GOBIERNO DE
EL SALVADOR

CENTRO INTERNACIONAL
DE FERIAS Y CONVENCIONES
DE EL SALVADOR

PLAN DE CONTINGENCIA

UNIDAD DE INFORMATICA

San Salvador, El Salvador

2022

Contenido

I. INTRODUCCIÓN

El Centro Internacional de Ferias y Convenciones de El Salvador (CIFCO), considera que la información es uno de los patrimonios principales de toda Institución, por lo que se deben aplicar todas las medidas de seguridad necesarias para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos que podrían poner en riesgo la operatividad de la Institución.

Toda la evolución de la tecnología ha hecho que a lo largo de los años se cree todo un clima que ha llevado a los sistemas de información a tener máxima importancia e impacto en las instituciones públicas y privadas, la seguridad del entorno informático (hardware, software, comunicaciones, entre otros elementos tecnológicos) se ha convertido en una de las grandes preocupaciones de todos los profesionales involucrados en esta actividad. Esta preocupación debe ser adecuadamente comprendida y compartida por las instancias que toman las decisiones dentro de la institución, los cuales deben considerar las inversiones en medidas de seguridad informática, como un gasto necesario, que contribuye a mantener la operatividad y rentabilidad de la Institución.

Esto implica que los responsables del Servicio Informático, deban explicar con la suficiente claridad y con un lenguaje que sea fácil de asimilar, las potenciales consecuencias de una política de seguridad insuficiente o incluso inexistente.

Con el propósito de proteger la información y asegurar la continuidad del procesamiento de la información necesaria para el adecuado desempeño de las funciones Institucionales.

El presente documento pretende ayudar a comprender mejor la problemática implícita de los sistemas de información soportados por el computador, de las medidas de seguridad adecuadas, tanto en su número como en su rigor y nivel de aplicación, ya que toda institución debe estar preparada para el caso de ocurrencias imprevistas.

II. OBJETIVOS

Se tendrá en consideración lo siguiente:

a. Servir como referencia y guía al personal de CIFCO, ante eventos que pudieran comprometer el normal funcionamiento de procesos críticos, estableciendo fases, etapas y responsabilidades mientras dure la contingencia.

b. Proteger y conservar los activos de la Institución, de riesgos, de desastres naturales o actos mal intencionados.

c. Evaluación tanto del impacto de los riesgos, como de los costes de las medidas de contingencia, de forma que sólo se invierta lo necesario y con un objetivo claro de rentabilidad.

d. Minimizar el número de decisiones que deben ser tomadas durante la duración de un desastre o suceso de emergencia, de manera que la correcta recuperación de los sistemas y procesos queden totalmente garantizada.

e. Reanudar tan rápidamente como sea posible las funciones más críticas de CIFCO, minimizando el impacto.

f. Minimizar la pérdida económica y de información y en general, preservar la buena imagen institucional de CIFCO.

g. Evitar en la medida de lo posible la dependencia de personas o áreas específicas de CIFCO en el proceso de recuperación.

h. Reparar rápidamente los sistemas y procesos afectados volviendo a la normalidad lo antes posible.

III. ALCANCE

El Plan de Contingencia tiene como alcance a todas las Oficinas del Centro Internacional de Ferias y Convenciones de El Salvador.

IV. BASE LEGAL

Normas Técnicas de Control Interno Especificas (NTCIE) Art. 95 del Centro Internacional de Ferias y Convenciones de El Salvador.

Art. 95.- Presidencia y Dirección Ejecutiva a través de la Unidad de Informática y tomando en consideración el análisis de riesgos, deberá establecer un Plan de Contingencia adecuado para la protección de los equipos computacionales, a fin de asegurar la continuidad y restablecimiento oportuno de los sistemas de información, en caso de desastres y cualquier otro evento que los afecte. Deberá dejar documentación de prueba de los simulacros del plan de contingencia; será la Junta Directiva quien apruebe el Plan de Contingencia.

