Academia de la Magistratura

RESOLUCIÓN N° 54 -2017-AMAG-CD/P

Lima, 22 de junio de 2017

VISTOS:

El Informe N° 174-2017-AMAG/DG de Dirección General, el Informe Legal N° 157-2017-AMAG-DG/OAJ de la Oficina de Asesoría Jurídica, el Informe N° 122-2017-AMAG/OPP de la Oficina de Planificación y Presupuesto, el Memorando N° 1500 -2017-AMAG/SA de la Secretaria Administrativa, el Informe N° 0069-2017-AMAG/INF de la Subdirección de Informática, y;

CONSIDERANDO:

Que, la Ley N° 28612, establece medidas que permiten a la Administración Pública la contratación de Licencias de Software y Servicios informáticos en condiciones de neutralidad, vigencia tecnológica, libre concurrencia y trato justo e igualitario de proveedores;

Que, en el marco de la Ley 28716 - Ley de Control Interno de las Entidades del Estado, que tiene por objeto establecer las normas para regular la elaboración, aprobación, implementación, funcionamiento, perfeccionamiento y evaluación del control interno en las entidades del Estado, con el propósito de cautelar y fortalecer los sistemas administrativos y operativos con acciones y actividades de control previo, simultaneo y posterior, contra los actos y prácticas indebidas o de corrupción, propendiendo al debido y transparente logro de los fines, objetivos y metas institucionales;

Que, el Artículo 4° de la referida Ley de Control Interno de las Entidades del Estado, establece que "Corresponde al titular y a los funcionarios responsables de los órganos directivos y ejecutivos de la entidad, la aprobación de las disposiciones y acciones necesarias para la implementación de sus sistemas de control interno y que estos sean oportunos, razonables, integrados y congruentes con las competencias y atribuciones de las respectivas entidades". Asimismo la parte in fine del Artículo 5° del mismo cuerpo legal establece que "Los mecanismos y resultados del funcionamiento del Control Interno son objeto de revisión y análisis permanente por la administración institucional con la finalidad de garantizar la agilidad, confiabilidad, actualización y perfeccionamiento del Control Interno";

Que, de conformidad con lo establecido en el Reglamento de Organización y Funciones – ROF de la Academia de la Magistratura aprobado mediante Resolución Administrativa del Pleno del Consejo Directivo N° 06-2012-AMAG-CD, corresponde la Subdirección de Informática, mediante el Artículo 59°, las siguientes funciones: literal f) Garantizar el correcto funcionamiento de la infraestructura tecnológica, hardware, software, comunicaciones) de la Institución; y el literal i) Investigar, analizar y evaluar las tecnologías de información existentes y emergentes, así como la utilidad e impacto de su

implementación existentes y emergentes, así como la utilidad e impacto de su implementación e integración a fin de recomendar la adquisición de nuevas tecnologías informáticas (hardware, software y comunicaciones) que requiera la Institución;

Que, el Plan de Contingencia Informático, adjunto a la presente Resolución, tiene como objetivo general "Garantizar la continuidad de las Actividades de la Academia de la Magistratura ante eventos que podrían alterar el normal funcionamiento de la Tecnología de la Información y Comunicaciones – TIC´s, a fin de mitigar el riesgo no previsible, críticos o de emergencia y responder de forma inmediata hacia la recuperación de las actividades normales";

Que, entre los objetivos específicos del referido Plan de Contingencia Informático se establecen: a) Contar con la documentación práctica y actualizada que garantice la continuidad de las operaciones de los sistemas informáticos sin sufrir paralizaciones o pérdidas relevantes, b) Identificar y analizar riesgos posibles que puedan afectar las operaciones y procesos informáticos de la institución, c) Establecer las Estratégicas adecuadas para asegurar la continuidad de los servicios informáticos en caso de interrupción y que ésta no exceda las 24 horas, y d) Contar con personal debidamente capacitado y organizado para afrontar adecuadamente las contingencias que puedan presentarse en las actividades de la Academia de la Magistratura;

Que, en ese sentido, resulta necesario aprobar el Plan de Contingencia Informático de la Academia de la Magistratura elaborado por la Subdirección de Informática y visado por la Oficina de Planificación y Presupuesto, y la Oficina de Asesoría Jurídica de la Academia de la Magistratura;

Que, conforme al TUO de la Ley N° 27444 - Ley de Procedimientos Administrativos General en virtud de los considerandos expuestos y en uso de las facultades conferidas por la Ley Orgánica de la Academia de la Magistratura N° 26335 y el Estatuto de la Academia de la Magistratura, aprobada mediante Resolución N° 06-2012-AMAG-CD y en ejercicio de sus atribuciones.

SE RESUELVE:

Artículo Primero.- APROBAR *el Plan de Contingencia Informático de la Academia de la Magistratura, el mismo que forma parte de la presente Resolución.*

Artículo Segundo*: Encargar a la Subdirección de Informática la ejecución y control de lo dispuesto en la presente Resolución.*

Artículo Tercero*: Publicar la presente Resolución en el portal institucional de la Academia de la Magistratura.*

Regístrese, comuníquese y cúmplase.

DR. PEDRO GONZALO CHÁVARRY VALLEJOS
Fiscal Supremo Titular
Presidente del Consejo Directivo
de la Academia de la Magistratura

ACADEMIA DE
LA MAGISTRATURA

PLAN DE CONTINGENCIA INFORMÁTICO

ACADEMIA DE LA MAGISTRATURA

2017

SUBDIRECCIÓN DE INFORMÁTICA

Contenido

I.-OBJETIVOS

1.1. General

Garantizar la continuidad de las actividades de la Academia de la Magistratura, ante eventos que podrían alterar el normal funcionamiento de la Tecnología de la Información y Comunicaciones – TIC's, a fin de mitigar el riesgo no previsible, críticos o de emergencia, y responder de forma inmediata hacia la recuperación de las actividades normales.

1.2. Específicos

- Contar con documentación práctica y actualizada que garantice la continuidad de las operaciones de los sistemas informáticos sin sufrir paralizaciones o pérdidas relevantes.
- Identificar y analizar riesgos posibles que pueden afectar las operaciones y procesos informáticos de la institución.
- Establecer las estrategias adecuadas para asegurar la continuidad de los servicios informáticos en caso de interrupción y que ésta no exceda las 24 horas.
- Contar con personal debidamente capacitado y organizado para afrontar adecuadamente las contingencias que puedan presentarse en las actividades de la Academia de la Magistratura.

II.- BASE LEGAL

1. Ley N° 26335, Ley Orgánica de la Academia de la Magistratura.
2. Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
3. Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado.
4. Ley N° 28612, Ley que norma el uso, adquisición y adecuación del software en la administración pública.
5. Ley Nº 29733, Ley de protección de datos personales.
6. D. S. Nº 003-2013-JUS., Reglamento de la Ley de protección de datos personales.
7. D.S. N° 024-2006-PCM, Reglamento de la ley N° 28612.
8. D.S. N° 081-2013-PCM, Decreto Supremo mediante el cual se aprueba la Política Nacional de Gobierno Electrónico 2013-2017.
9. R.M. N° 004-2016-PCM, Se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014. "Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información: Requisitos 2da Edición", en todas las entidades integrantes del Sistema Nacional de Informática".
10. R.M. N° 188-2015-PCM, Aprueba los lineamientos para la formulación de planes de contingencia.
11. RJ. Nº 386-2002-INEI, Normas Técnicas para el almacenamiento y respaldo de la información procesada por las Entidades de la Administración Pública.
12. RJ. Nº 090-95-INEI, Recomendaciones Técnicas para la protección física de los equipos y medios de procesamiento de la información en la administración pública.

13. Resolución de Contraloría General N° 320- 2006-CG, Sobre Normas de Control Interno.

III.- ALCANCE

La Implementación del Plan de Contingencia Informático, incluye los elementos referidos a los sistemas de información, equipos, infraestructura, personal, servicios y otros relacionado con las TIC's, direccionado a mitigar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la Institución.

IV.- DISPOSICIONES GENERALES (MARCO TEÓRICO)

El Plan de Contingencia Informático es un documento que reúne conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las TIC's, cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la institución.

Acciones a ser consideradas:

- **Antes**, como un plan de respaldo o de prevención para mitigar los incidentes.
- **Durante**, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
- **Después**, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

El Plan de Contingencia Informático permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna.

El término "incidente" en este contexto debe ser entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático.

4.1 Plan de Prevención

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en los factores identificados en el presente plan.

El Plan de Prevención es la parte principal del Plan de Contingencia Informático porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

4.2 Plan de Ejecución

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente de contingencia y que activa un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible.

Las acciones descritas dentro del Plan de Ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

Ver Anexo A01: Formato de ocurrencia de evento.

4.3 Plan de Recuperación

Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

Todo Plan de Contingencia Informático debe tener un carácter recursivo que permita retroalimentar y mejorar continuamente los planes en cada una de las etapas descritas, logrando así tener un documento dinámico.

4.4 Plan de Pruebas

El Plan de Pruebas, será presentado a la Dirección General de la Academia de la Magistratura para su aprobación previa a su implementación. El resultado de las pruebas efectuadas será presentado igualmente para su conformidad.

Las pruebas relacionadas, se ejecutaran en forma anual y durante el primer trimestre del año, con el fin de evaluar la preparación de la organización ante la ocurrencia de un siniestro y realizar los ajustes necesarios.

V.- DISPOSICIONES ESPECÍFICAS

Metodología

La presente metodología es el resultado de las buenas prácticas en la implementación de planes de contingencia informático, mitigación de riesgos y seguridad de la información, también en base a las experiencias de otras instituciones, lo cual garantiza que el documento final sea necesariamente objetivo y práctico, a fin de contar con una herramienta efectiva en caso de una contingencia informática real.

Para elaborar el Plan de Contingencia Informático se seguirá una metodología que tiene las siguientes fases:

- **Fase 1:** Organización del Plan de Contingencia Informático
- **Fase 2:** Identificación y priorización de riesgos
- **Fase 3:** Definición de eventos susceptibles de contingencia
- **Fase 4:** Elaboración del Plan de Contingencia Informático
- **Fase 5:** Definición y Ejecución del Plan de Pruebas
- **Fase 6:** Implementación del Plan de Contingencia Informático

5.1 Organización del Plan de Contingencia Informático

Uno de los aspectos que evidencia un carácter formal y serio en toda organización es que ésta se encuentre siempre preparada para afrontar cualquier evento de contingencia o dificultades en general y que le permitan poder superarlos por lo menos de manera transitoria mientras dure dicho evento.

Es necesario entonces que la definición de un Plan de Contingencia Informático se deba hacer de manera formal y responsable de tal forma que involucre en mayor o menor medida a toda la organización en el Plan de Prevención, Ejecución y Recuperación, pero definiendo un grupo responsable para su elaboración, validación y mantenimiento.

Por lo que se propone la siguiente organización según el siguiente gráfico:

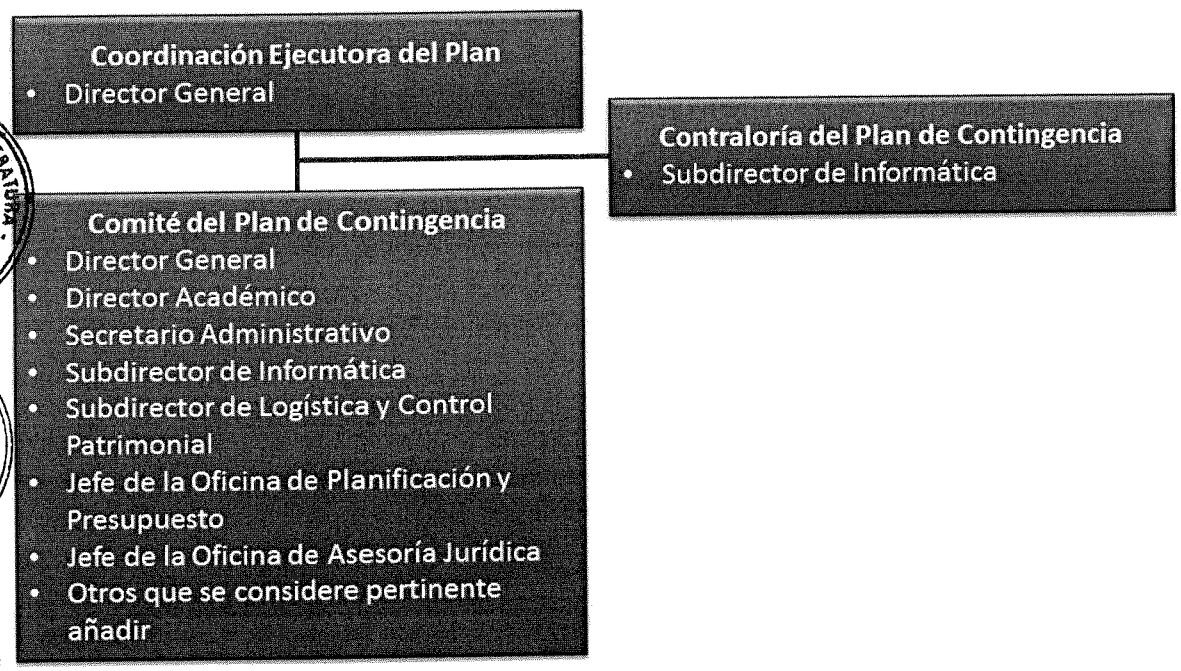


Gráfico 1 – Organización Administrativa del Plan de Contingencia

A continuación se describe las funciones y roles de la Organización

Administrativa del Plan de Contingencia Informático:

5.1.1 Coordinación Ejecutora del Plan

La Coordinación Ejecutora del Plan de Contingencia Informático será responsabilidad del Director General, definiendo todas las políticas y acciones a llevarse a cabo durante un evento de contingencia, también será responsable de que todas las actividades se cumplan de acuerdo a lo planeado. Dicha coordinación será asistida y ejecutada en colaboración de las Unidades Orgánicas de Línea.

Funciones y Roles de la Coordinación Ejecutora del Plan:

- Mantener permanentemente actualizado el Plan de Contingencia Informático
- Ser responsable de la ejecución del Plan de Contingencia Informático, cuando se presenten los eventos que lo activan
- Evaluar el impacto de las contingencias que se presenten
- Elaborar los informes referidos al Plan de Contingencia Informático
- Proponer incorporaciones de eventos al Plan de Contingencia Informático al Comité de Contingencia
- Proponer la capacitación al personal del servicio, sobre las actividades que deben ejecutar cuando se presente la contingencia
- Velar que el personal se encuentre debidamente capacitado y preparado para ejecutar el Plan de Contingencia Informático
- Proponer reuniones periódicas sobre el Plan de Contingencia Informático.

1.2 Comité del Plan de Contingencia Informático

El Comité de Contingencias es el órgano donde se coordinan y aprueban todas las actividades previamente planificadas para ejecutarse en el caso de contingencias del servicio.

