A-GEI-PL01

PLAN DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN – IMEBU 2018

PLAN DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN – IMEBU 2018

ELABORO INGENIERO DE SISTEMAS	**FECHA**	**REVISO** DIRECTOR GENERAL	**FECHA**	**APROBÓ** COMITÉ DE PLANEACIÓN Y GESTIÓN	**FECHA**

El plan de seguridad de las Tecnologías de la Información – 2018, ha sido elaborado tomando como referencia el Plan para la implementación de la estrategia de gobierno en línea: seguridad y privacidad de la información y el PETI de la Alcaldía municipal de Bucaramanga.

1. MARCO DE LA SEGURIDAD DE LA INFORMACIÓN

El marco de la seguridad y privacidad de la información establece los lineamientos generales para implementar la estrategia de acuerdo a la necesidad del Municipio y su misión y visión además es el documento de partida que regula las políticas, alcances, objetivos y limitaciones de la implementación del SGSI. Está compuesto por los siguientes ítems:

1.1. DEFINICIÓN

En cumplimiento del decreto 1078 de 2015 para la implementación de la estrategia de gobierno en línea donde se estable la necesidad de gestionar los riesgos de la seguridad y privacidad de la información de las entidades territoriales como el Instituto Municipal de Empleo y Fomento Empresarial de Bucaramanga - IMEBU, es de vital importancia la toma de decisiones que establezcan mecanismos y acciones para asumir los retos de la seguridad de la información, este ha de ser la carta de navegación para alcanzar las metas del plan de seguridad de la información articulado con los diferentes procesos del instituto y otros modelos de gestión institucional.

1.2. CONTEXTO

Colombia es uno de los 40 países con mayor número de ataques y amenazas cibernéticas[1] con alrededor de 10 millones de ciberataques diarios (cifra 2015), lo que evidencia la necesidad de la gestión de riesgos digitales para evitar la ciberdelincuencia y el cibercrimen donde pueden verse afectados las instituciones de carácter público como lo es el IMEBU. Es de considerar también el crecimiento de la gobernanza del internet para la realización de trámites y servicios a través de este medio donde actualmente se supera en más de cien

[1] Tomado de: https://cybermap.kaspersky.com/

(100) funciones que pueden realizarse en línea[2] registrados ante la SI virtual Y el SUIT (Sistema único de información de trámites) , es de vital importancia reconocer las tendencias tecnológicas que aportan productividad a entidades como son la internet de las cosas (IoT, Internet of things), la gestión de dispositivos de usuarios (BYOD, Bring your own device) y el teletrabajo.

Las instituciones de carácter gubernamental según estadísticas del ColCERT son las segundas con mayores incidentes digitales con una representación del 23,9% del número reportado a esta entidad[3]; la misión del IMEBU contempla Liderar, orientar, coordinar y socializar todas las acciones del sector público y privado para mejorar la calidad de vida de las familias mediante la solución de sus necesidades de empleo y el impulso de programas de fomento empresarial, utilizando para ello los instrumentos establecidos por la Ley[4]. Por lo cual, con la implementación de los componentes de gobierno digital, se hará un mayor uso de las tecnologías de la información para lograr las metas definidas en la misión y visión del instituto a nivel estratégico en el municipio de Bucaramanga.

1.3. ALIADOS ESTRATÉGICOS

Los aliados estratégicos para el funcionamiento del plan se consideran como actores que en cualquier momento pueden intervenir para la gestión, colaboración, reporte e investigación de incidentes de carácter informático para la gestión de la seguridad de la información, entre ellos se encuentran:

- ColCERT: Grupo de respuestas ante emergencias Cibernéticas de Colombia.
- CCP: Centro cibernético policial
- Fiscalía general de la nación: Órgano investigativo para delitos informáticos

[2] Tomado de: https://www.sivirtual.gov.co/ y http://www.suit.gov.co/
[3] Tomado de: Documento CONPES 3854 de Seguridad Digital.
[4] Tomado de http://www.imebu.gov.co/web32/index.php/institucional/mision-y-vision

- SIC: Superintendencia de industria y comercio, autoridad para la protección de datos personales.
- MINTIC: Ministerio de Tecnologías de la información y Comunicaciones líder la implementación de estrategia de Gobierno en línea.
- Universidades y otras entidades del sector tecnológico.

