Devolvemos vida al planeta

ACTIVOS MINEROS S.A.C.

PLAN DE TRABAJO PARA PROBAR ESQUEMAS DE RECUPERACION DE SERVICIOS TIC DEL PLAN DE CONTINGENCIAS Y CONTINUIDAD INFORMATICO 2025

Departamento de Tecnología de la Información y Comunicaciones – AMSAC

Jefe del departamento de Tecnologías de la Información y Comunicaciones

Firmado digitalmente por: PALOMINO SUAREZ Moises Reynaldo FAU 20103030791 hard
Motivo: Doy V° B°
Fecha: 08/07/2025 16:17:36-0500

Especialista de Redes y Comunicaciones

Firmado digitalmente por: PRADO VIERA Erik Alonso FAU 20103030791 hard
Motivo: Doy V° B°
Fecha: 23/12/2024 16:46:56-0500

INDICE

1. INTRODUCCION

El Departamento de Tecnología de la Información y Comunicaciones (DTIC), tiene la responsabilidad de administrar y salvaguardar la operatividad de los Servicios y Recursos Informáticos de Activos Mineros SAC (AMSAC) con el propósito de brindar disponibilidad y continuidad operativa a sus procesos de negocio. En ese sentido DTIC brinda respuesta obligatoria, adoptando políticas y tomando acciones basadas en buenas prácticas.

AMSAC, se preocupa por la seguridad de su información e infraestructura tecnológica (hardware, software, comunicaciones, etc.) y por actualizar, innovar e implementar, las acciones a seguir dentro de los lineamientos de su Plan de Contingencia y Continuidad Informática.

El presente documento proporciona los pasos a seguir para probar los esquemas de recuperación enmarcados en el Plan de Contingencia y continuidad Informático, a través de la ejecución de un conjunto de acciones, apuntando al efecto de situaciones de fallas o situaciones inesperadas, imprescindibles o no complementadas.

2. PLAN DE CONTINGENCIAS

El Plan de Contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los servicios Informáticos y la infraestructura de cómputo, así como la información contenida en los diversos medios de almacenamiento, determina cómo reducir su posibilidad de ocurrencia y los procedimientos de recuperación y restablecimiento a seguir en caso de que se presentara el problema.

El esquema de recuperación considera dos ámbitos:

- El primero define las actividades que se deben realizar y el responsable de operarlas.
- El segundo, la verificación del cumplimiento del estado de los controles y su efecto al activarse.

El Plan de Contingencia y Continuidad Informática de AMSAC se ha definido los siguientes riesgos relevantes:

Riesgo		Controles
Desastres Naturales		• Gabinetes del Centro de Datos
		• Tableros de energía eléctrica
		• Estado del Cableado eléctrico y tomas de energía
Antrópicas	Ausencia de Personal de soporte	• Medios de conexión local y remoto
		• Manuales y/o protocolos de operación para soporte
	Accesos no autorizados	• Desactivación de cuentas
		• Niveles de autorización
		• Políticas de contraseñas
		• Acceso al Centro de datos
	Captura del perfil Administrador	• Claves administradores restringido
	Incendio	• Sistema contra incendio
Tecnológicas	Interrupción de energía eléctrica	• Equipos UPS
	Caídas de la Red Wan	• Línea de contingencia
	Fallas en la red LAN	• Línea de contingencia
	Desperfectos en PC y equipos de impresión	• Mantenimiento Correctivo /reemplazo
	Fallas en los servidores	• Información replicada en ambiente alterno
	Perdida de información por daños en hardware	• Información relevante almacenada
	Daños por virus y software malicioso	• Antivirus actualizado

3. PRUEBA DEL PLAN DE CONTINGENCIA

3.1 ACTIVIDADES DE PRUEBA DEL PLAN DE CONTINGENCIA

El plan de contingencia se prueba una vez año, con una programación de tres meses previos. La programación considera las siguientes actividades:

ACTIVIDADES	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
I. Validación de Activos a. Inventario de Hardware - PC e Impresoras - Servidores - Equipos de comunicaciones - Equipamiento de protección eléctrica	X	X	X	X								
b. Inventario de Software - Software de Oficina - Software de Servicios - Software especializado				X	X	X						
II. Elaboración de protocolo de pruebas a. Riesgos Desastres Naturales b. Riesgos Antrópicos c. Riesgos Tecnológicos							X	X				
III. Aplicación de las Pruebas a. Riesgos Desastres Naturales b. Riesgos Antrópicos c. Riesgos Tecnológicos									X	X	X	
IV. Informe a. Elaboración del Informe b. Presentación del Informe												X

