentos, plataformas de comunicación, aplicaciones públicas, y la infraestructura de red y servidores. Cubre la salvaguarda de datos personales y registros históricos, establece procedimientos para respaldo, recuperación y respuesta a incidentes, y define roles y responsabilidades del personal, junto con su capacitación.

Además, abarca la infraestructura física y tecnológica, los protocolos de comunicación durante incidentes, y la coordinación con proveedores externos. Finalmente, incluye la revisión y actualización continua del plan para asegurar su efectividad en la preservación de la operatividad del Concejo Municipal.

3. GLOSARIO

- 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.

- 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 que 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.

- Plan de Continuidad de Negocio. Procedimientos documentados que guían orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel pre-definido de operación debido una vez presentada / tras la interrupción.

- Análisis del impacto al negocio (BIA por sus siglas en ingles). Proceso del análisis de actividades las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas. [Fuente: ISO 22300]

- Nivel de Criticidad. Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y operativa constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra.

- Interrupción. Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar el normal curso de las operaciones en alguna de las ubicaciones de la organización.

- Recuperación de desastres de tecnología y telecomunicaciones (ITCTIC). Habilidad Capacidad de los elementos de tecnología y telecomunicaciones (ITC)de las TIC de la organización para soportar sus funciones críticas a un nivel aceptable dentro de un periodo predeterminado de tiempo después de una interrupción.

- Plan de recuperación de desastres de ICT LAS TIC (ICT DRP). Plan claramente definido y documentado el cual permite recuperar las

capacidades de tecnología y Telecomunicaciones LAS TIC cuando se presenta una interrupción.

NOTA: En algunas organizaciones es llamado el plan de continuidad de tecnología y telecomunicaciones las TIC.

- Modo de falla. Manera Forma en por la cual se observa una falla es observada. NOTA: Esta generalmente describe la manera en que la falla ocurre y su impacto para en la operación del sistema.

- Preparación de las ICT TIC para la continuidad de negocio (IRBC). Capacidad de una organización para soportar sus operaciones de negocio mediante la prevención, detección y respuesta a una interrupción, así como la recuperación de sus servicios de ICTTIC.

- Objetivo mínimo de continuidad de negocio (MBCO). Mínimo nivel de productos y/o servicios que es aceptable para que la organización alcance sus objetivos de negocio durante una interrupción.

- Punto objetivo de recuperación (RPO). Punto en el tiempo en el cual los datos deben ser recuperados después de que una interrupción ocurra.

- Punto Tiempo objetivo de tiempo de recuperación (RTO). Periodo de tiempo en el cual los mínimos niveles de productos y/o servicios y los sistemas, aplicaciones, o funciones que los soportan deben ser recuperados después de que una interrupción ocurra.

- Resiliencia. Habilidad Capacidad para que una organización para resistir cuando es afectada al ser afectada por una interrupción.

- Disparador o detonante. Evento que hace que el sistema inicie una respuesta.

  NOTA: También conocido como evento activador.

- Registro vital. Registro electrónico o en papel que es esencial para preservar, continuar o reconstruir las operaciones de una organización y proteger los derechos de una organización, sus empleados, sus clientes y sus partes interesadas.

4. PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO EN EL CONCEJO MUNICIPAL DE CARTAGO

Dentro del proceso de continuidad del negocio, la preparación de las Tecnologías de la Información y Comunicación (TIC) para la continuidad del negocio (IRBC) se refiere a un sistema de gestión que complementa y apoya el Plan de Seguridad de TI del Concejo Municipal de Cartago. Este sistema tiene como objetivo mejorar la capacidad de la entidad para:

a) Adaptarse a un entorno de riesgos en constante cambio.

b) Asegurar la continuidad de las operaciones críticas respaldadas por servicios de TIC.

c) Prepararse para anticipar y responder a posibles disrupciones en los servicios de TIC, identificando eventos o series de eventos relacionados con incidentes.

d) Responder y recuperarse de incidentes, desastres y fallas, minimizando su impacto en la operatividad de la organización.

4.1. COMPONENTE – PLANIFICACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

La alta dirección del Concejo Municipal debe aprobar los requerimientos de continuidad del negocio y estos requerimientos darán lugar a un tiempo objetivo de recuperación (RTO) y un punto objetivo de recuperación (RPO) para el objetivo mínimo de continuidad del negocio (MBCO) por producto, servicio o actividad.

Estos RTOs comienzan desde el punto en el cual la interrupción ocurrió y va hasta que el producto, servicio o actividad está disponible nuevamente.

4.1.1. ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA)

El Análisis de Impacto del Negocio BIA (Bussiness Impact Analysis, por sus siglas en inglés), permite identificar con claridad los procesos misionales del Concejo y analizar el nivel de impacto con relación a la gestión del negocio.