V. DESARROLLO DE LA ESTRUCTURA DEL PLAN DE CONTINGENCIA

El siguiente flujo muestra en detalle las fases y etapas por las que CIFCO atravesará una vez producido el evento que conlleve a aplicar el Plan de Contingencia.

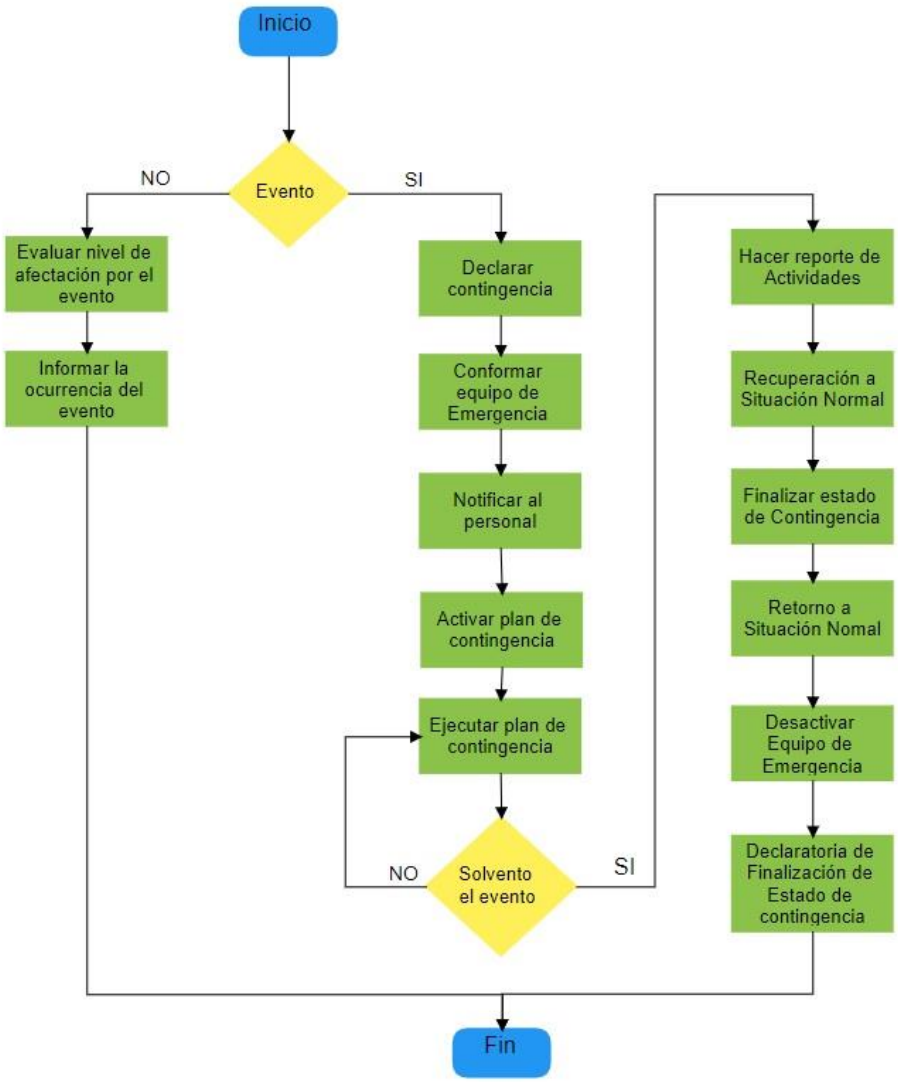


Diagrama 1. Pasos a seguir en caso de desastre y activación del Plan de Contingencia

Flujo de proceso:

Ocurrencia del evento: Cuando se suscita un evento al cual se aplicará el plan de contingencia.

Declarar contingencia: Se indica que se aplicará contingencia al evento suscitado.

Conformación equipo de Emergencia: Definición de las personas que atenderán dicho evento.

Notificación al personal: Difusión al personal afectado directa o indirectamente del evento suscitado y estado de la contingencia.

