1. PRESENTACIÓN

- Ante el incremento de la cultura informática derivada del creciente empleo de la Tecnología de la Información, surge la necesidad y responsabilidad de la protección de la misma, de sus medios de almacenamiento y de su ambiente de operación. La información que se maneja en la EMAB S.A. ESP., por ser materia prima para la propia gestión y toma de decisiones, es considerada como un activo importante y como tal, debe ser sujeta de custodia y protección para asegurar su integridad, confidencialidad y disponibilidad.

- La cantidad de datos guardados en los medios y equipos de almacenamiento se acrecienta día a día y su integridad va relacionada con su pérdida o destrucción intencional o no intencional. Es por ello, que los usuarios o personal directamente relacionado con el uso y operación de bienes informáticos deben propiciar la adopción de medidas de seguridad para proteger su información.

- Con base en este manual cada una de las áreas que componen esta empresa, deberán perseguir los siguientes fines:

    a. Establecer mecanismos y procedimientos para proporcionar confidencialidad, integridad y disponibilidad de la información.
    b. Estimular la creación de una cultura de seguridad en informática, así como fomentar la ética entre funcionarios de la EMAB S.A. ESP.
    c. Definir los requerimientos mínimos de seguridad en cada área, dependiendo del tipo de información que se procese: confidencial, restringida, de uso interno, general o público, estableciendo los procedimientos para identificación y uso de cada categoría de información.

Promover el establecimiento de procedimientos alternos en prevención a contingencias de cualquier naturaleza que garanticen en la medida de lo posible, la continuidad del procesamiento de la información y la prestación de servicios, mismos que al incorporarse al presente documento lo irán enriqueciendo y de esta manera se logrará contar cada vez con una mejor herramienta que apoye a superar las contingencias que se presenten

2. OBJETIVO

Proporcionar a la EMPRESA DE ASEO DE BUCARAMANGA EMAB S.A. ESP. Un plan de contingencia TIC que contenga las directrices y procedimientos para la atención de siniestro, contingencia o incidentes de seguridad que afecten las bases de datos o la infraestructura que garantiza su disponibilidad, para poder continuar con las operaciones, procesos y servicios informáticos; estableciendo responsabilidades y acciones a tomar en dichos casos. Así como minimizar el impacto que dichos daños pudieran causar.

3. RESPONSABLE

Responsable de TIC

- Será el responsable de realizar el registro de los incidentes de seguridad presentados en relación con el tratamiento de datos personales y el reporte de los mismos en el aplicativo de la Superintendencia de Industria y Comercio, en los casos que sean necesarios.

- Es el encargado del seguimiento, documentación y análisis de los incidentes de seguridad reportados por los usuarios, así como la comunicación a las directivas de EMAB
- Debe crear y coordinar un comité que se encargue de la gestión y respuesta a incidentes de seguridad de la información.
- Junto con el jefe de la oficina de Talento Humano son responsables de poner en conocimiento los procedimientos de gestión de incidentes a los trabajadores y contratados al inicio de la relación laboral.
- Registrar, clasificar y asignar responsabilidad de solución a los incidentes de Seguridad de la Información.
- Implementar una plataforma tecnológica para la adecuada atención y registros históricos de incidentes de seguridad de la información.
- Tener y diligenciar un formato de reporte de Incidentes de Seguridad de la Información. (*Anexo A*).
- Generar reportes necesarios para el monitoreo de los incidentes.
- Crear junto con el Consejo de Administración el Equipo de Respuesta a Incidentes.
- Liderar el Equipo de Respuesta a Incidentes.
- Velar por el correcto funcionamiento y operación de la Gestión de Incidentes de Seguridad de la Información.
- Monitoreo constante de la oportuna solución de los Incidentes con problemas de cierre.
- Tener y diligenciar un formato de Historial de Incidentes de Seguridad de la Información. (*Anexo B*).

Coordinadores de Area

- Deben atender las convocatorias, solicitudes y consultas realizadas por el responsable de TIC, bajo el marco de la atención a incidentes de seguridad que puedan comprometer la integridad, disponibilidad y confidencialidad de la información.

Colaboradores

- Todo el personal de la organización es responsable de reportar debilidades e incidentes de seguridad oportunamente al responsable de TIC y cumplir con lo establecido en este documento.

4. PLAN DE ACCIÓN

a) Realizar un levantamiento de los servicios informáticos.

Llevar a cabo un inventario de equipo de cómputo, software y mobiliario, para determinar cuál es la información crítica que se tiene que resguardar, adicionalmente levantar un inventario de los servicios de cómputo, telecomunicaciones, internet, etc., que son requeridos para que los usuarios estén en posibilidad de llevar a cabo sus actividades normales.

b) Identificar un conjunto de amenazas.

Identificar los tipos de siniestros a los cuales está propenso cada uno de los procesos críticos, tales como falla eléctrica prolongada, incendio, terremoto, etc.
Identificar el conjunto de amenazas que pudieran afectar a los procesos informáticos, ya sea por causa accidental o intencional.

c) Revisar la seguridad, controles físicos y ambientales existentes, evaluando si son adecuados respecto a las amenazas posibles.

Se deben estar preparado para cualquier percance, verificando que dentro de la EMAB S.A. ESP se cuente con los elementos necesarios para salvaguardar sus activos.

d) Identificar los servicios fundamentales de la EMAB S.A. ESP (factores críticos).