En esta etapa, el análisis de impacto del negocio, debe poder clarificar los siguientes requerimientos:

- Identificar las funciones y procesos importantes para la supervivencia del Concejo Municipal al momento de la interrupción, esto es tener en cuenta cuales de los procesos son claves para que entren en operación rápidamente asignándoles la mayor prioridad posible, frente a los de menor prioridad; debe quedar claro que para los procesos identificados como no tan prioritarios se deben preparar también planes de recuperación.

- Revisar las consecuencias tanto operacionales como financieras, que una interrupción tendrá en los procesos considerados de alta prioridad.

- Estimar los tiempos de recuperación, en razón a las posibles alteraciones de los procesos considerados de alta prioridad para el funcionamiento de las infraestructuras de TI. El entregable de esta fase es un informe con el detalle de las funciones y procesos críticos del negocio.

Este documento debe contener la información básica de los recursos requeridos y los tiempos de recuperación para que las entidades puedan poner en funcionamiento los servicios y por ende la continuidad del negocio, el cual se debe realizar durante el primer cuatrimestre de cada vigencia.

El método estructurado que facilite la obtención de la información requerida para esta fase se hará mediante entrevistas, de esta forma la información del Análisis de Impacto del Negocio (BIA), se obtiene personalmente, entrevistando al personal que interactúe con los diferentes componentes TIC, especialmente el personal de planta.

4.1.2. REQUERIMIENTOS DE TIEMPO DE RECUPERACIÓN

Como parte del plan de continuidad del negocio del Concejo Municipal, es importante poder definir y entender los requerimientos de tiempo necesarios para recuperar a las entidades de servicios que han sido interrumpidos por

diferentes motivos dentro de la organización; estos requerimientos obedecen a varios componentes que hacen referencia concreta al tiempo disponible en la cual una organización puede recuperarse oportuna y ordenadamente a las interrupciones en los servicios e infraestructuras de TI. Los componentes se describen a continuación:

- MTD (Maximun Tolerable Downtime) o Tiempo Máximo de Inactividad Tolerable. Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse.

- RTO (Recovery Time Objective) o Tiempo de Recuperación Objetivo. Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.

- RPO (Recovery Point Objective) o Punto de Recuperación Objetivo. Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos y el evento de desastre.

- WRT (Work Recovery Time): Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos.

4.1.3. METODOLOGÍA DEL ANÁLISIS DE IMPACTO DEL NEGOCIO

La metodología del Análisis de Impacto del Negocio, consiste en definir una serie de pasos interactivos con el objeto de identificar claramente los impactos de las interrupciones y tomar decisiones respecto a aquellos procesos que se consideran críticos para la organización y que afectan directamente el negocio ante la ocurrencia de un desastre, estos pasos se muestran a continuación:

4.1.3.1. Identificación de Funciones y Procesos

Comité de Emergencia: Está conformado por el líder de contingencia TIC (Profesional Universitario Ingeniero de Sistemas) del Concejo Municipal y los funcionarios de la Alta Gerencia encargados de tomar las decisiones finales durante el evento contingente.

Líder de contingencia TIC: Es el líder del proceso TIC y responsable por declarar la contingencia y mantener continuo contacto con los superiores y áreas afectadas por el evento.

Apoyo en Recuperación: Personal de apoyo encargado de las funciones logísticas y operativas de tecnología que facilitan las actividades en caso de la materialización de un riesgo contra la continuidad de las operaciones.

Los rolos definidos anteriormente permiten que se pueda dar soporte a los siguientes aplicativos y componentes relacionados a continuación:

- Soporte Técnico de Sistemas.
- Sistema Financiero y Contable.
- Portal WEB.
- Red de área local.
- Acceso WiFi.Planta PBX.

Los aplicativos y componente enunciados anteriormente son lo que soportan

tanto los componentes Misionales como los Administrativos y Financieros que pueda tener el Concejo Municipal en un futuro.

4.1.3.2. Evaluación de Impactos Operacionales

El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles: A, B o C.

- Nivel A: La operación es crítica para el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse.

- Nivel B: La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica.

La tabla siguiente muestra los niveles de criticidad en el Concejo Municipal, donde se contempla un sistema de tolerancia a fallas por horas, cuya propiedad permite que un sistema pueda seguir operando normalmente a pesar de que una falla haya ocurrido en alguno de los componentes del sistema; por lo tanto la tolerancia a fallas es muy importante en aquellos sistemas que deben funcionar todo el tiempo.

