RESOLUCIÓN No 150 DE 2018

(Diciembre 28 de 2018)

POR MEDIO DEL CUAL SE ADOPTA EN EL INSTITUTO MUNICIPAL DE EMPLEO Y FOMENTO EMPRESARIAL DE BUCARAMANGA EL PLAN DE CONTINUIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN – IMEBU 2018

EL DIRECTOR GENERAL DEL INSTITUTO MUNICIPAL DE EMPLEO Y FOMENTO EMPRESARIAL DE BUCARAMANGA – IMEBU, en uso de sus facultades legales, en especial las conferidas en el acuerdo 030 de diciembre de 2002, y

CONSIDERANDO

1- Que mediante Acuerdo 030 de 2002 (Diciembre 19) expedido por el Concejo Municipal de Bucaramanga se crea el INSTITUTO MUNICIPAL DE EMPLEO Y FOMENTO EMPRESARIAL DEL MUNICIPIO DE BUCARAMANGA, como establecimiento público del orden municipal, dotado de personería jurídica, autonomía administrativa y financiera, con patrimonio independiente.

2- Que conforme a lo establecido en el artículo 209 de la Constitución Política de Colombia establece: "La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad".

3- Que la entidad ha requerido por recomendación de su auditoria interna y la adelantada por órganos de control y en cumplimiento del plan de mejoramiento. Adoptar el plan estratégico de las tecnologías de la información 2018-2022 – PETI – y el plan de seguridad de las tecnologías de la información, al cual se le dio cumplimiento bajo la Resolución 057 de junio 28 de 2018.

4- Que lo anterior se fundamenta en el Decreto Nacional 2573 de 2014, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones, el Decreto 1078 del 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones y el Decreto 415 del 2016, por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones, esto en relación con el PETI, que está proyectado en una vigencia de 4 años en el Instituto.

5- Que el plan de continuidad de las Tecnologías de la Información – 2018, ha sido elaborado tomando como referencia la "Guía para la preparación de las TIC para la continuidad del negocio", copiado/distribuido con permiso del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Todos los derechos reservados.

6- Que se debe contar la implementación de un proceso de preservación de la información pública ante situaciones disruptivas, permite minimizar el impacto y recuperación por perdida de activos de información de la organización, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.

7- Que la entidad expidió el plan estratégico de las tecnologías de la información 2018-2022 – PETI – y el plan de seguridad informática el cual fue elaborado por el Profesional Universitario, Ingeniero de Sistemas MANUEL ALBEIRO VARGAS y suscrito por la Dirección General.

8- Que La gestión de la continuidad del negocio, es un proceso para holístico a través del cual se identifican los impactos potenciales que amenazan la continuidad de las actividades del Instituto Municipal de Empleo y Fomento Empresarial de Bucaramanga - IMEBU, proveyendo un marco de referencia para la construcción de la resiliencia y la capacidad de una respuesta efectiva, que le permita proteger los intereses de la Entidad debido a disrupciones.

9- Que se requiere adoptar en el presente acto administrativo el plan de continuidad de las tecnologías de la información – IMEBU 2018, acorde con el plan de mejoramiento suscrito con la Contraloría Municipal de Bucaramanga y que serán anexos al presente acto administrativo, el cual fue discutido y aprobado por el comité MIPG del Instituto según acta No 09 de 28 de diciembre de 2018.

10- De esta forma la entidad da cumplimiento al plan de mejoramiento interno y el suscrito con el ente de control, así como a la normatividad en materia de Tecnologías de la Información.

Que en mérito de lo anteriormente expuesto,

RESUELVE:

ARTÍCULO 1°: Adoptar EL PLAN DE CONTINUIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN – IMEBU 2018, anexo a la presente Resolución.

ARTÍCULO 2°: Difundir, publicar y comunicar el presente Acto administrativo a través de los diferentes medios de comunicación que dispone la Entidad, así como la socialización con los funcionarios y contratista de la entidad.

ARTICULO 3°: Vigencia y derogatorias. La presente Resolución rige a partir de la fecha de su Suscripción y deroga las disposiciones que le sean contrarias.

Expedida en Bucaramanga Santander, a los veintiocho (28) días del mes de Diciembre del año dos mil dieciocho (2018).

