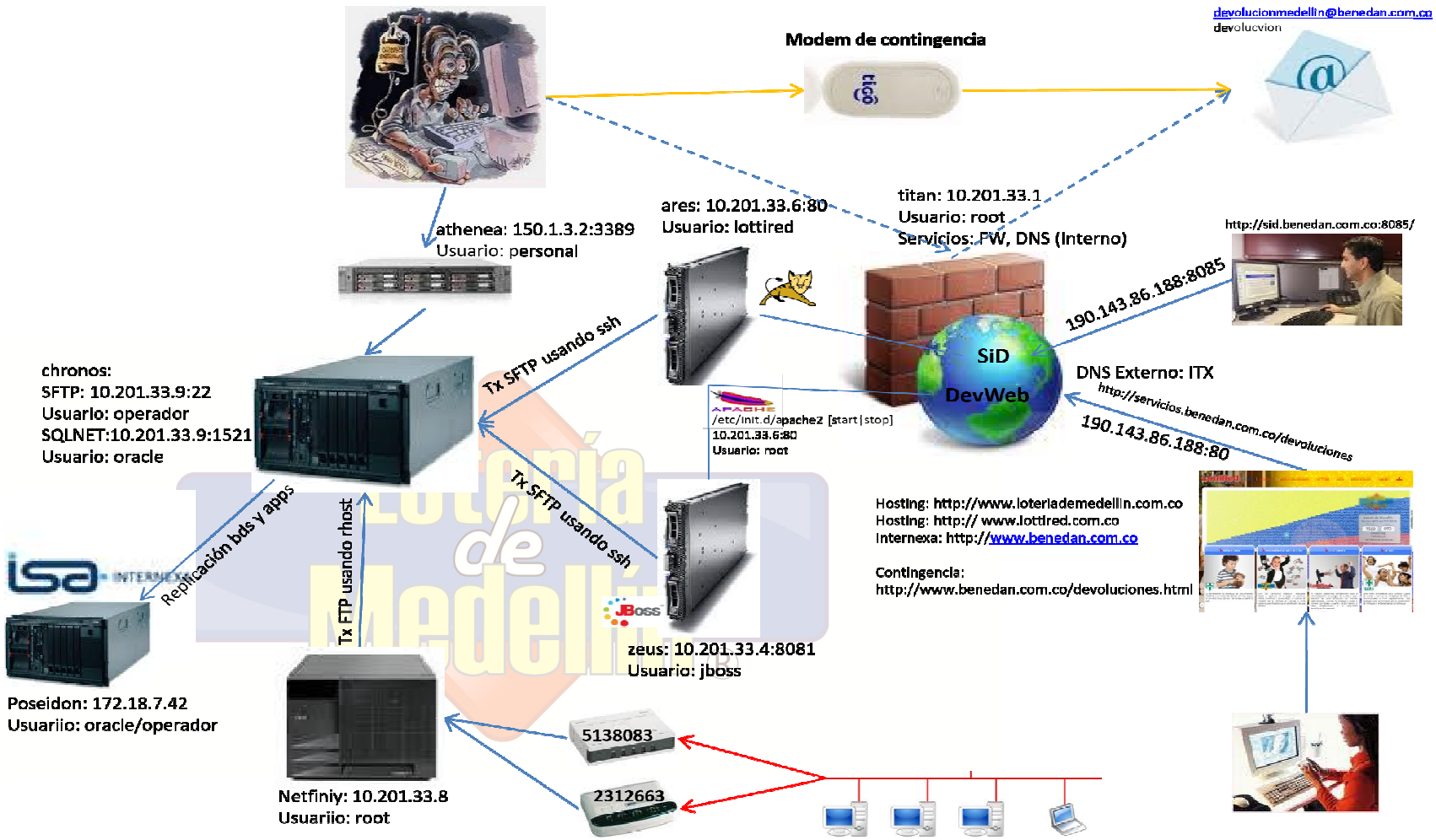
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