Categoría (Función del Negocio)	Proceso (Servicios)	Nivel	Tolerancia a Fallas (Horas)	Descripción
Portal WEB	Sitio web del Concejo	B	72	Capa de presentación
Seguridad de Información	Firewall	A	12	Servicio de firewall del Concejo
Comunicaciones	Acceso Local a Internet y a Voz	B	24	Comunicación de Internet y Voz del usuario local
Proveedores de Aplicaciones y/o comunicaciones	Externo	B	96	Desarrollo contratado por externos. Canales de comunicaciones
Recurso Humano	Internos/externos	B	24	Profesionales encargados de administrar las infraestructuras del Concejo

4.1.3.3. Identificación de Procesos Críticos

La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales tal y como se muestra en la siguiente tabla:

Valor	Interpretación del Proceso Crítico
A	Crítico para el negocio; la función del negocio no puede realizarse sin este proceso.
B	No es crítico para el negocio, pero la operación es una parte integral del mismo.
C	La operación no es parte integral del negocio.

Para el caso del Concejo Municipal se ha definido que los 13 procedimientos establecidos mediante el sistema de calidad corresponden al valor B, ya que todos hacen parte integral del negocio, pero si alguno falla, la función del

negocio puede continuar siempre y cuando la falla se corrija lo más rápido posible.

A continuación, se listas los 11 procesos.

- Direccionamiento
- Gestión Participación Ciudadana
- Gestión Acuerdos
- Cestión Control Politico
- Gestión Talento Humano
- Gestión Financiera
- Gestión Documental
- Gestión de Bienes y Servicios
- Gestión TICS
- Gestión Juridica
- Gestión Control Interno

4.1.3.4. Establecimiento de Tiempos de Recuperación

Una vez identificados los procesos críticos del negocio, se deben establecer los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios; el entendimiento de estos componentes es fundamental para comprender el BIA.

Los tiempos de recuperación se enunciaron en el apartado 4.1.2. REQUERIMIENTOS DE TIEMPO DE RECUPERACIÓN.

Ya que se han identificado los procesos críticos del Concejo, se procede a identificar el MTD, que corresponde al tiempo máximo de inactividad que puede tolerar la Corporación antes de colapsar y se hace la clasificación a fin de priorizar la recuperación del proceso (servicio). Esto quiere decir que si por ejemplo un proceso tiene un periodo máximo de tiempo de inactividad (MTD) de un (1) día, este debe tener mayor prioridad para iniciar el evento de recuperación, en razón al poco tiempo de tolerancia de la inactividad, frente a otros que tienen mayor tolerancia.

A continuación, se muestran los tiempos de recuperación:

Categoría	Proceso Crítico (Servicios)	MTD (en días)	Prioridad de Recuperación
Portal WEB	Sitio web del Concejo	3	4
Base de Datos	SQL nómina	1	2
Seguridad de Información	Firewall	0.5	1
Comunicaciones	Acceso Local a Internet y a Voz	2	3
Proveedores de Aplicaciones y/o Comunicaciones Externos	Servicios externos	4	5
Soporte Informático	Equipo PC de usuario	1	2

Este cuadro proporciona una visión clara sobre la importancia y las necesidades de recuperación de cada proceso crítico en función de su categoría.

4.2 GESTIÓN DEL RIESGO

Ante la posible materialización de algún evento que ponga en riesgo la operatividad del Concejo y con el fin de establecer prioridades para la mitigación de los riesgos, se hace necesario disponer de metodologías para su evaluación.

La metodología del plan de continuidad del negocio, determina los diversos escenarios de amenazas para la Corporación, el cual permite desarrollar las estrategias de continuidad y los planes para reanudar los servicios que estaban en operación.

4.2.1. Política de seguridad de la información.

Para el Concejo Municipal la información es un activo valioso para la toma de decisiones, la gestión del cambio y el conocimiento; así como la apropiación de la iniciativa de Gobierno Digital. La necesidad de articular los valores de gobierno “Lógica, Ética y Estética” para establecer una política de seguridad de la información que ha de brindar a los usuarios y ciudadanos las herramientas para la defensa de lo público contenido en los servicios y activos de TI en la Corporación.

La necesidad de mitigación de riesgos alrededor de la información requiere planes de manejo de incidentes y herramientas para respaldar las actividades ejecutadas en el Concejo considerando que las TIC son un proceso de apoyo a toda la Corporación.

Además de incentivar la cultura de seguridad de la información a los usuarios ante ataques informáticos, virus y robos o pérdidas de información. Es de vital importancia la gestión del conocimiento y las revisiones de la política que lleven a una mejora continua para lograr un mejor desempeño de las actividades y la articulación de la normatividad colombiana e internacional en protección de datos, delitos informáticos y seguridad de la información además de tendencias tecnológicas para que puedan ser implementadas entorno a la eficacia de las actividades relacionadas, considerando siempre los tres principios de la seguridad de la información: Confidencialidad, disponibilidad e integridad.