Activar Plan de Contingencia: Lo que incluye reportes de actividades, recuperación a situación normal, finalización del estado de la contingencia, todo esto dependerá del resultado de revertir los cambios a su situación normal.

Ejecutar Plan de Contingencia: Esta parte es la ejecución de cada uno de los elementos definidos en el plan de contingencia, desde la declaratoria de contingencia hasta llegar a la situación normal de las actividades.

Declaración de finalización de estado de contingencia: Determinar la situación bajo control total.

Notificar al personal: Notificar al personal afectado directa o indirectamente, que todo está restablecido.

Una vez que el evento ha sido solventado, se deben desarrollar varios pasos previos a la declaración final del estado de contingencia, los cuales se explican a continuación:

Hacer reporte de actividades: Se deben documentar todas actividades desarrolladas dentro del estado de emergencia que puedan servir posteriormente de evidencia de todas las acciones tomadas para regresar al estado de normalidad.

Recuperación a situación normal: Una vez documentadas todas las actividades, se debe volver a la situación normal, esto debe ser avalado tanto por el coordinador del equipo de contingencia como por las áreas involucradas directamente.

Finalizar estado de contingencia: Cuando ya se ha vuelto a la situación normal se finaliza el estado de contingencia y por consiguiente se regresa a la normalidad.

Desactivar Equipo de emergencia: El equipo de emergencia conformado al inicio de la emergencia en este punto es desactivado y cada uno puede volver a las actividades propias del área al que pertenece.

Declaratoria de finalización del estado de contingencia: Una vez desactivado el equipo de emergencia se debe realizar la declaratoria de finalización del estado de contingencia con lo cual se le da fin al ciclo que se originó con el evento

VI. CONFORMACION DEL EQUIPO DE CONTINGENCIA

La conformación del Equipo de Contingencia debe ser creado de manera multidisciplinario por lo cual deben estar involucradas tanto la Unidad de Informática como las unidades afectadas directa como indirectamente, con lo anterior el equipo quedara conformado de la siguiente manera:

Diagrama 2. Equipo de emergencia

Coordinador del Plan de Contingencia:

El Coordinador es quien se encarga de llevar a cabo el Plan de Contingencia es quien conoce este Plan y sabe cuáles deben ser las acciones a tomar en caso que se presente una emergencia que afecte las operaciones informáticas de CIFCO, dentro de las funciones están:

- Activar la cadena de llamadas de los integrantes del Equipo de Emergencias.
- Evaluar las condiciones y magnitud de la Emergencia.
- Distribuir los diferentes recursos para la atención adecuada de la emergencia.
- Tomar decisiones en cuanto a la evacuación total o parcial de los equipos o recursos de información.
- Coordinar las acciones operativas en la atención de emergencias.
- Recoger y procesar toda la información relacionada con la emergencia.

Recursos Humanos (RRHH):

La función principal es llamar a los integrantes del equipo de emergencia para poder llevar a cabo el plan de contingencia.

Equipo de Emergencia:

La función principal del equipo de emergencia es apoyar todo el desarrollo del Plan de Contingencia durante y después que se presente la emergencia, hasta que se establezca la normalidad de las operaciones dentro del CIFCO.

Área Involucrada:

Son las áreas afectadas por la emergencia que han sufrido un impacto de operatividad por el evento suscitado, son ellos los que al final dan el aval para que se finalice la emergencia porque han vuelto a la normalidad total posterior a la evaluación de todas sus actividades.

VII. IDENTIFICACIÓN DE RIESGOS

En ésta etapa y basándonos en una evaluación cualitativa, se ha realizado un análisis de los diferentes escenarios de riesgo a los cuales estaría expuesta CIFCO.

1. Activos a Proteger.

- Documentación Física y lógica de informática.
- La documentación, Base de datos y los sistemas Informáticos con los que cuenta CIFCO.
- Equipos de cómputo y conectividad.
- Software de aplicaciones y copias de respaldo.

