

Municipio de Guadalupe, Nuevo León, México



Proporcionar Control y Protección de Datos con Soluciones de Symantec

En 2006, cuando Gabriel Navarro ocupó el puesto de jefe del Departamento de TI del Municipio de Guadalupe, sabía que sólo tenía tres años para modernizar completamente la infraestructura de software y hardware, y proteger la red contra las amenazas a la seguridad. Las soluciones de Symantec permitieron al equipo de TI proteger la red, reduciendo el tiempo que empleaba en corregir los programas maliciosos en más de un 99%. Además, pudo controlar el uso de Internet y mensajería instantánea de los empleados, redujo el spam en un 71% y proporcionó copias de respaldo confiables para proteger los datos fundamentales del municipio.

Suburbio de la “Sultana”

Fundada en 1716, Guadalupe es una ciudad de más de 600.000 habitantes en el norteño estado mexicano de Nuevo León. Es un suburbio de Monterrey, la capital de Nuevo León, a veces denominada Sultana del Norte, ya que representa el centro comercial e industrial de la nación, y es una de las regiones más tecnológicamente avanzadas de México. Como corresponde a esta posición, varias municipios del área metropolitana de Monterrey están trabajando para actualizar su tecnología, a fin de seguir el ritmo de la época y afrontar amenazas a la seguridad cada vez mayores, según Gabriel Navarro, director de TI para el Municipio de Guadalupe.

Navarro ocupó el puesto en noviembre de 2006, sabiendo que la actualización de los sistemas de Guadalupe sería como una carrera contra el tiempo, ya que los cargos administrativos allí duraban sólo tres años. Navarro se dio cuenta de que el trabajo estaba hecho justo para él. “La tecnología de la Municipio era vieja”, dice. “Tenían una HP 3000 con una base de datos Image. Las aplicaciones también tenían más de 15 años de antigüedad. La idea era modificarlo todo, implementar nuevo software y hardware, y obtener protección contra intrusos, tanto dentro como fuera”.

De Cinco Virus Por Semana a Uno Cada Seis Semanas

Para fortalecer la seguridad de los sistemas de Guadalupe, el Municipio implementó Symantec™ Endpoint Protection en noviembre de 2007. Este software tuvo un efecto inmediato y considerable. “Antes, teníamos que luchar contra cinco virus por semana”, afirma Navarro. “Era realmente una complicación. Ahora, esto ocurre con muy poca frecuencia, quizás, una vez cada seis semanas”.

La nueva solución ha ahorrado mucho tiempo al equipo de TI del Municipio, formado por 15 personas, lo que les permite trabajar en otros proyectos, comenta. “Para eliminar los virus, se necesitaban entre dos o tres personas ocho horas al día”, dice. “Tenían que ingresar en todos los equipos infectados para eliminar el problema”. Con Endpoint

PERFIL DE LA ORGANIZACIÓN

Guadalupe (www.guadalupe.gob.mx) es una ciudad de más de 600.000 habitantes y un suburbio de Monterrey, la capital del estado del norte mexicano Nuevo León. Esta región es un centro comercial, industrial y tecnológico, y la ciudad de Monterrey es conocida como la “Sultana del Norte”. El Municipio de Guadalupe tiene alrededor de 4.000 empleados, 800 usuarios de equipos y un equipo de TI formado por 15 personas.

SECTOR

Gobierno

SOLUCIÓN

Seguridad de los endpoints, seguridad de mensajería, copia de respaldo y recuperación

“Teníamos que luchar contra cinco virus por semana. Ahora, esto ocurre con muy poca frecuencia, quizás, una vez cada seis semanas.”

Gabriel Navarro

Director de TI

Municipality of Guadalupe

Symantec Endpoint Protection redujo las interrupciones de programas maliciosos de cinco a la semana a una cada seis semanas.

Protection, comenta, se necesitan una o dos personas durante aproximadamente media hora para combatir los virus que ahora son muy poco frecuentes. “Podemos detectarlos y, en muchos casos, luchar contra ellos mediante la red”, afirma.

Endpoint Protection también permite a Navarro aplicar políticas estrictas respecto al uso de Internet por parte de los empleados. “Queremos que utilicen Internet para realizar sus trabajos, no para buscar cosas ni hablar por chat”, comenta. “Endpoint Protection brinda ese control para limitar el acceso a Internet”.