COMUNIQUESE, PUBLIQUESE Y CUMPLASE

MEDARDO FABER MEJIA PALOMINO
Director General IMEBU

Anexo lo anunciado

Proyecto: Asesor Jurídico
Reviso: Subdirección técnica
Reviso: Profesional Ingeniero de Sistemas

A-GEI-PL03

PLAN DE CONTINUIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN – IMEBU 2018 - 2019

CUADRO CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
01	28/12/2018	Emisión inicial

ELABORO		

El plan de continuidad de las Tecnologías de la Información – 2018, ha sido elaborado tomando como referencia la "Guía para la preparación de las TIC para la continuidad del negocio", copiado/distribuido con permiso del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Todos los derechos reservados.

1. INTRODUCCIÓN

Teniendo en cuenta lo establecido en el Plan Vive Digital, liderado por el Ministerio de las Tecnologías de la Información y las Comunicaciones, en cuanto a la infraestructura, los servicios, las aplicaciones y los usuarios en el marco de un ecosistema digital; las recomendaciones brindadas en el Plan Nacional de Desarrollo 2015-2018 en cuanto a la necesidad de reconocer la seguridad y privacidad de la información, como un factor primordial para la apropiación de las TIC; la constante evolución de los mercados; y la dinámica de las entidades, plantea un marco de seguridad de la información para la prestación de servicios a los ciudadanos a través de las tecnologías de la información, el cual deberá ser respaldado por una gestión, unas políticas y unos procedimientos adecuados, que resalten el papel de las personas como el primer eslabón de una compleja cadena de responsabilidades y que esté orientado a preservar los pilares fundamentales de la seguridad y privacidad de la información.

La implementación de un proceso de preservación de la información pública ante situaciones disruptivas, permite minimizar el impacto y recuperación por perdida de activos de información de la organización, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.

En este proceso es conveniente identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

Las consecuencias de eventos disruptivos (desastres, fallas de seguridad, perdida del servicio y disponibilidad del servicio) se deberían ser someter a un análisis del impacto del negocio (BIA). Se deben desarrollar e implementar un plan de continuidad que permita garantizar la restauración oportuna de las operaciones esenciales.

La correcta implementación de la gestión de la continuidad del negocio disminuirá la posibilidad de ocurrencia de incidentes disruptivos y, en caso de producirse, la organización estará preparada para responder en forma adecuada y oportuna, de esa manera se reduce de manera significativa un daño potencial que pueda ser ocasionado por de ese incidente.

2. JUSTIFICACIÓN

La gestión de la continuidad del negocio, es un proceso para holístico a través del cual se identifican los impactos potenciales que amenazan la continuidad de las actividades del Instituto Municipal de Empleo y Fomento Empresarial de Bucaramanga - IMEBU, proveyendo un marco de referencia para la construcción de la resiliencia y la capacidad de una respuesta efectiva, que le permita proteger los intereses de la Entidad debido a disrupciones.

3. TERMINOLOGÍA

- **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

- **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. OBJETIVOS

- Establecer procedimientos especificos que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones criticas del negocio que se puedan ver comprometidas por eventos naturales, o sean ocasionados por el hombre.

- Identificar las aplicaciones y las plataformas consideradas críticas para la operación del negocio.

- Identificar al personal clave interno y externo requerido para la operación de las actividades criticas del negocio.

- Establecer los tiempos mínimos de recuperación requeridos en los que no se vea afectado el negocio.

- Definir la funcionalidad mínima que requiere el negocio en caso de contingencia.

- Identificar los riesgos presentes para la continuidad.

- Establecer los elementos esenciales requeridos en el plan de recuperación de desastres.

- Desarrollar e impartir la capacitación inicial para el correcto funcionamiento del plan.

5. PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

Como parte del proceso de continuidad del negocio, la preparación de las TIC para

complementa y suporta la continuidad del negocio de la organización y el Plan de Seguridad de TI del IMEBU, para mejorar la preparación de la Entidad que le permita:

a) Responder al cambiante ambiente de riesgos.
b) Asegurar la continuidad de las operaciones críticas del negocio soportadas por servicios de TIC.
c) Estar preparado para responder antes de que una disrupción de los servicios de TIC ocurra, identificar los eventos o las series de eventos relacionados provenientes de incidentes.
d) Responder y recuperarse de incidentes y/o desastres y fallas.

