

Tecnotec | www.tecnotec.cl

Plan de contingencia

Propuesta de plan de contingencia preparada para Pintopiga

Contenido

1	Introducción	6
2	Definiciones	7
2.1	Contingencia	7
2.2	Plan de contingencia	7
2.3	Planes	7
2.3.1	Elementos Esenciales de los Planes	8
3	Objetivos	8
4	Análisis de impacto en los procesos	9
4.1	Objetivo Principal	9
4.2	Objetivos específicos	9
5	Definiciones de términos utilizados	9
6	Plantilla de procedimientos alternos	11
6.1	Identificar contactos claves que dependan del sistema	11
6.2	Identificar Recursos del sistema	12
6.2.1	Detalle de servidores VPS Pintopiga	12
6.2.2	Detalle de servidores VPS Pintopiga / Tecnotec	12
6.3	Identificar impactos de la caída y tiempos aceptables de caída	13
6.3.1	Priorizar el recupero de recursos	13
7	Diseño de estrategia de continuidad de los procesos y servicios	14
7.1	Escenario I: No hay comunicación entre cliente-servidor en	14
7.1.1	Impacto	14
7.1.2	Tiempos aceptables de Caída	14
7.1.3	Recursos de contingencia	14
7.1.4	Procedimiento	15
7.2	Escenario II: Falla de Servidor Crítico	16
7.2.1	Impacto	16

7.2.2	Tiempos aceptables de Caída.....	16
7.2.3	Causas de fallas de servidor	16
7.2.4	Recursos de Contingencia	20
7.2.5	Procedimiento	20
7.3	Escenario III: Ausencia Parcial o Permanente del Personal del Área de Informática	21
7.3.1	Impacto	21
7.3.2	Recursos de contingencia.....	21
7.3.3	Procedimiento	22
7.4	Escenario IV: Interrupción del Fluido Eléctrico	23
7.4.1	Impacto	23
7.4.2	Recursos de contingencia.....	23
7.4.3	Procedimiento	24
7.5	Escenario V: Corte del Servicio de Internet.....	25
7.5.1	Impacto	25
7.5.2	Recursos de contingencia.....	25
7.5.3	Procedimiento	26
7.6	Proveedores Importantes	26
7.7	Escenario VI: Ciberataque	27
7.7.1	Impacto	27
7.7.2	Recurso de contingencia	27
7.7.3	Procedimiento	28
8	Plan de verificación y plan de pruebas.....	29
8.1	Plan de Verificación.....	29
8.2	Procedimientos para las Pruebas del Plan de Contingencia.....	30
8.2.1	Procedimiento	30
8.2.2	Objetivos.....	30

8.2.3	Procedimientos para las Pruebas del Plan de Contingencias Niveles de Prueba 30	
8.2.4	Procedimiento	33
9	Anexos	34
9.1	Aviso a persona responsable por el entrenamiento del plan	34
9.2	Control de Cambios al Plan.....	35
9.3	Responsabilidad en el Mantenimiento de Cada Parte del Plan	36
9.4	Estructura de red Actual	37
9.4.1	Enlace Internet	38
9.5	Telefonía IP	39
9.6	Esquema actual	39
9.6.1	Servicio de Correo Electrónico	39
9.6.2	Seguridad de la información	40
9.6.3	Respaldo de Información	40
9.6.4	Filtro de contenido.....	42

Ilustraciones

ILUSTRACIÓN 1 ORGANIGRAMA.....	11
ILUSTRACIÓN 2 PROCEDIMIENTO I.....	15
ILUSTRACIÓN 3 PROCEDIMIENTO II.....	20
ILUSTRACIÓN 4 PROCEDIMIENTO III.....	22
ILUSTRACIÓN 5 PROCEDIMIENTO IV.....	24
ILUSTRACIÓN 6 PROCEDIMIENTO V.....	26
ILUSTRACIÓN 7 PROCEDIMIENTO VI.....	28
ILUSTRACIÓN 8 PLAN DE PRUEBAS.....	33
ILUSTRACIÓN 9 ESQUEMA DE TOPOLOGÍA ENCONTRADA.....	37
ILUSTRACIÓN 10 ESQUEMA DE CONEXIÓN A INTERNET (MOVISTAR GENERICO).....	38
ILUSTRACIÓN 11 CONEXIÓN FÍSICA ENLACE INTERNET.....	38
ILUSTRACIÓN 12 ESQUEMA FILTRO CONTENIDO.....	42

1 Introducción

Para Pintopiga es indispensable recurrir a los recursos computacionales como un medio de proveer información a todos los niveles de la empresa, y es de vital importancia que dicha información sea lo más exacta posible.

Es importante resaltar que para que una organización logre sus objetivos necesita garantizar tiempos de indisponibilidad mínimos, tanto en sus recursos informáticos como en las comunicaciones; de este modo podrá mantener una contingencia eficiente en todas las áreas operativas.

Por todo lo anteriormente dicho, el estar sin el servicio del computador por un lapso mayor de 3 horas origina distorsiones al funcionamiento normal de los servicios y mayores costos de operación. De continuar esta situación por un mayor tiempo se expone al riesgo de paralizar las operaciones por falta de información para el control y toma de decisiones de la empresa.

Es necesario, por tanto, prever cómo actuar y qué recursos se necesitan ante una situación de contingencia con el objeto de que su impacto en las actividades sea lo mejor posible.

El presente documento es el Plan de Contingencia Informático en materia de Riesgos de Tecnología de Información (TI) para Pintopiga.

Establece el objetivo, alcance y metodología desarrollada. Incluye, además, las definiciones utilizadas, las políticas de seguridad, el análisis de la situación, el análisis de sensibilidad de la información manejada, la identificación de los riesgos y controles, y la clasificación de activos de TI.

La metodología práctica comprende: la identificación de riesgos, calificación de la probabilidad de que ocurra un riesgo, evaluación del impacto en los procesos críticos y la creación de estrategias de contingencias.

Permitirá mantener la contingencia operativa frente a eventos críticos de la entidad y minimizar el impacto negativo sobre la misma, los usuarios y clientes, deben ser parte integral para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución.

2 Definiciones

2.1 Contingencia

Interrupción, no planificada, de la disponibilidad de recursos informáticos.

2.2 Plan de contingencia

Conjunto de medidas (de DETECCIÓN y de REACCIÓN) a poner en marcha ante la presentación de una contingencia.

El Plan de Contingencia se subdivide en:

- Plan de Emergencia
- Plan de Restauración (BACKUP)
- Plan de Recuperación

El Plan de Contingencia suele combinarse con planes de seguridad general.