4.2.1.1. Objetivo

Establecer una Política de seguridad de la información junto con los procedimientos, mecanismos, controles y herramientas adecuadas que garanticen la integridad, disponibilidad y confidencialidad de los activos de información en el Concejo Municipal.

4.2.1.2. Alcance

La Política de Seguridad de la Información aplica para todos los usuarios internos en todos los niveles jerárquicos, usuarios externos o aquellos que de alguna manera manejen información del Concejo Municipal.

4.2.1.3. Propiedad de la información

El Concejo establece propiedad sobre los activos de información que están relacionados con su actividad. La información es entregada para su uso, operación o custodia a los servidores públicos, contratistas o terceros, de acuerdo a la función específica y necesidades del trabajo a realizar de acuerdo a lo establecido, además sin alterar en ningún momento la propiedad de los mismos.

Por lo tanto, las personas responsables de los procesos que controlan activos de información, lo hacen para su manejo operativo y de conservación sin perjuicio para el Concejo Municipal de perder la propiedad de la información.

4.2.1.4. Gestión de activos
Los activos de información en el Concejo Municipal se gestionarán de manera que:

- Se encontrarán inventariados
- Serán asignados a un responsable
- Se realizará una valoración de riesgos.
- Protegidos de acuerdo a su riesgo asignado.

4.2.1.5. Control de accesos

Es de vital importancia el control de acceso a la información mediante sistemas internos, redes externas o internas y activos de información por lo cual, ha de establecerse, mantenerse y actualizarse medidas de control de acceso soportados por una cultura de seguridad en la entidad y limitar el acceso de los usuarios hacia los activos de información al mínimo requerido para la realización de su trabajo, de acuerdo con el tratamiento correspondiente al nivel de clasificación de cada activo. Además, deben permitir identificar de manera inequívoca cada usuario y hacer seguimiento de las actividades que éste realiza.

4.2.1.6. Administración de redes y equipos

Los recursos tecnológicos del Concejp, son herramientas de apoyo a las labores y responsabilidades de los funcionarios y/o contratistas.
Por ello, su uso está sujeto a las siguientes directrices:

- Los bienes de cómputo se emplearán de manera exclusiva y bajo la completa responsabilidad por el funcionario y/o contratista al cual han sido asignados, y únicamente para el correcto desempeño de las funciones del cargo o de las obligaciones contraídas. Por tanto, no pueden ser utilizados con fines personales o por terceros, no autorizados por la Subdirección Administrativa y Financiera mediante solicitud formal.

- Sólo está permitido el uso de software licenciado por la Entidad y/o aquel que sin requerir licencia sea expresamente autorizado por el Profesional Universitario Ingeniero de Sistemas.

- Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional.

- No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los elementos tecnológicos, además se debe tener organizado el puesto de trabajo para evitar incidentes con estos recursos.

- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo la disponibilidad de la información por fallas en el suministro eléctrico a los equipos de cómputo.

- Los únicos autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar,

revisar y/o reparar sus componentes es el Profesional Universitario Ingeniero de Sistemas o el contratista que tenga este objeto contractual.

• La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, debe ser informada de inmediato a la Secretaria General del Concejo por el funcionario o contratista a quien se le hubiere asignado.

• La pérdida de información debe ser informada con el detalle de la información extraviada a la Secretaria General.

• El Profesional Universitario Ingeniero de Sistemas es la única dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.

•Todo acceso a la red de la Corporación mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por el Profesional Universitario Ingeniero de Sistemas previa autorización de la Presidencia del Concejo.

• Los equipos deben quedar apagados cada vez que el funcionario y/o contratista no se encuentre en la oficina durante la noche, esto es, con el fin de proteger la seguridad y distribuir bien los recursos de la Corporación, siempre y cuando no vaya a realizar actividades vía remota.

• Se debe evitar guardar documentos sobre el escritorio de trabajo del sistema operativo optando por un lugar seguro dentro del almacenamiento del equipo.

4.2.1.7 Uso de software y sistemas de información

Todos los funcionarios y/o contratistas del Concejo Municipal son responsables de la protección de la información que acceden y/o procesan y de evitar su pérdida, alteración, destrucción y/o uso indebido, para lo cual se dictan los siguientes lineamientos:

• Las credenciales de acceso a la red y/o recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los funcionarios y/o contratistas no deben revelar éstas a terceros ni utilizar claves ajenas.

• Todo funcionario y/o contratista es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.

• Todo funcionario y/o contratista es responsable de los registros y/o modificaciones de información que se hagan a nombre de su cuenta de usuario, toda vez que la clave de acceso es de carácter personal e intransferible.