Este comité se reunirá por lo menos con una periodicidad trimestral y en él se definirán los lineamientos a través de los cuales se sustentará el Plan de Contingencia.

Dicho comité estará integrado por los siguientes miembros:

- Director General
- Director Académico
- Secretario Administrativo
- Subdirector de Informática
- Subdirector de Logística y Control Patrimonial
- Jefe de la Oficina de Planificación y Presupuesto
- Jefe de la Oficina de Asesoría Jurídica

El Director General, el Director Académico y la Secretaria Administrativa, podrán designar a otros integrantes que consideren pertinentes a participar en el Comité.

Funciones y Roles del Comité del Plan de Contingencia Informático:

- Participar en las reuniones periódicas propuestas por el Coordinador del Plan de Contingencia Informático
- Proponer la incorporación y/o modificaciones del Plan de Contingencia Informático
- Aprobar y/o rechazar las incorporaciones y/o modificaciones del Plan de Contingencia Informático propuesta por el coordinador de contingencia o sus miembros
- Verificar que el personal a su cargo se encuentre debidamente capacitado en la ejecución del Plan de Contingencia Informático
- Coordinar la ejecución de las actividades del Plan de Pruebas
- Aprobar los informes presentados por la coordinación del plan respecto a cualquier evento relacionado con el mismo
- Determinar las prioridades y plazos de recuperación de los diferentes servicios que pudieran verse afectados
- Coordinar con los recursos y/o proveedores externos necesarios para soportar y restaurar los servicios afectados por la contingencia
- Coordinar y ejecutar la capacitación al personal del servicio sobre las actividades que se deben ejecutar cuando se presenta la contingencia

5.1.3 Contraloría del Plan de Contingencia

La Subdirección de Informática sería el órgano que supervise todos los elementos y recursos descritos para intervenir en una situación de contingencia estén disponibles y sean perfectamente viables de modo tal que se garantice que no se presenten carencias y/o fallas en una situación real bajo las Funciones y Roles siguientes:

- Verificar que el Plan de Contingencia Informático se encuentre actualizado
- Revisar y verificar que el documento de Plan de Contingencia Informático se enmarque dentro del alcance establecido
- Velar por suministrar los recursos necesarios para la viabilidad del Plan de Contingencia Informático
- Corroborar que el Plan de Contingencia Informático se cumpla correctamente
- Presentar los informes del Plan de Contingencia Informático al Comité de Contingencia
- Certificar que todos los recursos descritos en el Plan de Contingencia Informático (materiales, humanos, externos, etc.) sean viables y se encuentren disponibles para su uso cuando un evento de contingencia lo requiera

- Auditar los procesos que forman parte del Plan de Contingencia Informático, corroborando que se cumpla correctamente. Participar y visar las pruebas de validación del Plan de Contingencia Informático. Informar al Comité respecto a cualquier evento o anomalía encontrada que ponga en riesgo la ejecución de todo o parte del plan
- Proponer y recomendar actividades o procesos de mejora que permitan mitigar los riesgos de operación

5.2 Identificación y Priorización de Riesgos

Se denomina INCIDENCIA al hecho que se pueda presentar en cualquier momento, bajo una probabilidad de ocurrencia. Por otro lado, RIESGO es un suceso incierto que puede llegar a presentarse en un futuro dependiendo de variables externas o internas. Por lo tanto, es la cuantificación de una amenaza.

5.2.1 Análisis del Riesgo

El análisis del riesgo se basa en la información generada en la fase de identificación del riesgo y se convierte en información para la toma de decisiones. En la fase del análisis del riesgo, se consideran tres elementos que permiten aproximar un valor objetivo al riesgo y son:

- Probabilidad del Riesgo
- Impacto del Riesgo
- Exposición del Riesgo

Estos elementos permitirán al equipo coordinador categorizar los riesgos, lo que a su vez permite dedicar más tiempo a la administración de los riesgos más importantes.

5.2.2 Probabilidad del Riesgo

Es la probabilidad de que una condición se produzca realmente. La probabilidad del riesgo debe ser superior a cero, pues si no el riesgo no plantea una amenaza al servicio. Asimismo, la probabilidad debe ser inferior a 100% o el riesgo será una certeza; dicho de otro modo, es un problema conocido.

La probabilidad se puede entender también como la posibilidad de la consecuencia, porque si la condición se produce se supone que la probabilidad de la consecuencia será del 100%.

5.2.3 Impacto del Riesgo

El impacto del riesgo mide la gravedad de los efectos adversos o la magnitud de una pérdida, causados por la consecuencia del incidente ocurrido.

Es una calificación aplicada al riesgo, para describir su impacto en relación al grado de afectación al nivel de servicio normal. Cuanto mayor sea el número, mayor es el impacto, se clasificará el impacto con una escala del 1 al 4.

5.2.4 Exposición del Riesgo

La exposición al riesgo es el resultado de multiplicar la probabilidad por el impacto. A veces, un riesgo de alta probabilidad tiene un bajo impacto y se puede ignorar sin problemas; otras veces, un riesgo de alto impacto tiene una baja probabilidad, por lo que también se podría pensar en ignorarlo, en cuyo caso habrá que considerar también la criticidad de dicho evento. Los riesgos que tienen un alto nivel de probabilidad y de impacto son los que más necesidad tienen de administración, pues son los que producen los valores de exposición más elevados.

5.2.5 Definición de eventos controlables y no controlables

Como parte de la identificación de los riesgos, estos deben categorizarse en función a las acciones de prevención que pueden estar en manos de la Academia de la Magistratura y cuya ocurrencia no puede predecirse con antelación. Así, se tiene que los eventos pueden ser:

- **Eventos Controlables**, si al ser identificados se pueden tomar acciones que eviten su ocurrencia o minimicen el impacto en el servicio brindado.
- **Eventos No Controlables**, cuando su ocurrencia es impredecible y únicamente se puede tomar acciones que permitan minimizar el impacto en el servicio.

5.2.6 Definición de la Matriz de Riesgo

La ocurrencia de un evento tiene una implicancia sobre las actividades operativas del servicio, en tal sentido, resulta necesario conocer el impacto del evento cuando este se presenta. Por ello, se requiere cuantificar el impacto a efectos de ser objetivos en su análisis. El factor numérico asignado es directamente proporcional y va en ascenso con respecto al impacto o gravedad que su ocurrencia pueda generar sobre los diferentes alcances del servicio y se clasificarán como se indica en el siguiente cuadro:

Cuadro N°1 – Cuadro de Impactos

IMPACTO	DESCRIPCIÓN	VALOR
Poco impacto	Perdida de información y/o equipamiento no sensitivo	1
Moderado impacto	Perdida de información sensible	2
Alto impacto	Perdida de información sensible, retraso o interrupción	3
Gran Impacto	Perdida de información crítica, daño serio, patrimonial	4

Asimismo, la probabilidad de ocurrencia de un evento resulta de gran importancia para determinar qué tan posible es que dicho evento se presente en la realidad. La determinación de esta probabilidad se obtendrá por la opinión de expertos.

Cuadro N°2– Cuadro de Probabilidad de Ocurrencia

PROBABILIDAD DE OCURRENCIA	DESCRIPCIÓN	RANGO DE VALORES
Frecuente	Incidentes repetidos	80% a 99%
Probable	Incidentes aislados	20% a 79%
Ocasional	Sucede alguna vez	6% a 19%
Remoto	Improbable que suceda	1% a 5%

Exposición = Impacto x Probabilidad

Cuadro N°3: Exposición al Riesgo

Probabilidad de Ocurrencia	Impacto: Poco	Moderado	Alto	Gran
Frecuente				
Probable				
Ocasional				
Remoto				

Finalmente, después de haber ponderado y validado objetivamente las probabilidades de ocurrencia y los impactos asociados, se establecerán las políticas que se han de considerar para determinar cuáles son aquellos eventos que formarán parte del Plan de Contingencia, como sigue:

- Todo evento cuya calificación sea de "Gran Impacto: 4", será considerado obligatoriamente dentro del Plan de Contingencia Informático.
- Todo evento cuya exposición al riesgo sea mayor o igual a 0.15 será también considerado en el Plan de Contingencia Informático (ver

Cuadro N °4).

Después de todo lo expuesto, se elaborará la "Matriz de Riesgo de Contingencia" en la cual se tendrá en cuenta todos los eventos susceptibles de ser considerados en el Plan de Contingencia Informático, indicando su ponderación y categorización (controlable/ no controlable) para la elaboración del Plan de Contingencia Informático. Asimismo, se utilizarán los siguientes tópicos como una forma de agrupar a dichos eventos:

- Contingencias relacionadas a Siniestros
- Contingencias relacionadas a los Sistemas de Información
- Contingencias relacionadas a los Recursos Humanos
- Plan de Seguridad Física

5.3 Definición de eventos susceptibles de contingencia

El Plan de Contingencia Informático abarca todos los aspectos que forman parte del servicio informático, en tal sentido, resulta de vital importancia considerar todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia. Los principales elementos, que serán considerados para su evaluación son los siguientes:

- Hardware
  - Servidores
  - Estaciones de trabajo (Computadoras, Laptops)
  - Impresoras, fotocopiadoras, scanner
  - Equipos multimedia
- Comunicaciones
  - Equipos de comunicaciones (Switches, Router y LAN)
  - Equipos de telefonía fija
  - Enlaces
  - Cableado de Red de Datos
- Software
  - Base de Datos (ORACLE, MS-SQL)
  - Aplicativos utilizados en la Academia de la Magistratura
  - Software de Aplicaciones Web
  - Software Base (Sistemas Operativos y Ofimática)
  - Antivirus
- Información sobre Sistemas Informáticos
  - Base de Datos utilizado por los aplicativos
  - Respaldo de la información generada con Software Base
  - Respaldo de Aplicaciones
  - Respaldo de Base de Datos
  - Respaldo de la información y configuración de los Servidores

- Equipos diversos
  - UPS
  - Aire Acondicionado

- Infraestructura Física
  - Oficinas (Jr. Camaná 669 – Lima)

- Operativos
  - Logística operativa (suministros informáticos)

- Servicios Públicos
  - Suministro de energía eléctrica
  - Servicio de telefonía fija y móvil
  - Suministro de agua

- Recursos Humanos
  - Disponibilidad de personal de dirección
  - Disponibilidad de personal operativo

5.4 Elaboración de planes de contingencia

Una de las fases importantes del Plan de Contingencia Informático es la documentación y revisión de la información que se plasmará en una guía práctica y de claro entendimiento para el personal.

Es por ello, que una fase importante de la metodología considera un formato estándar de registro de todos los eventos definidos que forman parte del plan de contingencia informático. Así, se tendrá finalmente un entregable acorde con los requerimientos y políticas definidas para tal fin.

El contenido de todos los eventos que conformarán el Plan de Contingencia son:

5.4.1 Formato de Registro del Plan de Contingencia Informático

Para una lectura fácil y rápida del Plan de Contingencia, se ha diseñado un formato, Ver Anexo A02: "Formato Registro Plan de Contingencia", el mismo que describimos a continuación y que se compone de las siguientes partes:

- **Encabezado**: El formato tiene un encabezado, cuyo contenido se presenta como sigue:
  - **Elaborado**: En todos los casos se indica "Academia de la Magistratura".
  - **Código del Formato**: FPC – XX (ver matriz de riesgo de Contingencia).
  - **Nombre del evento**: Claro y de fácil entendimiento.
- **Cuerpo Principal**: En el cual se desarrollará cada uno de los

eventos que formarán parte del Plan de Contingencia y se describe el contenido que deberá ir en cada campo.

5.5 Definición y ejecución de planes de prueba

Conscientes que una situación de contingencia extrema puede presentarse en cualquier momento y por ende convertirse en un problema prioritario de atender si éste se produjera en el horario de oficina que pueda resultar impactante durante las actividades de la Academia de la Magistratura, se hace necesario definir de manera específica las acciones necesarias para asegurar que, en caso de presentarse una contingencia, tener un conjunto de prestaciones y funcionalidades mínimas que permitan posteriormente ejecutar el plan de recuperación de manera rápida y segura.

En este sentido, la garantía del "éxito" del Plan de Contingencia Informático se basa en una validación y certificación anticipada del mismo, en cada uno de sus procesos.

5.5.1 Objetivos

Dado que la mayor parte de los planes de contingencia informático están orientados a temas de Siniestros, Seguridad y Recursos Humanos, cuyas situaciones son imposibles de reproducir en la vida real (Ej.: terremotos, robos, accidentes, problemas logísticos, etc.), es que el plan de pruebas estará enfocado principalmente a simular situaciones de contingencia en caso de incidencias producidas sobre equipos, información y procesos, manejados en situaciones reales y cuyos respaldos si pueden ser empleados y replicados en una hipotética situación de contingencia.

En este contexto previo, podemos precisar los siguientes objetivos a alcanzar en la realización de las pruebas:

- Programar la prueba y validación de todas las actividades que se llevarán a cabo como parte del Plan de Ejecución del Plan de Contingencia Informático respecto a una posible interrupción de los procesos identificados como críticos para el servicio de la Academia de la Magistratura
- Identificar por medio de la prueba, las posibles causas que puedan atentar contra su normal ejecución y las medidas correctivas a aplicar para subsanar los errores o deficiencias que se deriven de ella (retroalimentación del plan).
- Determinar los roles y funciones que cumplirán los responsables en la prueba, los mismos que serán los asignados para su ejecución en caso de una situación real de contingencia.

Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que serán ejecutados por un

grupo determinado de usuarios de las diferentes Unidades Orgánicas de la Academia de la Magistratura, los cuales probarán, verificarán y observarán cualquier incidencia que se origine durante dicha prueba, a fin de retroalimentar cualquier acción que pueda corregir el plan.

La información que se desarrollará como parte del Plan de Pruebas, tiene el siguiente esquema:

I. OBJETIVO DE LA PRUEBA DEL PLAN DE CONTINGENCIA INFORMÁTICO
Definición de Objetivos

II. ALCANCES
Áreas Afectadas (relación)
Personal involucrado (relación)

III. DESCRIPCIÓN DE LA PRUEBA A EFECTUARSE
Evaluación de una situación de Emergencia
Medios disponibles para operar
Fechas y horas

IV. RESULTADOS ESPERADOS DE LAS PRUEBAS
Relación de posibles acciones

5.5.2 Alcance

Todas las actividades generales que forman parte de la prueba, deberán validarse, registrarse (incluyendo observaciones) y firmarse por todos los responsables que participaron en cada una de ellas, a fin de dar fe de su ejecución y certificación.

En el Anexo A03 "Control y Certificación de Pruebas de Contingencia" se muestra el formato que se usará para la validación y registro de dichas pruebas, así como el detalle de la información que deberá ser ingresada en cada campo.

5.6 Implementación del Plan de Contingencia

La implementación del presente plan se realizará en el segundo mes de su aprobación.

