Plan de Contingencia y Continuidad Informático

Versión	Fecha	Puntos Modificados
01	25/10/2018	• Se actualizó integralmente el Plan de contingencia y Continuidad Informático, de acuerdo con las necesidades actuales.
02	15/11/2024	• Se actualizaron los controles de contingencia.

Responsables	Visto y Sello
Elaborado: **Departamento de Tecnologías de la Información y Comunicaciones**	Especialista de Redes y Comunicaciones Firmado digitalmente por: PRADO VIERA Erik Alonso FAU 20103030791 hard Motivo: Soy el autor del documento Fecha: 23/12/2024 16:37:02-0500
Revisado y Homologado: **Oficina de Planeamiento y Mejora Continua**	Especialista en Calidad y Mejora de Procesos Firmado digitalmente por: BARTUREN HUAMAN Deymer Frank FAU 20103030791 hard Motivo: Doy V° B° Fecha: 23/12/2024 17:15:09-0500
Aprobado: **Gerencia de Administración y Finanzas**	

Jefe de Tecnología de la Información y Comunicaciones

Firmado digitalmente por: MOISES REYNALDO PALOMINO SUAREZ DNI:10713078 RUC:20103030791
Motivo: En señal de conformidad
Fecha: 23/12/2024 16:53:01-0500

Contenido

I. OBJETIVO

Establecer y ejecutar un conjunto de medidas de contingencia y continuidad operativa para asegurar la disponibilidad de los servicios TIC críticos de Activos Mineros S.A.C., con un enfoque en la restauración rápida, eficiente y económica de los sistemas en caso de incidentes.
Las medidas incluirán planes preventivos para reducir riesgos y minimizar el impacto en tiempos de inactividad, costos, y pérdida de información.

II. ALCANCE

Este procedimiento es de aplicación obligatoria para todo el personal de Activos Mineros S.A.C., sea cual fuese su régimen laboral.

III. DOCUMENTOS DE REFERENCIA

- Reglamento de Organización y Funciones Activos Mineros S.A.C.
- Resolución Directoral N° 022-2022-INACAL/DN, que aprueba la actualización de las Normas Técnicas Peruanas, entre ellas la NTP-ISO/IEC 27001:2022, conforme al procedimiento establecido en la Ley N° 30224, reemplazo de la NTP-ISO/IEC 27001:2014.
- Normas Técnicas de Control Interno, aprobadas por Resolución de Contraloría N° 320-2006-CH. Guía Práctica para el desarrollo de Planes de Contingencia de Sistemas de Información –ONGEI.
- Manual Corporativo de FONAFE: “Manual Metodológico para la Implementación de la Continuidad Operativa”
- Manual Corporativo: “Manual para el fortalecimiento de los activos como medida de mitigación de los riesgos de Ciberseguridad”

IV. VIGENCIA

Este documento entra en vigencia a partir del primer día hábil después de la fecha de aprobación.

V. CONTENIDO

1. DEFINICIONES / CONSIDERACIONES

- **Amenaza:** Factor o condición, como tendencias económicas, sociales, políticas y tecnológicas, o hechos específicos, que podría desencadenar un evento potencialmente dañino y poner en riesgo el cumplimiento de los objetivos estratégicos de Activos Mineros S.A.C.

- **Evento:** Suceso o conjunto de sucesos generados por una amenaza, incidente o situación interna o externa, que influye en el logro de los objetivos y puede tener un impacto tanto negativo como positivo, o incluso ambos.

- **Control:** Medida preventiva que mitiga o reduce el riesgo o amenaza, sin llegar a eliminarla por completo.

- **Riesgo:** Posibilidad de que un evento impacte negativamente el cumplimiento de los objetivos de la empresa.