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

La alta dirección del IMEBU 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.

5.1.1. 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 IMEBU 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 IMEBU 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.

5.1.2. REQUERIMIENTOS DE TIEMPO DE RECUPERACIÓN

Como parte del plan de continuidad del negocio del IMEBU, 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.

5.1.3. 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:

5.1.3.1. Identificación de Funciones y Procesos

Comité de Emergencia: Está conformado por el líder de contingencia TIC (Profesional Universitario Ingeniero de Sistemas) del IMEBU 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 Delfin GD – ECO FINANCIERO.
- Portal WEB.
- PASIVOCOL: Software del Ministerio de Hacienda y Crédito Público (Maneja las Historias laborales de activos y retirados)
- 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.

5.1.3.2. 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 IMEBU, 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
Sistema Financiero y Contable Delfin GD – ECO FINANCIERO.	Sistema de Presupuesto, Contabilidad y Tesorería	B	48	Contenedor de aplicaciones
Portal WEB	Sitio web del IMEBU	B	72	Capa de presentación
Base de Datos	SQL nómina	B	24	Contenedor de aplicaciones en SQL
Seguridad de Información	Firewall	A	12	Servicio de firewall del IMEBU
Comunicaciones	Acceso Local a Internet y a Voz	B	24	Comunicación de Internet y Voz del usuario local
Cuartos de Máquinas	Centro de Datos	A	12	Servicio de Centro de datos de la Entidad
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 IMEBU.

5.1.3.3. 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
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 IMEBU 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 13 procesos.

1. Planeación Estratégica.
2. Planeación Presupuestal.
3. Gestión Técnica Emprendimiento.
4. Gestión Técnica Fortalecimiento.
5. Gestión Técnica Fomento Empleo.
6. Gestión Jurídica.
7. Gestión Financiera.
8. Gestión Informática.
9. Gestión Talento Humano y SST.
10. Gestión Documental.
11. Gestión de Recursos Físicos.
12. Gestión de Control Interno.
13. Gestión Calidad.

5.1.3.4. 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 5.1.2. REQUERIMIENTOS DE TIEMPO DE RECUPERACIÓN.

Ya que se han identificado los procesos críticos del IMEBU, se procede a identificar el MTD, que corresponde al tiempo máximo de inactividad que puede tolerar el instituto 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 (Función Crítica del Negocio)	Proceso Crítico (Servicios)	MTD (en días)	Prioridad de Recuperación
Sistema Financiero y Contable Delfin GD – ECO FINANCIERO.	Sistema de Presupuesto, Contabilidad y Tesorería	2	3
Portal WEB	Sitio web del IMEBU	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
Cuartos de Máquinas	Centro de Datos	0.5	1
Proveedores de Aplicaciones y/o comunicaciones	externo	4	5
Soporte Informático	Equipo PC de usuario	1	2

5.2 GESTIÓN DEL RIESGO

Ante la posible materialización de algún evento que ponga en riesgo la operatividad del IMEBU 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 el instituto, el cual permite desarrollar las estrategias de continuidad y los planes para reanudar los servicios que estaban en operación.

5.2.1. Política de seguridad de la información.

Para el IMEBU 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 entidad.

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 IMEBU considerando que las TIC son un proceso de apoyo a toda la entidad. Además de incentivar la cultura de seguridad de la información a los usuarios ante

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.

5.2.1.1. 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 IMEBU.

5.2.1.2. 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 IMEBU.

5.2.1.3. Propiedad de la información

El IMEBU 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 IMEBU de perder la propiedad de la información.

5.2.1.4. Gestión de activos

Los activos de información en el IMEBU 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.

5.2.1.5. 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.

5.2.1.6. Administración de redes y equipos

Los recursos tecnológicos del IMEBU, 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 Subdirección Administrativa

- La pérdida de información debe ser informada con el detalle de la información extraviada a la Subdirección Administrativa y Financiera.
- 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 Entidad mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por el Profesional Universitario Ingeniero de Sistemas previa autorización de la dirección del IMEBU.
- 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 Entidad, 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.

