Operadores aislados o en red

El monitoreo en red: características, problemas y soluciones - 2º parte.

En el concepto tradicional de la central de monitoreo, el operador está anclado a una LAN en una PC. En la actualidad, el operador tiene la libertad de operar los eventos desde cualquier lugar con una notebook conectada a Internet. Ni siquiera requiere un software específico, sino que basta con acceder a servidores en la nube.

Ing. Modesto Miguez CPP
modesto@monitoreo.com.ar

La seguridad abarca múltiples matices y no es un tema menor. En el servicio de monitoreo, por ejemplo, el receptor es uno de los puntos clave. Sin embargo, antes de hablar de la seguridad del receptor, tendríamos que hablar de la confiabilidad de la recepción.

Trabajando en seguridad, tratamos de tomar todos los recaudos para evitar que pueda suceder alguna de las siguientes dos cosas:

- Que un evento generado por el panel de un abonado no llegue al sistema.
- Que un evento llegue erróneo, o sea, que provenga de otro abonado al que por error le cambiaron su número identificatorio por otro ya existente.

Sabemos que la seguridad máxima que puede ofrecer un sistema de elementos en serie será siempre inferior a la del componente más débil. A su vez, cada componente tiene diferentes causas por las que puede fallar.

En función de la experiencia obtenida en 17 años, desde la instalación del primer receptor/repetidor por Internet en 1997 en la ciudad de Córdoba, realizaremos un listado de los puntos más débiles de la recepción de señales.

¿QUÉ PUEDE PASAR?

QUE SE CORTE LA CONEXIÓN A INTERNET

Las conexiones hogareñas no garantizan la continuidad del servicio. En lugares alejados, los amplificadores de la red de cable se apagan ante cortes de luz generales. De la misma manera, la permanente expansión de la red IP motiva a las empresas a suspender el servicio cuando hacen ampliaciones y reconfiguran sus redes. Por otro lado, devolver el servicio a los usuarios no parece ser una prioridad para las empresas prestadoras; lo compensan con un call center en donde tienen gente adiestrada para decir "¿Probó resetear su computadora?", "Por favor apague y prenda el módem" o "Le tomo su reclamo y pasará un técnico por su domicilio".

Las fallas en una conexión a Internet se dan, principalmente, cuando se realizan instalaciones sin control ni certificación, con conexiones mal hechas o dispositivos mal configurados

En el mismo sentido, cuando se utiliza un enlace asimétrico por cable módem o ADSL, la disponibilidad de ancho de banda varía. El total disponible se distribuye entre todos los conectados; en los horarios de consumo pico, la calidad baja para todos los usuarios.

Las causas más frecuentes de fallas surgen de instalaciones de redes internas no certificadas ni controladas: falsos contactos, cables y fichas de baja calidad, routers y switchers mal configurados, usuarios de la red interna sin controlar (que ocupan todo el ancho de banda disponible), máquinas con virus que se conectan involuntariamente a servidores hackeados, entre otros.

Lamentablemente, aún hay técnicos que improvisan y muchos no saben instalar ni configurar correctamente una red IP. Esto se resolverá a medida que la capacitación surta efecto. En cuanto a las empresas proveedoras, la conectividad a Internet es un servicio relativamente nuevo y aún no hay suficiente competencia ni antigüedad para que la gente conozca y pueda exigir y elegir. Las empresas están invirtiendo en captar clientes y cuando esta etapa de crecimiento merme, serán ellas mismas quienes mejoren los servicios. Por lo tanto, este problema debería resolverse sin nuestra intervención.

QUE EL RECEPTOR SE DESCONECTE

Similar al punto anterior, ciertas fallas en la instalación (como la falta de una adecuada puesta a tierra) baten el récord de todas las causas. Le siguen los cables telefónicos aéreos mal instalados, empalmes con falsos contactos, sulfatados, tomas sin estar correctamente sujetas, cables UTP de mala calidad o con falsos contactos, tomas del receptor provisorias, etc.

Otra causa es la falta de restricciones para el acceso al recinto del receptor, cuya desconexión puede poner en riesgo la seguridad de muchos abonados. Los sabotajes son posibles, pero aún no ocupan una tasa considerable en la lista de causas; la evolución de la delincuencia aún no llegó a este punto. Sin embargo, sabemos que, lamentablemente, la inteligencia delictiva aumenta y, con ella, también lo hace el riesgo para los abonados.

QUE EL RECEPTOR SE QUEDE SIN ENERGÍA

Para los viejos esquemas de estación central de monitoreo aislada, la norma prevé que debe disponerse de una UPS con 20 minutos de autonomía y un grupo generador que debe entrar en servicio antes de los 20 minutos de producido el corte de energía. En la práctica, se observa en estos esquemas lo siguiente:

1. La autonomía de las baterías disminuye a medida que envejecen y antes de los dos años de vida no alcanzan a abastecer durante los 20 minutos requeridos.
2. Las UPS más comunes (los que se venden en casas de informática) no soportan la variación de tensión y frecuencia del grupo generador, se desenganchan y no funcionan.
3. Si el generador no tiene el man-

tenimiento apropiado o no es probado con una metodología y frecuencia preestablecida, es muy probable que cuando se lo necesite no encienda o no tenga combustible suficiente.