• En ausencia del funcionario y/o contratista, el acceso a la estación de trabajo le será inactivada con una solicitud a la Secretaria General, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. La Dirección de Recursos Humanos o quien haga sus veces debe reportar, las vacaciones y cualquier tipo de licencia de los funcionarios y la Oficina Jurídica o quien haga sus veces las suspensiones temporales y/o permanentes de los contratistas; no obstante, el funcionario y/o contratista deberá solicitar a la Secretaria General el bloqueo de su usuario por la ausencia temporal o definitiva.

- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de un contrato con el Conejo Municipal, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente.

- Cuando un funcionario y/ o contratista cesa en sus funciones o culmina la ejecución de un contrato con el Concejo Municipal, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información y de informar a la Secretaria General la culminación de permisos para los contratistas. Solo las aplicaciones aprobadas por la Presidencia del Concejo serán instaladas o utilizadas en cada dispositivo destinado al procesamiento de información clasificada o sensible, además de garantizar su debida aprobación de uso y licenciamiento de acuerdo a los permisos y controles asignados a los usuarios.

4.2.1.8. Correo electrónico

El servicio de correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios y/o contratistas del Concejo Municipal, con los siguientes lineamientos:

- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Corporación, por lo tanto, la responsabilidad del contenido es netamente del autor.

- Está prohibido el uso de correos masivos tanto internos como externos, salvo con la autorización de los directivos del Concejo Municipal.

- Todo mensaje SPAM o CADENA debe ser inmediatamente reportado a la plataforma de correo de Google. No está permitido el envío y/o reenvío de mensajes en cadena.

- Todo mensaje sospechoso respecto de su remitente o contenido debe ser inmediatamente reportado al Profesional Universitario Ingeniero de Sistemas y proceder de acuerdo a las indicaciones que le sean dadas, lo anterior, debido a que puede ser contenido de virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, tengan explícitas referencias no relacionadas con la misión de la Entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos).

- La cuenta de correo institucional no debe ser ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o a cualquier otra ajena a los fines de la Corporación.

- Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.

- Está expresamente prohibido distribuir información del Concejo Municipal, no pública, a otras entidades o ciudadanos sin la debida autorización de la Dirección General.

- El único servicio de correo electrónico autorizado para el manejo de la información institucional en la Corporación es el asignado por el Profesional Universitario Ingeniero de Sistemas, previa solicitud realizada por algún directivo,

el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.

4.2.1.9. Uso de Internet

De acuerdo al buen uso de los recursos de navegación de la Corporación se deben tener en cuenta los siguientes lineamientos:

- El uso del servicio de Internet está limitado exclusivamente para propósitos laborales.

- Los servicios a los que un determinado usuario pueda acceder desde internet dependerán del rol o funciones que desempeña el usuario en el Concejo Municipal y para los cuales esté formal y expresamente autorizado.

- Todo usuario es responsable de informar al Profesional Universitario Ingeniero de Sistemas de los contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones dentro del Concejo Municipal.

- Está expresamente prohibido el envío, y/o descarga, y/o visualización, de páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.

- Está expresamente prohibido el envío y/o descarga de cualquier tipo de software o archivos de fuentes externas, y/o de procedencia desconocida que puedan causar cualquier tipo de daños en los equipos y redes.

- Está expresamente prohibido acceder a páginas que agredan la ética y el buen comportamiento.

El Concejo Municipal se reserva el derecho de monitorear los accesos, y por tanto el uso del servicio de internet de todos sus funcionarios o contratistas, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Corporación.

4.2.1.10. Responsabilidades y contraseñas

Todos los funcionarios, contratistas y/o colaboradores que hagan uso de los activos de información del Concejo Municipal, tienen la responsabilidad de seguir las reglas establecidas en la presente política y sus documentos anexos a la misma, entendiendo que el uso no adecuado de los recursos puede poner en riesgo la continuidad de la misión institucional.

La gestión de usuarios se asignará con previo conocimiento de las funciones a implementar en el Concejo Municipal, por lo tanto, el manejo de documentos, cuentas de correo, accesos a sistemas de información y activos de información es responsabilidad de cada usuario, por lo cual la sensibilización de los usuarios frente a sus responsabilidades ha de ser constante.

4.2.1.11. Seguridad física

El tratamiento a amenazas tales como acceso no autorizado, robo, pérdida, daño, entre otros (riesgos físicos y ambientales) que puedan afectar los activos

de información, medios de procesamientos y comunicaciones, así como las instalaciones donde que se encuentran ubicados.

Esto es el control de medios extraíbles, control sobre dispositivos a puertos de red y seguridad del entorno.