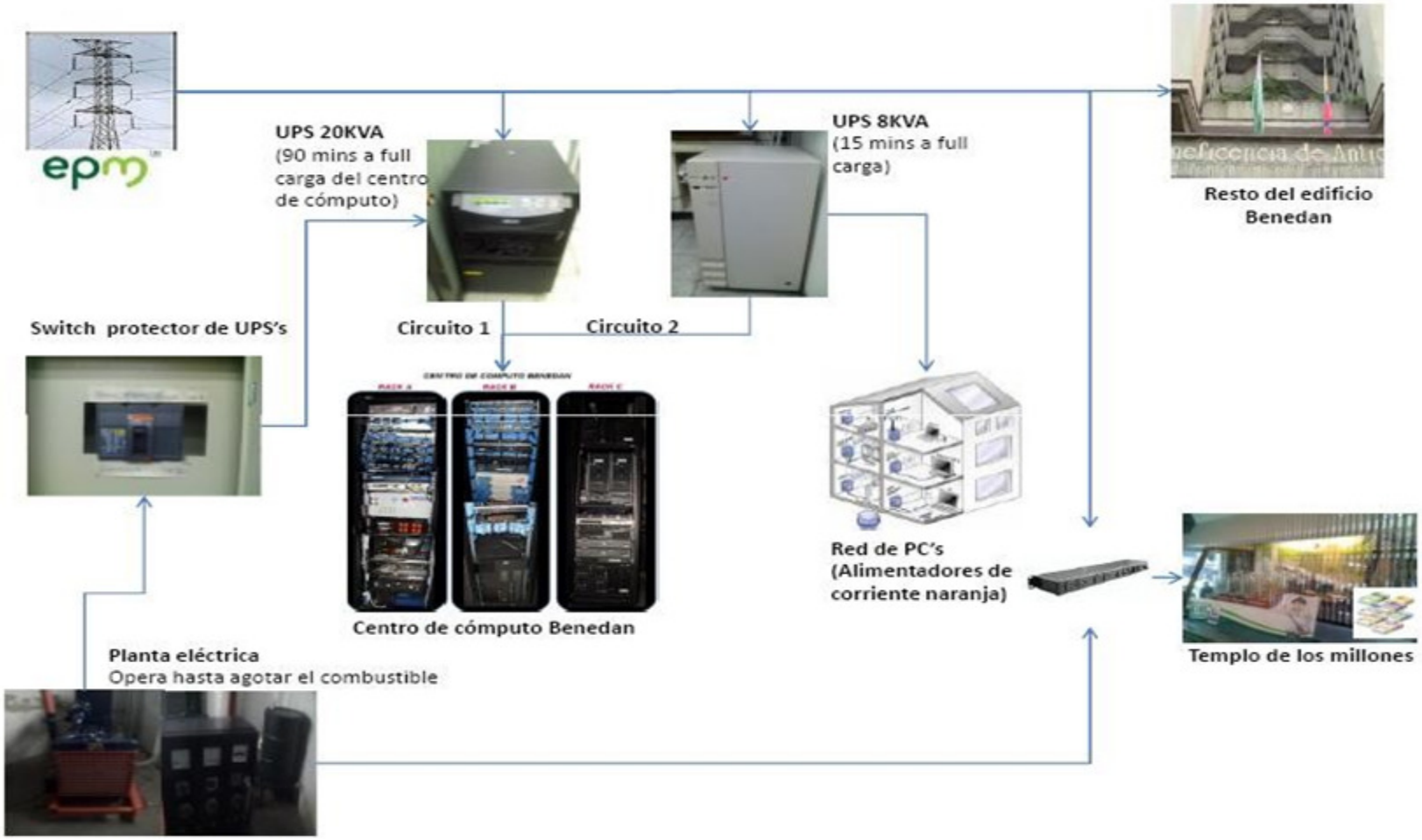
2019

LOTERÍA DE MEDELLÍN

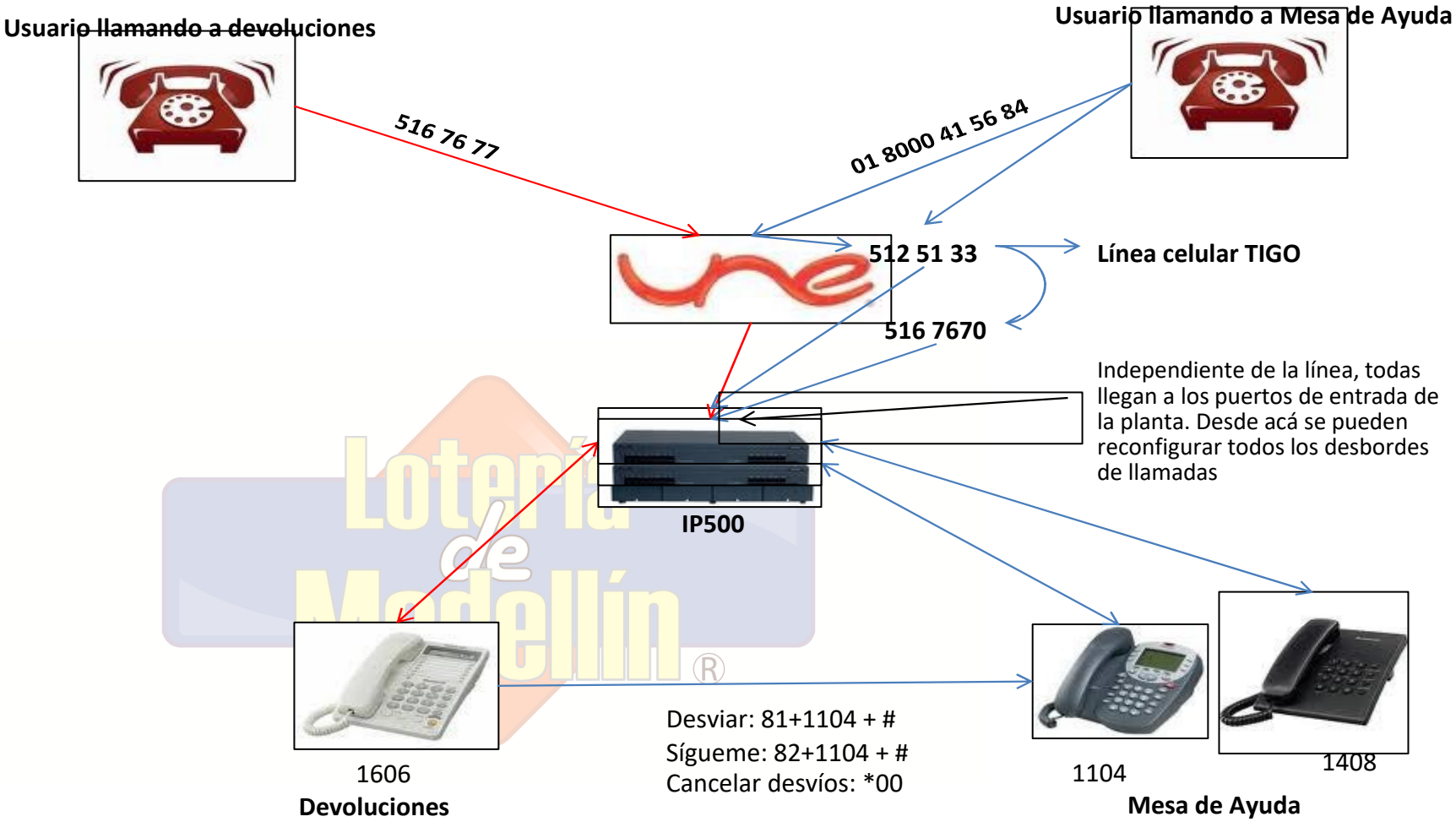
SOLUCIÓN DE DEVOLUCIÓN ACTUAL



SISTEMA ELÉCTRICO



COMUNICACIONES DE VOZ



¿QUÉ PODRÍA FALLAR?

