



PLAN DE CONTINGENCIA INFORMÁTICO
Y CONTINUIDAD DE LAS OPERACIONES DE
J & V RESGUARDO SAC

2015

J&V RESGUARDO SAC

CONTENIDO	PAGINA
1 OBJETIVOS ESPECIFICOS	3
2 ALCANCE	3
3 MARCO TEORICO	3
4 METODOLOGIA	4
4.1 Organización del Plan de Contingencia	5
4.2 Identificación y Priorización de Riesgos	7
4.3 Definición de Eventos susceptibles de Contingencia	9
4.4 Elaboración de los Planes de Contingencia	10
4.5 Definición y Ejecución de Plan de Pruebas	11
4.6 Implementación del Plan de Contingencia	12
5 DESARROLLO DE LAS FASES, ACTIVIDADES, ESTRATEGIAS, PROGRAMAS Y POLITICAS	13
5.1 Fases	13
6 RIESGOS IDENTIFICADOS (ACTIVIDADES, ESTRATÉGIAS, PROGRAMAS Y POLÍTICAS)	15
5.1 Riesgo de Incendio	15
5.2 Riesgo de Sismo	18
5.3 Riesgo de Apagón o Corte de Suministro Eléctrico	21
5.4 Riesgo de Ataques de Virus Informáticos	24
5.5 Riesgo de Inoperancia de los Sistemas Operativos	27
5.6 Riesgo de Pérdida de Información–Backups	29
5.7 Riesgo de Mal funcionamiento de Disco Duro de Equipos Servidores	32
5.8 Riesgo de Ausencia de Personal de Soporte	35
5.9 Riesgo de Ausencia de Jefes de Area	37
Anexo N° 1 - COPIAS DE RESPALDO	40
Anexo N° 2 - EVIDENCIA DE PUESTA A PRUEBA Y FUNCIONAMIENTO	42
Anexo N° 3 - RECOMENDACIONES PARA EL USO DE CORREOS ELECTRONICOS	45

1. OBJETIVOS GENERALES Y ESPECÍFICOS

Generales

- Garantizar la continuidad de las actividades de J&V RESGUARDO SAC, ante eventos que podrían alterar el normal funcionamiento de la Tecnología de la Información y comunicaciones, a fin de minimizar el riesgo no previsible, críticos o de emergencia, y responder de forma inmediata hacia la recuperación de las actividades normales.

Específicos

- Contar con documentación práctica y actualizada que garantice a J&V RESGUARDO SAC 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 del J&V RESGUARDO SAC.

2. ALCANCE

La Implementación del Plan de Contingencia informático, incluye los elementos referidos a los sistemas de información, equipos, infraestructura, personal, servicios y otros, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la institución.

3. MARCO TEORICO

El Plan de Contingencia informático es un documento que reúne conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones de J&V RESGUARDO SAC, cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización.

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 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 será entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático en J&V RESGUARDO SAC.

3.1 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 porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

3.2 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 alternativo 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.

3.3 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.

3.4 Plan de Pruebas

El Plan de Pruebas, será presentado a la Dirección Ejecutiva de J&V RESGUARDO SAC para su aprobación previa a su implementación. El resultado de las pruebas efectuadas será presentado igualmente para su conformidad.

Las pruebas relacionadas a este plan, se ejecutaría semestralmente, mes de Junio y Diciembre con el fin de evaluar la preparación de la organización ante la ocurrencia de un siniestro y realizar los ajustes necesarios.

4. METODOLOGÍA

La presente metodología es el resultado de la experiencia práctica de J&V RESGUARDO SAC en la implementación de planes de contingencia, mitigación de riesgos y seguridad, también en base a experiencias en 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 real.

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

- ✓ Fase 1: Organización
- ✓ Fase 2: Identificación y priorización de riesgos
- ✓ Fase 3: Definición de eventos susceptibles de contingencia

- ✓ Fase 4: Elaboración del Plan de Contingencia
- ✓ Fase 5: Definición y Ejecución del Plan de Pruebas
- ✓ Fase 6: Implementación del Plan de Contingencia

Fases de la metodología propuesta:

4.1 Organización del Plan de Contingencia

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 deba hacerse 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:

Organización Administrativa del plan de Contingencia

- I. Director Ejecutivo de J&V RESGUARDO SAC
- II. Gerente de Administración del J&V RESGUARDO SAC
- III. Jefe de la Unidad de Sistemas e Informática de J&V RESGUARDO SAC
- IV. Otros que el Director Ejecutivo considere pertinente incluir.

A continuación se describe las funciones y roles de la Organización Administrativa del Plan de Contingencia:

La Coordinación ejecutora del Plan de Contingencia será responsabilidad del Director Ejecutivo, 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 Direcciones de Líneas de J&V RESGUARDO SAC.

Funciones y Roles de la Coordinación Ejecutora del Plan:

- Mantener permanentemente actualizado el Plan de Contingencia.
- Responsable de la ejecución del plan de contingencia, cuando se presenten los eventos que lo activan.
- Evaluar el impacto de las contingencias que se presenten.
- Elaborar los informes referidos al Plan de contingencias
- Proponer incorporaciones de eventos al plan de contingencia al Comité de Contingencia.
- Proponer la capacitación al personal nuevo 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.
- Proponer reuniones periódicas sobre el plan de contingencia.

4.1.2 Comité de Contingencia

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:

- Gerente General
- Gerente de Administración
- Director de área de Informática y Sistemas de Información

El Director Ejecutivo designará a otros integrantes que considere pertinente a participar en el comité.

Funciones y Roles del Comité del Plan de Contingencia:

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

4.1.3 Contraloría del Plan de Contingencia

La Oficina de Auditoría Interna 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:

- 1) Verificar que el plan de contingencia se encuentre actualizado.
- 2) Revisar y verificar que el documento de plan de contingencia se enmarque dentro del alcance establecido.
- 3) Velar por suministrar los recursos necesarios para la viabilidad del plan de Contingencia y Seguridad.
- 4) Corroborar que el plan de contingencia se cumpla correctamente.

- 5) Presentar los informes del Plan de Contingencia al Comité de Contingencia de J&V RESGUARDO SAC.
- 6) Certificar que todos los recursos descritos en el Plan de Contingencia (materiales, humanos, externos, etc.) sean viables y se encuentren disponibles para su uso cuando un evento de contingencia lo requiera.
- 7) Auditar los procesos que forman parte del Plan de Contingencia, corroborando que se cumpla correctamente. Participar y visar las pruebas de validación del Plan de Contingencia. Informar al Comité respecto a cualquier evento o anomalía encontrada que ponga en riesgo la ejecución de todo o parte del plan.
- 8) Proponer y recomendar actividades o procesos de mejora que permitan minimizar los riesgos de operación.

4.2 Identificación y Priorización de Riesgos

Denominamos INCIDENCIA al hecho que se pueda presentar en cualquier momento, bajo una probabilidad de ocurrencia.

Riesgo: Es un suceso incierto que puede llegar a presentarse en un futuro dependiendo de variables externas o internas. Es entonces la cuantificación de una amenaza.

4.2.1 Análisis del Riesgo

El análisis del riesgo se basa en la información generada en la fase de identificación, que se convierte ahora en información para la toma de decisiones. En la fase del análisis, se consideran tres elementos que permiten aproximar un valor objetivo de riesgo de la lista de riesgos principales: la probabilidad, impacto y exposición del riesgo. Estos elementos permitirán al equipo coordinador categorizar los riesgos, lo que a su vez le permite dedicar más tiempo y principalmente a la administración de los riesgos más importantes.