5.7. Metodología

5.7.1 Fases

Como parte del presente capítulo, la Subdirección de Informática, plantea el

desarrollo de los tópicos, utilizando la metodología expuesta anteriormente. Este desarrollo incluirá las siguientes fases de la metodología:

- Identificación y Priorización de riesgos
- Definición de Eventos susceptibles de contingencia informática
- Elaboración del Plan de Contingencia Informático

5.7.1.1 Identificación y Priorización de Riesgos

El cuadro N °4 muestra la matriz de Riesgo de Contingencia, ponderado de acuerdo a los valores de riesgo e impacto en el servicio (operatividad), usando el conocimiento y la experiencia práctica de Informática en Gestión de Sistemas de Información:

Cuadro N° 4 – Matriz de Riesgo de Contingencia

Id	Descripción del Riesgo	Probabilidad	Impacto	Ponderación	Alerta	Categoría
Sub Factor. Riesgos relacionadas a Siniestros						
	INFRAESTRUCTURA					
1	Incendio					
2	Sismo					
3	Inundación por desperfecto de los sistemas sanitarios					
	SERVICIOS PÚBLICOS					
4	Interrupción de la energía eléctrica					
5	Falta de suministro de agua					
6	Interrupción de los servicios de telefonía e Internet					
Sub Factor: Riesgos relacionados a Sistemas de Información						
	INFORMACIÓN					
7	Extravío de documentos					
8	Sustracción o robo de información					
	SOFTWARE					
9	Infección de equipos por virus					
10	Pérdidas de los sistemas centrales					
11	Pérdida del servicio de correo electrónico					
12	Falla del motor de la base de datos					

Id	Descripción del Riesgo	Probabilidad	Impacto	Ponderación	Alerta	Categoría
13	Falla del sistema operativo					
	COMUNICACIONES					
14	Fallas en la red de comunicación interna					
	HARDWARE					
15	Falla de equipos personales					
	RECURSOS OPERATIVOS Y LOGÍSTICOS					
16	Falla en equipos multimedia, impresoras, scanners y otros					
Sub Factor. Riesgos relacionadas a Recursos Humanos						
	RECURSO HUMANO					
17	Ausencia imprevista del personal de soporte técnico					
18	Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático					
19	Falta de idoneidad del personal en la reserva de información de la base de datos					
Sub factor: Plan de seguridad Física						
	INFRAESTRUCTURA					
20	Sustracción de equipos y software diversos					
21	Sabotaje					
22	Vandalismo					
23	Actos terroristas					

Nota: El color rojo de la alerta representa que el evento es altamente impactante en el servicio por lo tanto debe ser obligatoriamente controlado.

En la columna CATEGORÍA por cada evento, se considera la identificación de aquellos eventos Controlables (C), y No Controlables (NC).

En los cuadros N° 5 y N° 6 se resumen los eventos según la categorización de eventos controlables y no controlables.

Cuadro N° 5 – Eventos Controlables

Id del Cuadro N° 4	Eventos controlables
1	Incendio
3	Inundación por desperfecto de los sistemas sanitarios
7	Extravío de documentos
8	Sustracción o robo de información
9	Infección de equipos por virus
10	Pérdidas de los sistemas centrales
11	Pérdida del servicio de correo electrónico
12	Falla del motor de la base de datos
13	Falla del sistema operativo
14	Fallas en la red de comunicación interna
15	Falla de equipos personales
16	Falla en equipos multimedia, impresoras, scanners y otros
17	Ausencia imprevista del personal de soporte técnico
18	Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático
20	Sustracción de equipos y software diversos

Cuadro N° 6 – Eventos no Controlables

Id del Cuadro N° 4	Eventos no controlables
2	Sismo
4	Interrupción de la energía eléctrica
5	Falta de suministro de agua
6	Interrupción de los servicios de telefonía e Internet
19	Falta de idoneidad del personal en la reserva de información de la base de datos
21	Sabotaje
22	Vandalismo
23	Actos terroristas

5.7.1.2 Definición de Eventos susceptibles de Contingencia

Una vez identificados los eventos de contingencia, presentamos el cuadro N °7 "Elementos vs. Subfactores", donde se muestra la relación existente entre los elementos mínimos definidos por la Unidad de Informática, haciendo una referencia de todos los Planes de Contingencia relacionados al mismo e indicando a que subfactor desarrollado pertenecen.

Cuadro N° 7 – Elementos vs. Subfactores a desarrollar

Elemento	Plan de Contingencia Desarrollo		
	Código Alcance		Subfactor
HARDWARE			
Servidores	FPC-04	Servicios Públicos	Contingencia Siniestros
	FPC-08	Información	Contingencia Sistemas Información
	FPC-09	Software	Contingencia Sistemas Información
	FPC-10	Software	Contingencia Sistemas Información

Elemento	Plan de Contingencia Desarrollo		
	Código Alcance		Subfactor
	FPC-12	Software	Contingencia Sistemas Información
	FPC-13	Software	Contingencia Sistemas Información
	FPC-21	Infraestructura	Contingencia Seguridad Física
Estaciones de trabajo (Computadoras y Laptops)	FPC-04	Servicios Públicos	Contingencia Siniestros
	FPC-07	Información	Contingencia Sistemas Información
	FPC-09	Software	Contingencia Sistemas Información
	FPC-14	Comunicaciones	Contingencia Sistemas Información
	FPC-24	Infraestructura	Contingencia Seguridad Física
	FPC-23	Infraestructura	Contingencia Seguridad Física
Impresoras, fotocopiadoras, scanner	FPC-16	Operativo	Contingencia Sistemas Información
Equipos multimedia	FPC-16	Operativo	Contingencia Sistemas Información
COMUNICACIONES			
Equipos de comunicaciones (Switches, Router y LAN)	FPC-14	Comunicaciones	Contingencia Sistemas Información
Equipos de telefonía fija	FPC-14	Comunicaciones	Contingencia Sistemas Información
Enlaces	FPC-14	Comunicaciones	Contingencia Sistemas Información
Cableado de Red de Datos	FPC-14	Comunicaciones	Contingencia Sistemas Información
SOFTWARE			
Base de Datos (ORACLE, MS-SQL)	FPC-10	Software	Contingencia Sistemas Información
	FPC-12	Software	Contingencia Sistemas Información
Aplicativos utilizados en la Academia de la Magistratura	FPC-07	Información	Contingencia Sistemas Información
	FPC-08	Información	Contingencia Sistemas Información
	FPC-09	Software	Contingencia Sistemas Información
	FPC-10	Software	Contingencia Sistemas Información
	FPC-12	Software	Contingencia Sistemas Información
	FPC-13	Software	Contingencia Sistemas Información
	FPC-14	Comunicaciones	Contingencia Sistemas Información
Software de Aplicaciones Web	FPC-10	Software	Contingencia Sistemas Información
	FPC-12	Software	Contingencia Sistemas Información
	FPC-13	Software	Contingencia Sistemas Información
	FPC-14	Comunicaciones	Contingencia Sistemas Información
Software Base (Sistemas Operativos y Ofimática)	FPC-10	Software	Contingencia Sistemas Información
	FPC-13	Software	Contingencia Sistemas Información
	FPC-14	Software	Contingencia Sistemas Información
Antivirus	FPC-10	Software	Contingencia Sistemas Información
	FPC-11	Software	Contingencia Sistemas Información
	FPC-12	Software	Contingencia Sistemas Información
	FPC-13	Software	Contingencia Sistemas Información
	FPC-14	Software	Contingencia Sistemas Información

Elemento	Plan de Contingencia Desarrollo		
	Código Alcance		Subfactor
INFORMACIÓN SOBRE SISTEMAS DE INFORMACIÓN			
Base de Datos utilizado por los aplicativos	FPC-10	Software	Contingencia Sistemas Información
	FPC-12	Software	Contingencia Sistemas Información
Respaldo de la información generada con Software Base	FPC-10	Software	Contingencia Sistemas Información
	FPC-12	Software	Contingencia Sistemas Información
	FPC-13	Software	Contingencia Sistemas Información
Respaldo de Aplicaciones	FPC-10	Software	Contingencia Sistemas Información
	FPC-13	Software	Contingencia Sistemas Información
Respaldo de Base de Datos	FPC-10	Software	Contingencia Sistemas Información
	FPC-12	Software	Contingencia Sistemas Información
	FPC-13	Software	Contingencia Sistemas Información
Respaldo de la información y configuración de los Servidores	FPC-12	Software	Contingencia Sistemas Información
	FPC-13	Software	Contingencia Sistemas Información
EQUIPOS DIVERSOS			
UPS	FPC-04	Servicios Públicos	Contingencia Siniestros
Aire Acondicionado	FPC-04	Servicios Públicos	Contingencia Siniestros
INFRAESTRUCTURA FÍSICA			
Oficinas de la Academia de la Magistratura	FPC-01	Infraestructura	Contingencia Siniestros
	FPC-02	Infraestructura	Contingencia Siniestros
	FPC-03	Infraestructura	Contingencia Siniestros
	FPC-22	Infraestructura	Contingencia Seguridad Física
	FPC-23	Infraestructura	Contingencia Seguridad Física
SERVICIOS PÚBLICOS			
Suministro de energía eléctrica	FPC-04	Servicios Públicos	Contingencia Siniestros
Servicios de telefonía fija y móvil	FPC-06	Servicios Públicos	Contingencia Siniestros
Suministro de agua	FPC-05	Servicios Públicos	Contingencia Siniestros
RECURSOS HUMANOS			
Disponibilidad de personal de dirección	FPC-18	Recursos Humanos	Contingencia Recursos Humanos
	FPC-19	Recursos Humanos	Contingencia Recursos Humanos
	FPC-21	Infraestructura	Contingencia Seguridad Física
	FPC-22	Infraestructura	Contingencia Seguridad Física
Disponibilidad de personal operativo	FPC-17	Recursos Humanos	Contingencia Recursos Humanos
	FPC-19	Recursos Humanos	Contingencia Recursos Humanos
	FPC-21	Infraestructura	Contingencia Seguridad Física
	FPC-22	Infraestructura	Contingencia Seguridad Física

ACADEMIA DE LA MAGISTRATURA - PRESIDENCIA - Consejo Directivo

ACADEMIA DE LA MAGISTRATURA - DIRECTOR GENERAL

ACADEMIA DE LA MAGISTRATURA - Oficina de Asesoría Jurídica

ACADEMIA DE LA MAGISTRATURA - Vº Bº OPP

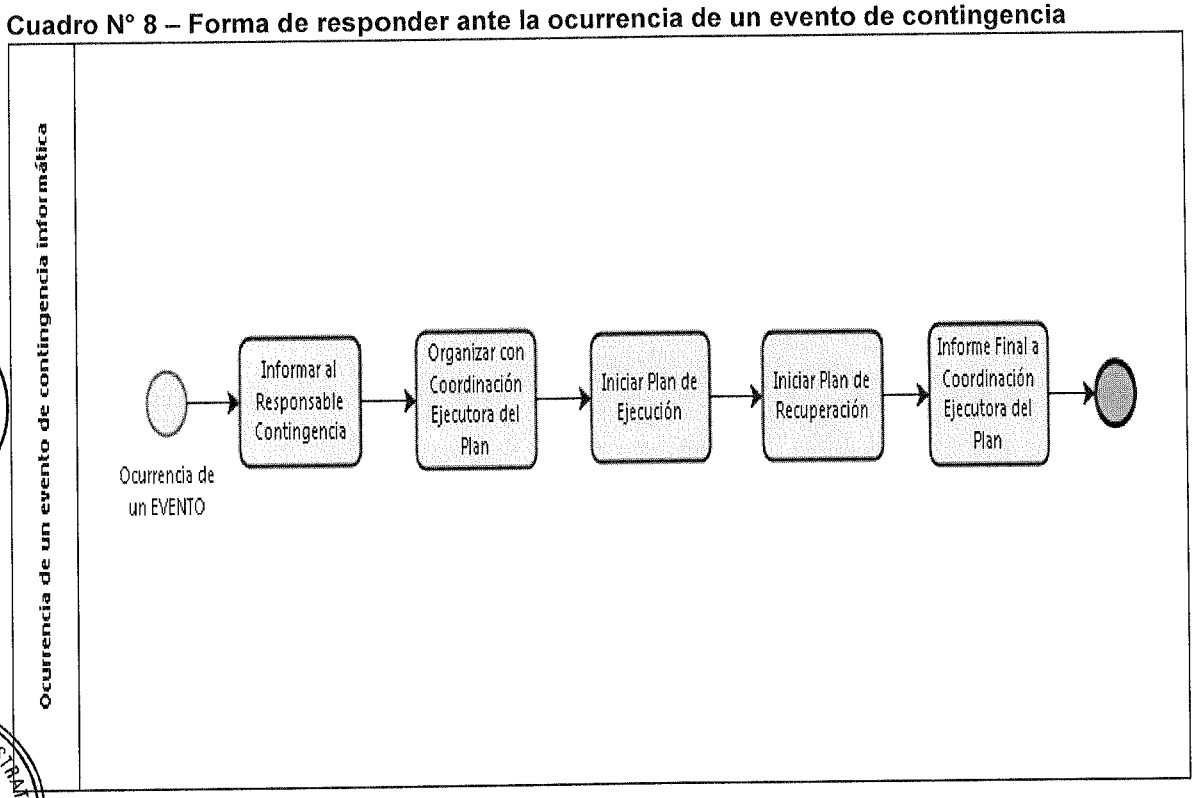
ACADEMIA DE LA MAGISTRATURA - Vº Bº - Oficina de Informática

5.7.1.3 Elaboración del Plan de Contingencia Informático

Una vez identificados los eventos de contingencia y los elementos considerados afectados o causantes de los mismos, pasamos a desarrollar los Planes de Contingencia agrupados por los Subfactores.

A manera de resumen, presentamos un flujo general que explica la forma de responder ante la ocurrencia de un evento de contingencia:

Cuadro N° 8 – Forma de responder ante la ocurrencia de un evento de contingencia



5.8 Desarrollo de las Actividades

5.8.1 Sub-factor: Contingencias relacionadas a Siniestros

Se entiende por Siniestro a las emergencias originadas por la naturaleza (sismos, inundaciones, erupciones volcánicas, deslizamientos, entre otros), y aquellas producidas por causas no controlables tales como choques eléctricos, explosiones, derrames, etc.

A continuación se indica los puntos a desarrollarse para el presente sub-factor:

5.8.1.1 Objetivo

Incluir en el Plan de Contingencia Informático todos los eventos relacionados a siniestros que permitan proveer de un conjunto de acciones destinadas a

planificar, organizar, preparar, controlar y mitigar una emergencia que se presente en las instalaciones, con la finalidad de reducir al mínimo las posibles consecuencias humanas y operativas TIC que pudieran derivarse de la misma.

5.8.1.2 Alcance

El alcance está circunscrito a los eventos de contingencia o emergencias que pudieran afectar, paralizar o dañar las instalaciones, el personal o los recursos TIC's.

Una consideración adicional a tenerse en cuenta ante la ocurrencia de un siniestro que inhabilite total o parcialmente el "Centro de Datos", es la coordinación que debe realizarse con la Dirección General de la Academia de la Magistratura para determinar el uso de un ambiente alterno para la continuidad de la operación, hasta que se restablezca el funcionamiento normal.