4.2.2. Política de tratamiento y protección de datos personales

La política de tratamiento y protección de datos personales fue adoptada mediante Resolución 076 de octubre 11 de 2024 y se encuentra disponible en la página electrónica del Concejo Municipal: Enlace MIPG, Dimensión 3: Gestión con valores para resultados y Politica 8: Seguridad Digital. https://www.concejodecartago.gov.co/mipg/

4.2.3. Plan de contingencia

Debido al avance de la tecnología y los sistemas de información, hoy en día las organizaciones están soportando cada vez más sus procesos de negocio (tanto críticos como no críticos) en plataformas tecnológicas que permitan facilitar y optimizar el desarrollo de las actividades dentro de la Corporación.

Sin embargo, la plataforma tecnológica que soporta estos servicios, continuamente se encuentra expuesta a riesgos de diferentes fuentes que podrían ocasionar una interrupción o no disponibilidad de los sistemas de información y por ende de los procesos de negocio.

Es por esto, que el Concejo Municipal se encuentra comprometido con el establecimiento de un Plan de Contingencia TIC que busque estrategias para responder de forma adecuada ante un evento de falla. Las principales estrategias están dirigidas a recuperar y/o restaurando los servicios informáticos en el menor tiempo posible sin impactar los procesos críticos de la Corporación.

4.2.3.1 Objetivos

- Desarrollar un Plan de Contingencia TIC que garantice la operación de los servicios informáticos en los procesos de la Corporación ante eventos o desastres que afecten su disponibilidad.

- Cumplir con los acciones de mitigación de riesgo relacionados con el Proceso de Gestión, Implementación y Soporte de las TIC identificados en el Mapa de Riesgos de la Oficina Control Interno o quien haga sus veces.

- Actualizar el modelo de gestión para el Plan de Contingencia TIC de la Corporación con el fin de promover el mejoramiento continuo del plan y evitar la obsolescencia del mismo.

4.2.3.2. Objetivos específicos

- Maximizar la efectividad de las operaciones de contingencia TIC a través de un plan establecido, que consiste de las siguientes fases:
  - Fase de Notificación/Activación: Se detecta y evalúa el daño para activar el plan.
  - Fase de Reanudación: Se reanudan temporalmente los servicios informáticos.

➢ Fase de Recuperación: Los servicios informáticos originales se recuperan del daño que activó el plan.
➢ Fase de Restauración: Se recuperan las capacidades de procesamiento en operación normal y se reanudan los servicios informáticos originales.

• Identificar las actividades, recursos y procedimientos necesarios para reanudar los servicios informáticos durante interrupciones prolongadas en la operación.

• Asignar responsabilidades al personal de la dependencia y proveer una guía para recuperar los servicios informáticos durante períodos prolongados de interrupción en su operación.

• Garantizar la coordinación con otras dependencias de la Corporación que participaran en las estrategias del Plan de Contingencia TIC.

• Garantizar la coordinación con puntos externos de contacto y proveedores que puedan participar en las estrategias del Plan de Contingencia TIC.

4.2.3.3. Alcance

El alcance del Plan de Contingencia TIC del Concejo Municipal incluye los siguientes aplicativos y componentes relacionados a continuación:
• Soporte Técnico de Sistemas.
• Sistema Financiero y Contable.
• Portal WEB.
• Acceso WiFi.

4.2.3.4. Criterios de operación

4.2.3.4.1. Roles y responsabilidades Comité de Emergencia: Está conformado por el líder de contingencia TIC (Profesional Universitario Ingeniero de Sistemas) del Concejo Municipal y los funcionarios de la alta Gerencia encargados de tomar las decisiones finales durante el evento contingente.

Líder de contingencia TIC: Es el líder del proceso TIC y responsable por declarar la contingencia y mantener continuo contacto con los superiores y áreas afectadas por el evento.

Apoyo en Recuperación: Personal de apoyo encargado de las funciones logísticas y operativas de tecnología que facilitan las actividades en caso de la materialización de un riesgo contra la continuidad de las operaciones.

4.2.3.5. Fase de notificación y activación

Esta fase se enfoca en las acciones iníciales para detectar y evaluar el daño causado por el evento, teniendo en cuenta:

- Es prioridad, en una situación de emergencia, preservar la integridad y vida de los funcionarios del Concejo Municipal. Antes de proceder a la notificación y activación del plan.

- Toda la información correspondiente debe ser dirigida al Líder de contingencia TIC.

- El Plan de Contingencia TIC debe ser activado por el Líder de contingencia TIC.

Para esto, se deben seguir los pasos a continuación:

Tan pronto como la situación de emergencia es detectada, se debe contactar con las autoridades correspondientes y tomar los pasos necesarios para minimizar la pérdida de vidas humanas y el daño a las instalaciones físicas.