4.2.2 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 al 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%.

4.2.3 Impacto del Riesgo

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

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

Para nuestro caso, clasificaremos el impacto con una escala del 1 al 4.

4.2.4 Exposición al 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.

4.2.5 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 J&V RESGUARDO SAC, o cuya ocurrencia no puede predecirse con antelación. Así tenemos que los eventos pueden ser:

Eventos Controlables, si al identificarlos podemos tomar acciones que eviten su ocurrencia o minimicen el impacto en el servicio brindado.

Eventos No Controlables, cuando su ocurrencia es impredecible y únicamente podemos tomar acciones que permitan minimizar el impacto en el servicio.

Esta identificación se hará en la matriz de riesgo explicada a continuación.

4.2.6 Definición de la Matriz de Riesgo

La ocurrencia de un evento tiene una implicancia sobre las actividades operativas del servicio, en tal sentido, resulta vital conocer el impacto del evento cuando este se presenta, por lo que resulta necesario cuantificar la misma, a efectos de ser muy 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 cuadro N° 1.

Cuadro N °1: Cuadro de Impactos

Poco Impacto	Pérdida de Información y/o equipamiento no Sensitivo 1
Moderado Impacto	Pérdida de información sensible 2
Alto Impacto	Pérdida de información sensible, retraso o interrupción 3
Gran Impacto	Información crítica, daño serio, patrimonial 4

Cuadro N °2: Cuadro de Probabilidad de Ocurrencia

Frecuente	: Incidentes repetidos	4
Probable	: Incidentes aislados	3
Ocasional	: Sucede alguna vez	2
Remoto	: Improbable que suceda	1

Asimismo, la probabilidad de ocurrencia de un evento resulta de gran importancia para determinar que tan posible es que dicho evento se presente en la realidad. La determinación de esta probabilidad se obtendrá de la estadística recogida de los eventos que se hayan presentado a lo largo de la administración del servicio por otros proveedores, así como la información obtenida de otros planes de contingencia para servicios similares.

Exposición = Impacto X Probabilidad

Cuadro N °3: Exposición al Riesgo

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:

Probabilidad de Ocurrencia vs. Impacto

- Todo evento cuya calificación sea de “Gran Impacto: 4”, será considerado obligatoriamente dentro del Plan de Contingencia.
- Todo evento cuya exposición al riesgo sea mayor o igual a 0.15 será también considerado en el Plan de Contingencia (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 entrar en contingencia, indicando su ponderación y categorización (controlable/ no controlable) para la elaboración del Plan de Contingencia.

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

4.3 Definición de eventos susceptibles de contingencia

El Plan de Contingencia 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:

- I. Hardware
 - Servidores
 - Estaciones de trabajo(Laptops y PC's)
 - Impresoras, fotocopadoras, scanner
 - Lectora de Códigos de Barra
 - Equipos de radiofrecuencia
 - Equipos multimedia
- II. Comunicaciones
 - Equipos de comunicaciones switch y conectores RJ-45
 - Equipo de comunicaciones Router y LAN.
 - Equipo de Telefonía fija

- Enlaces de cobre y fibra óptica.
- Cableado de Red de Datos.
- III. Software
 - Software de Base de Datos (MS SQL Server)
 - Aplicativos utilizados por el J&V Resguardo SAC.
 - Software Base (Sistemas operativos y Ofimática).
 - Antivirus para protección de servidores y estaciones de trabajo.
- IV. Información sobre Sistemas Informáticos
 - Base de datos utilizados por los Aplicativos.
 - Respaldo de información generada con Software Base y de Ofimática.
 - Respaldo de las Aplicaciones utilizadas por J&V Resguardo SAC.
 - Respaldo de Base de Datos.
 - Respaldo de información y configuración de los Servidores.
- V. Equipos diversos
 - Grupo Electrógeno
 - UPS
 - Aire Acondicionado
- VI. Infraestructura Física
 - Oficinas (Sede Central y local de Breña).
- VII. Operativos
 - Logística operativa (suministros Informáticos).
- VIII. Servicios Públicos
 - Suministro de Energía Eléctrica.
 - Servicio de Telefonía Fija analógico/digital y móvil.
- IX. Recursos Humanos
 - Disponibilidad de personal de dirección.
 - Disponibilidad de personal operativo.

4.4 Elaboración de los Planes de Contingencia

Una de las fases importantes del Plan de Contingencia es la documentación y revisión de la información que se plasmará en una guía práctica y de claro entendimiento por 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, 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:

4.4.1 Formato de Registro del Plan de Contingencia

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 "J&V Resguardo SAC".

Código del Formato: FPC – XX

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.

4.5 Definición y ejecución del plan de pruebas

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 J&V RESGUARDO SAC; es que se hace necesario definir de manera específica todas las acciones necesarias para asegurar que, en caso real de contingencia y 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 se basa en una validación y certificación anticipada del mismo, en cada uno de sus procesos.

4.5.1 Alcance y Objetivos

Dado que la mayor parte de los planes de contingencia 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 respecto a una posible interrupción de los procesos identificados como críticos para el servicio de J&V RESGUARDO SAC.
- 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 direcciones y jefaturas de J&V RESGUARDO SAC, 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:

4.5.2 Validación y Registro de Pruebas

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

1. OBJETIVOS DE LA PRUEBA DEL PLAN DE CONTINGENCIA

Definición Objetivos

2. ALCANCES

Áreas Afectadas (relación) Personal involucrado (relación)

3. DESCRIPCIÓN DE LA PRUEBA A EFECTUARSE

Evaluación de una situación de Emergencia

Medios disponibles para operar

Fechas y horas

4. RESULTADOS ESPERADOS DE LAS PRUEBAS

Relación de posibles acciones y pruebas, así como el detalle de la información que deberá ser ingresada en cada campo:

4.6 Implementación del Plan de Contingencia

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

5. DESARROLLO DE LAS FASES

5.1 Fases

Como parte del presente capítulo, la Unidad 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.
- Elaboración del Plan de Contingencia.

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

INFRAESTRUCTURA

- 1 Incendio
- 2 Sismo
- 3 Inundación por desperfecto de los servicios sanitarios

SERVICIOS PÚBLICOS

- 4 Interrupción de energía eléctrica
- 5 Interrupción de servicios de telefonía

EQUIPO

- 6 Falla de grupo electrógeno

INFORMACIÓN

- 7 Extravío de documentos
- 8 Sustracción o robo de información

SOFTWARE

- 9 Infección de equipos por virus
- 10 Perdidas de los sistemas centrales
- 11 Perdida del servicio de correo
- 12 Falla del Motor de la base de datos
- 13 Falla del sistema operativo

COMUNICACIONES

- 14 Fallas en la red de comunicaciones interna

HARDWARE

- 15 Fallas de equipos personales

RECURSO OPERATIVOS Y LOGÍSTICOS

16 Falla de equipos multimedia, impresoras, scanner y otros

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.