Por otro lado, consideramos que como parte del desarrollo del sub-factor de Siniestros, se debe incluir los elementos relativos a Servicios Públicos, por afectar o ser consecuencia de siniestros que pueden presentarse:

- Interrupción de Energía Eléctrica; al momento de restablecerse la energía eléctrica, pudiera realizarse con cargas altas que pudieran ocasionar algún tipo de siniestros, afectando la seguridad física.(resumir y orientado a siniestros)

El siguiente cuadro es un resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a los Siniestros:

Cuadro N° 10 – Matriz de Riesgos de contingencias relacionadas a los Siniestros

Código del Formato	Descripción del Evento de Contingencia	Probabilidad de Ocurrencia	Impacto	Exposición al Riesgo	Alerta
Sub-factor: Contingencias relacionadas a siniestros					
INFRAESTRUCTURA					
FPC-01	Incendio	4%	4	0.16	Crítico
FPC-02	Sismo	10%	4	0.40	Crítico
FPC-03	Inundación por desperfecto de los sistemas sanitarios	2%	1	0.02	No Crítico
SERVICIOS PÚBLICOS					
FPC-04	Interrupción de la energía eléctrica	10%	4	0.40	Crítico
FPC-05	Falta de suministro de agua	1%	3	0.03	No Crítico
FPC-06	Interrupción de los servicios de telefonía e Internet	1%	3	0.03	No Crítico

5.8.1.3 Plan de Pruebas

El plan de pruebas correspondiente a los eventos desarrollados como parte del Sub-factor Siniestros, seguirá la metodología expuesta en el punto 4.5 del Plan de Contingencia.

El plan de pruebas se determinará luego del análisis de los procesos críticos del servicio y de identificar los eventos que pudieran presentarse. La aprobación del plan de pruebas será efectuada por el Comité de Contingencias de Pruebas previamente a su ejecución.

5.8.1. 4 Descripción de Planes

Se detallarán los Planes de Contingencia de los eventos de mayor impacto identificados en la Matriz de Riesgo de Contingencia.

Academia de la Magistratura	Evento: Incendio	FCP-01

1. PLAN DE PREVENCIÓN

a. Descripción

Es un proceso de combustión caracterizado por la emisión de calor acompañado de humo, llamas o ambas que se propaga de manera incontrolable en el tiempo y en el espacio. Se producen en materiales sólidos, líquidos combustibles inflamables, equipos e instalaciones bajo carga eléctrica entre otros.

Este evento incluye los siguientes elementos mínimos identificados por la Academia de la Magistratura, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Infraestructura

- Centro de Datos

Recursos Humanos

- Personal debidamente entrenado para afrontar el evento

b. Objetivo

Establecer las acciones que se ejecutaran ante un incendio a fin de minimizar el tiempo de interrupción de las operaciones de la Academia de la Magistratura sin exponer la seguridad de las personas.

c. Criticidad

La Academia de la Magistratura determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d. Entorno

Este evento se puede dar en las instalaciones de la Subdirección de Informática.

e. Personal Encargado

El Subdirector de Informática, es quién debe dar cumplimiento a lo descrito en las Condiciones de Previsión de Riesgo del presente Plan.

f. Condiciones de Prevención de Riesgo

- Realizar inspecciones de seguridad periódicamente.
- Mantener las conexiones eléctricas seguras en el rango de su vida útil.
- Charlas sobre el uso y manejo de extintores de cada uno de los tipos.
- Acatar las indicaciones del INDECI, en torno al evento
- Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal de la Academia de la Magistratura responsable de las acciones de prevención y ejecución de la contingencia.

Igualmente se contará con los siguientes elementos para la detección y extinción de un posible incendio, los cuales cubrirán los ambientes del "Centro de Datos" y áreas afines a Informática de la Academia de la Magistratura:

- Implementar detectores de humo en el "Centro de Datos"
- Considerar la Implementación de la Central de detección de incendios
- Mantener actualizado los extintores (Agente Limpio FE-25)

2. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

La Contingencia se activará al ocurrir un incendio, el proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b. Procesos relacionados antes del Evento

- Identificar la ubicación de las estaciones manuales de alarma contra incendio.
- Identificar la ubicación de los extintores.
- Conocer el número de emergencia del Departamento de seguridad y Vigilancia de la Academia de la Magistratura.
- Tener número de teléfono del personal responsable en seguridad Informática y contingencia de la Academia de la Magistratura.
- Conocer el número de emergencia de los bomberos.

c. Personal que autoriza la Contingencia

El Subdirector de Informática pueden activar la contingencia.

d. Descripción de las actividades después de activar la Contingencia

- Tratar de apagar el incendio con extintores.
- Comunicar al personal responsable de la Academia de la Magistratura.
- Evacuar el área.
- En todo momento se coordinará con el Comité de Contingencia y Seguridad, para las acciones que deban ser efectuadas por ellos.

Luego de extinguido el incendio, se deberán realizar las siguientes actividades:

- Evaluación de los daños ocasionados al personal, bienes e instalaciones.
- En caso de daños del personal prestar asistencia médica inmediata
- Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- En caso se haya detectado bienes afectados por el evento, se evaluará el caso para determinar la reposición o restauración.

La Coordinación Ejecutora del Plan de Contingencias deberá coordinar con la Dirección General de la Academia de la Magistratura en caso se requiera la habilitación de ambientes provisionales alternos para restablecer la función de los ambientes afectados.

e. Duración

La duración de la contingencia dependerá del tiempo que demande controlar el incendio.

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El personal encargado del Plan de Recuperación es el Subdirector de Informática, cuyo rol principal es asegurar el normal desarrollo de las operaciones de la Academia de la Magistratura.

b. Descripción

El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

c. Mecanismos de Comprobación

El Subdirector de Informática presentará un informe a la Coordinación Ejecutora del Plan explicando que parte de las actividades u operaciones han sido afectadas y cuáles son las acciones tomadas.

d. Mecanismos de Recuperación

Se efectuará de acuerdo a las instrucciones impartidas que se menciona en el punto a.

e. Desactivación del Plan de Contingencia

El Subdirector de Informática desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la descripción del presente Plan de Recuperación, mediante una comunicación a la Coordinación Ejecutora del Plan.

f. Proceso de Actualización

El proceso de actualización será en base al informe presentado por el Subdirector de Informática afectada luego de lo cual se determinará las acciones a tomar.

Academia de la Magistratura	Evento: Sismo	FCP-02

1. PLAN DE PREVENCIÓN

a. Descripción

Los sismos son movimientos en el interior de la tierra y que generan una liberación repentina de energía que se propaga en forma de ondas provocando el movimiento del terreno.

Este evento incluye los siguientes elementos mínimos identificados por la Academia de la Magistratura, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

<u>Infraestructura</u>

- Sede de la Academia de la Magistratura

<u>Recursos Humanos</u>

- Personal

b. Objetivo

Establecer las acciones que se tomaran ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones de la Academia de la Magistratura sin exponer la seguridad de las personas.

c. Criticidad

La Academia de la Magistratura determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d. Entorno

Este evento se puede dar en las instalaciones de las Unidades Orgánicas.

e. Personal Encargado

Los Responsables de las Unidades Orgánicas, son quién debe dar cumplimiento a lo descrito en las Condiciones de Previsión de Riesgo del presente Plan.

f. Condiciones de Prevención de Riesgo

- Contar con un plan de evacuación de las instalaciones de la Academia de la Magistratura, el mismo que debe ser de conocimiento de todo el personal que labora.
- Realizar simulacros de evacuación con la participación de todo el personal
- Mantener las salidas libres de obstáculos.
- Señalizar todas las salidas.
- Señalizar las zonas seguras.
- Definir los puntos de reunión en caso de evacuación.

2. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

La Contingencia se activará inmediatamente después de ocurrir un sismo.

b. Procesos relacionados antes del Evento

- Tener la lista de los empleados por Unidades Orgánicas actualizada.
- Mantenimiento del orden y limpieza.
- Inspecciones diarias de seguridad interna.
- Inspecciones trimestrales de seguridad externa.
- Realización de simulacros internos en horarios que no afecten las Actividades

c. Personal que autoriza la Contingencia

El Director General, el Director Académico o la Secretaria Administrativa pueden activar la contingencia.

d. Descripción de las actividades después de activar la Contingencia

- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde.
- Evacuar las oficinas de acuerdo a las disposiciones del Director General y/o Secretaria Administrativa utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc. Por ningún motivo utilizar los ascensores.
- Verificar que todo el personal de la Academia de la Magistratura que labora en el

área se encuentren bien.

- Brindar los primeros auxilios al personal afectado si fuese necesario. (ver procedimiento FPC-21 en caso se presente una emergencia médica).
- Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc. En caso requerirse personal especializado (ejemplo INDECI), coordinar su presencia a través de la Coordinación Ejecutora del Plan de Contingencias.
- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- Limpieza de las áreas afectadas por el sismo.
- En todo momento se coordinará con personal de mantenimiento de la Academia de la Magistratura, para las acciones que deban ser efectuadas por ellos.

La Coordinación Ejecutora del Plan de Contingencias deberá coordinar con la Dirección General de la Academia de la Magistratura en caso se requiera la habilitación de ambientes provisionales alternos para restablecer la función de los ambientes afectado.

e. Duración

Los procesos de evacuación del personal de la Academia de la Magistratura serán calmados y demorará cinco (5) minutos como máximo.

La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El personal encargado del Plan de Recuperación es la Subdirección del Área afectada, cuyo rol principal es asegurar el normal desarrollo de las operaciones de la Institución

b. Descripción

El plan de recuperación estará orientado a recuperar en el menor tiempo posible la producción pendiente durante la interrupción del servicio.

c. Mecanismos de Comprobación

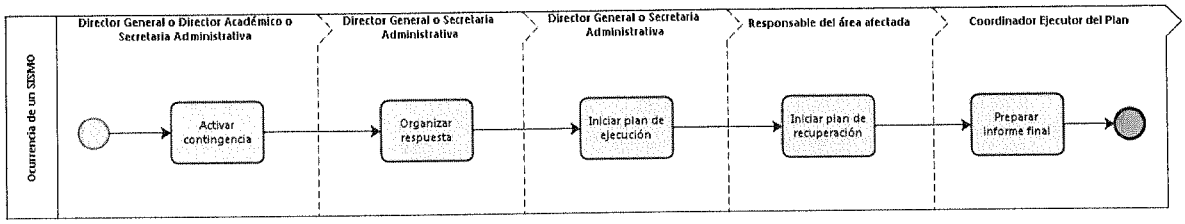
Los Responsables de las Unidades Orgánicas afectadas presentarán un informe a la Coordinación Ejecutora del Plan explicando qué parte del Servicio u operaciones ha sido afectada y cuáles son las acciones tomadas.

d. Desactivación del Plan de Contingencia

El Director General, el Director Académico y/o la Secretaria Administrativa desactivarán el Plan de Contingencia una vez que se haya tomado las acciones descritas en la Descripción del presente Plan de Recuperación, mediante una comunicación electrónica a la Coordinación Ejecutora del Plan.

e. Proceso de Actualización

El proceso de actualización será en base al informe presentado por los Responsables de las Unidades Orgánicas afectadas quien determinará las acciones a tomar.



Academia de la Magistratura	Evento: Interrupción de la Energía Eléctrica	FCP-04

1. PLAN DE PREVENCIÓN

a. Descripción

Falla general del suministro de energía eléctrica.

Este evento incluye los siguientes elementos mínimos identificados por la Academia de la Magistratura, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Servicio Público

- Suministro de energía eléctrica

Hardware

- Servidores
- Estaciones de Trabajo

Equipos diversos

- UPS

b. Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

c. Criticidad

La Academia de la Magistratura determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d. Entorno

Este evento se puede dar en las instalaciones de las Unidades Orgánicas.

e. Personal Encargado

La Secretaria Administrativa y/o Subdirector de Logística y Control Patrimonial son quiénes deben dar cumplimiento a lo descrito en las Condiciones de Previsión de Riesgo del presente Plan.

f. Condiciones de Prevención de Riesgo

- Durante las operaciones diarias del servicio u operaciones de la Academia de la Magistratura se contará con los UPS necesarios para asegurar el suministro eléctrico en las estaciones de trabajo consideradas como críticas.
- Asegurar que los equipos UPS cuenten con el mantenimiento debido y con suficiente energía para soportar una operación continua de 30 minutos como máximo. El tiempo variará de acuerdo a la función que cumplan los equipos UPS.
- Realizar pruebas periódicas de los equipos UPS para asegurar su correcto

funcionamiento.

- Contar con UPS para proteger los servidores de correo y desarrollo, previniendo la pérdida de datos durante las labores. La autonomía del equipo UPS no deberá ser menor a 30 minutos.
- Contar con UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones de la Academia de la Magistratura (puertas, contactos magnéticos, etc.)
- Contar con equipos de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.
- Contar con procedimientos operativos alternos para los casos de falta de sistemas, de tal forma que no se afecten considerablemente las operaciones en curso.

2. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

La Contingencia se activará inmediatamente después de ocurrir un corte de energía eléctrica en los ambientes de la Academia de la Magistratura.

b. Procesos relacionados antes del Evento

Cualquier actividad de servicio dentro de las instalaciones de la Academia de la Magistratura.

c. Personal que autoriza la Contingencia

La Secretaria Administrativa y/o el Subdirector de Logística y Control Patrimonial pueden activar la contingencia.

d. Descripción de las actividades después de activar la Contingencia

- Informar al Secretario Administrativo y/o Subdirector de Informática del problema presentado.
- Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas y coordinar las acciones necesarias.
- Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.
- En el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente.
- En caso la interrupción de energía sea mayor a quince minutos, se deberán apagar los servidores de producción y desarrollo hasta que regrese el fluido eléctrico (Anexo A05: Procedimientos para el apagado y encendido de los Equipos del Centro de Datos de la Academia de la Magistratura).

e. Duración

La duración total del evento dependerá del proveedor externo de energía eléctrica.

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El personal encargado del Plan de Recuperación es el Subdirector de Informática, quien se encargará de realizar las acciones de recuperación necesarias.

b. Descripción

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de

eventos.

Se informará a la Coordinación Ejecutora del Plan el problema presentado y el procedimiento usado para atender el problema.

En función a esto, se tomarán las medidas preventivas del caso.

c. Mecanismos de Comprobación

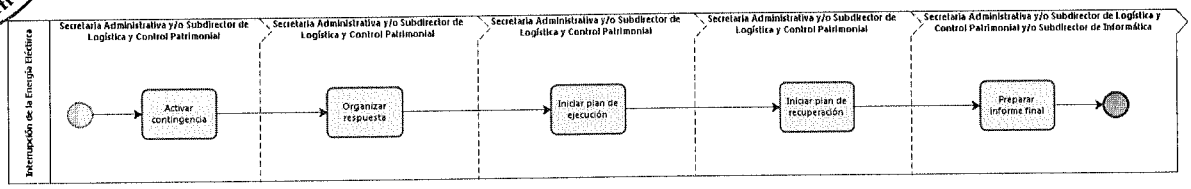
La Secretaria Administrativa, el Subdirector de Logística y Control Patrimonial y/o el Subdirector de Informática presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

d. Desactivación del Plan de Contingencia

La Secretaria Administrativa y/o el Subdirector de Logística y Control Patrimonial desactivarán el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

e. Proceso de Actualización

En base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.