Se deben analizar las funciones de mayor prioridad de la EMAB S.A. ESP, por medio de flujogramas de procesos específicos para medir el alcance de cada actividad.

5. DESCRIPCIÓN

5.1. ETAPAS DE METODOLOGÍA

En el Plan de Contingencia Informático se establecen procedimientos preventivos para el manejo de casos de emergencia que se presenten en la EMAB S.A. ESP al sufrir una situación anormal, protegiendo al personal, las instalaciones, la información y el equipo.
Existen diferentes tipos de contingencia de acuerdo a los daños sufridos:

Menor: Es la que tiene repercusiones sólo en la operación diaria y se puede recuperar o restablecer la operación de las actividades en menos de ocho (8) horas.
Grave: Es la que causa daños a las instalaciones, pero pueden reiniciar las operaciones en menos de veinticuatro (24) horas.
Crítica: Afecta la operación y a las instalaciones, éste no es recuperable en corto tiempo y puede suceder porque no existen normas preventivas o bien porque estas no son suficientes. También puede suceder por ocurrir algún tipo de desastre natural como un terremoto.

Tipos de contingencias de acuerdo al grado de afectación:

- En el mobiliario.
- En el equipo de cómputo en general (procesadores, unidades de disco, impresoras, etc.) En Comunicaciones (hubs, ruteadores, nodos, líneas telefónicas, etc).
- Información.
- Instalaciones.

a) Establecer un grupo de trabajo y definir roles

En caso de presentarse algún tipo de inconveniente que amerite iniciar el Plan de Contingencia TIC el o los Líderes del proceso afectado o afectados de común acuerdo con el Gerente establecerán los roles y acciones a tomar para reactivar el servicio, corrigiendo de forma definitiva la inconsistencia.
El Gerente es el responsable de aprobar la realización del Plan de contingencia TIC, dirigir los comunicados de concientización y solicitud de apoyo a los jefes y/o Gerentes de las diferentes áreas involucradas.
Al declararse una contingencia el Gerente y el Profesional de sistemas deberán tomar las decisiones correspondientes a la definición de las ubicaciones para instalar el centro de cómputo alterno y autorizará las inversiones a realizar, así como el fondo de efectivo a asignarse para los gastos necesarios iniciales.

El líder del proceso y el Gerente mantendrán permanentemente informado respecto de la activación del Plan hasta la declaración de conclusión.
Durante la realización del Plan, el profesional de sistemas, el gerente y el subgerente administrativo, coordinarán la realización de las pruebas del Plan de Contingencia, la aprobación de las ubicaciones alternas que sea necesario definir, la aceptación de los gastos y/o adquisiciones o contratos de servicios que sean necesarios para la realización del Plan, de forma coordinada con los involucrados en las acciones a tomar.

b) Pruebas y mantenimiento del plan de continuidad

El plan de continuidad se considera válido al momento de superar satisfactoriamente un plan de pruebas que asegure la viabilidad de las soluciones adoptadas. Este plan de prueba debe tener como objetivos:

- Evaluar la capacidad de respuesta ante una situación que afecte activos de la organización.
- Probar efectividad de los tiempos de respuesta.
- Identificar en cuales áreas de la organización se deben realizar mejoras.
- Comprobar si los procedimientos establecidos son suficientes para soportar la recuperación total de las operaciones.
- Evaluar si el personal que pertenece a cada una de las áreas está bien capacitado sobre las acciones que debe realizar en un escenario de contingencia.
- Capacitar a los colaboradores.

c) Tipos de pruebas

Las pruebas del plan de continuidad deben tener dos características principales:
realismo y exposición mínima.

- Realismo: se deben proporcionar escenarios que entreguen un nivel de entrenamiento adecuado a las situaciones de riesgo.
- Exposición mínima: las pruebas deben causar un impacto en las operaciones del negocio, es decir, que si se programa una prueba que suponga una parada de los sistemas de información, debe realizarse una ventana de tiempo que impacte lo menos posible para el negocio.

d) Ejercicios Técnicos

En estos tipos de ejercicios se requiere ejecutar procedimientos de reporte y operativos, uso de software y hardware y centros alternativos para asegurar un rendimiento adecuado. En un ejercicio de simulación se debe verificar:

- Canales de comunicación para el reporte de las emergencias.
- Canales de telecomunicaciones de respaldo.
- Capacidad y rendimiento del hardware.
- Portabilidad del software.
- Acceso a los centros de respaldo.
- Movilización de los equipos de trabajo.
- Recuperación de datos.

e) Mantenimiento del plan de continuidad

Debido a la dinámica de las operaciones de la organización, pueden aparecer nuevos procesos, nueva infraestructura, nuevos sistemas de información y nuevos activos informáticos que deben ser incluidos dentro del plan. Es por esto que se debe planificar correctamente el mantenimiento del plan para evitar que queden procesos o actividades del negocio por fuera y que en caso de contingencia no se pueda dar respuesta a las necesidades.

Al término de la realización de las pruebas, será el profesional de sistemas quien da visto bueno de la conclusión de éstas y de los resultados obtenidos, rindiendo un informe de forma coordinada con los responsables de proceso involucrados, y en caso de ser necesario, convocar a la realización de una segunda prueba, corrigiendo previamente las fallas que se hubieran presentado. Una vez que se encuentre aprobado el Plan de Contingencia, será el líder de proceso quien lleve a cabo formalmente la declaración de una contingencia grave y de inicio formal a la aplicación del Plan, cuando así lo considere conveniente, propiciando que la contingencia desaparezca con el objeto de continuar normalmente con las actividades, será el responsable de dar por concluida la declaración de contingencia por escrito o vía electrónica.