2. Riesgos en la Seguridad Informática (equipos y archivos).

- **Incendios.**

  A pesar que CIFCO tiene una buena protección contra incendios, y el personal ha sido capacitado y de esta forma se está preparado, sin embargo, no se está exento a que suceda una catástrofe de este tipo y que ocasionaría pérdidas totales de información o parciales e irreparables.

- **Robo común.**

  A pesar que se tiene un buen control interno relacionado al activo fijo y la seguridad de CIFCO, no se está exento a que los equipos caigan en manos inescrupulosas y pueda suceder un hecho como este y la información quede expuesta.

- **Fallas en los equipos.**

  Se posee un buen mantenimiento de equipos e instalaciones adecuadas y acondicionadas con buena ventilación, sin embargo, no se está exento a que los equipos fallen y que de esta forma pueda haber pérdida de información.

- **Equivocaciones.**

  El nivel de preparación del empleado para afrontar una equivocación.

- **Acción de virus.**

  En CIFCO se posee un excelente antivirus, sin embargo, jamás se está exento de una infección de virus y que pueda ocasionar daños en el software y archivos de los equipos.

- **Terremotos**

  Ninguna institución está exenta a un desastre natural de esta magnitud, por lo cual se debe poseer algún tipo de medida para el resguardo de la información.

- **Inundaciones.**

  Un incremento en las precipitaciones pluviales hiciera que las alcantarillas se colapsen provocando el deterioro de la infraestructura de la oficina, así como la documentación, y el adecuado ambiente de trabajo para el personal.

- **Fallo en el suministro eléctrico.**

  Provocado por la discontinuidad en el servicio de energía eléctrica para el uso de los equipos.

- **Falla total o parcial del cableado.**

  Ocasiona pérdidas totales o parciales, por lo tanto, las actividades se encuentran interrumpidas hasta solucionar el problema.

- **A la falla de Software**

  Se produce debido a que no se hicieron las pruebas y la validación correspondiente del software para su utilización en implementaciones nuevas o de terceros (no diseñadas en CIFCO).

3. Probabilidad de Ocurrencia de Riesgos

	TIPOS DE RIESGO	PROBABILIDAD
1	Fallas en los equipos	Alta
2	Inundaciones	Alta
3	Fallo en el suministro eléctrico	Alta
4	Robo de datos	Alta
5	Incendios	Media
6	Fallo de Software	Media
7	Acción de virus	Media
8	Fraude	Baja
9	Equivocaciones	Baja

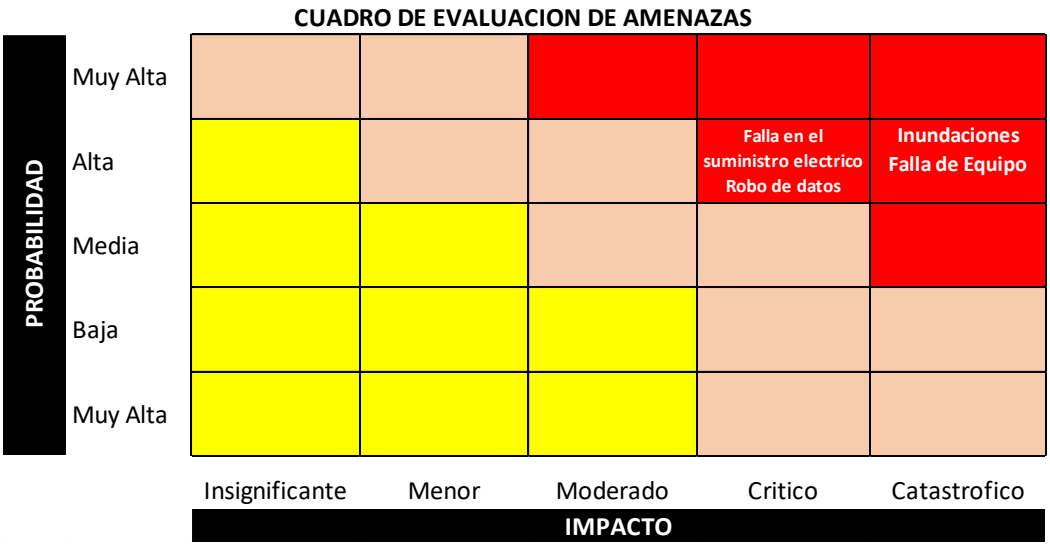
	TIPOS DE RIESGO	PROBABILIDAD
10	Fallo en el Cableado	Baja
11	Robo común	Baja
12	Terremotos	Baja