5.8.2 Sub-factor: Contingencias relacionadas a los Sistemas de Información

A continuación se muestra los puntos a desarrollarse para el presente sub-factor:

5.8.2.1 Objetivo

Los planes de contingencia de los eventos relacionados a los Sistemas de Información tienen por objetivo que ante cualquier evento que atente contra la normal operación tanto en hardware, software como en cualquier elemento interno o externo relacionado a los mismos, se dispongan de alternativas de solución frente al problema a fin de asegurar la operación del servicio y/o minimizar el tiempo de interrupción.

5.8.2.2 Alcance

El alcance de dichos planes se circunscribe a las actividades de uso de sistemas y/o aplicaciones, así como a las operaciones del servicio que son afectadas durante la operatividad de la Academia de la Magistratura.

Resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a los Sistemas de Información.

Cuadro N° 11 – Matriz de Riesgos de contingencias relacionadas a los Sistemas de Información

Código del Formato	Descripción del Evento de Contingencia	Probabilidad de Ocurrencia	Impacto	Exposición al Riesgo	Alerta
Sub-factor: Contingencia relacionada a Sistemas de Información					
INFORMACIÓN					
FCP-07	Extravío de documentos	2%	3	0.06	No Crítico
FCP-08	Sustracción o robo de información	2%	3	0.06	No Crítico
SOFTWARE					
FCP-09	Infección de equipos por virus	5%	4	0.20	Crítico
FCP-10	Pérdidas de los sistemas centrales	5%	4	0.20	Crítico
FCP-11	Pérdida del servicio de correo electrónico	1%	2	0.02	No Crítico
FCP-12	Falla del motor de la base de datos	4%	4	0.16	Crítico
FCP-13	Falla del sistema operativo	4%	4	0.16	Crítico
COMUNICACIONES					
FCP-14	Fallas en la red de comunicación interna	2%	4	0.08	No Crítico
HARDWARE					
FCP-15	Falla de equipos personales	2%	2	0.04	No Crítico
RECURSOS OPERATIVOS Y LOGÍSTICOS					
FCP-16	Falla en equipos multimedia, impresoras, scanners y otros	1%	2	0.02	No Crítico

5.8.2.3 Plan de Pruebas

El plan de pruebas correspondiente a los eventos desarrollados como parte del Sub Factor Sistemas de Información, seguirá la metodología expuesta en el punto 4.5 del Plan de Contingencia.

El plan de pruebas se determinará luego del análisis de los procesos críticos de las operaciones y de identificar los eventos que pudieran presentarse. La aprobación del plan de pruebas será efectuada por el Comité de Contingencias de Pruebas previamente a su ejecución.

5.8.2.4 Descripción de Planes

Se detallarán los Planes de Contingencia de alguno de los eventos identificados en la Matriz de Riesgo de Contingencia.

Academia de la Magistratura	Evento: Infección de equipos por virus	FCP-09

1. PLAN DE PREVENCIÓN

a. Descripción

Virus informático es un programa de software que se propaga de un equipo a otro y que interfiere el funcionamiento del equipo. Además, Un virus informático puede dañar o eliminar los datos de un equipo.

Este evento incluye los siguientes elementos mínimos identificados por la Academia de la Magistratura, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores
- Estaciones de Trabajo

Software

- Software Base
- Aplicativos utilizados en la Academia de la Magistratura

b. Objetivo

Restaurar la operatividad de los equipos después de eliminar los virus o reinstalar las aplicaciones dañadas.

c. Criticidad

La Academia de la Magistratura determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d. Entorno

Los servidores y las estaciones de trabajo PC´s, se encuentran instaladas en la Academia de la Magistratura.

e. Personal Encargado

El Subdirector de Informática es el responsable en la supervisión del correcto funcionamiento de los servidores y de las estaciones de trabajo PC´s

f. Condiciones de Prevención de Riesgo

- Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.
- Restringir el acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.
- Eliminación de lectores de DVD de las estaciones de trabajo que no lo requieran.
- Deshabilitar los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo.

- Aplicar filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo por virus.
- Contar con antivirus instalados en cada estación de trabajo, el mismo que debe estar actualizado permanentemente.
- Contar con equipos de respaldo ante posibles fallas de las estaciones, para su reemplazo provisional hasta su desinfección y habilitación.

2. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

- Mensajes de error durante la ejecución de programas.
- Lentitud en el acceso a las aplicaciones.
- Falla general en el equipo (sistema operativo, aplicaciones).

b. Procesos relacionados antes del Evento

Cualquier proceso relacionado con el uso de las aplicaciones en las estaciones de trabajo.

c. Personal que autoriza la Contingencia

El Subdirector de Informática puede activar la contingencia.

d. Descripción de las actividades después de activar la Contingencia

- Desconectar la estación infectada de la red de la Academia de la Magistratura
- Verificar si el equipo se encuentra infectado, utilizando un detector de virus actualizado.
- Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.)
- Eliminar el agente causante de la infección.
- Remover el virus del sistema.
- Probar el sistema.
- En caso no solucionarse el problema :
  - Realizar backup de la información del usuario, para esto utiliza la Ficha de Reinstalación de Equipos
  - Formatear el equipo
  - Personalizar la estación para el usuario
- Conectar la estación a la red de la Academia de la Magistratura.
- Efectuar las pruebas necesarias con el usuario.
- Solicitar conformidad del servicio, cierre del ticket de soporte según lo contemplado en el .Procedimiento de soporte técnico.

e. Duración

La duración del evento no deberá ser mayor a CUATRO HORAS en caso se confirme la presencia de un virus. Esperar la indicación del personal de soporte para reanudar el trabajo

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El personal de Soporte Técnico de la Subdirección de Informática, luego de restaurar el correcto funcionamiento de la estación de trabajo (PC), coordinará con el usuario responsable y/o Responsable de la Unidad Orgánica para reanudar las labores de trabajo con el equipo.

b. Descripción

- Se informará al Subdirector de Informática el tipo de virus encontrado y el

procedimiento usado para removerlo.

- En función a esto, se tomarán las medidas preventivas del caso enviando una alerta vía correo al personal de la Academia de la Magistratura.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

c. Mecanismos de Comprobación

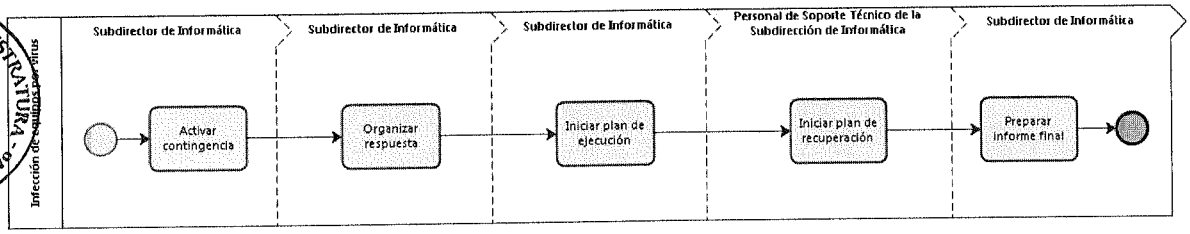
El Subdirector de Informática presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

d. Desactivación del Plan de Contingencia

El Subdirector de Informática desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con las estaciones de trabajo PC's.

e. Proceso de Actualización

En base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.



Academia de la Magistratura	Evento: Pérdidas de los sistemas centrales	FCP-10

1. PLAN DE PREVENCIÓN

a. Descripción

Es la ausencia de interacción entre el Software y el Hardware haciendo inoperativa la máquina, es decir, el Software no envía instrucciones al Hardware imposibilitando su funcionamiento.

Este evento incluye los siguientes elementos mínimos identificados por la Academia de la Magistratura, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Software

- Software base
- Software de base de datos
- Aplicativos utilizados en la Academia de la Magistratura

Hardware

- Servidores

Información

- Respaldo de base de datos
- Respaldo de los aplicativos utilizados en la Academia de la Magistratura
- Respaldo de software base

b. Objetivo

Mantener operativo los servidores de producción donde se ejecutan las aplicaciones de la Academia de la Magistratura.

c. Criticidad

La Academia de la Magistratura determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d. Entorno

Los servidores de aplicaciones están situados en el centro de datos de la Academia de la Magistratura.

e. Personal Encargado

El Subdirector de Informática es el responsable de asegurar el correcto funcionamiento de los servidores durante los servicios. Asimismo, coordinará las acciones necesarias para restablecer el servicio en caso se produzca el evento.

El Subdirector de Informática es el encargado de coordinar las acciones necesarias con el personal de las áreas usuarias, para asegurar un servicio continuo de los servidores y sus aplicaciones, de tal forma que no afecten el servicio brindado.

f. Condiciones de Prevención de Riesgo

La Subdirección de Informática debe tener en cuenta las siguientes acciones preventivas para asegurar el servicio de las aplicaciones:

- Contar con equipos de respaldo ante posibles fallas de los servidores.
- Contar con mantenimiento preventivo para dichos equipos.
- Contar con los backups de información necesarios para restablecer las aplicaciones (ver Resolución N° 61-2012-AMAG-CD/P que aprueba el Procedimiento de ejecución del respaldo y restauración de la información).
- Contar con backups de las aplicaciones y de las bases de datos (ver Resolución N° 61-2012-AMAG-CD/P que aprueba el Procedimiento de ejecución del respaldo y restauración de la información).
- Almacenar en un lugar seguro los backups referidos a aplicaciones y datos. Se recomienda el almacenamiento de los backups en un lugar externo fuera de las instalaciones de la Academia de la Magistratura.

2. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

- Falla de acceso a las aplicaciones.
- Mensaje Pérdida de Conexión a la base de datos.

b. Procesos relacionados antes del Evento

Cualquier proceso relacionado con el uso de las aplicaciones en los servidores de la Academia de la Magistratura.

c. Personal que autoriza la Contingencia

El Subdirector de Informática puede activar la contingencia.

d. Descripción de las actividades después de activar la Contingencia

- Realizar los procedimientos para la recuperación de los sistemas de la

Academia de la Magistratura

e. Duración

La duración del evento estará en función de la complejidad del problema encontrado. Esperar la indicación de la Subdirección de Informática para reanudar la operación normal con las aplicaciones.

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El Subdirector de Informática, luego de verificar la corrección del problema de acceso a los servidores, coordinará con los Responsables de las Unidades Orgánicas para la reanudación de los trabajos operativos con las aplicaciones.

b. Descripción

- Se informará a la Dirección General la causa que motivó la paralización del servicio.
- En función a esto, se tomarán las medidas preventivas del caso enviando y se revisará el Plan de Contingencia Informático para actualizarlo de ser necesario.

c. Mecanismos de Comprobación

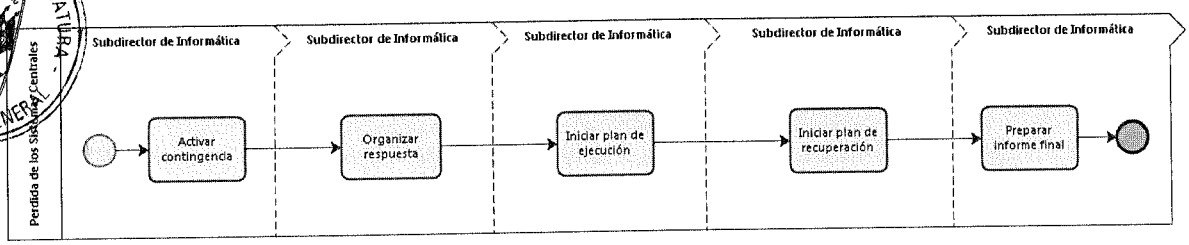
El Subdirector de Informática presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

d. Desactivación del Plan de Contingencia

El Subdirector de Informática desactivará el Plan de Contingencia una vez que se recupere la funcionalidad del servicio.

e. Proceso de Actualización

En caso de existir información pendiente de actualización, debido a la falla de los sistemas centrales, se coordinará con los Responsables de las Unidades Orgánicas, para iniciar las labores de actualización de los sistemas.



Academia de la Magistratura	Evento: Falla del motor de base de datos	FCP-12

1. PLAN DE PREVENCIÓN

a. Descripción

Ausencia del servicio principal de base de datos para acceder, almacenar, procesar y proteger los datos y así cumplir con los requisitos de las aplicaciones.

Este evento incluye los siguientes elementos mínimos identificados por la Academia de la Magistratura, que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Software

- Aplicativos utilizados

Hardware

- Servidores

Información

- Respaldo de la Base de Datos
- Respaldo de Software Base

b. Objetivo

Asegurar la continuidad de las operaciones, a través de los medios de respaldo adecuados para restaurar la base de datos de las aplicaciones ejecutadas en los servidores centrales.

c. Criticidad

La Academia de la Magistratura determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d. Entorno

Se puede producir durante el servicio, afectando a las aplicaciones utilizadas para dar soporte a las operaciones de la Academia de la Magistratura.

e. Personal Encargado

El Subdirector de Informática es el responsable de asegurar el correcto funcionamiento de la base de datos durante los servicios. Asimismo, coordinará las acciones necesarias para restablecer el servicio de la base de datos en caso se produzca el evento.

El Subdirector de Informática es el encargado de coordinar las acciones necesarias con el personal de las áreas usuarias, para asegurar un servicio continuo de la base de datos, de tal forma que no afecten el servicio brindado.

f. Condiciones de Prevención de Riesgo

- Revisión periódica de los logs de la BD para prevenir mal funcionamiento de la Base de Datos.
- Contar con los backups diarios de datos de las aplicaciones en desarrollo/producción en la Institución. Se realizan copias de la información o de los registros con la finalidad de asegurar la información mantenida en la base de datos.
- La copia de seguridad de la información es un proceso diario, en donde se busca asegurar la integridad de la información. También se obtienen copias de seguridad de la base de datos de acuerdo a requerimientos antes o después de un determinado proceso (ver Resolución N° 61-2012-AMAG-CD/P que aprueba el Procedimiento de ejecución del respaldo y restauración de la información).
- Mantener actualizado el software de gestión de BD, con todos los parches del producto según el fabricante del producto.
- Contar con servicios de soporte vigentes para el software de gestión de BD. En caso sea necesario, este soporte debe incluir actividades de prevención, revisión del sistema y mantenimiento general a la base de datos.

2. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

- Fallas en la conexión. Indisponibilidad del sistema aplicativo.
- Identificación de falla en la pantalla de las estaciones de trabajo y/o servidores de aplicaciones.

b. Procesos relacionados antes del Evento

Copia de respaldo de la base de datos disponible para el uso de las aplicaciones en los servidores de la Academia de la Magistratura.

c. Personal que autoriza la Contingencia

El Subdirector de Informática puede activar la contingencia.

d. Descripción de las actividades después de activar la Contingencia

- Sistemas de Proveedores.- De producirse una falla al momento de la operación de estos sistemas por efecto del programa ejecutable (cliente) o base de datos, deberá ser comunicado y coordinado inmediatamente con el proveedor, para su corrección.
- Sistemas Desarrollados y/o con mantenimiento por parte del personal de la Subdirección de Informática.- De producirse una falla al momento de la operación de estos sistemas, el Subdirector de Informática asumirá, delegará y/o coordinará los trabajos de corrección y/o modificación.

e. Duración

El tiempo máximo de la contingencia no debe sobrepasar las OCHO horas.

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El Subdirector de Informática, luego de verificar la corrección del problema de acceso a la base de datos, coordinará con los Responsables de las Unidades Orgánicas para la reanudación de los trabajos operativos con las aplicaciones.

b. Descripción

- Se informará al Subdirector de Informática la causa del problema presentado y el procedimiento usado para atender el problema.
- Se tomarán las medidas preventivas del caso enviando una alerta vía correo al persona.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

c. Mecanismos de Comprobación

El Subdirector de Informática presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

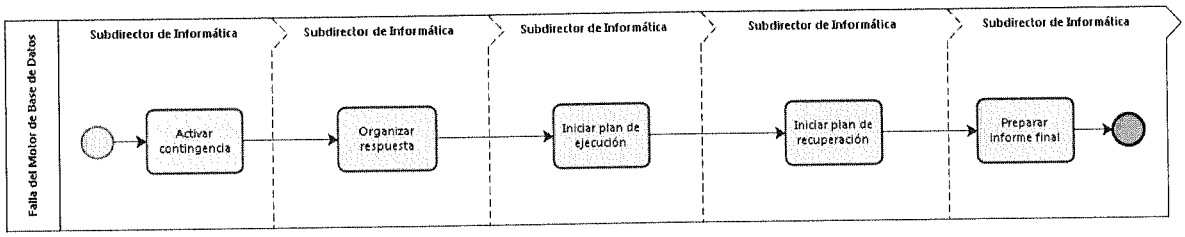
d. Desactivación del Plan de Contingencia

El Subdirector de Informática desactivará el Plan de Contingencia una vez que se recupere la funcionalidad del servicio.

e. Proceso de Actualización

En base al informe presentado que identifica las causas, se determinará las acciones de preventivas necesarias que deberán incluirse en el presente plan.

En caso exista información pendiente de actualización, debido a la falla se coordinará con los Responsables de las Unidades Orgánicas, para iniciar las labores de actualización de los sistemas.



Academia de la Magistratura	Evento: Falla del sistema operativo	FCP-13

1. PLAN DE PREVENCIÓN

a. Descripción

Falla en el sistema operativo de las computadoras.

Este evento incluye los siguientes elementos mínimos identificados por la Academia de la Magistratura, que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Software

- Aplicativos utilizados

Hardware

- Servidores
- Computadoras

Información

- Respaldo de la Base de Datos
- Respaldo de Software Base

b. Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados para restaurar las funciones de los elementos identificados.

c. Criticidad

La Academia de la Magistratura determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d. Entorno

Se puede producir durante la operatividad, afectando a las estaciones de trabajo y/o servidores de aplicaciones usados para dar soporte a las operaciones.

e. Personal Encargado

El Subdirector de Informática es el responsable de coordinar las acciones necesarias para asegurar el correcto funcionamiento de las aplicaciones.

f. Condiciones de Prevención de Riesgo

Se debe asegurar de cubrir los siguientes aspectos:

- Contar con los backups diarios de datos de las aplicaciones en producción en la institución (ver Resolución N° 61-2012-AMAG-CD/P que aprueba el Procedimiento de ejecución del respaldo y restauración de la información).
- Contar con servicios de soporte vigentes para los principales causantes del evento:
  - Se debe mantener acuerdos con Proveedores de Servicio.
  - Revisión periódica de los logs de actividad de los servidores para prevenir su mal funcionamiento.
  - Estaciones de trabajo y servidores deberán contar con antivirus actualizados.

2. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

- Detención de las funciones de trabajo en estaciones de trabajo y/o servidores de aplicaciones.
- Identificación de falla en el monitor de los servidores de aplicaciones y/o estaciones de trabajo.

b. Procesos relacionados antes del Evento

Respaldo disponible de los sistemas operativos para la ejecución de las aplicaciones en los servidores.

c. Personal que autoriza la Contingencia

El Subdirector de Informática puede activar la contingencia.

d. Descripción de las actividades después de activar la Contingencia

En el caso de las estaciones de trabajo :

- Proceder a la revisión de la estación de trabajo para determinar la causa de la falla.
- Probar el sistema.
- En caso no solucionarse el problema :
  - Realizar el respaldo de información del usuario.
  - Formatear el equipo
  - Personalizar la estación para el usuario
  - Conectar la estación a la red del Archivo.
- Efectuar las pruebas necesarias con el usuario.
- Solicitar conformidad del servicio, cierre del ticket de soporte según lo contemplado en el .Procedimiento de soporte técnico.

En el caso de los servidores de aplicaciones :

- Direcciones y/o Jefaturas:
  - Reportar el problema al área de soporte Técnico.
  - Coordinar las acciones a realizarse y el tiempo aproximado de interrupción del servicio.
  - Comunicar a los Responsables de las Unidades Orgánicas para que se tomen las acciones del caso y no se afecte en sus operaciones.

e. Duración

El tiempo máximo de la contingencia no debe sobrepasar las OCHO horas

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El Subdirector de Informática, luego de verificar la corrección del problema del sistema operativo, coordinará con los Responsables de las Unidades Orgánicas para la reanudación de los trabajos operativos con las aplicaciones.

b. Descripción

- Se informará al Subdirector de Informática la causa del problema presentado y el procedimiento usado para atender el problema.
- En función a esto, se tomarán las medidas preventivas del caso enviando una alerta vía correo al personal.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

c. Mecanismos de Comprobación

El Subdirector de Informática presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

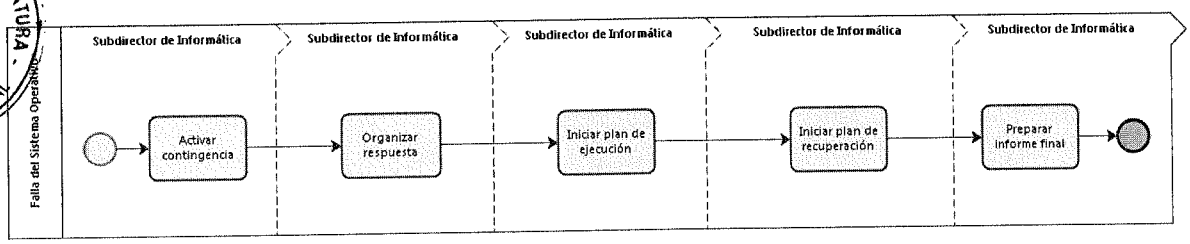
d. Desactivación del Plan de Contingencia

El Subdirector de Informática desactivará el Plan de Contingencia una vez que se recupere la funcionalidad del servicio.

e. Proceso de Actualización

En base al informe presentado que identifica las causas de la pérdida del sistema operativo en las estaciones de trabajo y/o servidores, se determinará las acciones de prevención a tomar.

En caso existiese información pendiente de actualización, debido a la falla de los sistemas centrales, se coordinará con los Directores y/o Subdirectores de Área, para iniciar las labores de actualización de los sistemas.



5.8.3 Sub-factor: Contingencias relacionadas a los Recursos Humanos

A continuación se muestra los puntos a desarrollarse para el presente sub-factor:

5.8.3.1 Objetivo

El desarrollo de este tipo de contingencias está relacionado con todos los elementos y factores que pueden afectar y/o ser afectados por el personal de la

5.8.3.2 Alcance

La seguridad referida al personal se contemplará desde las etapas de selección del mismo e incluirá en los contratos y definiciones de puestos de trabajo para poder cumplir el objetivo de reducir los riesgos de:

- Actuaciones humanas
- Indisponibilidad por enfermedades
- Emergencias médicas
- Incapacidad temporal o permanente por accidentes
- Renuncias o ceses

Se deberá comprobar que las definiciones de puestos de trabajo contemplan todo lo necesario en cuanto las responsabilidades encomendadas.

A continuación se presenta un resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a los Recursos Humanos que se describirán en detalle más adelante:

Cuadro N° 12 – Matriz de Riesgos de contingencias relacionadas a los Recursos Humanos

Código del Formato	Descripción del Evento de Contingencia	Probabilidad de Ocurrencia	Impacto	Exposición al Riesgo	Alerta
Sub-factor: Plan de Seguridad Física					
FPC-17	Ausencia imprevista del personal de soporte técnico	5%	3	0.15	Crítico
FPC-18	Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático	5%	3	0.15	Crítico
FPC-19	Falta de idoneidad del personal en la reserva de información de la base de datos	1%	4	0.04	No Crítico

5.8.3.3 Plan de Pruebas

El plan de pruebas correspondiente a los eventos desarrollados como parte del tópico Recursos Humanos, seguirá la metodología expuesta en el punto 4.5 del Plan de Contingencia Informático.

El plan de pruebas se determinará luego del análisis de los procesos críticos

del servicio y de identificar los eventos que pudieran presentarse. La aprobación del plan de pruebas será efectuada por la Dirección de la Academia de la Magistratura previamente a su ejecución.

5.8.3.4 Descripción de Planes

Se detallarán los Planes de Contingencia de los eventos identificados en la Matriz de Riesgo de Contingencia.

Academia de la Magistratura	Evento: Ausencia imprevista del personal de Soporte Técnico	FCP-17

4. PLAN DE PREVENCIÓN

a. Descripción

Ausencias del personal de Soporte Técnico relevante (enfermedad, renuncias, ceses), en toma decisiones claves que garantice el normal funcionamiento de servidores y redes de la institución.

Este evento incluye los siguientes elementos mínimos identificados por la Academia de la Magistratura, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Recursos Humanos

- Personal

b. Objetivo

Asegurar la continuidad del Servicio Informático de la Academia de la Magistratura.

c. Criticidad

La Academia de la Magistratura determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d. Entorno

Este evento se puede dar en las instalaciones de las Unidades Orgánicas.

e. Personal Encargado

El Subdirector de Informática es quién debe disponer se cumplan las Condiciones de Previsión de Riesgo del presente Plan.

f. Condiciones de Prevención de Riesgo

La existencia del presente evento se puede dar en cualquier momento, dependiendo de las circunstancias personales, por lo que se considera lo siguiente:

- Como primera prevención, el Subdirector de Informática, se asegurará en capacitar al personal de soporte técnico con el fin que cumpla el perfil, conocimiento y capacidad para reemplazar la ausencia ante la presencia de este evento.
- Como segunda prevención, el Subdirector de Informática se asegurara en tener como mínimo a dos profesionales técnicos en el área de soporte técnico.
- Incluir como parte de las funciones del personal, comunicar anticipadamente la inasistencia a su centro de labores.

- Para el control del personal se cuenta con un software de control de asistencia, de donde se proveerá información al Subdirector de Informática, para que tome las acciones preventivas correspondientes.

5. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

Reporte de inasistencia del personal de Soporte Técnico.
El proceso de contingencia se activa durante las DOS (02) HORAS iniciales del día.

b. Procesos relacionados antes del Evento

Se podría dar por:

- Conocimiento del Subdirector de Informática por parte del reporte de inasistencia del Sistema de Control de Asistencia.
- Conocimiento del Subdirector de Informática por comunicación telefónica por parte del personal de Soporte Técnico ausente o algún familiar.

c. Personal que autoriza la Contingencia

El Subdirector de Informática

d. Descripción de las actividades después de activar la Contingencia

- Confirmado la inasistencia del personal de Soporte Técnico, el Subdirector de Informática asignará la responsabilidad al Asistente del área de soporte técnico capacitado para reemplazar en las funciones que el personal titular de soporte técnico poseía.
- El Subdirector de Informática solicitará al Secretario Administrativo el reemplazo del personal.

e. Duración

Máximo OCHO (08) horas. El fin del presente evento es la presencia del reemplazo que asume la responsabilidad; hasta que se confirme la presencia del personal de Soporte Técnico en caso de renuncia u otras por fuerza mayor.

6. PLAN DE RECUPERACIÓN

a. Personal Encargado

El personal encargado del Plan de Recuperación es el Subdirector de Informática, cuyo rol principal es asegurar el normal funcionamiento del Servicio Informático.

b. Descripción

- Regularización en los servicios pendiente durante la ausencia.
- Revisión de los servicios atendidos si fuera el caso.
- Definir los ajustes para asegurar rápida y mejora en la acción y prevención del presente evento.

c. Mecanismos de Comprobación

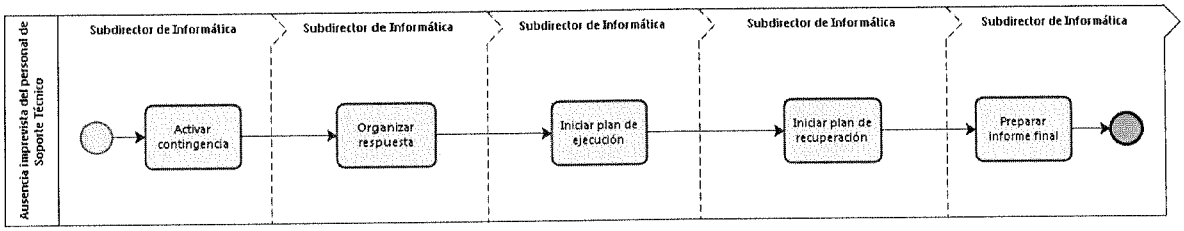
El Subdirector de Informática presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del Servicio Informático ha sido afectado y cual son las acciones tomadas.

d. Desactivación del Plan de Contingencia

El Subdirector de Informática desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la Descripción del presente Plan de Recuperación, mediante una comunicación electrónica a la Coordinación Ejecutora del Plan.

e. Proceso de Actualización

En base al informe presentado por el Subdirector de Informática y las causas identificadas en el Servicio informático se determinará las acciones a tomar.



Academia de la Magistratura	Evento: Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático	FCP-18

1. PLAN DE PREVENCIÓN

a. Descripción

Ausencias del personal de Dirección y/o Subdirecciones (enfermedad, renuncias, ceses, licencias), en toma decisiones claves que garantice el normal funcionamiento de las actividades.