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

1 Incendio

3 Inundación por desperfecto de los servicios sanitarios

9 Falla del grupo Electrónico

10 Extravió de documentos

11 Sustracción o robo de información

12 Infección de equipos virus

13 Perdidas de los sistemas centrales

14 Perdida del servicio de correo

15 Falla del motor de la base de datos

16 Falla del sistema operativo

17 Fallas en la red de comunicaciones internas

18 Fallas de equipos personales

19 Falla de equipos multimedia, impresoras, scanner y otros

20 Ausencia imprevista del personal de soporte técnico

21 Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático

23 Sustracción de equipos y software diversos

Cuadro N °6: Eventos no Controlables

2 Sismo

4 Inundación por oleajes anómalos

5 Tsunamis

6 Interrupción de energía eléctrica

7 Falta de suministro de agua

8 Interrupción de servicios de telefonía

22 Falta de idoneidad del personal en la reserva de información de la Base de Datos.

24 Sabotaje

25 Vandalismo

26 Actos terroristas

6. RIESGOS IDENTIFICADOS (ACTIVIDADES, ESTRATÉGIAS, PROGRAMAS Y POLÍTICAS)

6.1 RIESGO DE INCENDIO

1. PLAN DE PREVENCIÓN

a. Descripción del evento

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 J&V Resguardo SAC, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Infraestructura

- “Centro de Datos” de la Sede central de J&V RESGUARDO SAC
- “Centro de Datos” del Local de la Av. Juan del Mar y Bernedo.

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 J&V RESGUARDO SAC sin exponer la seguridad de las personas.

c. Criticidad

J&V RESGUARDO SAC 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 Alta Dirección, Direcciones de Líneas y Unidades Operativas de la Sede Central de San Isidro y el Local de Breña.

e. Personal Encargado El Director y/o Jefe de área, es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención 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 J&V RESGUARDO SAC 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 J&V RESGUARDO SAC.:

- 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 J&V RESGUARDO SAC.
- Tener número de teléfono del personal responsable en seguridad Informática y contingencia de J&V RESGUARDO SAC.
- Conocer el número de emergencia de los bomberos.

c. Personal que autoriza la contingencia.

El Director de Administración o sus Representantes 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 J&V RESGUARDO SAC.
- 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 Alta Dirección de J&V RESGUARDO SAC en caso se requiera la habilitación de ambientes provisionales alternos para restablecer la función de los ambientes afectado.

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 la Dirección Administrativa y el equipo del área afectada, cuyo rol principal es asegurar el normal desarrollo de las operaciones de J&V RESGUARDO SAC.

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 Jefe y/o Director del área afectada presentará un informe a la Coordinación Ejecutora del Plan explicando qué parte de las actividades u operaciones ha sido afectada y cuáles son las acciones tomadas.

d. Mecanismos de Recuperación

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

e. Desactivación del Plan de Contingencia

Director de Administración o sus representantes 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 Director de Administración y/o Director Científico luego de lo cual se determinará las acciones a tomar.

6.2 RIESGO DE SISMO

1. PLAN DE PREVENCIÓN

a. Descripción del evento

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 J&V RESGUARDO SAC, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Infraestructura

Sede central de J&V RESGUARDO SAC

Oficinas de J&V RESGUARDO SAC en el local de la Av. Juan del Mar y Bernero.

Recursos Humanos

Personal

b. Objetivo

Establecer las acciones que se tomarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones de J&V RESGUARDO SAC evitando exponer la seguridad de las personas.

c. Criticidad

J&V RESGUARDO SAC 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 Alta Dirección, Direcciones de Líneas y Unidades Operativas de la Sede Central y el Local de la Av. Juan del Mar y Bernero

e. Personal Encargado

El Director y/o Jefe de Área, es quien debe de dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan

f. Condiciones de Prevención de Riesgo

- Contar con un plan de evacuación de las instalaciones de J&V RESGUARDO SAC, el mismo que debe ser de conocimiento de todo el personal que labora.
- Realizar simulacros de evacuación con la participación de todo el personal de la Sede Central y del local de la Av. Juan del Mar y Bernero de J&V RESGUARDO SAC.
- 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

- Sismo.

El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b. Procesos Relacionados antes del evento.

- Tener la lista de los empleados por Direcciones y/o Oficinas 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 Ejecutivo y/o Director científico y/o Director de Administración 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 de administración 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 ascensores.
- Verificar que todo el personal de J&V RESGUARDO SAC que labora en el área se encuentren bien.
- Brindar los primeros auxilios al personal afectado si fuese necesario. (ver procedimiento FPC-24 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 del J&V Resguardo SAC, para las acciones que deban ser efectuadas por ellos.
- La Coordinación Ejecutora del Plan de Contingencias deberá coordinar con la Alta Dirección de J&V RESGUARDO SAC 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 J&V RESGUARDO SAC serán calmados y demorará 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 Jefatura y el equipo 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

El Director y/o Jefe del área afectada presentará 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 científico y/o Director de Administración 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

El proceso de actualización será en base al informe presentado por El Director científico y/o Director de Administración quien determinará las acciones a tomar.

6.3 RIESGO DE APAGON O CORTE DE SUMINISTRO ELECTRICO

1. PLAN DE PREVENCIÓN

a. Descripción del evento

Falla general del suministro de energía eléctrica.

Este evento incluye los siguientes elementos mínimos identificados por J&V RESGUARDO SAC, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Servicios Públicos

- 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

Este evento se considera como CRITICO.

d. Entorno

Se puede producir durante la operatividad, afectando el fluido eléctrico de las instalaciones de J&V RESGUARDO SAC.

e. Personal Encargado

El Director de Administración y/o Jefe de Informática de J&V RESGUARDO SAC son responsables de realizar las coordinaciones para restablecer el suministro de energía eléctrica.

f. Condiciones de Prevención de Riesgo

- Durante las operaciones diarias del servicio u operaciones de J&V RESGUARDO SAC 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 J&V RESGUARDO SAC (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

Corte de suministro de energía eléctrica en los ambientes de J&V RESGUARDO SAC.

b. Procesos Relacionados Antes del evento.

Cualquier actividad de servicio dentro de las instalaciones de J&V RESGUARDO SAC.

c. Personal que autoriza la contingencia

El Director de administración y/o Jefe de Informática pueden activar la contingencia.

d. Descripción de las procedimientos después de activar la contingencia

- Informar al Director de Administración y/o Jefe de Informática del problema presentado.
- Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas de J&V RESGUARDO SAC 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, desarrollo y correo hasta que regrese el fluido eléctrico.

e. Duración

El tiempo máximo de duración de la contingencia dependerá del proveedor externo de energía eléctrica.

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El personal encargado del Plan de Recuperación son el Jefe de Informática y/o el Director de administración, quienes se encargarán 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

El Director de Administración y/o Jefe 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 Director de Administración y/o Jefe de Informática desactivará 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.

5.2.2 Subfactor: Contingencias relacionadas a los sistemas de información

A continuación se muestra los puntos a desarrollarse para el presente subfactor:

5.2.2.1 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.

5.2.2.2 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 J&V RESGUARDO SAC.

Resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a los Sistemas de Información que se describirán en detalle más adelante

6.4 RIESGO DE ATAQUES DE VIRUS INFORMATICOS

1. PLAN DE PREVENCIÓN

a. Descripción del evento

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 J&V RESGUARDO SAC, 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 por J&V RESGUARDO SAC

b. Objetivo

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

c. Criticidad

El nivel de éste evento es considerado CRITICO.

d. Entorno

Las estaciones de trabajo PC's, se encuentran instaladas en la Sede Central y el local de la Av. Argentina de J&V RESGUARDO SAC.

e. Personal Encargado

Jefe de Informática de J&V RESGUARDO SAC es el responsable en la supervisión del correcto funcionamiento de las estaciones 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 disketeras, quemadores de CD, Dispositivos USB, etc. en 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

- Jefe de Informática de J&V RESGUARDO SAC
- Técnico de Soporte de Sistemas de J&V RESGUARDO SAC

d. Descripción de las Actividades después de activar la contingencia

- Desconectar la estación infectada de la red de J&V RESGUARDO SAC
- 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 :
 - Formatear el equipo
 - Personalizar la estación para el usuario
- Conectar la estación a la red de J&V RESGUARDO SAC.
- Efectuar las pruebas necesarias con el usuario.
- Solicitar conformidad del servicio.

e. Duración

La duración del evento no deberá ser mayor a DOS 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 Técnico de Soporte de Sistemas de J&V RESGUARDO SAC, luego de restaurar el correcto funcionamiento de la estación de trabajo (PC), coordinará con el usuario responsable y/o Jefe del área para reanudar las labores de trabajo con el equipo.

b. Descripción

Se informará al Jefe de Informática de J&V RESGUARDO SAC 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 J&V RESGUARDO SAC.

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

c. Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá a la Coordinación Ejecutora del Plan para su revisión.

d. Desactivación del Plan de Contingencia

Con el aviso del Técnico de Soporte de Sistemas de J&V RESGUARDO SAC, se desactivará el presente Plan.

e. Proceso de Actualización

El problema de infección presentado en la estación de trabajo, no debe detener la Aplicación de actualización de datos en las Aplicaciones del J&V RESGUARDO SAC.

6.5 RIESGO DE INOPERANCIA DEL SISTEMA OPERATIVO

1. PLAN DE PREVENCIÓN

a. Descripción Del Evento

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 el J&V RESGUARDO SAC, que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Software

- Software base
- Software base de datos
- Aplicativos utilizados por el J&V RESGUARDO SAC

Hardware

- Servidores

Información

- Respaldo de base de datos
- Respaldo de las aplicaciones utilizadas por J&V RESGUARDO SAC
- Respaldo De Software Base

b. Objetivo

Mantener operativo los servidores de producción donde se ejecutan las aplicaciones de J&V RESGUARDO SAC.

c. Criticidad

El nivel de este evento es considerado crítico.

d. Entorno

Los servidores de aplicaciones están situados en el centro de datos del J&V RESGUARDO SAC.

e. Personal Encargado

Jefe de Informática de J&V RESGUARDO SAC es el responsable de asegurar el correcto funcionamiento de los servidores durante los servicios. Se coordinarán las acciones necesarias para restablecer el servicio en caso se produzca el evento.

El Jefe de Informática de J&V RESGUARDO SAC 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 en el J&V RESGUARDO SAC.

f. Condiciones de Prevención de Riesgo

Tomar las siguientes acciones preventivas que debe implementar la Unidad de Informática de J&V RESGUARDO SAC 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

- Anexo N°1 - Copias de Respaldo.
- Contar con backups de las aplicaciones y de las bases de datos Anexo N° 1
- Copias de Respaldo.
- 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 J&V RESGUARDO SAC.

2. PLAN DE EJECUCIÓN

a. Eventos que Activan La Contingencia

- Falla de Acceso a Aplicaciones.
- Mensaje Pérdida de Conexión a La BD.

b. Procesos Relacionados Antes Del Evento.

Cualquier proceso relacionado con el uso de las aplicaciones en los servidores de J&V RESGUARDO SAC.

c. Personal que autoriza la contingencia

- Jefe de Informática de J&V RESGUARDO SAC.

d. Descripción de Las Actividades Después de Activar La Contingencia

Remitirse a los Procedimientos de recuperación de sistemas de J&V RESGUARDO SAC.

e. Duración

La duración del evento estará en función de la complejidad del problema encontrado.

Esperar la indicación del jefe de Informática de J&V RESGUARDO SAC para reanudar la operación normal con las aplicaciones.

3. PLAN DE RECUPERACIÓN

a. Personal encargado

El Jefe de Informática de J&V RESGUARDO SAC, luego de verificar la corrección del problema de acceso a los servidores, coordinará con los Directores y/o jefes de áreas para la reanudación de los trabajos operativos con las aplicaciones de J&V RESGUARDO SAC.

b. Descripción

Se informará a la Alta Dirección la causa que motivó la paralización del servicio.

En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

c. Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá a la coordinación ejecutora del plan para su revisión.

d. Desactivación del plan de contingencia

Con el aviso del jefe de Informática de J&V RESGUARDO SAC, se desactivará el presente plan.

e. Proceso de actualización

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

6.6 RIESGO DE PERDIDA DE INFORMACION - BACKUPS

1. PLAN DE PREVENCIÓN

a. Descripción del evento

Ausencia del servicio principal para almacenar, procesar y proteger los datos, para acceso controlado y procesamiento de transacciones rápidos para cumplir con los requisitos de las aplicaciones consumidoras de datos más exigentes de J&V RESGUARDO SAC.

Este evento incluye los siguientes elementos mínimos identificados por J&V RESGUARDO SAC, que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Software

- Aplicativos utilizados por J&V RESGUARDO SAC

Hardware

- Servidores

Información

- Respaldo de Base de Datos
- Respaldo del Software Base

b. Objetivo

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

c. Criticidad

Este evento se considera como CRITICO.

d. Entorno

Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte a las operaciones de J&V RESGUARDO SAC.

e. Personal Encargado

El Jefe de Informática de J&V RESGUARDO SAC encargará al responsable de la base de datos (DBA) las acciones correspondientes.

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 Anexo N° 1 Copias de Respaldo.
- 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.

Respaldo disponible para el uso de las aplicaciones en los servidores del J&V RESGUARDO SAC.

c. Personal que autoriza la contingencia

El Jefe de Informática de J&V RESGUARDO SAC es quien considera activar la contingencia.

d. Descripción de los procedimientos 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 por J&V RESGUARDO SAC.- De producirse una falla al momento de la operación de estos sistemas, el Jefe de Informática asumirá, delegará o coordinará los trabajos de corrección o modificación.

e. Duración

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

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El personal encargado del Plan de Recuperación para las operaciones de J&V RESGUARDO SAC es el Jefe de Informática.

b. Descripción

Se informará al Jefe de Informática de J&V RESGUARDO SAC 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 de J&V RESGUARDO SAC.

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

c. Mecanismos de Comprobación

El Jefe de Informática de J&V RESGUARDO SAC presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del Servicio ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

d. Desactivación del Plan de Contingencia

El Jefe de Informática de J&V RESGUARDO SAC desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con la BD de las aplicaciones.

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 preventivas necesarias que deberán incluirse en el presente plan.

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

6.7 RIESGO DE MAL FUNCIONAMIENTO DE DISCO DURO DE EQUIPOS SERVIDORES

1. PLAN DE PREVENCIÓN

a. Descripción del evento

Falla en el control de computadoras, en el interfaz hombre-máquina, recursos hardware y software de J&V RESGUARDO SAC.