El subgerente administrativo y el profesional de sistemas es el responsable de determinar los procedimientos a seguir en caso de que se presente una contingencia que afecte las comunicaciones, servicios de internet, intranet, correo electrónico y red de la EMAB S.A. ESP, mantener actualizados dichos procedimientos en el plan de contingencia, determinar los requerimientos mínimos necesarios, tanto de equipo como de software, servicios, líneas telefónicas, cuentas de acceso a internet, enlaces dedicados, dispositivos de comunicación (ruteadores, switchs, antenas, etc.). Así mismo, deberá mantener actualizado el inventario de equipo de telecomunicaciones y redes, efectuar los respaldos correspondientes y llevar a cabo las pruebas de operatividad necesarias, para asegurar la continuidad del servicio, en caso de que se llegara a presentar alguna contingencia, ya sea parcial, grave o crítica.

El Subgerente administrativo y el personal a su cargo, son los responsables de mantener el directorio de contactos, proveedores y usuarios de los servicios antes descritos y mantenerlo permanentemente actualizado e incluirlo dentro del Plan de Contingencia TIC. Coordinará las actividades correspondientes a los servicios de comunicaciones al declararse una contingencia, hasta su restablecimiento total.

El profesional de sistemas y el personal a su cargo son los responsables de llevar a cabo el inventario de equipo, software y equipos periféricos, como impresoras, CD Writer, escáneres, faxes, copiadoras, etc., mantener los equipos en óptimas condiciones de funcionamiento; determinar la cantidad mínima necesaria de equipo y sus características para dar continuidad a las operaciones de la EMAB S.A. ESP; es responsable de elaborar o coordinar con los usuarios los respaldos de información.

Deberán realizar los procedimientos correspondientes para la emisión de los respaldos de cada uno de los servidores o equipos en donde se procese lo enunciado en el párrafo anterior, efectuar y mantener actualizado el directorio de proveedores de equipos, garantías, servicio de mantenimiento y reparaciones, suministros, refacciones y desarrollo de software, en su caso, e incluirlo dentro del Plan de Contingencia TIC.
En caso de que se declare alguna contingencia que afecte a los equipos y al software, sea cual fuere su grado de afectación, es el responsable de restablecer el servicio a la brevedad, con el objeto de que no se agrave el daño o se llegara a tener consecuencias mayores.

El Profesional de sistemas y el personal a su cargo serán los responsables de determinar los sistemas críticos de la EMAB, que, en caso de presentarse alguna contingencia como corte de energía eléctrica prolongada, temblor, incendio, falla del sistema de cómputo, pérdida de documentación, o alguna otra causa determinada, se llegara a afectar sensiblemente la continuidad de las operaciones en las áreas que utilicen dichos sistemas críticos. En caso de cambiar a otras instalaciones alternas, el Profesional de sistemas, deberá definir cuáles serían las actividades que se deberán seguir para la configuración o instalación de los sistemas desarrollados, optimizando los recursos con los que se cuente, realizando las pruebas necesarias hasta su correcto funcionamiento en las terminales destinadas para su operación. Deberá mantener actualizada la documentación, resguardándolos fuera de las instalaciones para su consulta y utilización al momento de requerirse.

El líder del proceso dará aviso al Gerente y al Subgerente administrativo, cuando a su juicio, las circunstancias que provocaron la activación del plan hubieran desaparecido y se estuviera en condiciones de continuar normalmente con las actividades. En caso de requerir de actividades complementarias para regresar a las actividades normales, especialmente cuando se trate de los sistemas informáticos de la EMAB S.A. ESP, deberán incluir el plan de actividades que se deberá seguir para retornar a la situación normal.

Determinar los eventos que pueden afectar adversamente a la EMAB S.A. ESP y su infraestructura, con interrupción o desastre en materia TIC

Los desastres y crisis son eventos que pueden inhabilitar a la EMAB S.A. ESP de proveer normalmente sus servicios a los usuarios internos y la atención al público en general, por lo que deben identificarse, analizar su nivel de riesgo y tomarse las medidas necesarias de prevención.

f) Análisis de Riesgos

Se deben identificar aquellas debilidades actuales que por su importancia puedan motivar la puesta en marcha del Plan de Continuidad del Negocio. Este análisis de riesgos debe centrarse en los procesos de la organización, iniciando con los que sean considerados como críticos y se debe extender a aquellos que no lo sean.
Este análisis de riesgos debe estar compuesto por:

- ✓ **Identificación de Activos:** es necesario realizar un inventario de los activos involucrados en los procesos que se van a incluir en el plan. Algunos ejemplos de activos pueden ser: Datos personales, equipamiento, propiedad intelectual, sistemas y aplicaciones.
- ✓ **Identificación de Amenazas:** al momento de analizar los riesgos, se debe hacer una evaluación de las distintas amenazas, que pueden ser: humanas (no intencionadas e intencionadas por personal interno o externo) y naturales (inundaciones, incendios, etc.). Una vez identificadas las amenazas, se debe establecer cuales pueden afectar en forma grave a la organización y se debe valorar la probabilidad de ocurrencia.
- ✓ **Evaluación de Vulnerabilidades:** se deben identificar las distintas situaciones en que una amenaza pueda cumplir su cometido, evaluando si el nivel de protección es suficiente para evitar que se materialice la amenaza. Se deben tener en cuenta diferentes escenarios al momento de evaluar las vulnerabilidades.