2. IDENTIFICACIÓN DE COMPONENTES CRÍTICOS

Para garantizar la contingencia y continuidad de los servicios TIC, se identifican los siguientes componentes críticos:

2.1 Colaboradores

- Jefe de Departamento de Tecnología de la Información y Comunicaciones.
- Especialista en Sistemas de la Información.
- Especialista en Redes y Comunicaciones.

2.2 Infraestructura

Disponibilidad de un entorno físico con la infraestructura mínima necesaria de servidores y servicios TIC para soportar la operación continua.

2.3 Recursos

Acceso a los recursos esenciales para la operación, tales como computadoras de escritorio, laptops, impresoras, y otros dispositivos necesarios.

3. IDENTIFICACION DE AMENAZAS

Los servicios TIC están expuestos a diversas amenazas que pueden afectar su funcionamiento normal. Estas amenazas se han clasificado en los siguientes grupos:

3.1 Naturales:

Corresponden a eventos causados por fenómenos de la naturaleza, como sismos, maremotos, entre otros. Estas amenazas pueden ocasionar pérdidas o daños físicos en las instalaciones de Activos Mineros S.A.C., afectando equipos, mobiliario e incluso recursos humanos.

3.2 Antrópicas:

Son aquellas amenazas donde interviene la mano del hombre. Se considera dentro de este grupo factores de Recursos Humanos.

- **Factores de Recursos Humanos**

Incluyen riesgos asociados con la falta o insuficiencia de personal necesario para mantener la operatividad de los servicios TIC. Esto puede resultar en demoras en la atención de fallas, daños a archivos, equipos y otros dispositivos que requieren personal capacitado para su manejo.

3.3 Tecnológicas:

Estas amenazas surgen debido a fallos tecnológicos y se dividen en factores de proveedor de servicios y factores de sistemas.

- **Factores de Proveedor de servicios**
  Riesgos asociados con la dependencia de proveedores externos, que pueden provocar interrupciones en el procesamiento de información en

línea y afectar gravemente el servicio a los usuarios, como cortes en los enlaces de comunicación dedicados.

- **Factores de Sistemas**
  Riesgos vinculados al funcionamiento y estado de los equipos, cuyo deterioro o mal uso puede causar:
  - ✓ Daños en componentes de hardware (disco duro, adaptadores de red, etc.), fallas en dispositivos de comunicaciones (switches, routers).
  - ✓ Desperfectos en equipos de cómputo e impresoras en las áreas usuarias, así como daños graves en archivos del sistema por errores de hardware y software.
  - ✓ Software corrupto o incompatible (uso de copias sin licencia).
  - ✓ Infección de virus que dañen archivos y equipos de cómputo.

4. IDENTIFICACION DE LOS CONTROLES

El riesgo es la posibilidad de que un evento afecte negativamente el logro de los objetivos. Por ello, comprender y analizar estos objetivos facilita la identificación de eventos que puedan interferir en su cumplimiento.

En este contexto, es esencial identificar y evaluar los controles asociados a cada factor de riesgo para mitigar su impacto en la operatividad de la empresa.

Estos controles permiten reducir posibles daños y se implementan de acuerdo con cada factor de riesgo identificado.

5. CONTROLES DE CONTINGENCIA

La identificación de riesgos permite clasificarlos por grupos de factores y aplicar los controles necesarios para mitigarlos.

El tratamiento de cada riesgo se determina en función de su probabilidad de ocurrencia (muy alta, alta, media, baja o muy baja) y el impacto que podría tener en los procesos críticos de la empresa.