Servicios de emergencia: Contacte las siguientes autoridades en situaciones de emergencia tales como fuego, explosión, terremoto, etc.:

Aquí tienes el cuadro con la información sobre los servicios de emergencia a contactar en diferentes situaciones:

Departamento de Situación	Teléfono de Contacto
Bomberos	Fuego, explosión, terremoto.
Policía	Atentado
Paramédicos	Fuego, explosión, terremoto.
Seguridad Física – Prof. Univ. Ingeniero de Sistemas	Fuego, explosión
Equipos de Cómputo	Si el problema detectado es concerniente con equipos

Este cuadro facilita la localización rápida de los contactos necesarios en situaciones de emergencia y problemas específicos relacionados con la seguridad y los equipos.

Equipos de Cómputo: Si el problema detectado es concerniente con Equipos de Cómputo, tales como insuficiencia eléctrica, corto circuito, inundación, excesivo calor, frío o humedad, entre otros que afecte el normal funcionamiento de estos equipos, contacte al Profesional Universitario Ingeniero De Sistemas.

Seguridad física: Si usted detecta que una persona no autorizada que se encuentra utilizando algún Equipo de Cómputo, notifique a la Secretaria General o al Profesional Universitario Ingeniero De Sistemas.

Nota: Si usted es una persona autorizada y tiene el conocimiento y entrenamiento adecuado proceda a responder inmediatamente a la emergencia, previa autorización y/o notificación del Líder de Contingencia TIC.

El Líder de contingencia TIC contacta al Comité de Emergencia y da instrucciones para el procedimiento de respuesta a emergencias y evaluación del daño.

Nota: Si el evento presentado afectó la infraestructura física del Concejo Municipal, contacte a la Secretaria General. De lo contrario contacte sólo al Profesional Universitario Ingeniero de Sistemas.

El Comité de Emergencia da respuesta a la emergencia y aplica las acciones correctivas posibles e inmediatas que puedan desarrollar; hasta que personal especializado interno o externo a la entidad llegue al sitio del evento.

Nota: Es prioridad, en una situación de emergencia, preservar la integridad y vida de los funcionarios y contratistas del Concejo Municipal.

El Comité de Emergencia realiza los pasos abajo descritos para determinar la evaluación del daño y el tiempo estimado de recuperación. Si la evaluación del daño no puede realizarse porque no existen las condiciones de seguridad adecuadas se utiliza el procedimiento alternativo de evaluación.

Procedimiento de evaluación de daños: Diligencie un acta donde se realice una Evaluación de Daños, determine el impacto causado por el evento y notifique al Líder de contingencia TIC.

Procedimiento alternativo de evaluación: Con base en la observación, evalué el impacto causado por el evento y notifique al Líder de contingencia TIC inmediatamente.

El Líder de contingencia TIC evalúa los resultados y determina si el plan de contingencia debe ser activado. El plan de contingencia TIC debe ser activado si una o más de las siguientes condiciones son verdaderas:

- Equipos de cómputo no disponibles, conectividad disponible.

- Equipos de cómputo disponibles, conectividad no disponible.

- Otro criterio, que se considere apropiado.

Si el plan es activado, el Líder de contingencia de TIC notifica a los integrantes del Comité de emergencia, a las autoridades pertinentes, proveedores y contratistas que tengan incidencia en el plan de contingencia TIC. Establece el Centro de Operación de Emergencias (EOC) de ser necesario e inicia la ejecución del Plan de contingencia TIC de acuerdo al Escenario presentado:

Escenario 1: Existe Equipos de Cómputo alternos que posibilita la continuidad de los procesos informáticos en la Corporacion.

Escenario 2: Existe una red virtual alterna que posibilita la continuidad de los procesos informáticos en la Corporación.

4.2.3.6. Fase de reanudación

El Comité de Emergencia inicia la recuperación de los servicios informáticos. Para esto se realizan los siguientes pasos:

- El Comité de Emergencia se establece en el Centro de Operación de Emergencias para coordinar las actividades de reanudación desde allí y como punto central de contacto para información relacionada con la emergencia, si es necesario.

- El Comité de Emergencia decide y publica lo que debe comunicar a los empleados, directivos, y público en general sobre la emergencia, si es necesario.

- El Comité de Emergencia notifica a los líderes de proceso que activen los procedimientos de contingencia necesarios para que operen en emergencia los servicios afectados.

- Se inicia la reanudación de los servicios afectados empezando por los más críticos y terminando por los menos críticos, asegurando que cumplan con el tiempo y la información requerida por los procesos.

- Se notifica a los líderes de procesos y a las personas afectadas que los servicios se encuentran operando en contingencia.

4.2.3.7. Fase de recuperación

El Comité de Emergencia autoriza el inicio de la recuperación de los servicios informáticos afectados.