Este evento incluye los siguientes elementos mínimos identificados por J&V RESGUARDO SAC, que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Software

- Aplicativos utilizados por el J&V RESGUARDO SAC

Hardware

- Servidores

Información

- Respaldo de Base de Datos
- Respaldo de las Aplicaciones utilizadas por J&V RESGUARDO SAC

b. Objetivo

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

c. Criticidad

Este evento se considera 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 Jefe de Informática de J&V RESGUARDO SAC 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
- Copias de Respaldo.
- Contar con servicios de soporte vigentes para los principales causantes del evento
- J&V RESGUARDO SAC debe asegurarse de mantener acuerdos con sus 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 Jefe de Informática de J&V RESGUARDO SAC es quién considera 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.
- 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.)
- Remover el virus del sistema.
- Probar el sistema.
- En caso no solucionarse el problema :
 - 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.
- 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 directores y/o jefes de áreas 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 CINCO horas.

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El personal encargado del Plan de Recuperación para las operaciones del J&V RESGUARDO SAC es el Jefe de Informática.

b. Descripción

Se informará al Jefe de Informática de J&V RESGUARDO SAC 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 de J&V RESGUARDO SAC.

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

c. Mecanismos de Comprobación

El Jefe de Informática de J&V RESGUARDO SAC presentará un informe a la Coordinación Ejecutora del Plan, explicando que parte del Servicio ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

d. Desactivación del Plan de Contingencia

El Jefe de Informática de J&V RESGUARDO SAC desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

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 jefes de áreas, para iniciar las labores de actualización de los sistemas.

5.2.3. Subfactor: Contingencias relacionadas a los Recursos Humanos

A continuación se muestra los puntos a desarrollarse para el presente subfactor:

5.2.3.1 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 J&V RESGUARDO SAC.

5.2.3.2 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.

6.8 RIESGO DE AUSENCIA DE PERSONAL DE SOPORTE

1. PLAN DE PREVENCIÓN

a. Descripción del evento

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 J&V RESGUARDO SAC, 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 J&V RESGUARDO SAC.

c. Criticidad

J&V RESGUARDO SAC 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 Alta Dirección, Direcciones de Líneas y Unidades Operativas de la Sede Central y el Local de la Av. Argentina

e. Personal Encargado

El Director Ejecutivo y/o Jefe 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 Jefe de Informática, se asegurará en capacitar a los analistas de sistemas del área 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 jefe de informática se asegurara en tener como mínimo a dos profesionales técnicos en el área de soporte técnico y un asistente.
- 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 Jefe de Informática, para que tome las acciones preventivas correspondientes.

2. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

Reporte de inasistencia del personal de Soporte Técnico: administrador de la Red, administrador de la Base de Datos, helpdesk, etc.

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

c. Personal que autoriza la contingencia

El Jefe de Informática.

d. Descripción de las Actividades después de activar la contingencia

- Confirmado la inasistencia del personal de soporte Técnico, el Jefe 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 Jefe de Informática solicitará al Director Ejecutivo de J&V RESGUARDO SAC, 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.

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El personal encargado del Plan de Recuperación es el Jefe 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 Jefe 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 Jefe 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 Jefe de Informática y las causas identificadas en el Servicio informático se determinará las acciones a tomar.

6.9 RIESGO DE AUSENCIA DE JEFES DE AREA

1. PLAN DE PREVENCIÓN

a. Descripción del evento

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

Este evento incluye los siguientes elementos mínimos identificados por J&V RESGUARDO SAC, 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 jefaturas de J&V RESGUARDO SAC, evitando el quiebre en la cadena de mandos, a través de reemplazos de personal ejecutivos.

c. Criticidad

J&V RESGUARDO SAC 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 Alta Dirección, Direcciones de Líneas y Unidades Operativas de la Sede Central y el Local de la Av. argentina

e. Personal Encargado

El Director Ejecutivo y/o Director científico, es quién debe 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 a personal Direccional y/o Jefatural, por lo que se considera lo siguiente:
- Como primera prevención, la Alta Dirección asegurará en capacitar a un empleado con más de 5 años de experiencia en la Institución que cumpla el perfil, conocimiento y capacidad para reemplazar ante el evento.
- Incluir como parte de las funciones del personal en comunicar anticipadamente la inasistencia a su centro de labores, siempre y cuando se trate de ocasiones premeditadas.

2. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

Reporte de inasistencia de algún Director y/o jefe de área.

El proceso de contingencia se activa durante las DOS HORAS iniciales del día.

b. Procesos Relacionados Antes del evento.

Se podría dar por:

- Falta de decisión del Jefe Director y/o Jefe de Área 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 científico y/o director Administrativo.

d. Descripción de las Actividades después de activar la contingencia

- Confirmado la inasistencia del Director Ejecutivo, se coordinará el reemplazo con el Director Científico y/o Directores de línea de J&V RESGUARDO SAC
- Confirmado la inasistencia del jefe de área, el Director científico y/o director de área coordinará con los Jefes de la Dirección el reemplazo correspondiente

e. Duración

Máximo tres 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 jefe de área o Nuevo Director y/o Jefe de área 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 jefe de área o Nuevo director y/o jefe de área, cuyo rol principal es asegurar el normal funcionamiento de las operaciones de J&V RESGUARDO SAC.

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 jefe 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 científico y/o director de administración 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 Jefe de Área y las causas identificadas en la operatividad, se determinará las acciones a tomar.

5.2.3 Subfactor: Contingencias relacionadas a Seguridad Física

A continuación se muestra los puntos a desarrollarse para el presente subfactor:

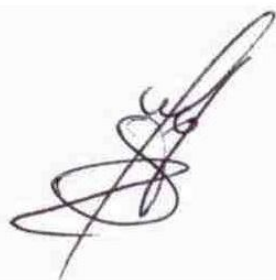
5.2.4.1 Objetivo

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.

5.2.4.2 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.



Mirtko F. González Riva
Jefatura de Sistemas e Informática



Jose Iñigo La Riva
Gerente de Administración y Finanzas

Anexo N° 1 - COPIAS DE RESPALDO

Todo nuevo desarrollo de aplicaciones que el J&V RESGUARDO SAC realice, considerará un proceso de respaldo de la información que incluye programas fuentes, ejecutables, objetos, base de datos, documentación, configuraciones de los equipos y software entre otros.

La ejecución de los respaldos será responsabilidad del área de Soporte Técnico de la Unidad de Informática, estará basada en una rutina de copias de seguridad tipo Normal o Básico y la frecuencia y contenido de estas copias de respaldo se hará tal como se indica en el cuadro siguiente:

CUADRO 06: Rutinas de Respaldo

En forma trimestral se registrará la realización de los backup de las PC's en el formato de Control de Backup (SGI-F-22-02-01).

Si en un caso no fueron elaborados los backups, el Jefe de Sistemas () previa coordinación con el usuario, forzará el backup a esa fecha, registrándose luego en el formato de Control de Backup (SGI-F-22-02-01).

En Provincias deberán de registrar la realización del Backup en el formato de Control de Backup (SGI-F-22-02-01).

Una vez que se tiene la información de los backup de las PC's, el Jefe de Sistemas programará tareas automáticas para copiar cada viernes esta información en una unidad de almacenamiento externo (Hard Disk Storage Server).

El sistema actualmente, en forma automática realiza 4 backups diarios de la base de datos, en intervalos de 6 horas cada uno, en una unidad de disco auxiliar en el mismo servidor de Base de datos, protegiendo esta información con una copia adicional de los mismos en un disco externo (Hard Disk Storage Server).