- ✓ **Evaluación del Impacto:** la valoración del impacto se puede hace de forma cuantitativa, estimando las pérdidas económicas que causaría la ocurrencia de un incidente, o de forma cualitativa, asignando un valor dentro de una escala (alto, medio, bajo). Un ejemplo sería el robo de información personal sensible, lo que puede causar un impacto alto por sanciones económicas por parte de la SIC y adicionalmente afectaciones a la imagen de la organización.

- ✓ **Evaluación del Riesgo:** El riesgo depende de la probabilidad de la ocurrencia de incidentes y es directamente proporcional a los valores de las amenazas y el impacto calculado.

- ✓ **Evaluación de Controles:** los controles que se utilizan para mitigar los riesgos identificados se pueden clasificar en *controles preventivos, controles detectivos y controles correctivos.*
    - *Controles preventivos:* son aquellos que identifican riesgos potenciales antes de que ocurran y previenen errores o actos maliciosos. Ejemplos: backups de las bases de datos, políticas de seguridad, pólizas de seguros.
    - *Controles Detectivos:* son aquellos que identifican y reportan la ocurrencia de una falla o un acto malicioso. Ejemplo: Software antivirus, detectores de intrusos, sensores de humo, auditorías periódicas a los procesos.

Controles correctivos: son los que minimizan el impacto causando por una amenaza, solucionan las fallas detectadas por los controles detectivos, identifican la causa de la falla y la corrigen y permiten modificar los procedimientos actuales con el fin de minimizar futuras ocurrencias de la misma falla.

5.2. SELECCIÓN DE ESTRATEGIAS

Existen diferentes estrategias para mitigar el impacto que pueda causar una interrupción, por eso es importante que la organización conozca muy bien sus procesos y la criticidad de cada uno de ellos, para que seleccione adecuadamente sus estrategias teniendo en cuenta unos parámetros de tiempo, disponibilidad y costos, dependiendo de las funciones del negocio.
A continuación, se relacionan algunas de las estrategias que se pueden implementar al interior de la organización:

- ✓ No hacer nada es una estrategia que se puede utilizar en aquellas situaciones que se hayan clasificado como “no urgentes” en el análisis de impacto.
- ✓ Utilizar espacios propios de la compañía, alternos a los de operación (cafeterías, salas de juntas, etc.).
- ✓ Reutilización de recursos, reubicando personal que pertenezca a procesos NO urgentes en otras tareas que requieran mayor prioridad.
- ✓ Teletrabajo o trabajo remoto que da la posibilidad de trabajar desde el exterior mediante conexión remota.
- ✓ Realizar acuerdos recíprocos con otra organización o entre áreas propias de la organización que tengan características de espacio e infraestructura similares, que permita recuperar funciones en la otra locación.
- ✓ Contratación con empresa especializadas de espacios alternativos para la recuperación de la operación. Estas compañías pueden proporcionar diferentes soluciones tales como: espacio dedicado, espacio compartido, espacios móviles y módulos prefabricados.
- ✓ Implementar localizaciones diversas donde se traslada la operación, pero no el personal.
- ✓ Tener un centro replicado (*mirror*) que permita trasladar de forma inmediata la operación.

Identificacion de amenazas:

- Terremoto
- Incendio
- Inundación y humedad
- Corte de energía
- Falla de la red de voz y datos
- Fallas en hardware o software
- Sabotaje o daño accidental

a. Terremoto

Sin pérdida o daños menores de las instalaciones: El siniestro puede afectar únicamente parte de la estructura de las instalaciones, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera de las instalaciones, el impacto provocaría en la Gobernación sería menor, puesto que las actividades se interrumpirían por unas horas o hasta por un día completo.
Con pérdida de las instalaciones: La pérdida de las instalaciones afectaría gravemente a las operaciones de la Gobernación del Meta y los datos pueden verse dañados seriamente. En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente.

b. Incendio

(Site de cómputo): Se tiene gran impacto en la información ya que los sistemas utilizados residen en los servidores y dispositivos de comunicación localizados en el Sitio de Cómputo y en caso de sufrir algún daño, se requerirá adquirir un nuevo equipo, así como de instalar nuevamente el sistema, configurar el Servidor y restaurar los respaldos para continuar trabajando.
Áreas distintas al site de cómputo: Un incendio dependiendo de su magnitud, puede afectar desde las estaciones de trabajo o periféricos y dispositivos de comunicación localizados en el Centro de Cómputo. En el caso de las primeras el impacto que tendría en la EMAB S.A. ESP es menor, puesto que la información o tiempo de operación que se pierde no tiene gran repercusión en las operaciones generales, ya que puede restablecerse en un tiempo relativamente corto.

c. Inundación y humedad

Puesto que es equipo electrónico el que se maneja dentro de la institución, una inundación severa dañaría los dispositivos irremediablemente deteniendo las operaciones de la misma totalmente.
Un daño grave correspondería a una inundación en el Centro de Cómputo, en tanto que una inundación parcial o limitada a parte de las instalaciones (no al Centro de Cómputo) podría ocasionar un daño medio sí no va seguido de corto circuito.
Corte de energía
Las operaciones informáticas de la EMAB S.A. ESP se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolonga por tiempo indefinido se provocaría un trastorno en las operaciones del día, sin afectar los datos.
Fallas de la red de voz y datos
RED: Representa la columna vertebral de las operaciones de la EMAB S.A. ESP, si la red falla en su totalidad, las operaciones se detienen con la consecuente falta del servicio informático.