Para esto se realizan los siguientes pasos:

- El Comité de Emergencia evalúa la situación actual de la emergencia y decide si es seguro iniciar la Fase de Recuperación.

- El Comité de Emergencia notifica a los líderes de proceso que activen los procedimientos de recuperación necesarios para recuperar el funcionamiento normal de los servicios afectados en el sitio original.

- Se deben realizar pruebas de los servicios y de los controles de seguridad que aseguren el apropiado funcionamiento simulando una carga normal.

4.2.3.8. Fase de restauración

El Comité de Emergencia establece la fecha y hora de inicio para retornar al sitio original, previendo el mínimo impacto a los procesos que se encuentran operando en contingencia.

- El Comité de Emergencia notifica a los líderes de proceso las actividades de restauración.

- Se inicia la restauración de los servicios menos críticos hasta los servicios críticos, probando la veracidad de los datos del servicio y su funcionamiento para asegurar que se encuentran trabajando normalmente, en el sitio original.

- Procedimientos técnicos

- Se notifica a los líderes de procesos y a las personas afectadas que los servicios se encuentran operando normalmente.

- Se hace revisión y seguimiento durante un tiempo prudencial a los servicios restaurados, en caso de presentarse un evento inesperado.

- Se consolida la información del proceso de contingencia y acciones tomadas, y se presenta al Comité de Emergencia.

- El Comité de Emergencia notifica al Líder de Contingencia TIC sobre las mejoras a realizar en el Plan y emite un comunicado desactivando la contingencia.

- Todos los procesos operan normalmente.

Nota: Una vez superado el evento contingente, el Líder de contingencia TIC debe realizar las acciones correctivas y preventivas, y desarrollar los cambios y/o actualizaciones del Plan que se requieran.

4.3. COMPONENTE – IMPLEMENTACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

Este componente le permitirá al Concejo Municipal llevar acabo la implementación del componente de planificación, teniendo en cuenta los aspectos más relevantes en los procesos de implementación de la estrategia de IRBC, las cuales deberán ser implementadas después de la aprobación de la alta dirección.

La alta dirección debe gestionar y proporcionar los recursos necesarios, procedimientos y operación del IRBC, así como los programas de entrenamiento y concientización.

La implementación se debe gestionar como un proyecto a través del proceso de control de cambios formales del Concejo Municipal y de los controles de gestión del proyecto de la Gestión de Continuidad del Negocio con el fin de asegurar visibilidad completa de la gestión y del reporte.

Para lograr la implementación de los elementos de la estrategia IRBC, se debe realizar concientización, tener las habilidades y el conocimiento general de la preparación de los elementos de servicios de TIC: personas, infraestructura, tecnología, datos, procesos y proveedores, así como sus componentes críticos.

La infraestructura de los sistemas de recuperación de TIC y la información crítica deben, en lo posible, ser físicamente separada del sitio operacional para prevenir que sea afectada por el mismo incidente. Los acuerdos para la disponibilidad de los datos deben estar alineados con los requerimientos de la estrategia.

El Concejo Municipal debe asegurar que los proveedores críticos están en capacidad de soportar los servicios de la estrategia, conforme a los requerimientos de la Corporación Así implementar el plan de respuesta de incidentes que permita confirmar la naturaleza y grado del incidente, tomar control de la situación, contener el incidente y comunicar a las partes interesadas.

4.4. COMPONENTE – EVALUACIÓN DE DESEMPEÑO PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

Este componente le permitirá al Concejo Municipal evaluar el desempeño y la eficacia de la implementación, a través de instrumentos que permita determinar la efectividad de la implantación del Plan de Seguridad en TI.

Para la medición de la efectividad de los procesos y controles del Plan de Seguridad en TI, se deben tomar los indicadores definidos en el componente de implementación para llevar a cabo el plan de seguimiento, evaluación y análisis del Plan de Seguridad en TI.

Con el Plan de Seguridad en TI se debe realizar una evaluación y análisis para la preparación de las TIC para la continuidad del negocio (IRBC), apoyado mediante la auditoria interna (realizada por la oficina de Control Interno) para la preparación de las TIC para la continuidad del negocio (IRBC), evaluando el desempeño de la preparación para las TIC para la continuidad del negocio.

4.5. COMPONENTE – MEJORA CONTINUA PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

Este componente le permitirá al Concejo Municipal realizar acciones correctivas apropiadas a los potenciales impactos determinados por el análisis de impacto

del negocio BIA (Bussiness Impact Analysis, por sus siglas en inglés) de la Corporación.

Para ello se debe realizar las acciones correctivas, identificando las fallas, mediante una auditoria interna (realizada por la oficina de Control Interno), comunicando los resultados y realizando un plan de mejoramiento. Todo lo anterior debe tener revisión y aprobación por la alta Dirección.