Cuadro 1. Probabilidad de ocurrencia de Riesgo

VIII. EVALUACIÓN DE RIESGOS

El análisis de riesgos es un proceso formal por el cual la organización toma conciencia de cuáles son sus activos de información, de cuál es el valor de la pérdida de uno de sus atributos (confidencialidad, integridad o disponibilidad), de cómo estos activos están amenazados y de su vulnerabilidad.

El presente Plan con base a una previa identificación de riesgos, considerará sólo aquellos riesgos con mayor probabilidad de ocurrencia (muy alta y alta).



Cuadro 2. Cuadro de Evaluación de Amenazas.

Resumen de Riesgos

Riesgo	Consecuencia	Medidas de Control
Fallas en los equipos	Perdida de información, interrupción de servicios y de la atención.	Activar Plan de Contingencia: Fallo de Equipos.
Inundaciones	Interrupción del Servidor de Datos e Internet y de la atención.	Activar Plan de Contingencia: Inundaciones.
Fallo en el suministro eléctrico	Interrupción del Servidor de Datos e Internet y de la atención.	Activar Plan de Contingencia: Fallo Suministro eléctrico.
Robo de datos	Robo o distribución de información sensible para la Institución.	Aplicación de restricciones en los dispositivos para evitar que exista fuga de información. Utilización de herramientas tecnológicas que detecten la fuga de información.

Cuadro 3. Resumen de Riesgos

La columna *Medidas de Control* nos muestra un rumbo de lo que hacer en caso se produzca alguno de los eventos mencionados. Posteriormente se detallará las características de cada una de ellas.

IX. ASIGNACIÓN DE PRIORIDADES A LAS APLICACIONES O PROCESOS

1. Fallo en los equipos.

Es factible que durante la operatividad diaria, se presenten problemas o desperfectos en los equipos donde se tienen los aplicativos o software o herramientas de control y también en los equipos asignados a los empleados debido a la obsolescencia, los cuales pueden manifestarse a consecuencia de daños por perdida de la vida útil de cualquier de los componentes de los mismo, danto pie a la perdida de información de clientes u otro tipo de información sensible de la institución lo que obligaría a no prestar atención a los clientes.

1. Presentado el problema el Jefe de Informática deberá declarar el estado de Contingencia, comunicar al personal a su cargo sobre tal hecho, formar el equipo de emergencia y reportarlo a Dirección Ejecutiva y Presidencia.
2. El departamento de Informática, deberá disponer de los backups o versiones anteriores del software, imágenes de los servidores virtuales y backups de las bases de datos de todos los sistemas.
3. Una vez identificada la falla del equipo se debe solicitar ya sea la reparación de ser posible o el reemplazo del equipo, para el caso del servidor se debe evaluar la disponibilidad del resto de servidores para poder colocar los aplicativos del servidor dañado. De no ser factible se debe realizar una compra de manera

inmediata, en el caso de los equipos de los empleados de no ser reparable la Unidad de Informática debe brindar un préstamo temporal mientras se obtiene un equipo nuevo que cumpla con las características necesarias.

4. Una vez solucionado el problema, la Unidad de Informática deberá declarar finalizado el estado de contingencia para el retorno a las actividades normales, se desactivará el equipo de emergencias y se notificará sobre el retorno a la normalidad.

2. Inundaciones.

Las inundaciones es uno de los principales riesgos a los que se puede enfrentar CIFCO debido a la ubicación de las instalaciones actuales y la vulnerabilidad que el país representa ante este acontecimiento cada vez más recurrente por los fenómenos atmosféricos.