1.4. CONTEXTO NORMATIVO Y ESTANDARIZACIÓN

1.4.1. ESTÁNDARES INTERNACIONALES

- ISO 27000:2013: Estándar internacional para la implementación de los sistemas de gestión de la seguridad de la información.
- ITIL v3: Es una librería de buenas práctica para la gestión de servicios de tecnología de la información (TI), una de las librerías es la gestión de la seguridad de la información; actualmente en su versión 3.

1.4.2. NORMATIVIDAD COLOMBIANA

- Ley 1213 de 2009, código penal colombiano
- Ley 1341 de 2009, Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- Ley 1581 de 2012, Decreto 1377 de 2013; normatividad para la gestión de datos personales.
- Decreto 32 de 2013, Por el cual se crea la Comisión Nacional Digital y de Información Estatal para la atención de incidentes de ciberdefensa y ciberseguridad.
- Ley 1712 de 2014, Ley de transparencia de la información pública Decreto 1008 de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte

2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. CONPES 3854, Documento para la seguridad digital.

- Otra normatividad vigente en derecho de autor propiedad intelectual y comercio electrónico.

1.5. POLÍTICAS

Con la necesidad de gestionar la seguridad y privacidad de la información se requiere crear, documentar y socializar las siguientes políticas:

- Política de seguridad de la información: Documento en el cual se establecen las indicaciones generales para el manejo de la seguridad de la información.
- Política de tratamiento y protección de datos personales: Documento por el cual se da cumplimiento a la ley 1581 de 2012 y el decreto reglamentario 1377 de 2013 para el manejo de datos personales en el IMEBU.
- Plan de contingencia: Documento en el cual se establecen los lineamientos para responder ante un evento de falla.
- Plan de copias de seguridad: Documento mediante el cual se indica el proceso de salvaguarda de la información importante mediante copias de seguridad.
- Plan de mantenimientos: Documento que permite seguir un procedimiento que garantice el óptimo funcionamiento de los equipos de cómputo que dan soporte al IMEBU.

1.6. ARTICULACIÓN ESTRATÉGICA

La gestión de la seguridad de la información es importante asumirlo desde diferentes puntos de vista de la organización con el fin de lograr los alcances del Plan de Seguridad de las Tecnologías de la Información de manera que se articulen con las herramientas institucionales para el control de la entidad para lograr una completa integración.

1.7. CAPACITACIÓN, PROMOCIÓN Y SENSIBILIZACIÓN

Para articular las acciones y documentos alrededor del Plan de Seguridad de las Tecnologías de la Información es importante capacitar a los servidores públicos, funcionarios y contratistas sobre los riesgos de digitales y tendencias en el manejo de la información. Por lo cual las acciones tomadas para dicho fin serán:

- Capacitación en seguridad de la información, políticas y documentación asociada al Plan de Seguridad de las Tecnologías de la Información: Según los requerimientos se pueden establecer al menos dos jornadas de capacitación sobre la seguridad de la información para contratistas y funcionarios del Instituto, incluyendo la actualización de políticas, procedimientos y acciones que ayuden a garantizar buenas prácticas a nivel de usuario sobre el Plan de Seguridad de las Tecnologías de la Información.
- Promoción de las herramientas de protección, tendencias y amenazas frecuentes en la entidad mediante campañas de sensibilización con el uso de herramientas tecnológicas y otros medios (impresos, pantallazos, material audiovisual, etc.). Esta estrategia estará constantemente actualizando a los usuarios sobre riesgos digitales para identificarlos y mitigarlos para evitar incidentes como robo, secuestro o perdida de la información vital para el IMEBU.
- Portal web de la entidad sobre el manejo de la seguridad y privacidad de la información, con el cual se podrá mantener la documentación del Plan de Seguridad de las Tecnologías de la Información de manera actualizada, el

plan de sensibilización y capacitación, tendencias tecnológicas relacionadas con seguridad y la administración de incidentes y eventos dentro de la misma plataforma.