(En orden de impacto e importancia)

1. Falla en el Fluido eléctrico
2. Falla en las Telecomunicaciones Internas y Externas(LAN/WLAN)
3. Falla grave en equipos de cómputo (Hardware)
4. Falla en Servicios específicos
5. Falla en Comunicaciones de Voz

1. FALLA EN EL FLUIDO ELÉCTRICO

A. Falla en el fluido eléctrico de EPM

En caso de falla del fluido electrico de EPM y todo lo demás funciona, no pasa nada dado que existe una planta electrica con capacidad de abastecimiento para el fluido eléctrico del tempo de los millones, el centro de computo y los puntos de conexión de poder que disponen de voltaje regulado (conexiones de poder naranja).

B. Falla en la Planta eléctrica

- Si hay fluido eléctrico de EPM, no sucede nada.
- Si no hay fluido de EPM y las UPS's están operativas, se dispone de hasta 90 minutos de operación con UPS

C. Falla en la UPS Principal

- Si todo lo anterior ha fallado y falla también la UPS principal, sólo quedan 10 minutos de operación. Debe procederse a cerrar y bajar sistemas.

D. Falla en la UPS Secundaria

Si se ha dado I,II,III y IV, debe validarse tiempos de recuperación y de acuerdo con esto se reciba, por escrito, la autorización de Gerencia para activar sitio alterno. PROCEDIMIENTO C01.

2. FALLA EN LAS TELECOMUNICACIONES

A. Falla en Telecomunicaciones Internas

Se debe reemplazar el componente por uno de menor criticidad, por ejemplo, un switch de otro piso o en otra ubicación. En última instancia, comunicar los servidores directamente, particularmente

athenea y el Blade S, en su interfaz de servicio. Por estar ambos servidores en la misma subred, tendrán visibilidad el uno sobre el otro sin necesidad de cambios en la configuración lógica.

B. Falla en Telecomunicaciones Externas (Navegación y Exposición de servicios)

- ***Falla en el enlace de exposición de servicios (Telmex):*** Deben direccionarse los servicios al enlace de navegación(Internexa). Si no se cuenta con suficiente tiempo para cambiar el DNS externo (PROCEDIMIENTO C02), debe utilizarse la resolución servicios2.benedan.com.co la cual direcciona en todo momento a el enlace de Internet de Internexa (Navegación).

- ***Falla en enlace de Navegación (Internexa):*** Cambiar redireccionamiento por defecto de navegación a enlace de Telmex. (PROCEDIMIENTO C03)

- ***Falla en enlaces de exposición de servicios y navegación (Telmex e Internexa):*** Dado que todos los servicio expuestos en Internet estarán por fuera, la devolución debe realizarse por modem GPRS y con envío de archivos por parte de los distribuidores al correo electrónico devolucionmedellin@benedan.com.co. Para conectarse al email, debe utilizarse el Internet móvil que está dispuesto en el servidor athenea del Centro de Cómputo.

C. Falla en Telecomunicaciones Externas (Servicios transaccionales)

Ante una falla en las comunicaciones externas que afecten los servicios transaccionales, deben solicitarse a Internexa la activación del enlace de contingencia de Internet (512kbps) de última milla. Con esta solicitud, el tráfico es reenrutado por otro enlace, teniendo continuidad de servicio. Ante la falla de este mecanismo, debe solicitarse a los end-point de las VPN el cambio de la dirección de origen de Benedan y reiniciar las conexiones VPN. En última instancia,

activar transacciones por Internet, dado que la información intercambiada con las terminales, es cifrada.

Si la falla es masiva en todo el centro de cómputo de Benedan, a la fecha no hay contingencia para dar continuidad inmediata a los servicios transaccionales. Debe solicitarse a Internexa conexión a Internet desde el servidor de Sitio Alterno y habilitar todos los servicios transaccionales en dicha ubicación. No obstante, ante esta circunstancia y dados los costos de la numeración que posee Benedan y la comercializadora, la decisión del proceder debe ser emitida por la Gerencia.