A continuación, se detallan los controles que deben implementarse para minimizar los riesgos de interrupción de los servicios TIC:

5.1. Naturales

Responsable líder	**Jefe de Departamento de Tecnologías de la Información y Comunicaciones**
Riesgo	**Desastres naturales (sismo, maremotos, etc.)**
Probabilidad de Ocurrencia	**Mediana**

Impacto	• Posible deterioro/inutilización del local de Activos Mineros S.A.C. • En casos muy graves, inutilización total de los Servicios TIC (ERP, Correo electrónico, internet, carpetas compartidas, comunicaciones, etc). • Incapacidad temporal para utilizar la infraestructura del Centro de Datos (servidores, comunicaciones) y equipos de cómputo de usuarios finales.
Controles	**Controles implementados**: • Sistemas de detección y extinción de fuego (alarma de humo, y extinguidores). • Mobiliario especial (gabinete de pared) para los equipos críticos (servidores, equipos de comunicaciones). • Retiro o reemplazo de todo tipo de objetos que en caso de incendio puedan ayudar a la expansión del fuego. • Revisión continúa del estado de la red eléctrica. • Los tomacorrientes eléctricos están instalados a un nivel de altura normado por el código nacional de electricidad. • Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca de las conexiones eléctricas. • El Centro de Datos cuenta con una caja principal de corriente. • Política de respaldo de información, teniendo en consideración el volumen, frecuencia, entre otros. **Oportunidades de mejora:** • Entrenamiento del personal TIC para asumir funciones alternas en caso de desastre. • Mantener contacto con proveedores y/o instituciones que provean equipos de características similares a los de Activos Mineros S.A.C., con capacidad de arrendar o préstamo en caso de quedar inutilizada totalmente la capacidad operativa.
Acciones de Recuperación	**Acciones:** • En ese momento cualesquiera sean los procesos que se estén ejecutando se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de la Red y Apagar el Computador". Seguidamente apagar los servidores. • Proveer cubiertas protectoras para cuando el equipo esté apagado. • Se apagará (poner en OFF) la caja principal de corriente del Centro de Datos. **Tiempo de recuperación** • 36 horas

5.2 Antrópicas

a) Factores de Recurso Humano

Responsable líder	**Jefe de Departamento de Tecnologías de la Información y Comunicaciones**
Riesgo	**Ausencia de personal**
Probabilidad de ocurrencia	**Media**
Impacto	• En el caso que el personal encargado de la administración especializada de los Sistemas de Información y/o Redes y Comunicaciones no se hubiera presentado a laborar, se podría ver afectada la operatividad del mismo y no se daría una adecuada atención a los usuarios.

	• La administración especializada de los Sistemas de Información y Redes y Comunicaciones por personal no capacitado podría causar daños a los archivos, equipos y otros dispositivos que requieren entrenamiento para su operación.
Controles	**Controles implementados:** • El personal a contratar, así como el personal practicante, tiene disponibilidad para presentarse al centro de trabajo fuera del horario establecido como laborable, en caso sea necesario. **Oportunidades de mejora:** • Implementación de manuales de operaciones y procedimientos en los que se señalen claramente todas las labores diarias que se llevan a cabo por cada proceso operativo del sistema. • Aplicación de políticas de rotación para que cada persona esté familiarizada con las distintas labores que se llevan a cabo en cada área. • Contar con el número adecuado de personal encargado en la administración de Sistemas de Información y Redes y Comunicaciones, de tal manera que, si una persona no se presenta, las labores de los usuarios no se verían afectadas en alto grado.
Acciones de Recuperación	**Acciones:** • Identificar los procesos críticos de cada especialista del departamento TIC. • Realizar pruebas de los manuales de operación de los procesos críticos de cada especialista del departamento TIC. • Contacto con proveedores para suplir temporalmente los procesos críticos de cada especialista de ser el caso. **Tiempo de recuperación:** • 24 horas

Responsable líder	**Jefe de Departamento de Tecnologías de la Información y Comunicaciones**
Riesgo	**Acceso de personas no autorizadas a los sistemas implementados**
Probabilidad de ocurrencia	**Media**
Impacto	La manipulación del sistema por personas no autorizadas puede generar graves problemas, desde causar desperfectos en el funcionamiento hasta incluir modificaciones al mismo.