Aplicaciones: La falla en los sistemas utilizados, representa un impacto medio en las operaciones totales de la EMAB S.A. ESP, ya que pueden ser reinstalados casi de inmediato.

Fallas en hardware o software

Las alteraciones que sufran los servidores tanto en Hardware y Software pueden ser corregidas en la mayoría de los casos, sin embargo, si las alteraciones llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse hasta por días.

Sabotaje o daño accidental

La alteración de la información requiere de la restauración de los respaldos y de pruebas posteriores para contar con la integridad de los datos. Es posible que se requieran reprocesos de captura de datos, dependiendo de las fechas de los respaldos que se tengan disponibles.

5.2.1. Evaluar la efectividad de los controles y dispositivos de seguridad

Se debe contar con un sistema de seguridad en materia informática, considerando los medios a su alcance que permitan el normal desarrollo de las diversas actividades laborales, previniendo las posibles causas, condiciones de accidentes y siniestros, es necesario determinar las medidas más convenientes y llevarlas a cabo realizando inspecciones periódicamente.

Una vez que se tiene el inventario de los dispositivos de seguridad implantados junto a la gestión realizada en Salud Ocupacional a través del COPASO y de los brigadistas, evaluar su efectividad; lo anterior va muy relacionado al grado de actualización y modernidad de los elementos de seguridad identificados, por ejemplo, si se cuenta con extintores y estos son demasiado antiguos, deben probarse y certificarse, con el objeto de que llegado el momento sean realmente utilizables y efectivos, de lo contrario, deberán ser sustituidos por equipos modernos.

Actualmente las instalaciones cuentan con extintores de fuego instalados en todas las instalaciones que conforman cada secretaria, dichos extintores se les da el mantenimiento adecuado y se encuentran al alcance del personal en caso de suceder un conato de incendio.

5.3. PROCEDIMIENTO DE ACTIVACION DE LOS DISPOSITIVOS DE SEGURIDAD

5.3.1. Extintores

Los extintores tienen la intención de usarse en un tipo en particular de riesgo, así que se debe de poner especial atención en colocarlo cerca de las posibles áreas de riesgo que deben proteger.

Los letreros y símbolos que se detallan a continuación deberán revisarse con todo el personal que se espera pueda llegar a usar el extintor. Todos deberán estar familiarizados con estos símbolos y dibujos que identifican el tipo de fuego en los cuales se pueden usar.

CLASE A **CLASE B**
(COMBUSTIBLES ORDINARIOS) (LIQUIDOS FLAMABLES Y GASES)
Madera, papel, caucho, Gasolina, aceites,
Telas y plásticos pinturas, lacas y brea.
CLASE C **CLASE D**
(FUEGOS QUE INVOLUCRAN (METALES Y COMBUSTIBLES) EQUIPO ELECTRONICO)
CLASE K
(FUEGOS EN EQUIPOS DE COCINA)
Aceites y grasa vegetales y/o animales

Todo el personal debe conocer muy bien las instrucciones de cualquier extintor en caso de llegar a usarlo.

5.3.2. Procedimiento de respaldo y recuperación

Establecer normas de seguridad como son:

- Definir los procedimientos que indique los datos, programas, etc., que es importante respaldar; por servidor, sistema y ubicación.
- Identificar cada uno de los métodos que se utilizan, para llevar a cabo los respaldos de información, así como los procedimientos para su ejecución y restauración.
- Especificar el lugar donde se encuentran custodiados los respaldos de información o copia de los respaldos, lugar fuera de las instalaciones.

En esta parte, debe incluirse los procedimientos de respaldo y recuperación de la información de los sistemas, así como de los programas o aplicaciones y de los sistemas operativos.
Establecer los procesos informáticos críticos y las prioridades de recuperación de los sistemas, de forma tal que el tiempo de recuperación sea alcanzado
Determinar los tiempos de recuperación y los requerimientos mínimos de recursos.

Para cada una de las fases críticas que se cubrirán con el Plan de Contingencia Informático, se deben determinar los tiempos mínimos requeridos para el establecimiento del plan, esto es, cuanto tiempo debe transcurrir desde el momento en que se inicia o activa el plan, hasta que las actividades, funciones o sistemas de encuentren en operación total o parcialmente.
Es conveniente definir un tiempo aceptable y viable para que la red y la aplicación principal estén nuevamente activas.

Para situaciones críticas:

- Incluir el traslado de los medios de almacenamiento magnético que se encuentren fuera de las instalaciones.
- La copia de los datos a los nuevos medios de almacenamiento magnético y la habilitación de las comunicaciones, servicios de Internet, y correo electrónico.
- El personal mínimo requerido para continuar operando.
- Tiempo de restauración de cada uno de los servicios de Red, Comunicaciones, Internet y Correo Electrónico.
- el tiempo determinado debe ser conocido y aceptado por todos los usuarios principales que operan los sistemas o cuentan con un equipo crítico.