2.3 Planes

	EMERGENCIA	RESTAURACION	RECUPERACION
OBJETIVO	Limitar el daño	Continuar Procesos Vitales	Recuperar proceso total
ACTUACION	Inmediata	A corto plazo	A medio plazo
CONTENIDO	Evacuación Valoración de daños Arranque de acciones	Alternativas para los procesos vitales	Estrategias para la recuperación de todos los recursos
RESPONSABILIDAD PRINCIPAL	Organización (Empresa)	Usuarios	Unidad de Informática

2.3.1 Elementos Esenciales de los Planes

1. Consenso
 - a. Planes aprobados por la jefatura de Pintopiga
 - b. Planes elaborados con el apoyo de los servicios usuarios y el servicio de seguridad general.
 - c. La eventual reasignación de las prioridades debe haber sido pactada con anterioridad por las tres partes implicadas (Jefatura, Área de Informática y los Usuarios).
2. Recursos
 - a. Lugar alternativo de trabajo.
 - b. Computador con "hardware" Y "software" apropiados.
 - c. Copias de seguridad actualizadas.
3. Pruebas
 - a. Validez de las copias de seguridad.
 - b. Simulacros de emergencia (una vez por año como mínimo).
 - c. Formación y reciclaje del personal.
4. Seguros
 - a. Contratos negociados.
 - b. No se puede asegurar un riesgo seguro o voluntario.
 - c. Los actos internos de mala intención no siempre se pueden asegurar.

3 Objetivos

Definir las actividades de planeamiento, preparación, entrenamiento y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.

Establecer un plan de recuperación, formación de equipos y entrenamiento para restablecer la operatividad del sistema en el menor tiempo posible.

Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general.

4 Análisis de impacto en los procesos

4.1 Objetivo Principal

El objetivo principal del Análisis del Impacto de los procesos, es determinar las funciones, procesos e infraestructura de soporte que son críticos para la contingencia operativa de la empresa.

4.2 Objetivos específicos

Para lograr el objetivo principal se definieron los siguientes objetivos específicos:

- Identificar las preocupaciones y prioridades de la jefatura de Pintopiga en el caso que exista una indisponibilidad en los sistemas informáticos producida por una contingencia.
- Identificar el tiempo máximo en el que un proceso crítico de la empresa deberá ser restaurado para su normal y eficiente continuidad.
- Identificar el impacto en las aplicaciones que soportan los procesos críticos de la empresa.
- Proporcionar las bases de una estrategia para la contingencia operativa en caso de un desastre.

5 Definiciones de términos utilizados

Para la mejor comprensión de los términos y contenido de este plan, se detallan las siguientes definiciones:

Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, y cuya falta o ejecución deficiente puede tener un impacto operacional o de imagen significativo para la empresa.

Impacto: El impacto de una actividad crítica se encuentra clasificado, dependiendo de la importancia dentro de los procesos TI, en:

Impacto Alto: se considera que una actividad crítica tiene impacto alto sobre las operaciones de la empresa, cuando ante una eventualidad en ésta se encuentran imposibilitadas para realizar sus funciones normalmente.

Impacto Medio: se considera que una actividad crítica tiene un impacto medio cuando la falla de esta, ocasiona una interrupción en las operaciones de la empresa por un tiempo mínimo de tolerancia.

Impacto Bajo: se considera que una actividad crítica tiene un impacto bajo, cuando la falla de ésta, no tiene un impacto en la continuidad de las operaciones de la Empresa.

Plan de Contingencia: Son procedimientos que definen cómo un negocio continuará o recuperará sus funciones críticas en caso de una interrupción no planeada.

- Los sistemas de TI son vulnerables a diversas interrupciones.
 - Leves: Caídas de energía de corta duración, fallas en disco duro, etc.
 - Severa: Destrucción de equipos, incendios, etc.
- Asegura que se dé una interrupción mínima a los procesos de negocios en caso de una interrupción significativa de los servicios que normalmente soportan esos procesos.
- Todos los aplicativos críticos y sistemas de soporte general deben tener un plan de contingencias.

6 Plantilla de procedimientos alternos

6.1 Identificar contactos claves que dependan del sistema

Identificar las personas, posiciones u oficinas dentro de la organización que dependen de o soportan el sistema; especificar su relación con el sistema.

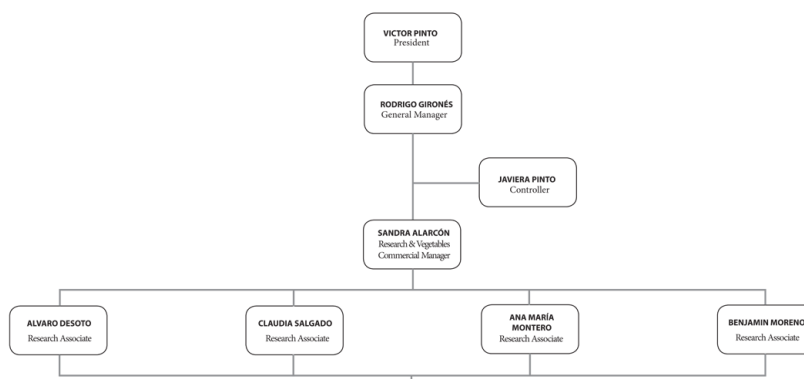


Ilustración 1 Organigrama

6.2 Identificar Recursos del sistema

Identificar el hardware, software y otros recursos específicos que incluye el sistema.

6.2.1 Detalle de servidores VPS Pintopiga

Nombre	Sistema operativo invitado
PINTOPIGA-Archivos	Debian GNU/Linux 6 (32-bit)
PINTOPIGA-Backup-SRV	Red Hat Enterprise Linux 6 (32-bit)
PINTOPIGA-Backup-SRV2	Ubuntu Linux (64-bit)
PintoPiga-DC-01	Microsoft Windows Server 2012 (64-bit)
PINTOPIGA-GSEEDS	Microsoft Windows Server 2003 Standard (32-bit)
PintoPiga-VPN-SRV-c7	Red Hat Enterprise Linux 7 (64-bit)
PINTOPIGA-WS2008R2	Microsoft Windows Server 2008 R2 (64-bit)
PPIGA-Filtro-20180801	Red Hat Enterprise Linux 7 (64-bit)
soporte.pintopiga.com	Red Hat Enterprise Linux 7 (64-bit)
SRV-W2008-64b-120G4G-02	Microsoft Windows Server 2008 R2 (64-bit)
SRV-W200864b-120G4G-01	Microsoft Windows Server 2008 R2 (64-bit)
SRVAPP-pintopiga.com	Microsoft Windows Server 2012 (64-bit)
SRVPLUS-pintopiga.com	Microsoft Windows Server 2012 (64-bit)
SRVSQL-pintopiga.com	Microsoft Windows Server 2012 (64-bit)

Adicionalmente a los servidores VPS, se identifican 3 servidores físicos y 2 storages encargados de respaldos.

6.2.2 Detalle de servidores VPS Pintopiga / Tecnotec

Nombre	Sistema operativo invitado
PIGA-DC02	Microsoft Windows Server 2016 (64-bit)
PIGA-PPFLEXLINE-SRV01-109	Microsoft Windows Server 2008 R2 (64-bit)

Maquinas VPS encendidas, adicionalmente a ellas, existen clones para emergencias.

6.3 Identificar impactos de la caída y tiempos aceptables de caída

Los tiempos de caídas, aceptables dentro de la organización se definen en una hora como promedio, siendo menos o más, dependiendo del sistema puntualmente afectado.