Así mismo, se mantendrá un Control del Backups del Sistema que se registrará en el formato del mismo nombre (SGI-F-22-02-01).

El Jefe de Sistemas es el responsable de salvaguardar la copia de los backup. Diariamente se suben a la Nube una copia comprimida de los backups de las bases de datos de todos los sistemas.

En el registro, Control de Backup (SGI-F-22-02-01) se anotará las fechas del backup de la información, el Gerente de Operaciones lo firmará trimestralmente como señal de revisión de la realización de backup.

En Provincia, guardará el backup fuera de las instalaciones de las oficinas.

- La terminología que se utilice para identificación de los backups, estará basada principalmente en la fecha de realización del mismo, y también en la naturaleza de la data archivada.
- Los información serán almacenados en las instalaciones de J&V RESGUARDO SAC. Como medida de contingencia, se genera una copia a una unidad virtual en la Nube.

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 7 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

Sistema Contra Incendio (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) distribuidos en todos los pisos de la institución desde el primer al tercer piso.

J&V RESGUARDO SAC cuenta con los siguientes tipos de extintores para las diversas clases de incendios:

- Incendios de Clase A: Todo lo referente a Materiales sólidos (Papel, Madera, Cartón).
- Incendios Clase B y C: Todo lo referente a Líquidos Inflamables y/o Equipos Eléctricos (Gasolina, Pinturas, Solventes, Equipos eléctricos conectados).
- Sistema Contra Incendio (Agente Limpio)

Así también tenemos en todas las oficinas y pasadizos extintores de gas carbónico y de polvo químico seco de conformidad a la norma establecida.

Luces de Emergencia

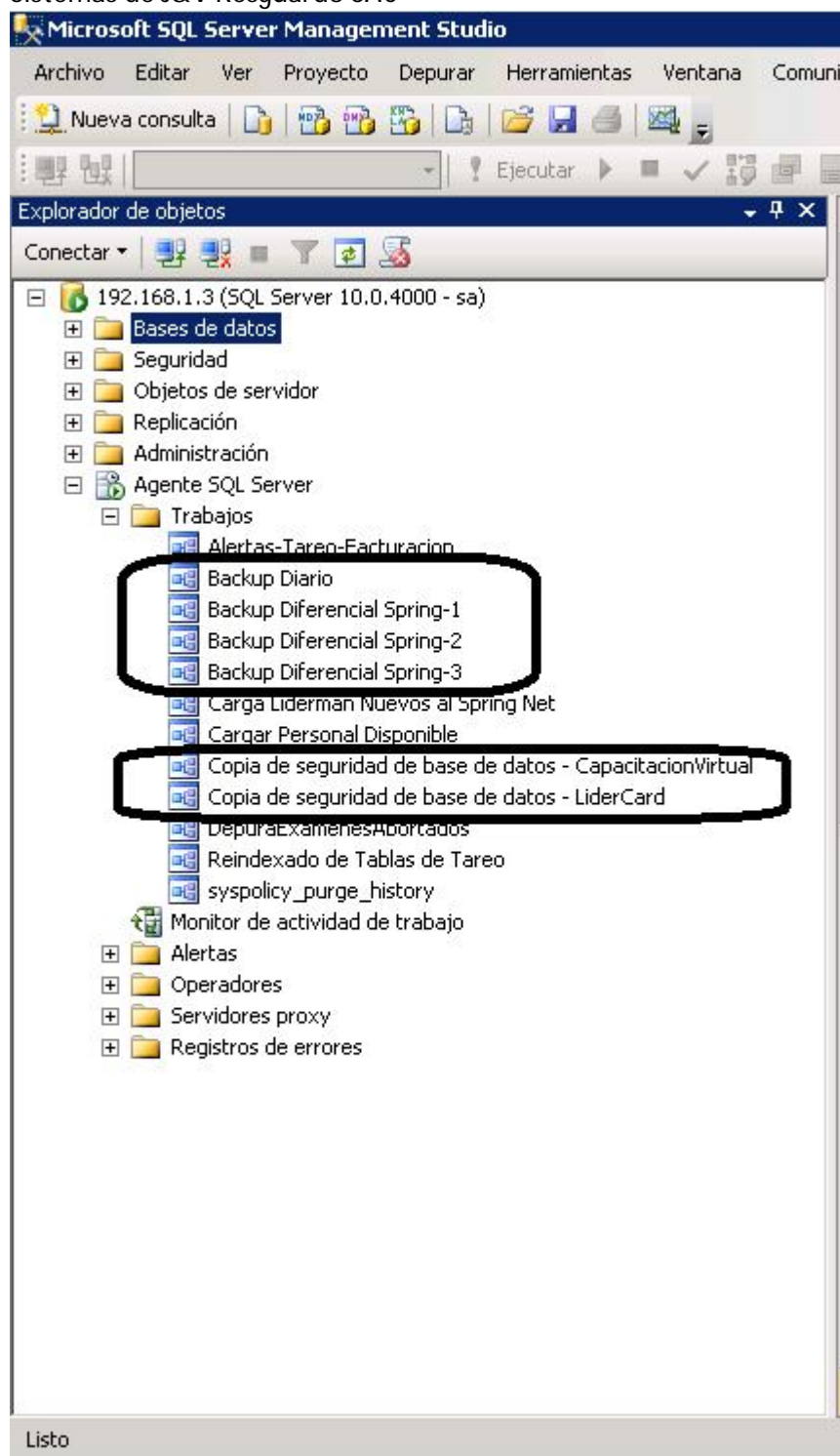
Se ha instalado sistema de luces de emergencia, las cuales tiene una batería interna que se activan ante un corte de fluido eléctrico con una autonomía de 02 horas y están distribuidos en todas las áreas los pasadizos de cada piso en la sede central. Se recomienda la activación de estas luces por encontrarse actualmente inoperativas.

Grupo Electrónico

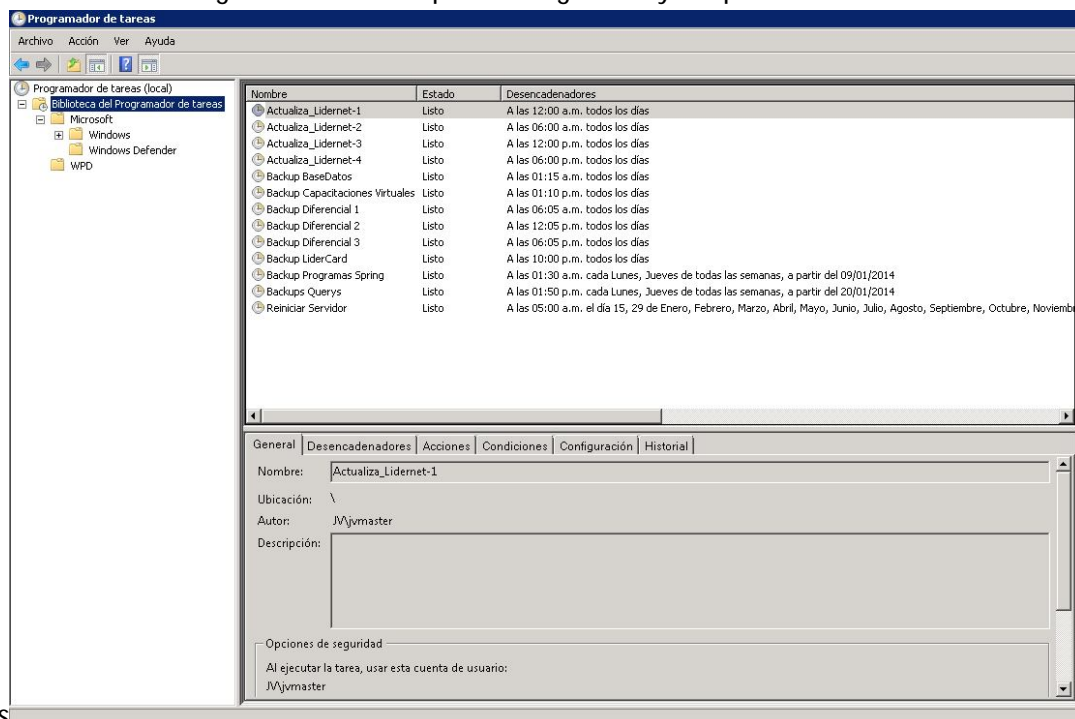
J&V Resguardo SAC contrata los servicios de una empresa especializada en alquiler de G.E. la cual provee la unidad en un plazo máximo de 2 horas.