Para situaciones de bajo riesgo:

- Tiempo de reparación o reposición de una estación de trabajo (PC)
- Tiempo de configuración de las PC
- Tiempo de respuesta del proveedor para la reparación de los servidores (verificar contratos garantías).
- Tiempos de reparación de fallas eléctricas.
- Tiempo de restauración de cada uno del servidor y sus aplicaciones.

5.3.3. Tiempos de recuperación y especificaciones

Situaciones críticas cuya afectación inutilice el centro de cómputo y las instalaciones de la EMAB S.A. ESP

- Establecer un centro de cómputo alterno de 72 hrs. Mínimo.
- Es necesario evaluar en primera instancia la gravedad del daño, si se determina que la reparación del equipo es viable en poco tiempo (8 hrs. Máximo), se requerirá al proveedor del mantenimiento del equipo o al fabricante, el envío inmediato de sus ingenieros de servicios y llevar a cabo la reparación del equipo.
- En caso de habilitarse un servidor emergente, aún con capacidad menor al dañado, deberá quedar configurado con carga de aplicaciones y de información en mínimo 48 hrs. De acuerdo con el personal del área, en términos generales, este tiempo estimado, es con base a su experiencia.
- Al concluirse la reparación del equipo, se regresará a servicio el servidor reparado, buscando realizar esto durante horas no hábiles o no críticas de atención al ciudadano, con el objeto de no entorpecer las actividades normales del personal usuario.
- Falla de cableado. - Para reparaciones mínimas el profesional experto en redes lo realizara máximo en 6 hrs. Para efectuar el recableado o sustitución del tramo de cable dañado, es importante remitirse a la garantía con el proveedor que realizo el cableado.
- Falla de enlaces y Router.- Se deberá solicitar al proveedor la restauración del servicio, el cual por lo regular tarda 24 horas en restablecerse, a menos de que se trate de daño mayor, el cual puede tardar aprox. 72 horas.
- Fallas en PC: Remitirse a procedimiento soporte usuarios y mantenimiento correctivo.
- Fallas de Internet: Cuando se trate de fallas de acceso en Internet causadas por el proveedor del servicio (TELEBUCARAMANGA), se deberá tener comunicación con el ejecutivo de cuanta para realizar el soporte del daño y para establecer el tiempo en el que se estará sin servicio.

5.4. REQUERIMIENTOS MINIMOS DE RECURSOS

Los PC´s para los usuarios y para personal que operaría en las instalaciones alternas, deberá contar con la siguiente configuración mínima:

- Windows 7 o superior.
- Office 2013 o Superior.
- Antivirus

Impresoras:

- 2 impresoras de alto volumen.

Red:

- Cableado estructurado mínimo CAT 6 interconectado mediante Switchs.
- Salida a Internet por medio de la Red.
- Proveedor de servicio de internet.

5.4.1. Seleccionar los sitios alternativos y el almacenaje off-siete (fuera de lugar habitual)

Es un factor importante prepararse para algo que probablemente pueda ocurrir, especialmente cuando se involucra a os sistemas de cómputo. Cuando se depende de los anteriormente mencionados, un desastre puede o no dejar continuar las operaciones de la EMAB S.A. ESP.

En el momento que se presenten situaciones de desastre, el regresar a la normalidad va más allá de mantener los sistemas de información en orden y consistentes. Por lo anterior, es importante saber qué se va a recuperar y quien puede hacerlo en caso de pérdidas humanas.

Las instituciones se enfrentan a una amplia gama de desastres: desde los locales, que ocurren en el interior de la empresa, en un espacio determinado del edificio, hasta los que afectan todas las instalaciones de la misma o aquellos que abarcan una región entera.
Es importante considerar al seleccionar el sitio alterno los costos tangibles que estos provocan y no siempre pueden certificarse: incumpliendo con contratos, pérdida de activos y la necesidad de reemplazarlos, el tiempo improductivo de personal, etc.
Los desastres mayores pocas veces ocurren con frecuencia. Sin embargo, las consecuencias negativas que ocasionan pueden ser tan graves que la mayoría de las instituciones han estado estableciendo como una política indispensable el contar con un plan de recuperación ante contingencias.

5.4.2. Desarrollar los procedimientos detallados de respuesta a emergencia
Desarrollar e implementar los procedimientos de respuesta a emergencia de la situación que sigue a un incidente o evento, incluyendo establecer y gestionar un centro de operaciones de emergencia.

5.4.2.1. Terremoto
Análisis de daños:

- **En caso de daño mayor e imposibilidad de acceder a las instalaciones**

Este tipo de procedimiento se tomará únicamente cuando el daño en las instalaciones haga imposible la continuación de las actividades, por lo que es preciso el traslado de las mismas a las instalaciones consideradas como alternas con el proveedor correspondiente que proporcione dicho servicio.
Mientras las operaciones continúan en las instalaciones alternas se evaluará la posibilidad de regresar a las instalaciones de la EMAB S.A. ESP, o establecer operaciones en un nuevo sitio.

Procedimientos y responsables

1. Trasladar los respaldos de datos, programas, manuales y claves, al centro de respaldo u oficinas alternas correspondientes con el propósito de reiniciar operaciones. *Responsable:* Profesional de Sistemas.
2. Restaurar la información de las bases de datos y programas. Responsable: Profesional sistemas.
3. Revisar y probar la integridad de los datos. Responsable: Profesional sistemas.
4. Iniciar las operaciones. Responsable: Profesional sistemas

- **En caso de daño menor:**

Procedimientos y responsables

1. Proceder a tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable: Subgerencia administrativa, Profesional de compras y activos fijos, y Profesional de sistemas.
2. Recoger los respaldos de datos, programas, manuales y claves del lugar en donde se encuentren resguardados. Responsable: profesional de sistemas.
3. Instalar el sistema operativo. Responsable: sistemas.