Controles	**Controles implementados:** • Cuando un empleado renuncie su clave de acceso es desactivada del sistema para evitar que en su ausencia otra persona pueda acceder al mismo y manipular los dispositivos. • Toda modificación de la estructura de la información en las bases de datos es autorizada por el personal encargado del Departamento TIC. • El uso de contraseñas personales para la operación de los sistemas es de responsabilidad y uso exclusivo del dueño de la contraseña. • Doble Factor de Autenticación para identificar el acceso a los sistemas. • La contraseña tiene una longitud mínima de ocho caracteres alfanuméricos. • El acceso al Centro de Datos de Activos Mineros S.A.C. está restringido sólo al personal autorizado. **Oportunidades de mejora:** • Cuando un empleado salga de vacaciones, su clave de acceso deberá ser desactivada del sistema para evitar que en su ausencia otra persona pueda acceder al mismo y manipular los dispositivos.
Acciones de Recuperación	**Acciones:** • Luego de la detección del uso de credenciales no autorizado se modificará la contraseña para luego ser notificado al usuario y pueda cambiar su clave. **Tiempo de recuperación:** • 01 hora

Responsable líder	**Jefe de Departamento de Tecnologías de la Información y Comunicaciones**
Riesgo	**Pérdida de claves del usuario administrador de los sistemas de información, redes y servidores**
Probabilidad de ocurrencia	**Baja**
Impacto	• El uso de las contraseñas con privilegios de administración de la plataforma tecnológica por personas no autorizadas puede generar graves problemas, desde causar desperfectos en el funcionamiento hasta incluir modificaciones al mismo.
Controles	**Controles implementados:** • El uso de las contraseñas de administración de la plataforma tecnológica se realiza en las estaciones de trabajo asignado a cada especialista. • El acceso al Centro de Datos de Activos Mineros S.A.C. está restringido sólo al personal autorizado. **Oportunidades de mejora:** • El acceso a los ambientes de trabajo de los especialistas del departamento DTIC deberá estar restringido solo al personal autorizado.
Acciones de Recuperación	**Acciones**: • Luego de la detección del uso de credenciales no autorizado se modificará la contraseña inmediatamente. **Tiempo de recuperación:** • Inmediato

Responsable líder	**Jefe de Departamento de Tecnologías de la Información y Comunicaciones**
Riesgo	**Incendio**
Probabilidad de ocurrencia	**Media**
Impacto	• Se afectaría la operatividad de los servidos de TI y no se daría una adecuada atención a los usuarios. • Perdida de la información de los servidores del centro de datos. • Perdida de comunicación en la empresa, mediante teléfonos (IPs, digitales). • Incapacidad temporal para utilizar la infraestructura del Centro de Datos (servidores, comunicaciones).
Controles	**Controles implementados:** • Sistemas de detección y extinción de fuego (alarma de humo, temperatura y extinguidores). • Mobiliario especial (gabinete de piso) para los equipos críticos (servidores, equipos de comunicaciones). • Retiro o reemplazo de todo tipo de objetos que en caso de incendio puedan ayudar a la expansión del fuego. • Revisión continúa del estado de la red eléctrica. • Los tomacorrientes eléctricos están instalados a un nivel de altura normado por el código nacional de electricidad. • Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca de las conexiones eléctricas. • El Centro de Datos cuenta con una caja principal de corriente. • Prohibición total de fumar en áreas sensibles. • Contar con vigilancia privada las 24 horas al día. • Política de respaldo de información, teniendo en consideración el volumen, frecuencia, entre otros. **Oportunidades de mejora:** • Mantener contacto con proveedores y/o instituciones que provean equipos de características similares a los de Activos Mineros S.A.C., con capacidad de arrendar o préstamo en caso de quedar inutilizada totalmente la capacidad operativa. • Implementación de manuales de operaciones y procedimientos en los que se señalen claramente todas las labores diarias que se llevan a cabo por cada proceso operativo relacionado a TI y puedan provocar un incendio. • Monitorear el funcionamiento del Sistemas de detección y extinción de fuego (alarma de humo, y extinguidores). • Realizar la monitorización periódica de la temperatura y su climatización del centro de datos.
Acciones de Recuperación	**Acciones**: • En ese momento cualesquiera sean los procesos que se estén ejecutando se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de la Red y Apagar el Computador". Seguidamente apagar los servidores. • Proveer cubiertas protectoras para cuando el equipo esté apagado. • Se apagará (poner en OFF) la caja principal de corriente del Centro de Datos. • Se debe tratar en lo posible de trasladar los servidores y el Storage fuera del local. **Tiempo de recuperación:** • 36 horas