QUE EL RECEPTOR SE DAÑE

Todo aparato puede dañarse, pero si está fabricado según estándares de calidad reconocidos, está suficientemente probado y la puesta a tierra está correctamente conectada, la posibilidad de que se rompa es muy baja. De todos modos, como el receptor puede fallar, no basta con tener uno de repuesto; el operador también debe contar con las herramientas y los conocimientos necesarios para hacer el reemplazo. Sin embargo, el mayor problema no es saber hacer el reemplazo sino darse cuenta de que hay un problema en el receptor.

Obviamente que los receptores standalone dedicados son mucho más confiables que las placas instaladas en PCs. No porque las placas sean malas sino porque las PCs tienen sistemas operativos que pueden colgarse.

QUE LAS LÍNEAS TELEFÓNICAS ESTÉN OCUPADAS

Cuando una línea telefónica está en corto o da ocupado puede ser un problema de saturación, debido, básicamente, a paneles mal programados, que funcionan mal, o a abonados que se dan de baja y, por distintos factores, no pueden ser desprogramados. Hay distintas soluciones que pueden adoptarse para superar estos problemas. Para evitar la saturación, por ejemplo, pueden programarse reportes de test cada de 24 horas, 72 horas, una semana o 30 días de acuerdo al nivel de servicio contratado.

Los cortes de luz producen congestión de eventos cuando no se programan los paneles con diferentes demoras. Esta función de delay respecto del evento "restauración de corte de luz" no la tienen muchos paneles y la congestión se produce cuando la energía regresa en una zona con una gran cantidad de abonados ubicados en ella.

Cuando las líneas telefónicas no funcionan l as principales causas son el robo de cables o el corte de un troncal, hecho que se da, por ejemplo, cuando se realiza una obra en la vía pública

Una buena práctica consiste en no permitir que los técnicos ingresen a la programación de los paneles desde los domicilios y hagan pruebas para ver cómo funcionan. Cada marca y modelo de alarma tiene una configuración óptima para cada aplicación y esta es la que integrará el servicio contratado con el abonado. Salvo que haya una modificación, no se justifica ingresar en la programación del panel bajo ningún concepto.

Por último, para evitar la saturación deben instalarse suficientes líneas de recepción, las cuales deben ser cabeceras de rotativas. Además, debe llevarse un control frecuente de la ocupación a medida que la cantidad de abonados aumenta.

QUE LAS LÍNEAS TELEFÓNICAS NO FUNCIONEN

Puede ocurrir cuando en la vía pública se realizan trabajos, excavaciones o se cortan cables troncales. En los países latinoamericanos no hay compañías alternativas que brinden telefonía básica, ya que ésta llegó a su techo e incluso se está dando de baja, convirtiéndose a IP.

Otro riesgo consiste en el robo de cables o la falla de un acceso troncal. En un esquema de estación de monitoreo convencional, cuando se produce el robo de cables telefónicos o la falla de un troncal, la falla es simultánea tanto para la línea principal como para las de backup, impidiendo la comunicación entre el panel del abonado y la empresa de monitoreo. Para evitarlo, la única solución radica en colocar receptores en diferentes sitios con diferentes compañías telefónicas, donde las llamadas, tanto para la cabecera como para el backup, se canalicen por cables troncales distintos.

QUE HAYA QUE EVACUAR EL EDIFICIO

Aunque se tengan suficientes líneas de receptores standalone de marcas reconocidas, en una contingencia grave e imprevista que implique evacuar el edificio, como una fuga de gas, incendio, inundación, terremoto, vandalismo o atentado de bomba, por más que se disponga de gran cantidad de receptores, el servicio no se brindará.

La solución a este riesgo es simple: una vez creada la red de receptores, se debe elegir, para cada abonado, los dos receptores autónomos más cercanos, pero independientes, en dos sitios distintos con compañías telefónicas y redes diferentes, uno como principal y otro como backup. El riesgo puede expresarse como un número que indica la probabilidad de ocurrencia de una catástrofe. Digamos que un lugar tiene una probabilidad de ocurrencia de 1 en 10.000 = 0,01%. Que haya dos contingencias graves y simultáneas en dos lugares independientes es la multiplicación de ambas probabilidades (Pa x Pb), o sea de 1 en 100.000.000 = 0,000001%. De la misma manera, otro beneficio de compartir recursos es que todos los miembros utilizan la misma red al mismo costo que el de tener un solo receptor.

Amar una red de receptores para una única empresa resulta inconveniente y hasta imposible de mantener. Por eso es que las empresas pequeñas corren más riesgos que las grandes y si no se agrupan en redes: simplemente dejarán de ser competitivas o incluso de existir. ■