INTERNET: Las caídas del servicio de Internet se da normalmente por averías propias del proveedor. También se debe considerar las fallas de Hardware (de equipamiento asociado al proveedor, en este caso Movistar), o por alguna desconfiguración en las reglas de firewall.

ANEXOS TELEFONICOS: En caso de alguna falla en el anexo telefónico, cada oficina tendrá que requerir el servicio de un tercero para la reparación del mismo.

RED INTERNA: En caso de fallas puntuales de red, se debe requerir asistencia en terreno para verificar la causa de la falla.

6.3.1 Priorizar el recupero de recursos.

RECURSO	PRIORIDAD
PC	Alto
IMPRESORA	Alto
INTERNET	Alto
ANEXO TELEFONICO	Medio
HERRAMIENTAS DE OFFICE (WORD EXCEL. ETC)	Medio
SISTEMA INTERNO DE GESTION	Alto
CORREO ELECTRONICO	Alto

7 Diseño de estrategia de continuidad de los procesos y servicios

7.1 Escenario I: No hay comunicación entre cliente-servidor en

7.1.1 Impacto

IMPACTO	ÁREA AFECTADA
NO SE PUEDE TRABAJAR CON LOS RECURSOS DE LA RED. (INFORMACIÓN).	Área en que labora
INTERRUPCIÓN DE ACTIVIDADES	Área en que labora

7.1.2 Tiempos aceptables de Caída

RECURSO	PRIORIDAD DE RECUPERACIÓN
SISTEMAS INFORMÁTICOS (GESTION, ETC)	ALTO
SERVIDOR DE ARCHIVOS / DC	ALTO
CORREO ELECTRÓNICO	ALTO
INTERNET	ALTO

7.1.3 Recursos de contingencia

Componentes de Reemplazo: Tarjeta de Red, Conector RJ-45, Jack RJ-45, Testeador, herramientas de Cableado Estructurado, etc.

7.1.4 Procedimiento

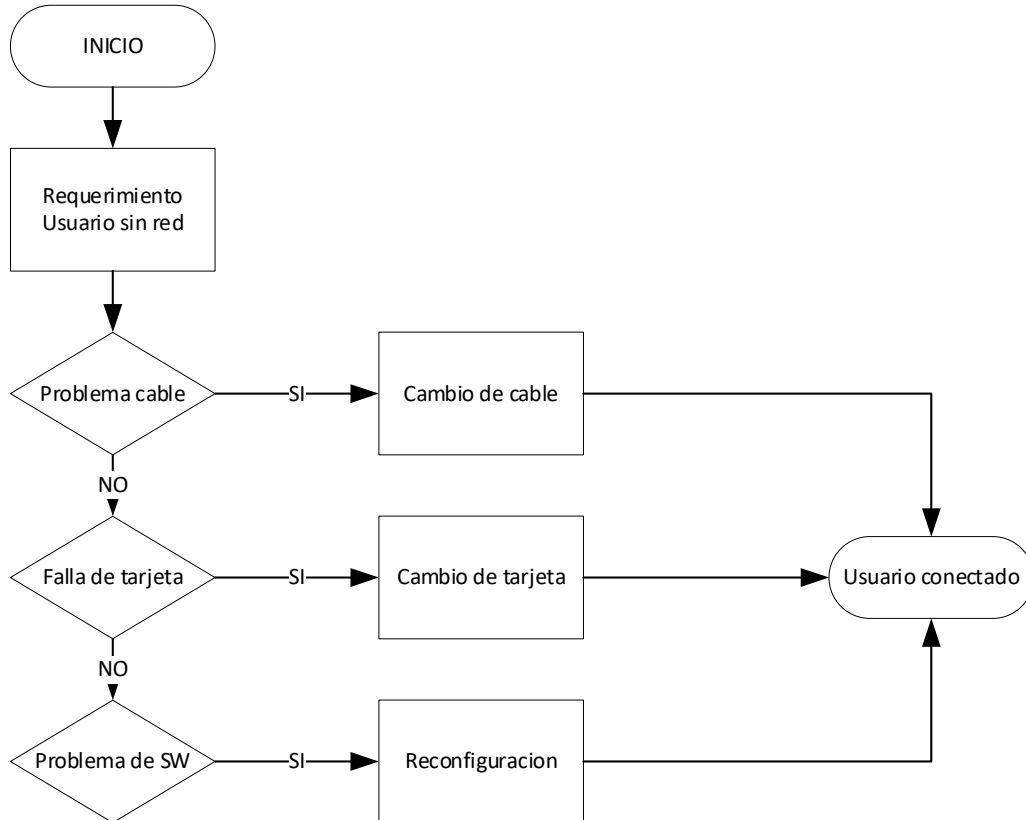


Ilustración 2 Procedimiento I

7.2 Escenario II: Falla de Servidor Crítico.

7.2.1 Impacto

Impacto	Área Afectada
Paralización de los sistemas o aplicaciones que se encuentran en los servidores que presentan fallas.	Todas las Áreas
Posible Pérdida de Hardware y Software.	Unidad de informática
Perdida del proceso automático de Backup y restore.	Unidad de informática
Interrupción de las operaciones.	Unidad de informática

7.2.2 Tiempos aceptables de Caída.

Recurso	Prioridad de recuperación
Servidor Web	MEDIO
Servidor de Aplicaciones - GESTION	ALTO
Servidor de Controlador de Dominio Primario	ALTO
Servidor de Correo	ALTO
Servidor FIREWALL - PROXY	MEDIO
Servidor FILESERVER	ALTO
Servidor Antivirus, Controlador de Dominio Secundario	ALTO
Servidor Backup	ALTO

7.2.3 Causas de fallas de servidor

7.2.3.1 CASO A: Error Físico de Disco de un Servidor (Sin RAID).

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

- 1) Ubicar el disco con falla.
- 2) Avisar a los usuarios, utilizar mensajes por red y teléfono a jefes de área.
- 3) Retirar el disco malo y reponerlo con otro del mismo tipo, reinicializar el arreglo.
- 4) Recorrer los sistemas que se encuentran en dicho servidor y verificar su buen estado.

7.2.3.2 CASO B: Error de Memoria RAM

En este caso se dan los siguientes síntomas:

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
- Ante procesos mayores se congela el proceso.
- Arroja errores con mapas de direcciones hexadecimales.
- Es recomendable que el servidor cuente con ECC (error correctchecking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por Pintopiga, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

- 1) Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
- 2) El servidor debe estar apagado, dando un correcto apagado del sistema.
- 3) Ubicar las memorias con mal funcionamiento.
- 4) Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
- 5) Retirar la conexión del servidor con el Switch de datos, ésta se ubica detrás del servidor, ello evitará que, al encender el sistema, los usuarios ingresen.
- 6) Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
- 7) Probar los sistemas que están en red en diferentes estaciones.