2. MATRIZ DE RIESGOS

Los riesgos que se han identificado en cuanto a posible pérdida de información y falla de equipos cuanta con su respectivo procedimiento de atención y mitigación tal como se describe a continuación:

RIESGO	CONTINGENCIA
Que se haga uso indebido de la información que utiliza el IMEBU para su normal funcionamiento.	Política de seguridad de la información.
Que se haga mal uso de los datos obtenidos de las personas que utilizan los servicios del IMEBU.	Política de tratamiento y protección de datos personales.
Que se presenten situaciones críticas tanto en sistemas de información como en equipos de cómputo que alteren el normal funcionamiento del IMEBU.	Plan de contingencia.
Que se presente pérdida de información que afecte procesos y procedimientos en el IMEBU.	Plan de copias de seguridad.
Que se presenten fallas en los equipos de cómputo del IMEBU.	Plan de mantenimientos.

3. CONTINGENCIAS

A continuación se describe cada una de las contingencias enunciadas en el anterior numeral como forma de prevenir la ocurrencia de los riesgos enunciados.

3.1. 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 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.

3.1.1. 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.

3.1.2. 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.

3.1.3. 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.

3.1.4. 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.

3.1.5. 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.

3.1.6. 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 y Financiera 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 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.

3.1.7 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 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 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.

3.1.8. 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 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 revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o a cualquier otra ajena a los fines de la Entidad.
- 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.

3.1.9. 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 Entidad.

3.1.10. 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.

3.1.11. 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.

3.2. 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

3.3. 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.

3.3.1 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.

3.3.2. 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 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.

3.3.3. 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.

3.3.4. Criterios de operación

3.3.4.1. 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.

3.3.5. 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, 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 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.

3.3.6. 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.

3.3.7. 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.

3.3.8. 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.

3.4. Plan de copias de seguridad

Semanalmente se hará copia de seguridad a los siguientes equipos de cómputo:

Dirección General

Secretaria Ejecutiva

Oficina Jurídica

Apoyo a oficina jurídica

Apoyo a Subdirección Administrativa y Financiera

Control Interno

Subdirección Técnica

Profesional Universitario

Profesional Universitario Contador

Profesional Universitario Tesorero

Para la realización de dicho procedimiento se cuenta con un disco duro externo con capacitad de 1 TB, el cual está en la oficina de sistemas, dicha copia de seguridad será realizada por el Profesional Universitario Ingeniero de Sistemas o personal contratado para este fin.

3.5. Plan de mantenimientos

Teniendo en cuenta que el objetivo del proceso de Gestión de Tecnologías de Información y Comunicaciones es desarrollar, implementar, mantener y gestionar la plataforma tecnológica existente en el IMEBU y el objetivo del procedimiento de Soporte Técnico a equipos informáticos y puntos de red es asegurar que los equipos informáticos y puntos de red de la institución operen en óptimas condiciones con el propósito de garantizar el normal desarrollo de las actividades y en aras del mejoramiento continuo, se hace necesario elaborar e implementar del Plan Anual de mantenimiento preventivo a los equipos informáticos del Instituto.

Es importante destacar que el no realizar mantenimientos preventivos a los equipos de cómputo puede ocasionar daños irreversibles ocasionando altos

costos a la institución, por lo que se vuelve necesario e indispensable mantener una programación como mecanismo de prevención a posibles daños

3.5.1. Objetivo

Realizar mantenimiento preventivo, y en caso de ser necesario correctivo, a los equipos informáticos con el propósito de determinar las condiciones de operación de los mismos y disminuir posibles daños ocasionados por factores de falta de limpieza y atención de fallos.

3.5.2. Beneficios de los mantenimientos preventivos

- Ampliar la vida útil y mantener en óptimas condiciones de operatividad los equipos de cómputo y así mejorar su rendimiento.
- Disminuir costos, aumentar eficiencia y eficacia en el soporte técnico de los equipos.
- Realizar y mantener actualizado el inventario de los equipos.

3.5.3. Alcance

Se realizará mantenimiento preventivo a todos los equipos de cómputo del Instituto y en caso de ser necesario mantenimiento correctivo a los equipos que lo ameriten.