5.3 Tecnológicas

a) Factores de Servicios

Responsable líder	**Especialista en Redes y Comunicaciones**
Riesgo	**Corte Prolongado de la red eléctrica comercial**
Probabilidad de ocurrencia	**Media**
Impacto	Paralización total de las actividades de Activos Mineros S.A.C. Servicio restringido, se mantendría la operatividad con equipamiento mínimo.
Controles	**Controles implementados:** • Uso de equipos UPS de 30KVA (Módulos Nº 3, 4, 5, 8) y de 10KVA (Centro de Datos) para suministrar de red eléctrica estabilizada ininterrumpida ante la ausencia de energía comercial por un corto plazo dependiendo de la carga. **Oportunidades de mejora:** • Contar con un grupo electrógeno capaz de suministrar energía a los equipos informáticos críticos. • Realizar pruebas de operación del grupo electrógeno de periodicidad mensual.
Acciones de Recuperación	**Acciones:** • Poner en funcionamiento una fuente de red eléctrica alterna para la alimentación por medio de UPS a los equipos del Centro de Datos. • Distribuir la red eléctrica estabilizada que suministra el grupo electrógeno por áreas y equipos, de acuerdo a lo crítico de su actividad.

Responsable líder	**Especialista en Redes y Comunicaciones**
Riesgo	**Caídas de red WAN (enlaces de datos dedicados Bases e internet)**
Probabilidad de ocurrencia	**Media**
Impacto	• Se produciría una paralización de los servicios de telecomunicaciones. • Imposibilidad de acceso a internet. • Imposibilidad de acceder a los sistemas internos desde afuera de la Entidad.
Controles	**Controles implementados:** • Mantener contrato anual de soporte y renovación de garantía para el equipo Firewall (acceso a internet). • Verificación de estado del equipo UPS, con periodicidad semanal, exclusivo para el Centro de Datos. **Oportunidades de mejora:** • Implementar enlace de datos de contingencia para la red WAN (enlaces dedicados Bases e Internet). • Implementar un protocolo de verificación del estado del equipamiento de la Sala de UPS.
Acciones de Recuperación	**Acciones:** • Realizar los procedimientos establecidos para verificar si el corte es producido por la empresa de telecomunicaciones o fallas en los equipos de comunicaciones. • Coordinar con la empresa de telecomunicaciones la reposición del servicio o enmendar la falla del equipo de comunicaciones. **Tiempo de recuperación:** • 4 horas

b) Factores de Sistema

Responsable líder	**Especialista en Redes y Comunicaciones**
Riesgo	**Falla en componentes de la red de comunicación de datos (LAN)**
Probabilidad de ocurrencia	**Mediana**
Impacto	• Fallas en switches principales paralizarían la red totalmente, hasta su reemplazo.
Controles	**Controles implementados:** • Contrato de mantenimiento anual y renovación de garantía para equipos de comunicaciones switches críticos. • Mantenimiento anual de sistema de pozos a tierra. • Verificar el estado del UPS de periodicidad semanal, exclusivo para el Centro de Datos y para los Módulos que tienen alcance la red eléctrica estabilizada. **Oportunidades de mejora:** • Enlaces de respaldo de los switches principales (Core) a los switches de distribución. • Implementar protocolos de verificación a los equipos UPS.
Acciones de Recuperación	**Acciones:** • Contactar con el proveedor de los equipos switches principales para el soporte técnico especializado (según contrato). **Tiempo de recuperación:** • 4 horas.