5.2.1.7 Uso de software y sistemas de información

Todos los funcionarios y/o contratistas del IMEBU 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 Subdirección Administrativa y Financiera, 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 Subdirección Administrativa y Financiera el bloqueo de su

- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de un contrato con el IMEBU, 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 IMEBU, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información y de informar a la subdirección administrativa y financiera la culminación de permisos para los contratistas.

Solo las aplicaciones aprobadas por la Dirección General 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.

5.2.1.8. 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 IMEBU, 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 Entidad, 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 IMEBU.
- Todo mensaje SPAM o CADENA debe ser inmediatamente reportado a la plataforma de correo de Google. No está permitido el envio y/o reenvio 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 revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales,

- 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 IMEBU, 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 Entidad 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.

5.2.1.9. Uso de Internet

De acuerdo al buen uso de los recursos de navegación de la Entidad 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 MUNICIPIO DE BUCARAMANGA 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 IMEBU.
- 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 IMEBU 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

5.2.1.10. Responsabilidades y contraseñas

Todos los funcionarios, contratistas y/o colaboradores que hagan uso de los activos de información del IMEBU, 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 IMEBU, 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.

5.2.1.11. 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.

5.2.2. Política de tratamiento y protección de datos personales

La política de tratamiento y protección de datos personales fue adoptada mediante resolución 072 de 29 de diciembre de 2016 y se encuentra disponible en la página Web del IMEBU en el siguiente enlace: http://www.imebu.gov.co/web32/atencion_al_ciudadano/2.Politica_tratamiento_proteccion_datos.pdf

5.2.3. 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 organización. 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 IMEBU 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 Entidad.

5.2.3.1 Objetivos

- Desarrollar un Plan de Contingencia TIC que garantice la operación de los servicios informáticos en los procesos de la Entidad 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.

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

5.2.3.2. 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 periodos prolongados de interrupción en su operación.

- Garantizar la coordinación con otras dependencias de la Entidad 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.

5.2.3.3. Alcance

El alcance del Plan de Contingencia TIC del IMEBU incluye los siguientes aplicativos y componentes relacionados a continuación:

- Soporte Técnico de Sistemas.
- Sistema Financiero y Contable Delfin GD – ECO FINANCIERO.
- Portal WEB.
- PASIVOCOL: Software del Ministerio de Hacienda y Crédito Público (Maneja las Historias laborales de activos y retirados)
- Red de área local.
- Acceso WiFi.
- Planta PBX.

5.2.3.4. Criterios de operación

5.2.3.4.1. Roles y responsabilidades

Comité de Emergencia: Está conformado por el líder de contingencia TIC (Profesional Universitario Ingeniero de Sistemas) del IMEBU 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.

5.2.3.5. 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 de la Alcaldía de Bucaramanga. 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.:

Departamento de	Situación	Teléfono de Contacto
Bomberos	Fuego, explosión, Terremoto.	6526666 - 6422450
Policía	Atentado	123
Paramédicos	Fuego, explosión, Terremoto.	123
Seguridad Física – Prof. Univ. Ingeniero de Sistemas	Fuego, explosión.	6706464 Ext - 115

Equipos de Cómputo: Si el problema detectado es concerniente con Equipos de Cómputo, tales como insuficiencia eléctrica, corto circuito, inundación, excesivo calor, frio 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 Subdirección Administrativa y Financiera 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 IMEBU, contacte a la Subdirección Administrativa y Fianciera. 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 IMEBU.

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 Entidad.

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

5.2.3.6. 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.

5.2.3.7. 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.

5.2.3.8. 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.

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

Este componente le permitirá al IMEBU 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 IMEBU 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 IMEBU debe asegurar que los proveedores críticos están en capacidad de soportar los servicios de la estrategia, conforme a los requerimientos de la Entidad. 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.

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

Este componente le permitirá al IMEBU 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.

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

Este componente le permitirá al IMEBU realizar acciones correctivas apropiadas a los potenciales impactos determinados por el análisis de impacto del negocio BIA de la Entidad.

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.

MEDARDO FABER MEJIA PALOMINO
Director General IMEBU

PROYECTO: Manuel Albeiro Vargas
Profesional- Universitario Ingeniero de Sistemas