3.2 VALIDACIÓN DE CONTROLES

3.2.1 Desastres Naturales

Las fuentes causales pueden ser terremotos, lluvias, inundaciones, tsunamis, deslizamientos de tierra. Las consecuencias impactan gravemente en los activos y recursos informáticos, por ello se establecen controles tales como:

a) Sistema contra incendio: Acondicionado en el Centro de Datos de la sede principal de AMSAC, tiene como principal función mitigar condiciones de fuego protegiendo los activos de cómputo más importante de la empresa:

- Servidores de datos
- Equipos de almacenamiento
- Switches
- Ruteadores
- Dispositivos de seguridad perimetral

b) Instalación e Gabinetes: Los equipos de comunicaciones y servicios centrales se encuentran instalados dentro de Gabinetes, acondicionados especialmente para darle soporte y estabilidad, protegiéndolos de condiciones externas.

c) Instalación de Tableros de energía eléctrica: Habilitados especialmente para los ambientes de cómputo y diferenciado del suministro de energía eléctrica convencional

d) Cableado eléctrico y tomas de energía: El acondicionamiento de la instalación eléctrica guarda las normas y condiciones de seguridad.

Condiciones básicas para seguir:

PUNTOS DE CONTROL	
Sistema contra incendio Responsable: Especialista de Redes Comunicaciones	• Verificación de panel de comando
	• Verificación de pulsadores
	• Verificación de alarmas
	• Verificación de detectores
	• Verificación de cable sensor
	• Verificación de los rociadores
	• Verificación del Balón contenedor de polvo extintor
Instalación e Gabinetes Responsable: Especialista de Redes y Comunicaciones	• Estabilidad del anclaje
	• Soporte de bandejas
	• Espaciado existente
	• Estado del Blindaje
Instalación de Tableros de energía eléctrica Responsable: Especialista de Redes y Comunicaciones	• Condiciones físicas del tablero
	• Distanciamiento de instalación
	• Estado de llaves y sistema de protección
	• Circuitería

	• Nivel de calentamiento y temperatura
	• Mediciones: Voltaje, amperaje, ohmiaje
Cableado eléctrico y tomas de energía Responsable: Especialista de Redes y Comunicaciones	• Condiciones físicas del cableado
	• Estado de la chaqueta del conductor
	• Condiciones de las acometidas
	• Exposición del cableado
	• Estado de las tomas

3.2.2 Antrópicas

Fuentes causales identificadas por el mal uso, falta de diligencia y/o inexperiencia al manipular los equipos, recursos y los sistemas puestos a disposición de las áreas usuarias. A efectos de evitar perjuicios el plan de contingencia estable los siguientes controles:

a) Ante la ausencia de personal de soporte:

El departamento de tecnología de la información garantiza la prestación del servicio de soporte y asistencia a las áreas usuarias, independientemente de no contar con personal in situ o indisponibilidad del especialista en el terreno, para lo cual mantendrá medios de conexión y asistencia remota.

b) Accesos no autorizados:

El objetivo es mantener la disponibilidad, integridad y confidencialidad de la información utilizando herramientas y mecanismos acreditados de acceso a los sistemas y al centro de datos para lo cual se ha previsto de dotar de
mecanismos:

- Desactivación de cuentas: Mantenimiento y monitoreo de cuentas de acceso al dominio, correo y sistemas de información en general.

- Niveles de autorización: Los requerimientos de acceso son validados por las gerencias y jefaturas respectivas con el propósito de garantizar el establecimiento adecuado del perfil.

- Políticas de contraseñas: Toda cuenta de acceso tiene que acreditarse a través de una contraseña, para el caso del acceso a la red se maneja políticas de caducidad, complejidad y longitud de las claves.