3. FALLA GRAVE EN EQUIPOS DE CÓMPUTO

A. Falla en Servidor de Base de Datos Chronos y Hércules

Es la falla más grave que puede ocurrir a nivel de servidores. Debe buscarse la recuperación inmediata dado que la base de datos sicof es fundamental para la operación de Lottired y la devolución de billetería. Hay varias alternativas de solución:

- De ser posible activar la devolución en el ambiente de pruebas. Se debe reconfigurar todas las aplicaciones de devolución, cambiando el acceso a datos.
- Si el problema es del servidor (la cuchilla) puede apagarse otro servidor (una cuchilla como Ares), remover la cuchilla chronos y activar en su lugar ares. Debe verificarse que la cuchilla tenga la tarjeta de compatibilidad SAS. Se recomienda en extremo realizar estas actividades en compañía de personal experto en base de datos y la tecnología IBM que se dispone.
- Si el problema es degradación de la bd por ejemplo y almacenamiento se puede reutilizar, se puede restaurar el backup RMAN de la bd (si se dispone de tiempo y recuperar de sitio alterno los últimos archives).

- Si por cuestiones de tiempo y/o conocimiento no se puede hacer nada de esto, con constancias, solicitar la orden de Gerencia para activar sitio alterno. **En Hércules**
- Una falla en este servidor afectaría la devolución por el SiD. Se requiere solicitar a los distribuidores que usan este sistema devolver por el sistema tradicional (previa activación de usuario) o que envíen la devolución a devolucionmedellin@benedan.com.co para ser cargada por el ingeniero a través de los otros sistemas.

B. Falla en el Servidor de devolución por Modem Netfinity

Este servidor no dispone de redundancia, en un momento determinado la alternativa puede ser conectar a alguna de las líneas telefónicas de devolución, un PC con modem y activar el programa hiperterminal en modo de recepción de archivos para posteriormente cargarlos por cualquiera de los sistemas de devolución disponibles.

C. Falla en el Servidor Firewall

Esta falla afecta de manera directa la conexión de Benedan con internet, interrumpiendo la navegación en Internet y la exposición de los servicios, afecta además servicios como DNS, DHCP, PROXY, ROUTER y VPN (Usuarios externos y proveedores (FULLCARGA, COMCEL)).

Si la falla llegase a ocurrir durante el proceso de devolución, debe recurrirse a que los usuarios con acceso internet hagan las devoluciones a devolucionmedellin@benedan.com.co para proceder luego con la carga a través del sistema de devolución tradicional, el SiD, modem o la ubicación de archivos para el script de Standard System devolucion.sh.

D. Falla en el Servidor de Aplicaciones Ares

Una falla en este servidor durante el proceso de devolución de lotería, afecta la exposición del servicio de devolución en Internet https://servicios.benedan.com.co/devoluciones y la devolución por el SiD. Lo primero obedece a que esta devolución utiliza el servidor apache de ares para redireccionar los requerimientos a http://10.201.33.4:8081/devoluciones, servicio que no está expuesto directamente en internet; lo segundo, a que en ares se encuentra desplegada la aplicación SiD.

E. Falla en Servidor de Aplicaciones Zeus

Una falla en este servidor durante el proceso de devolución de lotería, afecta la exposición del servicio de devolución en Internet https://servicios.benedan.com.co/devoluciones y la venta electrónica. Una alternativa de solución es activar en el servidor ares óurano un despliegue del jboss de la devolución y adicionarle al servidor una segunda interfaz con la IP de Zeus o exponer el puerto en Internet ó cambiar la configuración de apache para reenrutar a la nueva configuración. Se debe considerar todos los cambios requeridos de estructura de archivos y usuarios para que la operación se logre de forma transparente.