Responsable líder	**Especialista en Redes y Comunicaciones**
Riesgo	**Desperfectos en estaciones de trabajo y/o impresoras de las áreas usuarias**
Probabilidad de ocurrencia	**Mediana**
Impacto	• Imposibilidad de disponer de información en forma oportuna.
Controles	Controles implementados: • Realizar mantenimiento preventivo y correctivo para los equipos de cómputo (por la misma institución u outsourcing). Oportunidades de mejora: • Capacitar a los usuarios finales en el buen uso y cuidados de las estaciones de trabajo e impresoras. • Para el caso de equipos de propiedad de la empresa deberá contar con equipos de respaldo. • Se deberá estar en capacidad de reemplazar temporalmente el equipo averiado hasta su reparación. • Las áreas usuarias deberán respetar estrictamente el calendario del mantenimiento preventivo, lo cual servirá para evaluar el estado de los dispositivos.
Acciones de Recuperación	**Acciones:** • Para el caso de equipos en arrendamiento reportar la avería. • Para el caso de equipos de propiedad de la empresa reemplazar por el equipo de respaldo.

	Tiempo de recuperación: • Equipos arrendados: 24 horas. • Equipos propios: 02 horas.

Responsable líder	**Especialista en Sistemas de Información**
Riesgo	**Fallas en los Servidores de Producción**
Probabilidad de ocurrencia	**Baja**
Impacto	Paralización de atención a usuarios internos y externos, que utilicen las aplicaciones de los servidores
Controles	**Controles implementados:** • La implementación de tecnología de virtualización en configuración "recuperación ante fallo" nos permite continuar la operatividad de los servidores de producción hasta reemplazar por garantía el servidor físico que presenta la falla. • Contar con mantenimiento de los servidores de producción tanto preventivo como correctivo (preferentemente outsourcing). • Verificar el estado del equipo UPS con periodicidad semanal, lo que protegerá de fallas producidas por anormalidades en la provisión de energía eléctrica comercial. **Oportunidades de mejora:** • Contar con extensión de garantía y soporte técnico de los servidores que soportan la virtualización de los servidores de producción. • Contar con un procedimiento para recuperar la información, de ser el caso.
Acciones de Recuperación	**Acciones:** • Contactar con el proveedor de los equipos que soportan la virtualización de los servidores de producción para reportar la incidencia y/o cambie de garantía. **Tiempo de recuperación:** • 24 horas

Responsable líder	**Especialista en Sistemas de Información**
Riesgo	**Daños en los archivos de los sistemas mecanizados producido por fallas de hardware**
Probabilidad de ocurrencia	**Mediana**
Impacto	La pérdida total o parcial de datos ocasionaría problemas en la atención en línea y en la disponibilidad de la información. Paralización temporal en la atención de usuarios internos y externos
Controles	**Controles implementados:** • Realizar mantenimiento periódico a los dispositivos para las copias de seguridad, reemplazando las unidades defectuosas. • Política de respaldo de información, teniendo en consideración el volumen, frecuencia, entre otros. • Almacenamiento Externo de Copias de Seguridad en Nube. **Oportunidades de mejora:** • Almacenar los cartuchos de backup en un lugar que reúna las condiciones mínimas para su conservación.