Este evento incluye los siguientes elementos mínimos identificados por la Academia de la Magistratura, que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Recursos Humanos

- Personal

b. Objetivo

Asegurar la continuidad de las operaciones en las diferentes Direcciones y/o Subdirecciones de la Academia de la Magistratura, evitando el quiebre en la cadena de mando, a través de reemplazos de personal ejecutivos.

c. Criticidad

La Academia de la Magistratura determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d. Entorno

Este evento se puede dar en las instalaciones de las Unidades Orgánicas.

e. Personal Encargado

El Director General, el Director Académico y la Secretaria Administrativa, son quienes deben de asegurarse de que se cumpla lo descrito en las Condiciones de Previsión de Riesgo del presente Plan.

f. Condiciones de Prevención de Riesgo

La existencia del presente evento se puede dar en cualquier momento, dependiendo de las circunstancias personales que se presente al personal de Dirección y/o Subdirección, por lo que se considera lo siguiente:

- Como primera prevención, la Dirección General asegurará en capacitar a un

personal con más de 5 años de experiencia en la Institución que cumpla el perfil, conocimiento y capacidad para reemplazar la ausencia ante el evento.
- Incluir como parte de las funciones del personal, comunicar anticipadamente la inasistencia a su centro de labores, siempre y cuando se trate de ocasiones premeditas.

2. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

Reporte de inasistencia de algún Director o Subdirector.
El proceso de contingencia se activa durante las DOS (02) HORAS iniciales del día.

b. Procesos relacionados antes del Evento

Se podría dar por:
- Falta de decisión del Director y/o Subdirector para aplicar soluciones ante algún inconveniente en las actividades u operaciones de su competencia, donde se detecte la ausencia.
- Reporte de Control de Asistencia referente a inasistencias

c. Personal que autoriza la Contingencia

El encargado de autorizar el proceso de contingencia es el Director General, el Director Académico o la Secretaria Administrativa.

d. Descripción de las actividades después de activar la Contingencia

- Confirmado la inasistencia del Director General, se coordinará el reemplazo con el Secretario General.
- Confirmado la inasistencia del Director Académico, se coordinará el reemplazo con el Director General.
- Confirmado la inasistencia de la Secretaria Administrativa, se coordinará el reemplazo con el Director General.
- Confirmada la inasistencia de un Subdirector se coordinará el reemplazo con el Director Académico o la Secretaria Administrativa.

e. Duración

Máximo TRES (03) horas. El fin del presente evento es la presencia del reemplazo, o el empleado más antiguo que esté capacitado para que asuma la responsabilidad; hasta que se confirme la presencia del Director y/o Subdirector o Nuevo Director y/o Subdirector en caso de renuncia u otras por fuerza mayor.

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El personal encargado del Plan de Recuperación es el Director y/o Subdirector de Área o Nuevo Director y/o Subdirector de Área, cuyo rol principal es asegurar el normal funcionamiento de las actividades de la Academia de la Magistratura.

b. Descripción

- Regularización en las coordinaciones pendiente durante la ausencia.
- Definir los ajustes para asegurar rápida y mejora en la acción y prevención del presente evento.

c. Mecanismos de Comprobación

El Director y/o Subdirector de Área presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del servicio u operaciones ha sido afectado y cual son las

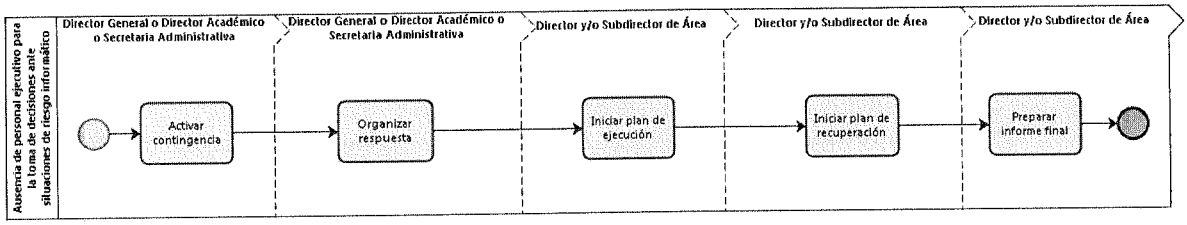
acciones tomadas.

d. Desactivación del Plan de Contingencia

El Director General, Director Académico y/o Secretario Administrativo desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la Descripción del presente Plan de Recuperación, mediante una comunicación electrónica a la Coordinación Ejecutora del Plan.

e. Proceso de Actualización

En base al informe presentado por el Director y/o Subdirector de Área y las causas identificadas en la operatividad, se determinará las acciones a tomar.



8.4 Sub-factor: Contingencias relacionadas a Seguridad Física

A continuación se muestra los puntos a desarrollarse para el presente sub-factor:

5.8.4.1 Objetivo

Definir acciones de prevención a fin de eliminar o mitigar riesgos de seguridad física tanto de las instalaciones como de todos los elementos que operan en su interior (equipos, documentación, mobiliario, etc.) por motivos de incidentes causados de manera intencional, eventual o natural y que puedan afectar las operaciones normales del servicio.

5.8.4.2 Alcance

Serán tomados en cuenta lo siguientes elementos:

- Ubicación y disposición física
- Elementos de seguridad de los ambientes de trabajo
- Control de accesos de personal interno y externo al servicio
- Actos terroristas o de vandalismo que pudieran afectar infraestructura, personal o documentación.

A continuación se presenta un resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a la Seguridad Física que se describirán en detalle más adelante:

Cuadro N° 13 – Matriz de Riesgos de contingencias relacionadas a la Seguridad

Física

Código del Formato	Descripción del Evento de Contingencia	Probabilidad de Ocurrencia	Impacto	Exposición al Riesgo	Alerta
Sub-factor: Plan de Seguridad Física					
FPC-20	Sustracción de equipos y software diversos	2%	2	0.04	No Crítico
FPC-21	Sabotaje	1%	2	0.02	No Crítico
FPC-22	Vandalismo	1%	3	0.03	No Crítico
FPC-23	Actos terroristas	1%	4	0.04	No Crítico

5.8.4.3 Plan de Pruebas

El plan de pruebas correspondiente a los eventos desarrollados como parte del Sub-Factor Seguridad Física, seguirá la metodología expuesta en el punto 6.4 del Plan de Contingencia Informático.

El plan de pruebas se determinará luego del análisis de los procesos críticos del servicio y de identificar los eventos que pudieran presentarse. La aprobación del plan de pruebas será efectuada por la Dirección General de la Academia de la Magistratura previamente a su ejecución.

5.8.4.4 Descripción de Planes

Estos eventos de contingencia son menores a 0.15.

5.9 Estrategias

La estrategia aplicada para el presente Plan de Contingencia es contar con:

- Plan de Prevención, Plan de Ejecución, Plan de Recuperación y Plan de Pruebas, desarrollados en el presente Plan de Contingencia Informático.
- Se propone una organización para la gestión del Plan de Contingencia Informático, el mismo que está desarrollado en el presente Plan "4.1 Organización".
- Tener desarrollado y documentado los principales eventos susceptibles planteados en el presente Plan de Contingencia Informático "5.2 Desarrollo de las Actividades".

5.9.1 Programas

En el presente Plan de Contingencia Informático se ha desarrollado un conjunto de ítems (cuadro Nro. 4), eventos o programas que permitan añadir valor a los sub-factores que ha priorizado la Academia de la Magistratura. Un resumen de los ítems desarrollados son los siguientes:

Cuadro N° 14 – Resumen de los ítem desarrollados.

Id	Alcance	Descripción del Evento de Contingencia
Sub-factor: Siniestros		
FPC-01	Infraestructura	Incendio
FPC-02	Infraestructura	Sismo
FPC-04	Servicios Públicos	Interrupción de la energía eléctrica
Sub-factor: Sistemas de Información		
FPC-09	Software	Infección de equipos por virus
FPC-10	Software	Pérdidas de los sistemas centrales
FPC-12	Software	Falla del motor de la base de datos
FPC-13	Software	Falla del sistema operativo
Sub-factor: Recursos Humanos		
FPC-17	Recursos Humanos	Ausencia imprevista del personal de soporte técnico
FPC-18	Recursos Humanos	Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático

5.9.2 Políticas

- El Plan de Contingencia Informático será actualizado con una periodicidad anual y entregado a la Dirección General de la Academia de la Magistratura para su validación y aprobación.
- Dicha actualización (a partir de la segunda versión en adelante) incluirá un capítulo donde se especificará las altas y bajas de los planes específicos de contingencia, así como aquellos que por uno u otro motivo fueron modificados respecto a su versión original.
- Se mantendrán 2 copias vigentes de respaldo y se repartirá una copia a todas las áreas involucradas en los planes.
- La implementación del Plan de Contingencia Informático está programado en el bimestre de su aprobación.
- Se realizará un Plan de Pruebas en forma anual.

En el literal "5. Desarrollo de las actividades, fases, estrategias, programas y/o políticas" del presente Plan; se ha considerado los responsables de la ejecución de los diferentes eventos susceptibles de contingencia. Para esto se ha desarrollado utilizando el formato Anexo A02: "Formato Registro Plan de Contingencia Informático" tanto para el Plan de Prevención, Plan de Ejecución, Plan de Recuperación y Plan de Pruebas.

5.9.3 Recursos

En el literal "5. Desarrollo de las actividades, fases, estrategias, programas y/o políticas" del presente Plan; se ha considerado los recursos a emplear durante la ejecución de los diferentes eventos susceptibles de contingencia. Para esto se ha desarrollado utilizando el formato Anexo A02: "Formato Registro Plan de Contingencia Informático" tanto para el Plan de Prevención, Plan de Ejecución, Plan de Recuperación y Plan de Pruebas.

5.9.4 Periodos y/o Plazos

En el numeral "5. Desarrollo de las actividades, fases, estrategias, programas y/o políticas" del presente Plan; se ha considerado los plazos a emplear durante la ejecución de los diferentes eventos susceptibles de contingencia. Para esto se ha desarrollado utilizando el formato Anexo A02: "Formato Registro Plan de Contingencia Informático" tanto para el Plan de Prevención, Plan de Ejecución, Plan de Recuperación y Plan de Pruebas.

5.9.5 Criterios empleados

Disminuir el impacto de los eventos de riesgo que se puedan presentar y que atenten contra la normal operatividad de la Academia de la Magistratura, llegándose a detallar los procedimientos a seguir durante la prevención, ejecución, recuperación y pruebas a desarrollarse.

VI.-RESPONSABILIDADES

Se ha considerado los responsables de la ejecución de los diferentes eventos susceptibles de contingencia. Para esto se ha desarrollado utilizando el formato Anexo A02: "Formato Registro Plan de Contingencia Informático" tanto para el Plan de Prevención, Plan de Ejecución, Plan de Recuperación y Plan de Pruebas.

Los cuadros siguientes muestran los funcionarios responsables de cada evento de contingencia identificado:

Cuadro N° 9 – Responsables de contingencias

Id	Descripción del Riesgo	Responsable(s) Titulares o sus Representantes	Teléfono
Subfactor: Siniestros			
FCP-01	Incendio	Director General	4280300 anx 171
		Secretaria Administrativa	4280300 anx 455
		Director Académico	4280300 anx 303
FCP-02	Sismo	Director General	4280300 anx 171
		Secretaria Administrativa	4280300 anx 455

Id	Descripción del Riesgo	Responsable(s) Titulares o sus Representantes	Teléfono
		Director Académico	4280300 anx 303
FCP-03	Inundación por desperfecto de los sistemas sanitarios	Secretaria Administrativa	4280300 anx 455
		Subdirector de Logística y Control Patrimonial	4280300 anx 303
FCP-04	Interrupción de la energía eléctrica	Secretaria Administrativa	4280300 anx 455
		Subdirector de Logística y Control Patrimonial	4280300 anx 462
FCP-05	Falta de suministro de agua	Secretaria Administrativa	4280300 anx 455
		Subdirector de Logística y Control Patrimonial	4280300 anx 462
FCP-06	Interrupción de los servicios de telefonía e Internet	Subdirector de Informática	4280300 anx 524
		Subdirector de Logística y Control Patrimonial	4280300 anx 462
Subfactor: Sistemas de Información			
FCP-07	Extravío de documentos	Director Académico	4280300 anx 303
		Secretaria Administrativa	4280300 anx 455
FCP-08	Sustracción o robo de información	Director Académico	4280300 anx 303
		Secretaria Administrativa	4280300 anx 455
FCP-09	Infección de equipos por virus	Subdirector de Informática	4280300 anx 524
FCP-10	Pérdidas de los sistemas centrales	Subdirector de Informática	4280300 anx 524
FCP-11	Pérdida del servicio de correo electrónico	Subdirector de Informática	4280300 anx 524
FCP-12	Falla del motor de la base de datos	Subdirector de Informática	4280300 anx 524
FCP-13	Falla del sistema operativo	Subdirector de Informática	4280300 anx 524
FCP-14	Fallas en la red de comunicación interna	Subdirector de Informática	4280300 anx 524
FCP-15	Falla de equipos personales	Subdirector de Informática	4280300 anx 524
FCP-16	Falla en equipos multimedia, impresoras, scanners y otros	Subdirector de Informática	4280300 anx 524
		Subdirector de Logística y Control Patrimonial	4280300 anx 462
Subfactor: Recursos Humanos			
FCP-17	Ausencia imprevista del personal de soporte técnico	Subdirector de Informática	4280300 anx 524
		Subdirector de Personal	4280300 anx 562
FCP-18	Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático	Director General	4280300 anx 171
		Director Académico	4280300 anx 303
		Secretaria Administrativa	4280300 anx 455
FCP-19	Falta de idoneidad del	Director Académico	4280300 anx 303

Id	Descripción del Riesgo	Responsable(s) Titulares o sus Representantes	Teléfono
	personal en la reserva de información de la base de datos	Secretaria Administrativa	4280300 anx 455
Subfactor: Seguridad Física			
FCP-20	Sustracción de equipos y software diversos	Secretaria Administrativa	4280300 anx 455
		Subdirector de Logística y Control Patrimonial	4280300 anx 462
FCP-21	Sabotaje	Secretaria Administrativa	4280300 anx 455
		Subdirector de Logística y Control Patrimonial	4280300 anx 462
FCP-22	Vandalismo	Secretaria Administrativa	4280300 anx 455
		Subdirector de Logística y Control Patrimonial	4280300 anx 462
FCP-23	Actos terroristas	Secretaria Administrativa	4280300 anx 455
		Subdirector de Logística y Control Patrimonial	4280300 anx 462

Los siguientes puntos de este capítulo, tratarán del desarrollo de los Planes de Contingencia Informático por cada Sub Factor identificado, utilizando el formato anexo A02.

VII. GLOSARIO DE TÉRMINOS.

- **Análisis de Riesgo:** Consiste en determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

- **Antispam**: Aplicación o herramienta informática que se encarga de detectar y eliminar el spam y los correos no deseados.
- **Backup**: También llamado copia de seguridad o de respaldo, es la copia total o parcial de información importante como respaldo frente a eventualidades.