El agua al igual que el fuego es considerado enemigo de los equipos sean estos informáticos o no, porque puede llegar a dañar completamente el equipo una vez entra en contacto con el agua.

Si se presenta una inundación en las instalaciones de CIFCO y se ven afectados equipos informáticos se procederá a lo siguiente:

1. Presentado el problema el jefe de informática evaluará si es necesario declarar el estado de Contingencia en caso que se encuentre en la ejecución de un proceso crítico, si es así comunicará al personal a su cargo sobre tal hecho, formará el equipo de emergencia y lo reportará a Dirección Ejecutiva y Presidencia.
2. El equipo de emergencia, bajo la supervisión del jefe de informática, realizará una revisión de lo acontecido para detectar cuales son los equipos de cómputo que han sido afectados, para realizar el respectivo análisis y validar su funcionamiento.
3. Si la inundación causó suficiente daño en los equipos de cómputo como para que operen normalmente, el equipo de emergencia procederá a levantar el inventario del equipo dañado, desde las baterías de respaldo, servidores, cargadores de laptop y las computadoras asignadas a los empleados y se deben preparar equipos para préstamo de tal manera que sean funcionales y operen con normalidad instalando el mismo software base y operacional. A si como los backups de los equipos, sistemas y base de datos.
4. Una vez terminada la evaluación, el equipo de emergencia deberá colocar en funcionamiento los equipos evaluados, asegurarse de la devolución de los equipos de cómputo prestados (si es que esto haya ocurrido) y notificar los hechos y presentar sus observaciones a Dirección Ejecutiva y Presidencia. Propondrá medidas que eviten futuros hechos similares (como por ejemplo la mejora de los sistemas de drenajes en la institución).
5. Una vez solucionado el problema, el Jefe de Informática levantará el estado de Contingencia, notificará al personal involucrado.

3. Fallo en el suministro eléctrico.

Los fallos en el suministro eléctrico se ha vuelto uno de los riesgos más recurrente, pues el nivel de incidencia refleja un incremento de los mismos, que pueden estar impulsados por diferentes factores tanto internos como externos, cuando se menciona interno es por una mala instalación eléctrica y externo por aquellos múltiples factores que pueden afectar el tendido eléctrico dentro de los cuales se pueden destacar fenómenos atmosféricos, incendios en el tendido eléctrico debido a descargar, accidentes viales, fallo en transformadores, entre otros.

A continuación, se presentan algunos elementos en la lucha contra este tipo de amenaza.

1. Presentado el problema el jefe de informática evaluará si es necesario declarar el estado de Contingencia en caso que se encuentre en la ejecución de un proceso crítico, si es así comunicará al personal a su cargo sobre tal hecho, formará el equipo de emergencia y lo reportará a Dirección Ejecutiva y Presidencia.
2. El equipo de emergencia, bajo la supervisión del jefe de informática, realizará una revisión de lo acontecido para detectar cuales son los equipos de cómputo se han sido afectados, para realizar el respectivo análisis y validar su funcionamiento.
3. Si por el corte de energía se han dañado equipos se debe proceder al levantamiento del inventario de los equipos dañados.
4. Cuando ya se tenga el inventario de los equipos dañados o que presentan mal funcionamiento, se debe evaluar la disponibilidad de equipos para poder hacer el reemplazo de manera inmediata para que se regrese al correcto funcionamiento de las actividades laborales.
5. El Equipo de Emergencia debe tratar en lo posible de trasladar los servidores fuera del Local de CIFCO, desalojando en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.
6. Una vez solucionado el problema, se deberá declarar el estado de emergencia haciendo una evaluación de los daños producidos por la falla electrica, e informar a Dirección Ejecutiva y Presidencia para su pronta normalidad del desarrollo de los procesos.