4. Restaurar la información de las bases de datos y programas. Responsable: Profesional sistemas.
5. Revisar y probar la integridad de los datos. Responsable: Profesional sistemas.
6. Iniciar las operaciones.

La continuidad de las operaciones en este tipo de siniestro dependerá del grado de afección de estructura de las instalaciones, ya que las afecciones pueden ir desde el no daño de la estructura, daño parcial, hasta la inhabilitación completa del edificio.

5.4.2.2. Incendio

Análisis de daños

- **En caso de daño mayor a imposibilidad de acceder a las instalaciones**

Este tipo de procedimientos se tomará únicamente cuando la reparación de las instalaciones llegase a tardar mucho tiempo, durante este periodo de restauración se debe dar continuidad a las operaciones por lo que es preciso el traslado de las operaciones a instalaciones alternas, que actualmente se tiene en la sede operativa de la Empresa de Aseo de Bucaramanga EMAB S.A. E.S.P.

Mientras las operaciones continúan en otras instalaciones, se evaluará la posibilidad de regresar a las instalaciones de la EMAB S.A. ESP inicialmente afectadas o establecer operaciones en un nuevo sitio.

Así mismo, el Gerente, Director Administrativo y los líderes de proceso deberán reunirse con el objeto de hacer un recuento rápido de los daños, determinar si es posible o no continuar utilizando las instalaciones y/o por cuanto tiempo aproximadamente se deberá operar fuer a de las instalaciones o si la emergencia afectará sólo una parte de las instalaciones.

En esa reunión se determinará la ubicación o ubicaciones alternas que ocupará cada una de las áreas y la manera como se llevará a cabo la coordinación y control de las operaciones de la EMAB S.A. E.S.P.

- **Reporte de Incidentes de Seguridad al CSIRT.**

Por medio del reporte se debe comunicar el incidente de seguridad de la información de manera oportuna a través de canales adecuados de comunicación como correo electrónico, teléfono o en forma física. En tanto, cuando sea necesario, se debe disponer del documento “Reporte incidente Seguridad de la Información” (*ver Anexo A*) para que los usuarios lo diligencien. Una vez recibidos y consolidados los registros internos de incidentes que involucren datos personales, el equipo de Gestión de Incidentes debe llevar a cabo la fase de identificación, la cual comprende lo siguiente:

- ✓ Verificar que lo reportado sea realmente un incidente de seguridad
- ✓ Poner en cadena de custodia las que sean consideradas evidencias potenciales.
- ✓ Determinar la gravedad del incidente.

- **Determinar la clasificación del incidente**

Se debe tener en cuenta la criticidad de cada uno de los recursos tecnológicos y de la información que estos procesan, con el fin de determinar los efectos negativos o potenciales que pueden causar los incidentes de seguridad para la organización. Así mismo, se deben definir los tiempos de respuesta a los incidentes dependiendo de su impacto a las operaciones de la organización.

- **Contención del Incidente de Seguridad**

Una vez el CSIRT haya confirmado la ocurrencia del incidente de seguridad, se debe hacer una evaluación completa de la situación, esto se debe hacer en conjunto con los administradores de los sistemas que se vieron afectados por el incidente, con el fin de coordinar las acciones que se llevarán a cabo.

Para realizar la contención se debe tener en cuenta lo siguiente:

- ✓ Activar al CSIRT para contener el incidente.
- ✓ Notificar a los responsables de los procesos que se hayan visto afectados por el incidente.
- ✓ Junto con el área de TI implementar estrategias de contención del incidente.
- ✓ Mantener la cadena de custodia de las evidencias.

- **Documentar los procedimientos realizados**

Erradicación de las causas del incidente

En esta fase se debe erradicar por completo la causa del incidente de seguridad, esto se puede hacer reestableciendo sistemas a un estado anterior, eliminar la causa raíz instalando parches de seguridad, analizar vulnerabilidades para evitar reincidencias, entre otras.
Es importante concluir las siguientes actividades:

- Determinar las causas del incidente (malware, desastre natural, denegación de servicio, etc.)
- Apoyarse en las versiones más recientes de respaldos de seguridad (backup de bases de datos, software aplicativo, sistemas operativos, etc.)
- Una vez identificada la causa, hay que eliminarla.
- Realizar una evaluación de las soluciones (evaluación de parches, análisis de vulnerabilidades, etc.)

- **Restablecimiento de las operaciones (recuperación)**

El restablecimiento de las operaciones depende del alcance del incidente de seguridad y los sistemas que se vieron afectados. Por lo anterior, se debe determinar si es posible restaurar el sistema afectado y realizar las mínimas alteraciones posibles o, por el contrario, si es necesario reconstruir por completo el sistema.
Algunas actividades que debe realizar el CSIRT son:

- Restablecer las operaciones a su estado normal (restaurando copias de seguridad, dispositivos de alta disponibilidad, activando plan de continuidad de negocio, entre otras)
- Validar si fueron correctas las acciones tomadas.
- Informar a los responsables de los procesos afectados del restablecimiento de las operaciones.