- Acceso al Centro de datos: El acceso al centro de datos es restringido solo a personal autorizado, contando con un sistema de electrónico de control de acceso y monitoreo constante de cámara de video vigilancia.

c) Claves administrador restringido

El acceso a nivel administrador es restringido al personal del Departamento de Tecnología de la Información y Compunciones y su uso se reserva al propósito de aplicar rutinas de configuración, mantenimiento y soporte

Condiciones básicas para seguir:

PUNTOS DE CONTROL	
Medios de conexión local y remoto	• Verificación de disponibilidad de herramientas de conexión y soporte remoto.
	• Asistencia en línea de proveedores de servicio.
Protocolos de Operación para soporte	• Verificación de Disponibilidad de manuales de operación para soporte.
	• Validación de niveles de escalamiento.
	• Atenciones según complejidad de las incidencias.
Desactivación de cuentas	• Verificación de estado de cuentas activas bloqueadas en el directorio activos y maestro de usuarios.
Niveles de autorización	• Verificación de que el requerimiento de acceso este validado por el gerente y/o jefe responsable de área.
Políticas de contraseñas	• Verificación de aplicación y despliegue de GPO para contraseñas en el directorio activo: complejidad, caducidad y longitud.
Acceso al Centro de datos	• Verificación del sistema de control de acceso al centro de datos.
	• Verificación del estado de grabación de la cámara de video vigilancia instalada en el centro de datos.
Claves administradores restringido	• Verificación de permisos a perfiles de usuario.

3.2.3 Tecnológicas

Los factores tecnológicos asociados a fallas en los servicios y sistemas. Los causales más relevantes son interrupción del servicio de energía, caídas del servicio de comunicaciones, problemas en la infraestructura de red, fallas de hardware y software, problemas en los servidores y sistema de seguridad. Los controles aplicados inciden en:

a) Equipamiento de Protección eléctrica: aseguran la disponibilidad del suministro de energía estabilizada para los equipos de cómputo instalados fundamentalmente en el centro de datos.
b) Línea de contingencia de internet: Ante la caída del circuito digital principal instalado en la cabecera de la sede principal de AMSAC, se activa la línea backup que se mantiene en modo pasivo en ambiente de producción.
c) Línea de contingencia LAN de la sede principal de AMSAC que consiste en dar capacidades de conectividad ante la rotura de la fibra o problemas de los enlaces internos que enlaza los módulos físicos de la sede principal.
d) Monitoreo y soporte técnico para los equipos servidores centrales instalados en el centro de datos.
e) Monitoreo y soporte técnico para las estaciones de trabajo y parque de impresión.
f) Monitoreo y soporte técnico para los equipos de almacenamiento central
g) Monitoreo y soporte de los sistemas de seguridad, software antivirus y antispam.

Condiciones básicas para seguir:

PUNTOS DE CONTROL	
Equipamiento de Protección eléctrica	• Verificación de condiciones físicas de equipos
	• UPS, Grupo Electrógeno.
	• Mediciones de carga
	• Estado de las Baterías externas
	• Estado de ventilación
	• Estado de las conexiones
Línea de contingencia de internet	• Disponibilidad del ingreso en línea del servicio con la línea backup.
	• Verificación Ancho de banda suministrado
Línea de contingencia LAN	• Disponibilidad del ingreso en línea del servicio con la línea backup.
	• Verificación Ancho de banda suministrado.

Monitoreo y soporte a los Servidores	• Condiciones físicas del equipamiento: consumo de recursos procesador, memoria, disco.
	• Temperatura
	• Estado de los leds de alertas
	• Estado de la conexión de energía
Monitoreo y soporte a las estaciones de trabajo	• Condiciones físicas del equipamiento: consumo de recursos procesador, memoria, disco.
	• Temperatura
	• Estado del led de alertas
	• Estado de la conexión de energía
Monitoreo y soporte para los equipos de almacenamiento central	• Condiciones físicas del equipamiento: consumo de recursos procesador, memoria, disco.
	• Temperatura
	• Estado del led de alertas
	• Estado de la conexión de energía
Monitoreo y soporte de los sistemas de seguridad	• Condiciones físicas del equipamiento: consumo de recursos procesador, memoria, disco.
	• Temperatura
	• Estado del led de alertas
	• Estado de la conexión de energía

4. CRONOGRAMA PRUEBAS DEL PLAN DE CONTINGENCIA

TAREA	DURACIÓN (Días)	COMIENZO	FIN
Inicio	0	1/01/2025	1/01/2025
Validación de Activos	180	1/01/2025	30/06/2025
Elaboración del Protocolo de Pruebas	60	01/07/205	30/08/2025
Aplicación de Pruebas	90	01/09/2025	30/11/2025
Elaboración de Informe	15	1/12/2025	30/12/2025
Fin	0	31/12/2025	31/12/2025