X. IMPLEMENTACION DEL PLAN (ACCIONES CORRECTIVAS Y PREVENTIVAS)

- **Los que afectan a la seguridad del edificio.** Preparar extinguidores, organizar las señales de evacuación, preparar bombas de extracción de agua, generadores eléctricos, etc.
- **Los que afectan la integridad de los datos.** Instalar: firewalls, antivirus, sistemas de respaldos de información, sistemas de protección de datos, entre otros.
- **Topología de Red.** Preparar planos de la topología, tener equipos de repuestos de la red, herramientas necesarias todo esto en lugar de fácil acceso.
- **Copias de Seguridad:** Se realizarán de la siguiente manera:

De forma periódica la información, es decir la base de datos de la institucion, es copiada en un disco extraíble. Esto permite salvar la información, en caso de ruptura parcial o total, de uno o ambos servidores, o de la propia base de datos.

- Respaldo de la información.

  Los respaldos del personal que labora en CIFCO se realiza de manera manual y de manera programada, esto con el objetivo de tener un mayor control y minimizar en la medida de lo posible la perdida de información o documentos.

  Los respaldos de los sistemas se realizan de manera manual a cada uno de los sistemas, así como también a las bases de datos.

  Los respaldos de los servidores en el centro de datos se resguardan en un servidor de backup en este se hacen las copias de: el servidor de correos, base de datos de sistemas de CIFCOCO, CIFCORE, CIFCOR, CIFCOFA, CIFCOIVA, sistema de Marcación por QR,

- Donde se realiza el respaldo.

  Los respaldos se realizan en dos sitios dependiendo el tipo si es de computadoras personales se realizan en Discos duros externos de aproximadamente 4TB de capacidad.

  En el caso de los sistemas y bases de datos se resguardan en el servidor de respaldo.

- Qué tipo de respaldo se hace.

  El primer respaldo es total es decir que si a una computadora de un usuario es la primera vez que se le hace el respaldo se hará de manera completa a todos sus archivos.

  Si ya el usuario tiene un respaldo inicial se buscará únicamente realizarle respaldo incrementales o deltas de la información que no esté contenida en el respaldo previo.

  Ante esto se puede decir que únicamente se realizan dos tipos de respaldos: Inicial Completo e incremental después del primer respaldo.

- Con que periodicidad se realiza.

  Se establece un calendario de respaldos a todos los equipos de manera programada con el uso de herramienta de respaldos.

- Quien es el responsable de resguardar la información.

  El responsable del resguardo de la información es el Jefe de Informática.

- Quienes tienen acceso a los respaldos.

- Jefe de Informática, por ser el responsable del resguardo de los mismos
- Soporte Técnico, porque al momento de formatear un equipo siempre debe realizar un respaldo de la información contenida en este.
- También los miembros de la Unidad de Informática tienen acceso a los respaldos, porque en cierta medida ellos son los encargados de llevar a cabo cada uno de los respaldos.

La restauración de la información, disminuye los tiempos de inactividad, en caso de rupturas parciales o totales de uno o ambos servidores o de las bases de datos, dado a que se cargaría el medio digital con el backup del día, o del mes (según corresponda) y se instalarían nuevamente los sistemas operativos en los terminales y de red, para levantar la contingencia.

XI. RECOMENDACIONES

- Revisar de manera constante el Plan de Contingencia para poderlo actualizar cada dos años.
- Realizar capacitaciones de manera constante al personal de informática en relación a seguridad informática con el fin de implementar nuevas estrategias en dicho plan.
- Realizar la evaluación de otro tipo de tecnologías para realizar respaldos de forma eficiente y eficaz.
- Adquirir herramientas que permitan realizar control de la datos y documentos, para evitar fuga de información en cualquier nivel administrativo.
- Realizar revisión constante en el sistema eléctrico de la institución y adquirir un sistema ininterrumpido de suministro energía UPS centralizado que permita mayor protección de los equipos informáticos y una planta eléctrica que suministre energía para la correcta normalidad de las operaciones en los casos que se presente un fallo de suministro de energía en tiempos prolongados.