Anexo N° 2 - EVIDENCIA DE PUESTA A PRUEBA Y FUNCIONAMIENTO

Tareas Automáticas Generadoras de las Copias de Respaldo de las Bases de datos de los Sistemas de J&V Resguardo SAC

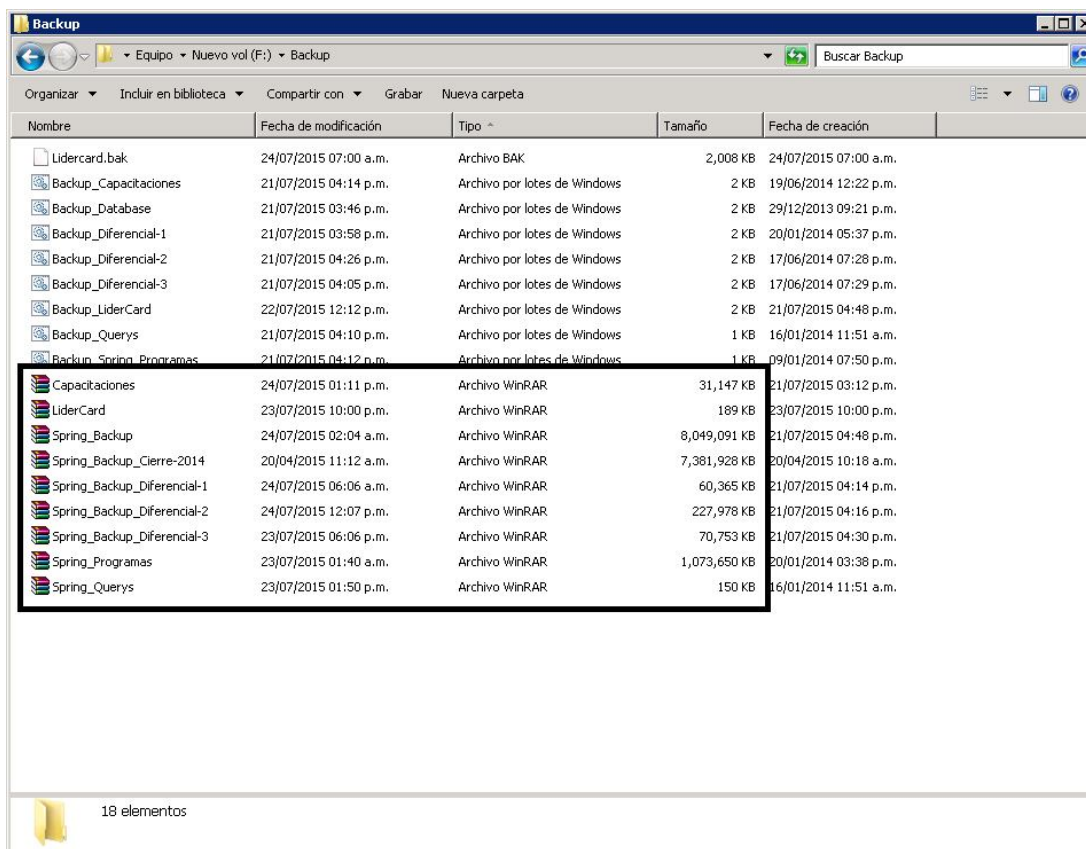


Tareas automáticas de generación de Copias de Seguridad y Respaldo

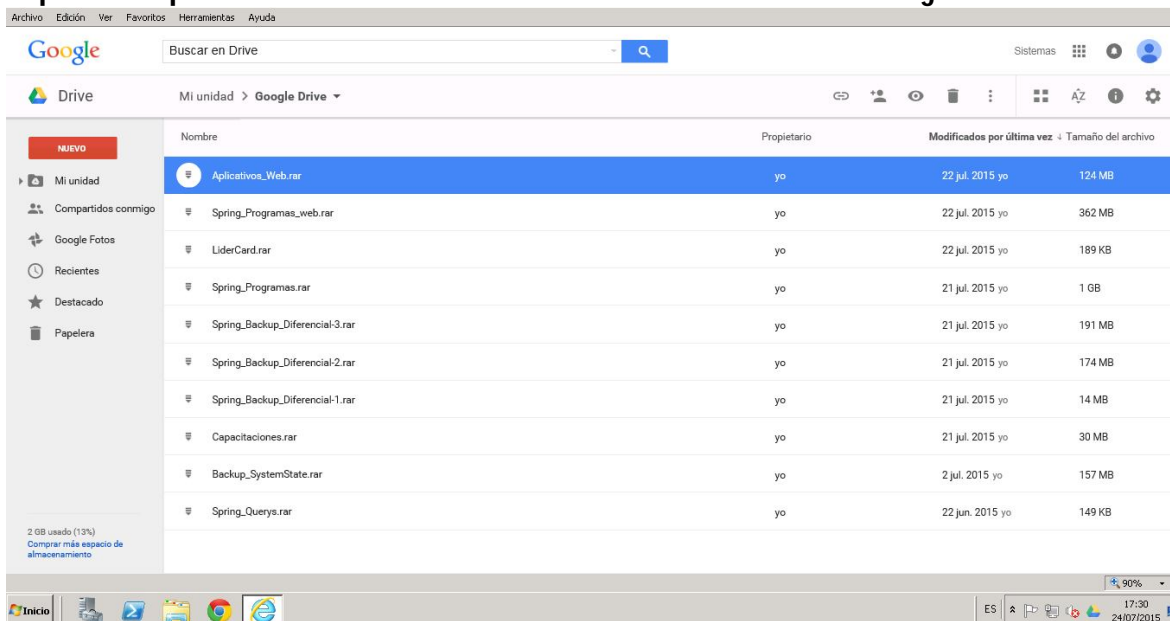


diarias

Archivos de Backup Generados automáticamente según Programacion Automatica.



Copia de Respaldo de la Información en Disco Virtual en la Nube de Google.



Anexo N° 3 - RECOMENDACIONES PARA EL USO DE CORREOS ELECTRONICOS

A continuación se detallan algunas recomendaciones importantes para el uso seguro y adecuado del Correo Electrónico y el por qué de ello. Finalmente propondremos una relación a manera de ayuda memoria que contenga los principales puntos a tener en cuenta.