- 8) Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

7.2.3.3 CASO C: Error de Tarjeta(s) Controladora(s) de Disco

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

- 1) Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
- 2) El servidor debe estar apagado, dando un correcto apagado del sistema.
- 3) Ubicar la posición de la tarjeta controladora.
- 4) Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
- 5) Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
- 6) Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
- 7) Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

7.2.3.4 CASO D: Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

- Caída del servidor de archivos por falla de software de red.
- Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- Bajar incorrectamente el servidor de archivos.
- Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

- 1) Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos.
- 2) Deshabilitar el ingreso de usuarios al sistema.
- 3) Descargar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá descargarlo también.
- 4) Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.
- 5) Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

7.2.3.5 CASO E: Caso de Virus

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

- Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación
- El antivirus muestra el nombre del archivo infectado y quién lo usó.
- Estos archivos (exe, com, ovl, nlm, etc.) serán reemplazados del medio original de instalación o del backup.
- Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

7.2.4 Recursos de Contingencia

- Componente de Reemplazo (Memoria, Disco Duro, etc.).
- Backup diario de información del servidor

7.2.5 Procedimiento

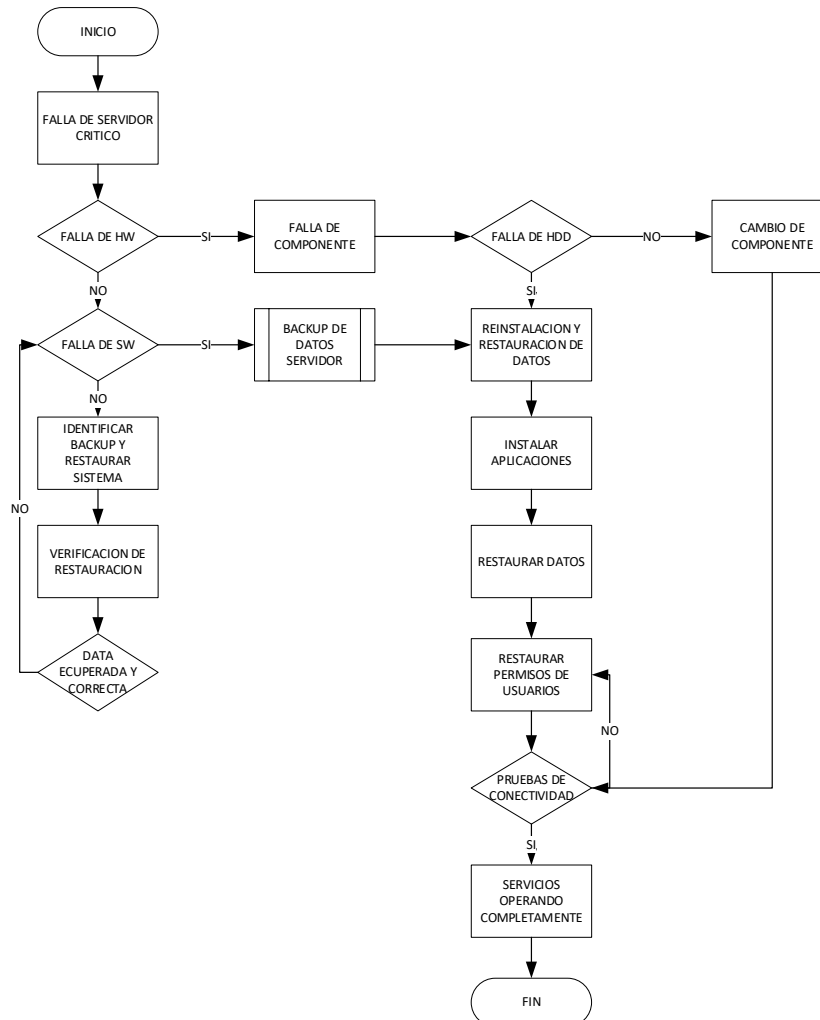


Ilustración 3 Procedimiento II

7.3 Escenario III: Ausencia Parcial o Permanente del Personal del Área de Informática

7.3.1 Impacto

Impacto	Área Afectada
Interrupción de funciones de la persona ausente	Todas las áreas
Administración de servidores	
Control y monitoreo de servidores	
Soporte a los usuarios	
Ajustes a programas críticos en producción	

7.3.2 Recursos de contingencia

Se presentan las funciones actuales que tienen a su cargo el personal del Área de Informática.

7.3.3 Procedimiento

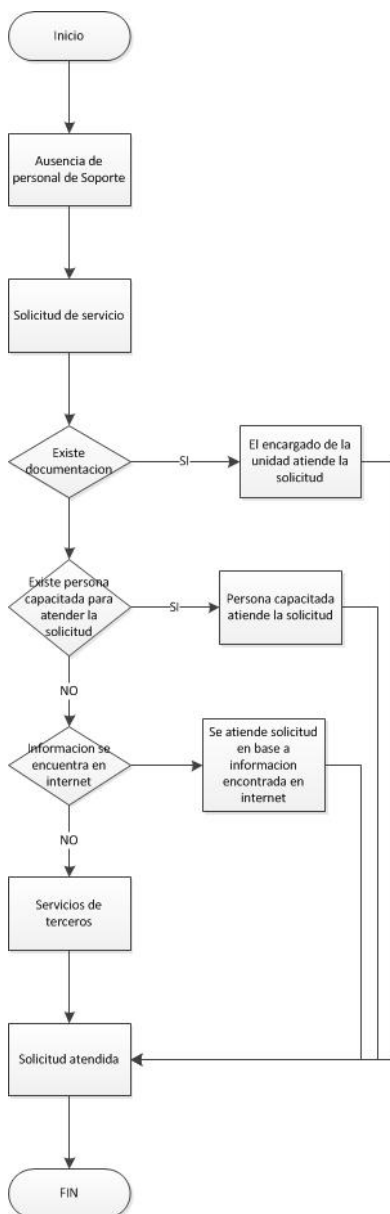


Ilustración 4 Procedimiento III

7.4 Escenario IV: Interrupción del Fluido Eléctrico

7.4.1 Impacto

Impacto	Área Afectada
Finalización incompleta de los Backup	Todas las áreas
Falla de un componente de equipo servidor	Todas las áreas
Pérdida total o parcial de la operatividad de los sistemas.	Todas las áreas

Se puede presentar lo siguiente:

- 1) Si fuera corto circuito, el UPS mantendrá activo los servidores, mientras se repare la avería eléctrica.
- 2) Para el caso de apagón se mantendrá la autonomía de corriente que la UPS nos brinda (corriente de emergencia¹ (*)), hasta que los usuarios completen sus operaciones (para que no corten bruscamente el proceso que tienen en el momento del apagón), hasta que finalmente se realice el By-pass de corriente con el grupo electrógeno, previo aviso y coordinación.
- 3) Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de grupo electrógeno a corriente normal² (o UPS).