- **Recolección de evidencias.**

Cuando se presenten incidentes de seguridad que generen responsabilidad civil o penal se debe considerar que las evidencias asociadas a estos tengan validez legal y reúnan los requisitos que establece la normatividad vigente que regula la recolección de evidencia digital. Así mismo se deberán tener en cuenta las siguientes consideraciones:

- ✓ La evidencia debe ser recolectada, retenida y presentada conforme a las reglas y requisitos establecidos en la ley.
- ✓ En la recolección, almacenamiento y procesamiento de la evidencia, ésta debe contar con un custodio y mecanismos de protección adecuados para respetar la cadena de custodia y garantizar su integridad.

- ✓ Cuando en la recolección de evidencia hay documentos en papel, el original debe ser guardado de forma segura y registrando los datos de la persona que hizo el hallazgo, consignando además el lugar donde lo encontró, la fecha y quien presenció el hallazgo, garantizando que los documentos originales no hayan sido alterados.
- ✓ El reporte de evidencias podrá adjuntar información como capturas de pantalla, archivos de error, archivos volátiles, lo que serviría de evidencia.
- ✓ El CSIRT debe crear un archivo que se llame "Historial de Incidentes de Seguridad de la Información", diligenciarlo y mantenerlo actualizado con información de los reportes de todos los incidentes de seguridad.
- ✓ Mantener actualizado el Directorio de Contactos para la atención de incidentes de seguridad de la información.

- **Documentación del Incidente de Seguridad (Lecciones aprendidas)**

En esta fase se debe hacer un informe con toda la información recopilada desde el momento de la detección del incidente, hasta el restablecimiento normal de las operaciones. Este informe debe contener:

- ✓ Tipo de incidente
- ✓ Causas
- ✓ Tipo y número de Titulares afectados
- ✓ Tipo y número de registros de datos personales afectados
- ✓ Activos comprometidos
- ✓ Afectaciones probables para los Titulares y la organización
- ✓ Medidas adoptadas para la Gestión del incidente.

- **Reporte del Incidente ante la SIC**

Con la información recolectada en el "Formato de Reporte de Incidentes de Seguridad" y el informe sobre la gestión del incidente, se debe notificar al Comité de Protección de Datos Personales sobre el incidente, para que se delegue al administrador de la cuenta en el RNBD, la función de reportar el incidente de seguridad en la base de datos que se vio afectada.

Anexo A: Formato de reporte de incidentes de seguridad
Medio Óptico://3. Documentación del SGSPD/TIC/A.I.12. GESTIÓN DE INCIDENTES DE LA SI/Protocolo 4.11/Anexo A Protocolo 4.11.xlsx

EMAB EMPRESA DE ASEO DE BUCARAMANGA	**Formato de reporte de incidentes de seguridad**	**Código:** **Versión:** **Página 1 de 1**
DATOS DE NOTIFICACIÓN		
Apellidos y Nombres		
Área		
Cargo		
Correo Electrónico		
Teléfono		
Fecha de notificación		
Hora de notificación		
INFORMACIÓN GENERAL DEL INCIDENTE		
Fecha de detección del incidente		

Hora de Detección del incidente	
Marque con una cruz las opciones que considere aplicables	
	Afectación de la confidencialidad e integridad de los datos personales.
	Afectación de la confidencialidad y disponibilidad de los datos personales.
	Afectación de la disponibilidad e integridad de los datos personales.
	Afectación de la confidencialidad de los datos personales.
	Afectación de la confidencialidad, disponibilidad e integridad de los datos personales.
	Afectación de la disponibilidad de los datos personales.
	Afectación de la integridad de los datos personales.
	Otro no contemplado (Descríbalo):
INFORMACIÓN SOBRE EL INCIDENTE	
Describa el incidente (sin omitir detalles):	
Describa brevemente como detectó el incidente:	
¿El incidente se encuentra en proceso? [ ] SI [ ] NO	
Tiempo estimado de duración del incidente:	
Si es posible, registre el nombre de las personas que han ingresado al sistema afectado desde que se detectó el incidente:	
INFORMACIÓN DEL RECURSO AFECTADO	
Sistema, aplicación, servidor, computadora, red afectada:	
Servicios afectados:	Localización física
Describa la información contenida en el sistema/computador:	
¿Existe copia de seguridad de los datos o software afectado?	[ ] SI [ ] NO
¿Hace cuánto se realizó la última copia de seguridad?	[ ] días [ ] meses
¿El recurso afectado está conectado a la red corporativa?	[ ] SI [ ] NO
¿El recurso afectado está conectado a internet?	[ ] SI [ ] NO
¿Nombre del sistema operativo?	

Anexo B: Historial de Incidentes de Seguridad de la Información.

Medio Óptico://3. Documentación del SGSPD/TIC/A.I.12. GESTIÓN DE INCIDENTES DE LA SI/Protocolo 4.11/Anexo B Protocolo 4.11.xlsx

EMAB EMPRESA DE ASEO DE BUCARAMANGA	Historial de Incidentes de Seguridad de la Información						Código: Versión: Página 1 de 1	
Incidente Nro.	Fecha de reporte del incidente	Tipo de incidente	Recursos e información afectados	Origen Resuelto SI	Origen Resuelto NO	Tiempo de la solución	Responsable de la solución	Firma del responsable de la solución.

6. HISTORIAL DE REVISIÓN

VERSIÓN	DESCRIPCIÓN	FECHA
1.0	Documento Original	12 de abril de 2022