Acciones de Recuperación	**Acciones**: • Ejecutar tareas de restauración utilizando el último backup para recuperar los archivos dañados de los sistemas mecanizados. **Tiempo de recuperación:** • 4 horas

Responsable líder	**Especialista en Redes y Comunicaciones**
Riesgo	**Daños en los archivos por virus informáticos**
Probabilidad de ocurrencia	**Alta**
Impacto	• Paralización de los servidores y estaciones de trabajo por ataque de virus informático al sistema operativo. • Destrucción y alteración de archivos causando paralización temporal de las actividades.
Controles	**Controles implementados:** • Contar con Software Antivirus, instalado y actualizado en cada servidor de aplicación y estación de trabajo. • Política de revisión con Software Antivirus todos los archivos provenientes desde el exterior de Activos Mineros S.A.C., vía dispositivos de almacenamiento masivo, correo electrónico, internet, etc. **Oportunidades de mejora:** • Restringir en lo posible, el uso libre de discos ópticos y dispositivos de almacenamiento masivo, al ser los principales medios de contaminación. • Aplicar la política de revisión con el software antivirus todos los archivos provenientes desde el exterior de Activos Mineros SAC vía dispositivos de almacenamiento masivo.
Acciones de Recuperación	**Acciones**: • Aislar el equipo informático comprometido por software virus informático. • Reemplazar el equipo informático por el de respaldo para que el usuario pueda continuar con sus actividades diarias. **Tiempo de recuperación:** • 4 horas

6. PROCEDIMIENTO DE MANTENIMIENTO

Este procedimiento tiene como objetivo definir las actividades y responsabilidades necesarias para mantener actualizado el Plan de Contingencia y Continuidad Informática, asegurando que la empresa esté preparada para gestionar incidentes.

Para documentar la actualización de este plan, se elaborará un informe que considere los siguientes factores de cambio que puedan requerir una revisión del Plan de Contingencia y Continuidad Informática:

a) Cambio en los aplicativos/sistemas o plataformas/servidores

Se refiere a los cambios funcionales en los aplicativos existentes y/o los requerimientos solicitados por los usuarios. Refiere además a los cambios de performance en software y hardware de plataformas o servidores de acuerdo a un análisis previo.

b) Cambio de proveedores o modificaciones contractuales

Se refiere al cambio de Proveedores y/o modificaciones de contrato de los proveedores existentes.

c) Cambio o implementación de procesos

Se refiere a los cambios de los procesos actuales y/o el surgimiento de nuevos procesos, en los cuales están soportados las operaciones de la empresa. El cambio o nuevo proceso puede convertirse en un proceso crítico y en consecuencia las aplicaciones que lo soportan también.

d) Crecimiento de locales o cambio de local

Se refiere a nuevos locales o cambios geográficos de local debido a necesidades operativas de la empresa o por riesgos de ubicación.

6.1 Responsabilidades, monitoreo y frecuencia en la actualización del documento

Responsable	Responsabilidades	Frecuencia
Jefe de Departamento TIC	Convoca y participa en las reuniones para la actualización del Plan de Contingencia y Continuidad Informático	Anual

Especialista en Sistemas de Información (ESI) **Especialista en Redes y Comunicaciones (ERC)**	Monitorear, actualizar y documenta el Plan de Contingencia y Continuidad Informático.	Anual

6.2 Procedimiento para el mantenimiento y actualización del Plan de Contingencia y Continuidad Informático

N°	Descripción de la actividad	Jefe de Departamento TIC	ESI y ERC	Oficina de Planeamiento y Mejora Continua
1.	Detección del Cambio según la frecuencia establecida en el punto 6.1	x	x	
2.	Informe de detección al Jefe de Departamento TIC, análisis y del impacto		x	
3.	Autorización del cambio	x		
4.	Actualización del Plan de Contingencia y Continuidad informático		x	
5.	Aprobación del documento actualizado	x		
6.	Difusión			x

6.3 Revisión de los controles del Plan

La verificación y seguimiento de los controles para cada riesgo identificado tendrá una frecuencia mensual aleatoria, esta actividad permitirá conocer el estado de los controles implementados, como también, poder identificar nuevas oportunidades de mejora para mitigar el riesgo.

La selección de los controles para la verificación del presente plan estan detalladas en el Plan de Trabajo para probar el Esquema de Recuperación de Servicios TIC.