7.4.2 Recursos de contingencia

Si se produjera en horas de la noche una interrupción del fluido eléctrico, se podrían paralizar los procesos de cierre y backup de los servidores. Por tal motivo es necesario revisar continuamente el estado de las baterías del UPS. Dichas baterías deben garantizar una autonomía de aproximadamente una hora. Es necesario establecer un procedimiento que permita al personal de seguridad de Pintopiga avisar al personal de Informática de este hecho. La UPS se caracteriza por emitir una alarma fácil de identificar, y también existe la posibilidad de configurar alarmas por correo electrónico o SMS por dichas fallas.

¹ Llámese corriente de emergencia a la brindada por grupo electrógeno y/o UPS

² Llámese corriente normal a la brindada por la compañía eléctrica

7.4.3 Procedimiento

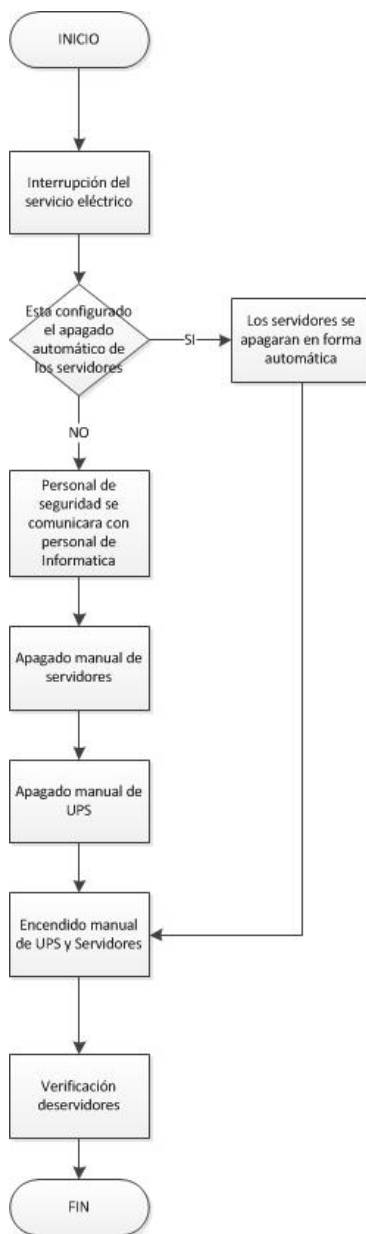


Ilustración 5 Procedimiento IV

7.5 Escenario V: Corte del Servicio de Internet

7.5.1 Impacto

Impacto	Área Afectada
Interrupción de la recepción y envío de información, mensajes y data a nivel nacional e internacional.	Todas las áreas

7.5.2 Recursos de contingencia

Backup de configuración de firewall

7.5.3 Procedimiento



Ilustración 6 Procedimiento V

7.6 Proveedores Importantes

Recurso	Empresa	Contacto	Fono Fijo	Fono Celular	E-Mail
Enlace Internet	Movistar				
Antivirus					
Soporte Externo					
Telefonia					

7.7 Escenario VI: Ciberataque

7.7.1 Impacto

Impacto	Área Afectada
Interrupción de la recepción y envío de información, mensajes y data a nivel nacional e internacional.	Todas las áreas

7.7.2 Recurso de contingencia

- Backup de configuración de firewall
- Backup diario de información del servidor

7.7.3 Procedimiento

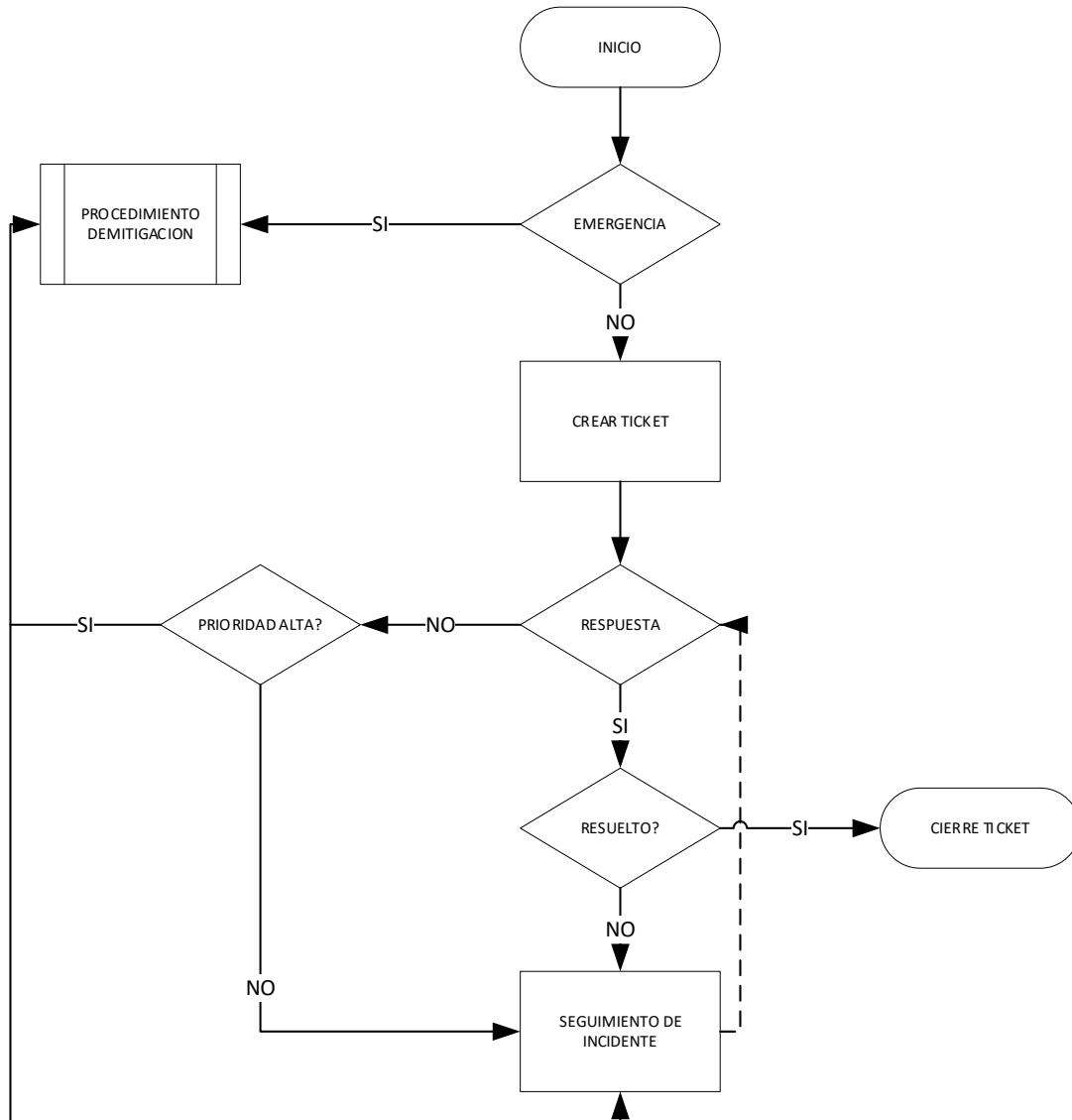


Ilustración 7 Procedimiento VI

8 Plan de verificación y plan de pruebas

Tres medidas de minimizar los riesgos de la tecnología son la:

- Verificación
- Prueba
- Mantenimiento de los sistemas.