F. Falla en servidor de Aplicaciones Athenea

Ante una falla en el servidor de athenea, se recomienda utilizar hera como configuración de contingencia habilitando el TNSNAMES.ora para direccionar a producción. Se debe tener en cuenta que si se está haciendo alguna prueba de funcionalidad nueva que involucre una librería, ésta debe devolverse a la versión de producción para tener total compatibilidad de ambientes. En caso contrario, activar la máquina virtual de athenea verificando previamente su última actualización y el usuario/contraseña para ingresar.

Alternativamente se puede utilizar el servidor atheneabk, instalado en el sitio alterno. Dado que el enlace de comunicaciones es el mismo para la replicación, podrían tenerse latencias por la concurrencia de datos en el enlace.

G. Falla en equipos de telecomunicaciones

- ***Falla en Telecomunicaciones Internas:*** Se debe reemplazar el componente por uno de menor criticidad, por ejemplo, un swiche de otro piso o en otra ubicación. En última instancia, comunicar los equipos directamente (athenea/chronos).

- ***Falla en todas las Telecomunicaciones Externas:***Dado que todos los servicio expuestos en Internet estarán por fuera, la devolución debe realizarse por modem y con envío al correo electrónico devolucionmedellin@benedan.com.co. Para conectarse al email, debe utilizarse el Internet móvil.

4. FALLA EN LOS PRINCIPALES SERVICIOS

Para el proceso de devolución de lotería, las estadísticas de devolución por los diferentes medios habilitados son los siguientes:

- Sistema de devolución Web Integrado al SiD (7.5%) (PROCEDIMIENTO C05)
- Sistema de devolución Web Tradicional (75%) (PROCEDIMIENTO C06)
- Sistema de devolución por Modem: Líneas 2312663 y 5138083 (17%)
- Devolución por Email (0.5%)

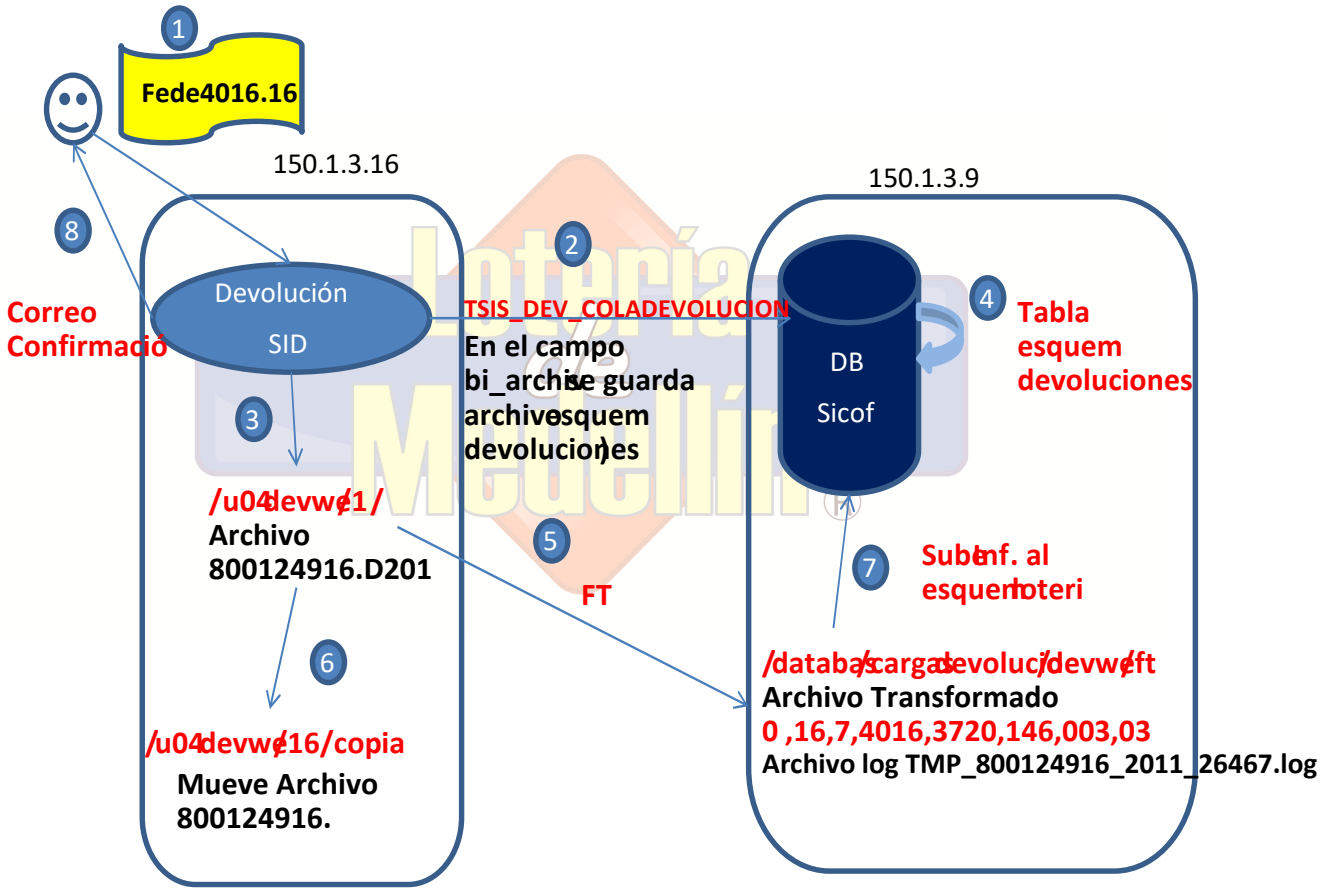
Estos servicios para su normal operación requieren otros como:

- DHCP (PROCEDIMIENTO C08)
- DNS (PROCEDIMIENTO C02)

- PROXY (PROCEDIMIENTO C09)
  - PÁGINA WEB DE BENEDAN (Proveedor contrato mtto Web)
  - OTROS SERVICIOS (PROCEDIMIENTO C10)

Por su alta criticidad, a continuación se detalla el funcionamiento del sistema de devoluciones.

DEVOLUCIÓN POR EL SID



Este ejemplo es con la devolución por el SID, la devolución por el sistema anterior funciona igual

5. FALLA EN LAS COMUNICACIONES DE VOZ

En caso de una falla grave en las comunicaciones de voz, el componente afectado sería puntualmente la planta telefónica. En cuyo caso, debo optarse por contestar las llamadas directamente desde el centro de cómputo, en las conexiones marcadas como líneas de entrada. De no disponer de esta capacidad, aprovechar el conocimiento que tienen los distribuidores del número de mesa de ayuda y solicitar a UNE el desborde de llamadas a otra línea. Para esto se requiere la autorización verbal ante UNE del Director Administrativo de Benedan. Mientras esto se realiza, también se puede aprovechar el conocimiento que tienen los distribuidores del número celular de mesa de ayuda LottiRed. Cabe precisar el contrato con el proveedor de la planta telefónica incluye cambios de partes defectuosas o activación de configuraciones alternas, por lo que se debe trabajar en conjunto con el proveedor, para recuperar el servicio tan pronto como sea posible.

ALGUNAS CONSIDERACIONES

- Ante nada, Informática es un equipo de trabajo y ante una falla grave, los ingenieros no deben quedarse solos con los problemas. Deben ser escalados y de ser requerido, recurrir a otros miembros del equipo para apoyar en el proceso.
- En cada proceso de devolución de lotería, se juega un monto de dinero lo suficientemente considerable para recurrir a cualquier medio o recurso para superar los percances.
- En una circunstancia de gravedad, no se deben desgastar esfuerzos en llamar a alguien, soliciten a otros que los apoyen en dichas actividades
- La devolución de lotería tiene prioridad sobre cualquier otro proceso de operación de la empresa
- Disponer siempre actualizado y en un lugar asequible, la lista de proveedores y personal de apoyo de informática.

- Para minimizar las probabilidades de que un evento ocurra, se han realizado inversiones en infraestructura con alta tecnología; datacenter, equipos de venta, seguridad integral, entre otros.