- **Base de Datos**: Almacén de datos relacionados con diferentes modos de organización. Una base de datos representa algunos aspectos del mundo real, aquellos que le interesan al diseñador. Se diseña y almacena datos con un propósito específico, con la palabra "datos" se hace referencia a hechos conocidos que pueden registrarse, como ser números telefónicos, direcciones, nombres, etc.

- **Centro de Datos**: Espacio donde se concentran los recursos tecnológicos necesarios para el procesamiento de la información de una organización.

- **Firewall**: Es una herramienta de seguridad que controla el tráfico de entrada y salida de una red.

- **Hardware**: Es cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con la computadora, no sólo incluye elementos internos como el disco duro, DVD, sino que también hace referencia al cableado, circuitos, gabinete, etc. incluso hace referencia a elementos externos como la impresora, el mouse, el teclado, el monitor y demás periféricos.

- **Incidente**: Interrupción de las condiciones normales de operación en cualquier proceso informático.

- **Matriz de Riesgo**: Herramienta de control y de gestión que permite identificar los posibles riesgos que pueden afectar una institución, cuantificar las repercusiones de la materialización de los mismos y elaborar un plan de contingencia que permita establecer los controles y acciones que puede tomar una institución para llevar una gestión eficiente y eficaz de los riesgos.

- **Ofimática**: Conjunto de técnicas, aplicaciones y herramientas informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionados.

- **Plan de Contingencia**: Es un documento en el que se establecen un conjunto de estrategias para hacer frente a un posible incidente a través de un conjunto de procedimientos alternativos a la operatividad normal de cada institución.
- **Red de Datos**: Es la interconexión de computadoras para compartir información, recursos y servicios, la interconexión puede ser a través de un enlace físico (alambrado) o inalámbrico.

- **Routers**: Dispositivo hardware o software para interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. El router interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

- **Seguridad Física**: Hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático, para proteger el hardware de amenazas físicas. La seguridad física se complementa con la seguridad lógica.

- **Seguridad Informática**: disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

- **Seguridad Lógica**: hace referencia a la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la

información y el software dentro de un sistema informático.

- **Servidor**: Computadora central de un sistema de red que provee servicios a otras computadoras.
- **Siniestro**: Suceso que produce un daño o una pérdida material considerables.
- **Sistema de Información**: Conjunto de elementos relacionados entre sí, que se encarga de procesar manual y/o automáticamente datos, en función de determinados objetivos.
- **Sistema Operativo**: Software que controla la computadora y administra los servicios, sus funciones y la ejecución de otros programas a través de un conjunto de órdenes y programas.
- **Software**: Es todo programa o aplicación programado para realizar tareas específicas.
- **Switches**: Dispositivo de interconexión de redes informáticas que permite interconectar redes operando.
- **Tecnología de Información**: Son aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información, se encuentra asociada con el uso de computadoras y las tecnologías afines aplicadas a la toma de decisiones.
- **TIC:** Acrónimo del término Tecnologías de la Información y Comunicaciones (TIC)

VIII.-ANEXOS

Anexo A01: Formato de Ocurrencias de Eventos

FORMATO DE OCURRENCIA DE EVENTOS

CÓDIGO DEL EVENTO | FECHA DEL EVENTO

DESCRIPCIÓN DE LA OCURRENCIA

ANOTACIONES AL PLAN DE PREVENCIÓN

ANOTACIONES AL PLAN DE EJECUCIÓN

ANOTACIONES AL PLAN DE RECUPERACIÓN

OBSERVACIONES

CONTINGENCIA AUTORIZADA POR:

CONTINGENCIA DESACTIVADA POR:

Anexo A02: Formato Registro Plan de Contingencia Informático

Academia de la Magistratura	Evento:	Formato

1. PLAN DE PREVENCIÓN

a. Descripción

En este punto se describe el evento producido.

b. Objetivo

En esta sección se describirá el objetivo y funciones principales de un proceso, ejecutándose a condiciones "normales", es decir, sin que se presente un evento que genere la contingencia.

c. Criticidad

Señala cuan crítico es un proceso, así como el nivel de impacto del mismo dentro del servicio como se clasifica a continuación:

- Crítico: El proceso o actividad es altamente crítico, no puede detenerse nunca y no deber ser interrumpido.
- Importante: El proceso o actividad puede ser suspendido por un breve lapso de tiempo no mayor a las 2 horas.
- Menos Importante: El proceso o actividad puede ser suspendido por un lapso de tiempo no mayor a 24 horas.

d. Entorno

En esta sección se describirá la ubicación y los ambientes, equipos informáticos, equipos diversos (automáticos, mecánicos o manuales) donde se ejecuta el proceso en forma normal, así como las condiciones básicas para su operación.

e. Personal Encargado

Aquí se especificará el cargo(s) del personal del servicio, encargado de ejecutar el proceso en forma normal, así como sus roles dentro del mismo.

f. Condiciones de Prevención de Riesgo

En esta sección se debe describir detalladamente las acciones que se ejecutan durante el proceso normal y los puntos de control implementados, a efectos de prevenir que se presente el evento que genere la activación de un estado de contingencia.

2. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

Aquí se describen los eventos que deciden la activación de la contingencia. Asimismo, se especifica el lapso de tiempo en el cual se empieza a ejecutar el proceso de contingencia.

b. Procesos relacionados antes del Evento

Aquí se establecerán en forma secuencial todos los procesos o actividades que se tengan que ejecutar con anterioridad al ingreso al proceso de contingencia.

c. Personal que autoriza la Contingencia

- Se especificará los cargos del personal que autorizará el inicio del proceso de contingencia.

- Se especificará los cargos del personal que iniciará el proceso de contingencia.
- Se especificará el nivel de coordinación con funcionarios o responsables.

d. Descripción de las actividades después de activar la Contingencia
Se describirá en forma detallada y secuencial los pasos a realizar para poner en marcha el proceso de contingencia.

e. Duración
Aquí se especificará, de ser posible, el lapso de tiempo por el cual estará activada la contingencia, así como el evento que determine el término del mismo.

3. PLAN DE RECUPERACIÓN

a. Personal Encargado
Aquí se especificará el (los) nombre(s) y cargo(s) del personal del servicio, encargado del proceso de Recuperación (volver al proceso normal), así como sus roles dentro del mismo.

b. Descripción
Se describirá en forma detallada y secuencial los pasos a ejecutar para retornar al proceso normal, debiendo indicar lo necesario para asegurar la recuperación efectiva del mismo.

Deberá tenerse en cuenta aquellas actividades que permiten actualizar los procesos con la nueva información generada en la contingencia, en caso sea necesario.

c. Mecanismos de Comprobación
En esta sección se describirán todas aquellas actividades a realizar y que permitan asegurar que el proceso recuperado opere en condiciones normales y sin volver a presentar la falla que origino la ocurrencia del evento.

Mientras esta etapa se realiza, aún sigue activado el Plan de Contingencia.

d. Desactivación del Plan de Contingencia
Se especificará en forma secuencial y lógica cual es el procedimiento a seguir para desactivar el proceso de contingencia.

e. Proceso de Actualización
Se especificará en forma detallada y secuencial las actividades a ejecutar para actualizar el proceso normal recientemente recuperado.

Anexo A03: Control y Certificación de Pruebas de Contingencia

Código Nº (del plan)

Control y Certificación de Pruebas de Contingencia

Proceso en Prueba: (Nombre del proceso a probar/certificar)

Area responsable: (Area responsable del proceso probar/certificar)

Fecha : / / Hora Inicio : Hora Fin : (de prueba)

Información del Proceso

Metodologia y Alcance: (Que se va a hacer en la prueba y hasta donde va a abarcar la misma)

Condiciones de Ejecución:

Equipo : (Nombre del servidor / pc / maquina en proceso de prueba o certificación)

Aplicación/Software : Version:

Fecha de Backup : / /

De la Prueba / Certificación

Resultado de la Prueba: Satisfactorio: ☐ Satisfastorio con Observaciones: ☐ Deficiente: ☐

Observaciones: (en el caso de haber observaciones o que la prueba haya sido deficiente se iniciaran los motivos de dichas deficiencias, así como resultados de las pruebas en todos los casos)

Actualalización del Plan de Contingencia

Cambios o actualizaciones en el Plan de Contingencia (Se indicará los cambios que se realizarán en el Plan de Contingencia como consecuencia de las observaciones detectadas en las pruebas correspondientes)

Participantes Vº Bº y Aprobación

Participante	Cargo	Firma

ACADEMIA DE LA MAGISTRATURA - PRESIDENCIA - Consejo Directivo

ACADEMIA DE LA MAGISTRATURA - DIRECTOR GENERAL

ACADEMIA DE LA MAGISTRATURA - Oficina de Asesoría Jurídica

ACADEMIA DE LA MAGISTRATURA - Vº Bº OPP

ACADEMIA DE LA MAGISTRATURA - Vº Bº - Oficina de Informática

Anexo A04: Sub-factores entregados como parte del Plan de Instalación

Sistema Anti-Intrusión

Se recomienda la instalación de sensores de movimiento para la sala de servidores, cuya finalidad es detectar el ingreso de personas y sonar una alarma cuando una persona no autorizada ha ingresado a la sala de servidores.

Sistema de Circuito Cerrado

Se recomienda un sistema de circuito cerrado compuesto por cámaras de vigilancia por video con grabadora digital que permita almacenar registros durante 30 días.

Este sistema nos permitirá obtener registro e imagen del área donde se encuentre para detectar intrusiones, eventos no deseados, sabotajes, entre otros.

Sistema Anti-Inundación

Se recomienda la instalación de un sistema de drenaje y la instalación de sensores de aniego.

Sistema Contraincendio (Extintores)

La Institución en la sede central cuenta con un sistema de protección contra incendios, el cual se basa en extintores de polvo químico seco (PQS) y gas carbónico (Co2). Sin embargo, estos no se encuentran debidamente ubicados y señalizados.

Sistema Contraincendio (Agente limpio)

Se recomienda contar con gabinetes de lucha contra incendios con una manguera de 50 metros de largo dos pulgadas de diámetro, un hacha y un extintor PQS de 6 kilos adicional. Así también tener en todas las oficinas y pasadizos extintores de gas carbónico y de polvo químico seco de conformidad a la norma NFPA 10.

Luces de emergencia

Se recomienda la instalación de un sistema de luces de emergencia, las

cuales tiene una batería interna que se activan ante un corte de fluido eléctrico con una autonomía de por lo menos 02 horas deben estar distribuidas en todas las áreas y los pasadizos de cada piso.

Grupo Electrógeno

Se recomienda la adquisición de un GRUPO ELECTROGENO de una potencia necesaria para la demanda de usuarios y equipos de la Academia de la Magistratura.

Anexo A05: Procedimientos para el apagado y encendido de los Equipos del Centro de Datos de la Academia de la Magistratura

Secuencia de apagado de servidores

- Conectarse a la PC Remota GUEMO-PC o al IP 172.24.20.131
- Conectarse vía Cliente VMWare a los HOST (hipervisor) con las IP: 172.25.16.60, 172.25.16.61, 172.25.16.63, 172.25.16.64, 172.25.16.65, 172.25.16.66 y 172.25.16.54
- Apagar todos las Computadoras Virtuales de las SEDES, IP Server: 172.25.16.63, AulaVirtualDESAapp_SGA, WSXPSEDELLIB, WSXPSEDEAQP, WSXPSEDEACHI y WSXPSEDEACUS
- Apagar todos los servidores virtuales de Desarrollo y de Producción no elementales
  - IP Server: 172.25.16.61 – aulavirtualdesa – srvjupiter2_DesaAPP – Saturno – listas
  - IP Server: 172.25.16.63 – AulaVirtualDESAapp_SGA – Neptuno – Proteus – ATLAS
  - IP Server: 172.25.16.64 – SRVDESAORABD – srvconsolaepo – srvncomput
  - IP Server: 172.25.16.65 – srvapp
  - IP Server: 172.25.16.66 – amagvirtualAPP-HIST – amagvirtualbd-HIST – WSSARH_Soporte – WSSGATES – GanimedesII – Srvvisitas
  - IP Server: 172.25.16.52 – NeptunoQA – Apolo
  - IP Server: 172.25.16.53 – SaturnoQA
- Apagar Servidores de Producción:
  - IP Server: 172.25.16.60 – srvapp2 – Urano
  - IP Server: 172.25.16.51 – Pluton – WSUS – hermes
  - IP Server: 172.25.16.52 – Crono – Mercurio
  - IP Server: 172.25.16.53 – Prometeo – Tetis
- Apagar Servidores físicos:
  - SRVWEBAMAG
  - SRVFS1
  - VULCANO
- Apagar Controladores de Dominio y Vcenter
  - IP Server: 172.25.16.53 – Zeus
  - IP Server: 172.25.16.51 – Poseidon – Vcenter
- Apagar los HOST de las Máquinas Virtuales: 172.25.16.60, 172.25.16.61, 172.25.16.63, 172.25.16.64, 172.25.16.65, 172.25.16.66, 172.25.16.54
- Apagar el Enclosure de la granja de Servidores DELL, presionar botón de Encendido/Apagado una vez y visualizará en su pantalla LED el mensaje que está apagando
- Apagar Servidor NAS IP: 172.25.16.50
- Apagar Librería de Backup, presionando el botón de Encendido/Apagado una vez y visualizará en su pantalla LED el mensaje que está apagando

- Apagar Antispam desde el acceso web
- Apagar el Analizador desde el acceso web
- Apagar la Central Telefónica
- Apagar el Controlador de los AP Ruckus
- Apagar el Firewall desde el acceso Web
- Apagar los dos Switches Core
- Opcionalmente, pueden apagar los PDU de los Gabinetes

Secuencia de encendido de los servidores

Se recomienda un sistema de circuito cerrado compuesto por cámaras de vigilancia por video con grabadora digital que permita almacenar registros durante 30 días.

- Encender los Switches Core
- Encender el Firewall
- Encender Analizador, Antispam y Librería de Backup
- Encender el Servidor NAS DELL (esperar unos 5 minutos)
- Encender el Enclosure DELL m1000e
- Encender los Servidores DELL: Blade 1, Blade 2 y Blade 3
- Encender todos los demás servidores (los Servidores Virtuales de Desarrollo deben encenderse manualmente)
- Verificar la operatividad de los servicios:
  - Correo Electrónico
  - Página Web
  - Sistema Académico (SGAc)
  - SIGA
  - SGA-Tesorería
  - Servidores de Archivos (Pluton y Srvfs1)
  - Internet
  - Sistema de Generación de Código de Pagos
  - Catálogo de Biblioteca
  - Repositorio Virtual de Biblioteca
  - DHCP
  - Servidor de Backup

Anexo A06: Anexos de Responsables, Titulares o sus Representantes

Responsable(s) Titulares o sus Representantes	Teléfono
Director General	4280300 anx 171
Secretaria Administrativa	4280300 anx 455
Director Académico	4280300 anx 303
Subdirector de Logística y Control Patrimonial	4280300 anx 303
Subdirector de Informática	4280300 anx 524
Subdirector de Personal	4280300 anx 562