Cada componente de un sistema de cómputo equipo, comunicaciones y programas debe ser verificado y probado rigurosamente antes de utilizarlo para un evento.

8.1 Plan de Verificación

Para el Plan de Contingencia es muy importante y es conveniente que una autoridad independiente aplique las pruebas de verificación.

Para sistemas de menor importancia, la verificación puede realizarse internamente.

Las pruebas de verificación (también conocidas como pruebas de calidad) pueden incluir:

- Probar los equipos bajo condiciones que simulen las de operación real.
- Probar los programas para asegurar que se siguen los estándares apropiados y que desempeñan las funciones esperadas.
- Asegurar que la documentación sea la adecuada y esté completa.
- Asegurar que los sistemas de comunicación se ciñan a los estándares establecidos y funcionen de manera efectiva.
- Verificar que los sistemas sean capaces de operar bajo condiciones normales, pero también bajo potenciales condiciones inesperadas.
- Asegurar que se cuente con las debidas medidas de seguridad y que estas se ciñan a las normas establecidas.

8.2 Procedimientos para las Pruebas del Plan de Contingencia

8.2.1 Procedimiento

Todos los planes de contingencia deben ser probados para demostrar su habilidad de mantener la continuidad de los procesos críticos de la empresa.

Las pruebas se efectúan simultáneamente a través de múltiples unidades, incluyendo entidades externas.

Realizando pruebas se descubrirán elementos operacionales que requieren ajustes para asegurar el éxito en la ejecución del plan, de tal forma que dichos ajustes perfeccionen los planes preestablecidos.

8.2.2 Objetivos

El objetivo principal, es determinar si el Plan de contingencia es capaz de proporcionar el nivel deseado de apoyo a la sección o a los procesos críticos de la empresa, probando la efectividad de los procedimientos expuestos en el plan de contingencias.

Las pruebas permiten efectuar una valoración detallada de los costos de operación en el momento de ocurrencia de una contingencia.

8.2.3 Procedimientos para las Pruebas del Plan de Contingencias Niveles de Prueba

Se recomiendan dos niveles de prueba:

- Pruebas en pequeñas Unidades Orgánicas.
- Pruebas en a nivel Gerencial.

La premisa es comenzar la prueba en las Unidades Orgánicas más pequeñas, extendiendo el alcance a nivel de jefatura más alto, para finalmente realizar las pruebas entre edificios o con otras instituciones externas

Métodos para Realizar Pruebas de Planes de Contingencia

A. Prueba Específica

Consiste en probar una sola actividad, entrenando al personal en una función específica, basándose en los procedimientos estándar definidos en el Plan de Contingencia. De esta manera el personal tendrá una tarea bien definida y desarrollará la habilidad para cumplirla.

B. Prueba de Escritorio

Implica el desarrollo de un plan de pruebas a través de un conjunto de preguntas típicas (ejercicios).

Características:

- La discusión se basa en un formato preestablecido.
- Está dirigido al equipo de recuperación de contingencias.
- Permite probar las habilidades gerenciales del personal que tiene una mayor responsabilidad.

Los ejercicios de escritorio son ejecutados por el encargado de la prueba y el personal responsable de poner el plan de contingencias en ejecución, en una situación hipotética de contingencia. Unos conjuntos de preguntas se pedirán que resuelva el personal. El encargado y el personal utilizarán el plan de contingencias para resolver las respuestas a cada situación. El encargado contestará a las preguntas que se relacionan con la disponibilidad del personal entrenado, suficiencia de los recursos, suficiencia de máquinas, y si los requerimientos necesarios están a la mano. Los ajustes serán hechos al plan o al ambiente determinado durante esta fase si cualquier parte del plan no cumple con los objetivos propuestos.

C. Simulación en Tiempo Real

Las pruebas de simulación real, en una Unidad Orgánica, a nivel de de alta jefatura en Pintopiga está dirigido a una situación de contingencia por un período de tiempo definido.

- Las pruebas se hacen en tiempo real.
- Son usadas para probar partes específicas del plan.
- Permiten probar las habilidades coordinativas y de trabajo en equipo de los grupos asignados para afrontar contingencias.

Comprobación de Plan de Contingencias

La prueba final debe ser una prueba integrada que involucre secciones múltiples e instituciones externas. La capacidad funcional del plan de contingencia radica en el hecho de que tan cerca se encuentren los resultados de la prueba con las metas planteadas.

El diagrama representa los pasos necesarios, para la ejecución de las pruebas del plan de contingencias.