Recomendaciones al Recibir Correos Electrónicos

1. **Verifique la autenticidad del remitente del mensaje** Los mensajes de correo electrónico pueden ser falsificados fácilmente. Tenga en cuenta que un atacante podría generar mensajes que parezcan ser originados por algún tercero en el cual Ud. confía. Si se trata de información crítica y el contenido del mensaje despierta alguna sospecha, trate de validar los datos del remitente por otro medio alternativo.
2. **Elimine mensajes no esperados o de un remitente desconocido** No conteste ni reenvíe mensajes de correo electrónico que no espera recibir. Si no reconoce el remitente o no esperaba el mensaje, no lo responda, ya que podría estar confirmando a un posible atacante que su cuenta de correo electrónico es válida y se encuentra activa.
3. **No abra archivos adjuntos que no está esperando** Muchos virus informáticos utilizan el correo electrónico como medio para propagarse, enviando copias de sí mismos como archivos adjuntos a los contactos que figuran en su libreta de direcciones. Los archivos adjuntos y el software de fuentes no confiables muchas veces contienen código malicioso (virus, troyanos, etc.) que podrían permitir a un atacante robar información de su equipo o afectar el funcionamiento de su computadora. » No abra archivos anexados a los mensajes por más que sean de un remitente conocido si no los está esperando. Ante la duda, consulte al remitente si él efectivamente lo envió antes de abrir el adjunto. » No abra archivos adjuntos que tengan extensiones ejecutables (.exe, .bat, .pif) » No abra archivos adjuntos que tengan más de una extensión (.jpg.exe, .doc.exe), ya que en estos casos, intentan engañar al destinatario a fin de que ejecute el programa adjunto utilizando mensajes sugestivos y pretendiendo ser una archivo de imagen o un documento. » Siempre analice los archivos recibidos con un antivirus.
4. **No visite los sitios web que figuran en los mensajes** No visite los sitios web mencionados en mensajes de correo electrónico cuyo remitente sea desconocido. Tenga especial cuidado si el sitio web mencionado en el mensaje recibido le pide que ingrese sus datos personales, sus claves de acceso, sus datos financieros, etc. El sitio podría estar siendo usado por un atacante para robar su identidad, técnica conocida como "phishing".
5. **El software antivirus de su computadora debe mantenerse actualizado**, Utilice un antivirus reconocido, con la configuración establecida por el Servicio Técnico de la Jefatura de Sistemas. Verifique que el software antivirus instalado en el equipo se encuentra activo y actualizado, ya que periódicamente se descubren nuevas vulnerabilidades y

aparecen nuevos virus. Analice siempre los medios removibles (discos, disquettes, pen-drives, mp3, celulares, cámaras digitales) que se conecten a la computadora. Ejecute un análisis completo del equipo al menos una vez por semana. Respalde periódicamente sus mensajes de correo. Proteja las copias de respaldo con contraseña y no las deje al alcance de terceros.

6. ***Si debe reenviar o "hacer forward" de un correo electrónico: Borre las direcciones de correo de los remitentes***, de no hacerlo, estará divulgando las direcciones a todos los destinatarios del mensaje, quienes podrán utilizar dichas direcciones para enviar correo masivo o spam. Copie el contenido del correo original y redacte uno nuevo. Si reenvía a más de una persona, ingrese las direcciones de los destinatarios en el campo Copia Oculta (CCO o BCC) del programa; de no ser así, cada receptor podrá conocer los demás destinatarios que recibieron el mismo mensaje de correo electrónico.
7. ***No utilice el correo electrónico como medio para difundir ideas políticas***, religiosas, propagandas, etc.
8. ***No envíe información crítica por correo electrónico sin utilizar un sistema de cifrado*** El contenido del mensaje puede ser capturado en cualquiera de los equipos informáticos por los que circula el mensaje desde que es enviado hasta que se entrega en el buzón del destinatario. Si debe enviar información crítica por correo electrónico, contacte al Departamento de Informática.
9. Con cierta frecuencia se reciben en los buzones de correo electrónico mensajes sospechosos solicitando a los usuarios que introduzcan sus datos de usuario y contraseña o hacerlo en una página web pinchando en un enlace del mensaje.
Nunca debe responder a esos mensajes ni pinchar en los enlaces porque sus datos de usuario llegarán a personas no autorizadas y pueden servir para realizar actividades fraudulentas.
Recuerde que los Servicios Informáticos de los centros financieros u organizaciones debidamente acreditadas nunca le solicitarán por email o teléfono su contraseña. Ésta sólo debe utilizarse para conectar a los sistemas de información autorizados que requieran autenticación y ésta siempre se transmitirá cifrada por un canal de comunicaciones seguro.

Recomendaciones al Enviar Correos Electrónicos

1. ***Escribe correos cortos***, Si una llamada de 5 minutos puede resolver un asunto, invertir una hora en redactar el correo tratándolo es una pérdida de tiempo.
2. ***Evita usar confirmaciones de apertura***, Si el asunto es importante es mejor tratarlo de frente. El correo es una herramienta y no sustituye a las personas.

3. ***Cuestiona siempre si el correo es la mejor vía***, Piensa tres veces antes de tratar un tema por correo. Evalúa si no es mejor tratarlo por teléfono, por mensajero instantáneo o en una reunión informal cara a cara, antes de ponerte a escribir.
 4. ***Mantén los archivos adjuntos bajo 2.3 MB***, Sólo adjunta los archivos cuando es estrictamente necesario, especialmente cuando es un correo dirigido a varias personas. Existen métodos alternos para compartirlos.
 5. ***Sólo copia a los involucrados***. A veces es más sencillo resolver un asunto entre dos personas sin involucrar a terceros. Copia a otros cuando así se te haya solicitado o cuando se trata de una minuta después una reunión. En vez de usar copia oculta, reenvía el correo a quien te interesa que esté enterado haciendo referencia explícita a que es “sólo para sus ojos” (FYEO – For your eyes only).
 6. ***Archiva los correos con más de 6 meses de antigüedad***, una buena práctica es crear carpetas para cada año y archivar allí los correos antiguos.
 7. ***Procura no usar tu correo de la empresa para asuntos personales***, es mejor que uses gmail, hotmail o Yahoo para esos correos.
 8. ***Resiste la tentación de poner “reply to all” o “responder a todos” cuando no es necesario***, Si la respuesta atañe solamente al remitente respóndele sólo a él. No es necesario copiar a todos con cada “OK”.
 9. ***Evita caer en un ping-pong de correos***, cuando van y regresan respuestas sobre el mismo asunto, uno se pregunta si no hay una mejor vía. Ten en cuenta la recomendación 3 y busca otro medio para resolverlo.
- .

RESUMEN

REGLAS PARA EL USO DE CORREOS ELECTRONICOS

1. Verifique la autenticidad del remitente del mensaje
2. No abra archivos adjuntos que no está esperando
3. No visite los sitios web que figuran en los mensajes (Links) activan los troyanos y Virus.
4. Escribe correos cortos. Ahorre espacio en el Servidor
5. Mantén los archivos adjuntos bajo 3 MB
6. Sólo copia a los involucrados
7. Procura no usar tu correo de la empresa para asuntos personales
8. No utilizar la opción “responder a todos” a menos que sea muy necesario. Límitese a responder al Remitente.
9. No usar el Correo para “pasarse” archivos de trabajo entre usuarios de la misma área. Utilice carpetas compartidas en el Disco para ello.