3.5.4. Plan de mantenimientos preventivos y correctivos

El profesional universitario Ingeniero de Sistemas planificará el mantenimiento preventivo tomando como base el inventario actualizado de los equipos de cómputo activos con que cuenta el IMEBU.

3.5.4.1 Actividades a realizar

- Verificar que el equipo tenga su respectivo código de inventario.
- Verificar el estado actual del equipo, al momento de realizar el mantenimiento.
- Iniciar el proceso de limpieza eliminando residuos de polvo de cada una de las partes de los equipos de cómputo e impresoras.
- Comprobar el estado del Antivirus, instalar y/o actualizarlo con el licenciamiento del IMEBU. Luego eliminar virus y malwares alojados en el equipo.
- Desinstalar todo software que no esté debidamente licenciado y dejar constancia de su desinstalación debidamente firmado por el responsable del equipo de cómputo
- En caso de encontrar un daño o desperfecto que amerite remplazo o compra de partes, en la ejecución del mantenimiento preventivo, será necesario realizar un mantenimiento correctivo. Para esto el personal de soporte técnico levantará el reporte técnico de diagnóstico que justifique dicho cambio.

3.5.4.2 Recomendaciones usuarios finales

Una vez terminada la parte técnica del mantenimiento, el Profesional Universitario Ingeniero de Sistemas realizará a los usuarios finales, unas recomendaciones mínimas que contribuyen a la conservación del estado de los equipos, la cuales se enuncian a continuación:

- No ingerir alimentos y bebidas en el área donde utilice equipo de cómputo.
- No apagar el equipo, sin antes salir adecuadamente del sistema.
- Hacer buen uso de los recursos de cómputo.
- Realizar respaldos de información crítica periódicamente.

- Consultar con el personal del área de soporte técnico cualquier duda o situación que se presente relacionada con los equipos informáticos.
- Cuidar las condiciones físicas de limpieza donde se encuentre el equipo.
- Ningún usuario puede instalar ningún tipo de software en los equipos de propiedad del IMEBU. Esta actividad es competencia únicamente del equipo de soporte técnico previa verificación de la existencia del licenciamiento.

3.5.4.3 Tiempo de operación

Como el trabajo que se realiza en cada equipo de cómputo es detallado, se estima el tiempo en promedio 90 min por equipo. Los mantenimientos se realizarán teniendo en cuenta las fechas establecidas en el presente plan y será previamente comunicado a los usuarios del servicio.

3.5.4.4 Cronograma de ejecución

- Primer trimestre: Verificar por parte del Profesional Universitario Ingeniero de Sistemas que el equipo tenga su respectivo código de inventario y el estado actual del equipo, antes de realizar el mantenimiento
- Segundo trimestre: Realizar proceso de contratación del mantenimiento preventivo y correctivo de los equipos de cómputo.
- Tercer trimestre: Ejecutar el contrato de mantenimientos preventivos y correctivos.
- Cuarto trimestre: Evaluar el informe de la vigencia y realizar nuevo plan de mantenimientos preventivos y correctivo para la siguiente vigencia.

3.5.5. Socialización del Plan de Mantenimientos Preventivos y Correctivos

El Plan de mantenimientos será publicado en el Portal Institucional y de igual manera se informará mediante circular las fechas programadas para el mantenimiento preventivo; con el fin de solicitar a los funcionarios la colaboración

pertinente para facilitar el desarrollo de las actividades programadas. Dicha circular debe ser presentada a los funcionarios como mínimo ocho (8) días antes de la ejecución de las actividades.

3.5.6. Informe de Mantenimiento Preventivo

El Profesional Universitario Ingeniero de Sistemas debe presentar al Director del IMEBU un informe donde se consoliden las actividades de mantenimiento preventivo y correctivo realizadas, los problemas identificados y las recomendaciones.

3.5.7. Revisión, Análisis del Informe y formulación de acciones de mejora

El Director General del IMEBU y el Profesional Universitario Ingeniero de Sistemas revisan el contenido del informe, con el fin de evaluar el cumplimiento del programa de mantenimiento preventivo y correctivo, identificar problemas y oportunidades de mejora y formular acciones para ajustar el programa de mantenimiento preventivo y correctivo para la siguiente vigencia.