8.2.4 Procedimiento

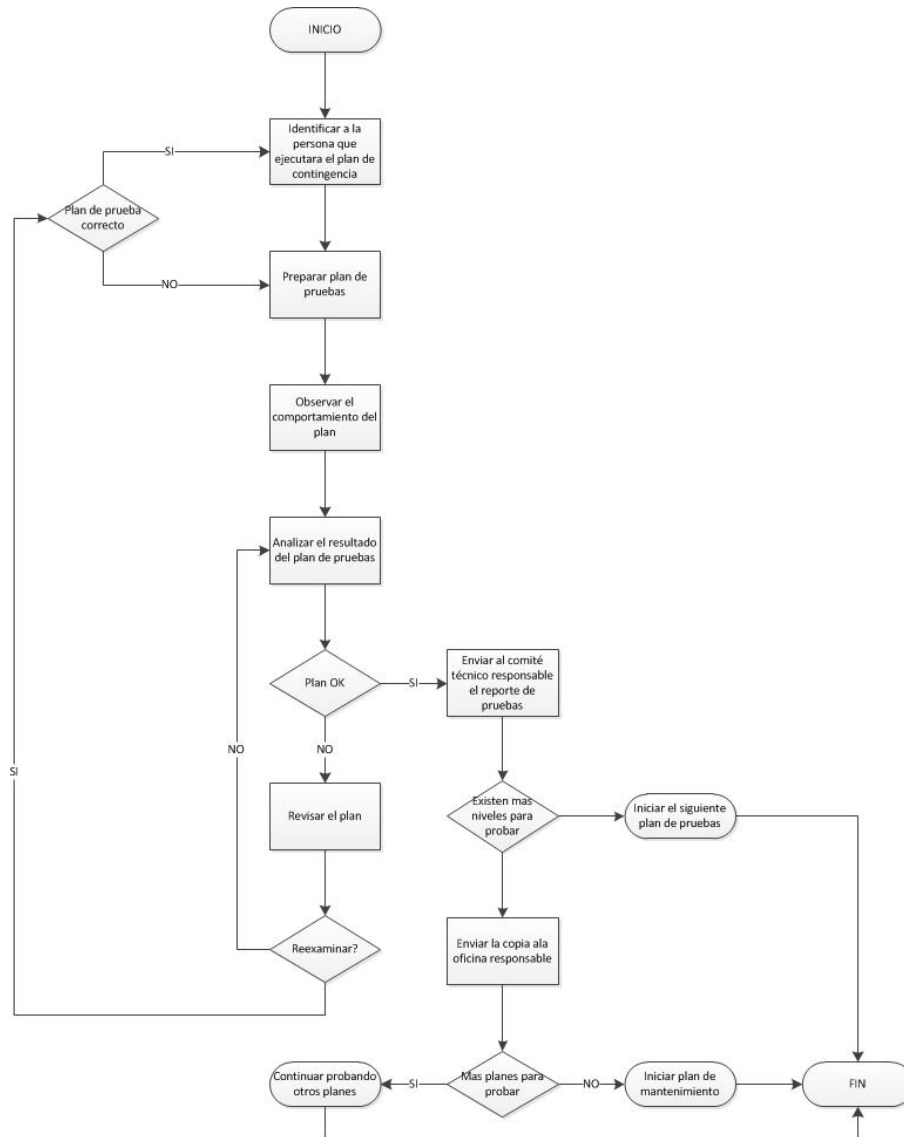


Ilustración 8 Plan de pruebas

9 Anexos

9.1 Aviso a persona responsable por el entrenamiento del plan

Sección del plan de contingencia cambiada	Resumen de cambios hechos	Fecha	Afecta los programas de entrenamiento	Se requiere re-entrenamiento (si/no)
COMENTARIOS:				
COMENTARIOS:				
COMENTARIOS:				
COMENTARIOS:				
COMPLETADO POR NOMBRE:			FECHA:	
REVISADO	POR NOMBRE:		FECHA:	

9.2 Control de Cambios al Plan

PLAN DE CONTINGENCIA	
Cambio Nro.	
Descripción del Cambio	
Justificación para el cambio	
Fecha en que se hace efectivo	
Alternativas consideradas o eliminadas	
Proceso(s) de la institución(es) impactadas	
Cronograma de Pruebas	
Entrenamiento Ajustado al cambio	
Solicitado por: Responsable del Plan NOMBRE: _____ FECHA ____/____/____ _____/____/____	FIRMA:
Aprobado por: NOMBRE: _____ CARGO _____ _____ FECHA ____/____/____	FIRMA:
COMPLETADO POR NOMBRE:	FECHA:
REVISADO POR NOMBRE:	FECHA:

9.3 Responsabilidad en el Mantenimiento de Cada Parte del Plan

CONTENIDO DEL PLAN	PERSONA	RESPONSABLE	DEL
	NOMBRE	POSICIÓN	
Inicio del proyecto			
Inicio de actividades			
Organización del proyecto			
Evaluación del riesgo			
Evaluación de incidentes y amenazas			
Evaluación de riesgos para Pintopiga			
Comunicaciones e IT			
Otros procedimientos de recuperación del desastre			
Sitios			
Preparación para una Posible Emergencia			
Estrategias de backup y recuperación			
Personal y proveedores claves			
Procedimientos y documentación Clave			
Fase de recuperación del desastre			
Planeación para manejar la emergencia			
Notificación			
Prueba			
Planeación de la prueba			
Dirección de la prueba			
Entrenamiento del personal			
Administración del programa de entrenamiento			
Evaluación del entrenamiento			
Mantenimiento del plan			
COMPLETADO POR NOMBRE:		FECHA:	
REVISADO POR NOMBRE:		FECHA:	

9.4 Estructura de red Actual

Una red de área local, red local o LAN (del inglés local area network) es la interconexión de una o varias computadoras y periféricos.

El actual esquema de conexión interna se puede identificar como “BUS”, lo cual se representa en el siguiente diagrama realizado con los datos obtenidos.

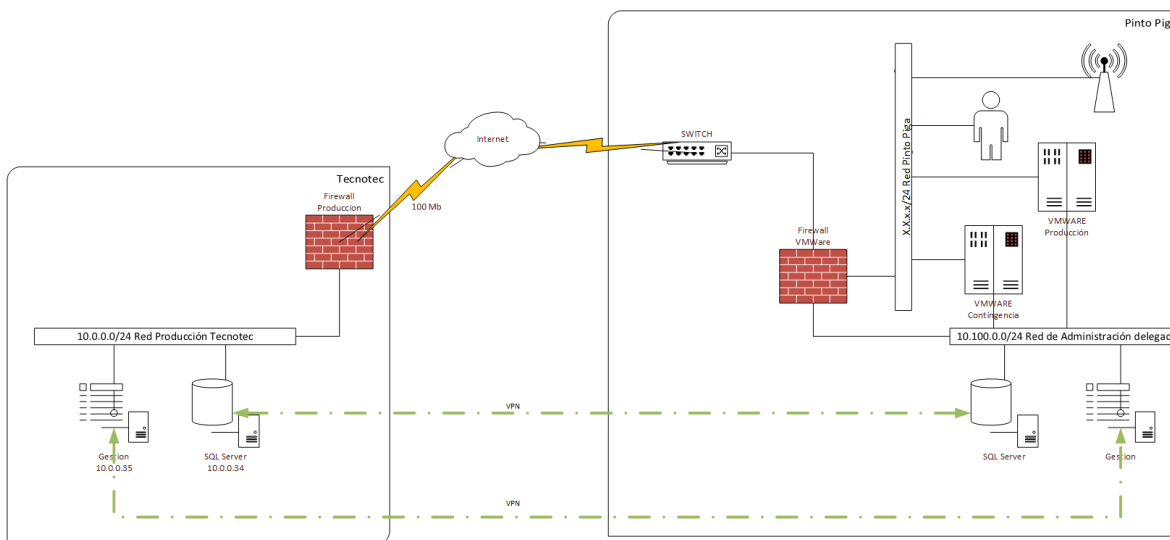


Ilustración 9 Esquema de topología encontrada

El mayor problema que se presenta es la administración de la red, la cual, como nos indica la ilustración 1, posee varios puntos de falla, siendo lo más recomendable en este caso una topología árbol, o potenciar la conexión inalámbrica de los distintos puntos de distribución.

La topología o estructura que se recomienda para la red cableada en las dependencias es la denominada “Arbol”, la que se explica a continuación:

La topología en árbol es una variante de la de estrella. Como en la estrella, los nodos del árbol están conectados a un concentrador central que controla el tráfico de la red. Sin embargo, no todos los dispositivos se conectan directamente al concentrador central.

9.4.1 Enlace Internet

La actual conexión a internet, correspondiente a un enlace dedicado de fibra mediante el proveedor de servicio "Movistar", posee una velocidad de 90/Mb, pero lamentablemente los tiempos de respuesta ante fallas no es lo más óptimo.

Se recomienda tener un enlace de internet de respaldo, de al menos 50M Nacional para un buen desempeño de las funciones que necesiten dicho acceso,

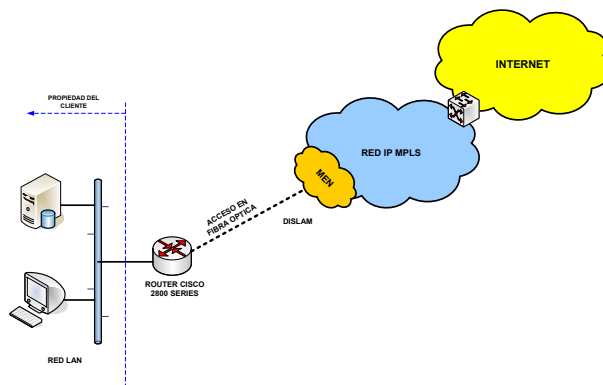


Ilustración 10 Esquema de conexión a internet (Movistar Generico)

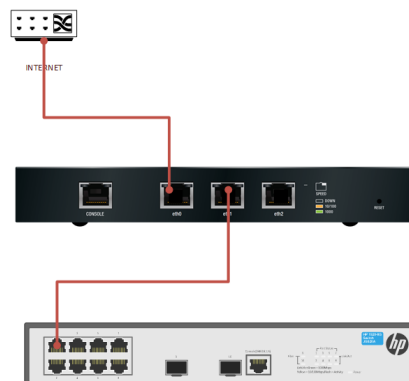


Ilustración 11 Conexión física enlace internet

9.5 Telefonía IP

Las mejoras anteriores dejan el camino preparado para la implementación de telefonía IP, la que, si bien en estos momentos dicha necesidad se encuentra cubierta por la actual central telefónica, se pueden ampliar los beneficios de dicho servicio por:

La implementación de Telefonía IP, debe contemplar al menos:

- Chequeo de las capacidades de la red física
- Compra de Servidor para central
- Instalación de central IP (Software)
- Compra, configuración e instalación de equipos telefónicos
- Compra, configuración e instalación de software de telefonía (SoftPhone)

9.6 Esquema actual

El actual diseño de Infraestructura TI, se divide en dos partes; Infraestructura externalizada e Infraestructura Interna.

En estos momentos, la infraestructura cuenta con servidores Windows y Linux, los cuales se utiliza como nodos independientes. La recomendación general es potenciar esta arquitectura, mejorando el actual pool de servidores, ya que físicamente se necesita aumentar la capacidad de almacenamiento y la redundancia de sus componentes, como fuentes de poder o conexión de red.

9.6.1 Servicio de Correo Electrónico

El servicio se encuentra externalizado.

9.6.2 Seguridad de la información

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

9.6.3 Respaldo de Información

La información constituye el activo más importante de la organización, pudiendo verse afectada por muchos factores tales como robos, incendios, fallas de disco, virus u otros. Desde el punto de vista de la empresa, uno de los problemas más importantes que debe resolver es la protección permanente de su información crítica.

La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups: Este debe incluir copias de seguridad completa (los datos son almacenados en su totalidad la primera vez) y copias de seguridad incrementales (sólo se copian los ficheros creados o modificados desde el último backup). Es vital para la organización elaborar un plan de backup en función del volumen de información generada y la cantidad de equipos críticos.

Un buen sistema de respaldo debe contar con ciertas características indispensables:

- Continuo
 - El respaldo de datos debe ser completamente automático y continuo. Debe funcionar de forma transparente, sin intervenir en las tareas que se encuentra realizando el usuario.
- Seguro

- Muchos softwares de respaldo incluyen cifrado de datos (128-2048 bits), lo cual debe ser hecho localmente en el equipo antes del envío de la información.
- Remoto
 - Los datos deben quedar alojados en dependencias alejadas de la empresa.
- Mantención de versiones anteriores de los datos
 - Se debe contar con un sistema que permita la recuperación de versiones diarias, semanales y mensuales de los datos.

La mayoría de los sistemas modernos de respaldo de información online cuentan con las máximas medidas de seguridad y disponibilidad de datos. Estos sistemas permiten a las empresas crecer en volumen de información sin tener que estar preocupados de aumentar su dotación física de servidores y sistemas de almacenamiento.

En cuanto al caso particular de Pintopiga, es recomendable seguir con el esquema actual, el cual es mantener un respaldo centralizado en la sala de servidores (para tener una mejor velocidad de recuperación en caso de alguna emergencia), y un segundo respaldo fuera de las dependencias.

El plan de respaldo es según lo siguiente:

A. Carpetas compartidas

- a) Servidor de respaldo realiza una copia de los archivos modificados durante el día, archivos que quedan almacenados en QNAP de RespalDOS
- b) Posteriormente se realiza una copia de esa carpeta fuera de las dependencias de Pintopiga, específicamente a Tecnotec.
- c) Este proceso es diario y automático

B. Bases de Datos

- a) Servidor de Bases de datos realiza un respaldo diario a una carpeta compartida.
- b) Servidor de respaldos realiza una copia de archivo generado por servidor de DB.
- c) Posteriormente se realiza una copia de esa carpeta fuera de las dependencias de Pintopiga, específicamente a Tecnotec.
- d) Este proceso es diario y automático

9.6.4 Filtro de contenido

Con el fin de mejorar la calidad de navegación y además agregar una capa adicional de seguridad, se implementó un filtro de contenido, el cual posee además un antivirus que analiza las paginas visitadas.

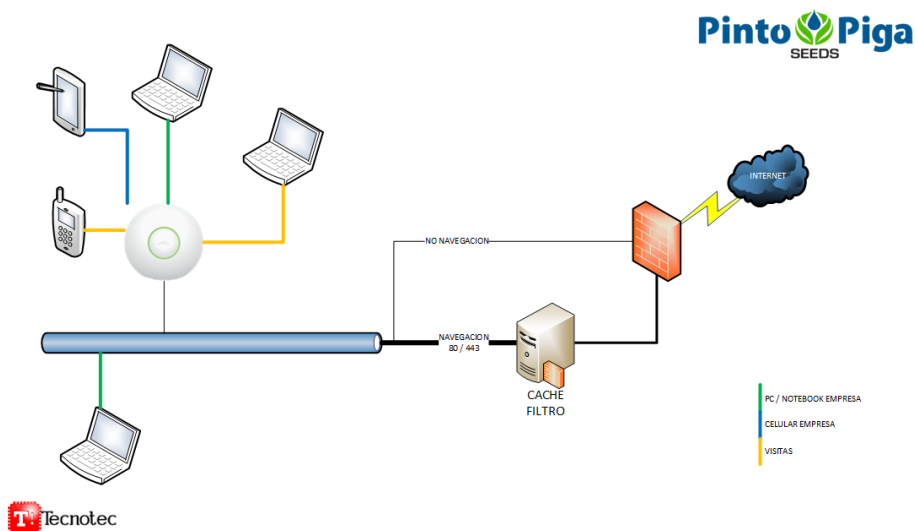


Ilustración 12 Esquema filtro contenido

Información Documento	Creación	Aprobación
Versión 8 Fecha VB 06-10-2020 14:53 CC 29868	Luis Soto Jefe Servicios TI lsoto@tecnotec.cl	Francisco Javier Verni Rep. Legal Tecnotec francisco@tecnotec.cl