Gracias a controles mayores, menos interrupciones y cargas de trabajo más sencillas para el personal de TI, estima que en un año se recuperará la inversión en Endpoint Protection.

El Spam Requiere Hasta 20 Horas por Semana

Otro gran desafío para el equipo de TI de Navarro era luchar contra el aluvión de spam que recibían los usuarios en sus buzones cada día. Alrededor del 70% de los mensajes entrantes eran spam, dice. Para evitar que estos mensajes se acumularan en los buzones, el personal de TI los eliminaba manualmente, lo que requería que un miembro del personal se dedicara a ello aproximadamente 20 horas por semana. No sólo eso, los empleados del Municipio generalmente encontraban sus mensajes de correo electrónico salientes bloqueados porque el spam entrante contenía programas maliciosos que utilizaban el sistema de Guadalupe para enviar más spam, lo que provocaba que muchos proveedores de servicios de Internet (ISP) colocaran su dirección IP en la lista negra.

A fin de resolver estos problemas, el Municipio implementó Symantec Premium AntiSpam. Ahora, sólo el 20% de los mensajes que ingresan son spam, comenta Navarro, y el personal sólo tiene que preocuparse cuando el software ocasionalmente bloquea un mensaje legítimo y los usuarios solicitan que sea recuperado.

Como el hecho de tener la dirección IP de Guadalupe bloqueada representaba un gran problema, el Municipio considera que el tiempo de recuperación de Premium AntiSpam fue inmediato. “Si el Gobierno nos solicita información, pero no reciben lo que les enviamos, es un gran problema”, comenta.

Administración de la Mensajería Instantánea

Otro problema, informa Navarro, fue el uso (o uso excesivo) de la mensajería instantánea por parte de los empleados de Guadalupe. “Utilizaban el chat todo el tiempo y, algunas veces, lo utilizaban para enviar información o documentos importantes”, dice. “Mi idea era evitar el uso indebido de este medio”.

Symantec IM Manager dio a Navarro el control que estaba buscando, por ejemplo, al impedir la incorporación de archivos adjuntos en mensajes instantáneos. “Tienen que enviar cosas de una manera diferente, utilizando Microsoft Outlook, en lugar del chat”, comenta. Además, si bien el departamento de TI normalmente no revisa las transcripciones de la mensajería instantánea, el hecho de tener esta capacidad ayuda a lograr que los empleados cumplan con sus obligaciones. “Quiero que utilicen el chat como corresponde, no para conversar con sus amigos”, dice. “Saben que existe supervisión, y por tanto no utilizan de forma incorrecta esta herramienta”.

Es decir, aquéllos que aún tienen acceso al chat completamente. El equipo de TI de Guadalupe utiliza IM Manager para controlar estrictamente quién tiene acceso al software de mensajería instantánea, y quién no lo tiene. Estima que sólo un 10% de los 800 usuarios de equipos de Guadalupe (quienes realmente lo necesitan para sus tareas) tienen acceso al chat. Actualmente, también se considera la posibilidad de permitir el uso del chat interno dentro de la red del Municipio para otros usuarios.

“MIGESA es un partner comercial. Nos apoyan, nos brindan las mejores respuestas, y escogieron Symantec.”

Gabriel Navarro

Director de TI
Municipality of Guadalupe

Protección de Datos Fundamentales

En otro gran cambio, el Municipio implementó Symantec Backup Exec™. “La idea era proteger el ERP, SIMUN, que también implementamos en ese momento”, comenta Navarro.

El Municipio ahora utiliza Backup Exec para realizar copias de respaldo de 100 GB de datos en cinta cada noche, un proceso que demora una hora, informa Navarro. Hasta el momento, no se necesitaban restauraciones, pero el personal de TI probó la solución ampliamente antes de implementarla y comprobó que las restauraciones tenían una precisión del 100%.

Navarro dice que piensa en la solución en cuanto a garantía de trabajo. “Si no contamos con copias de respaldo, no tendré trabajo este año”, dice. “Si se tienen, pero no se necesitan, está bien. Pero si no se tienen, olvídense”.

Un Partner Comercial Estratégico

El Municipio trabajó con Microsistemas Gerenciales, SA de CV, normalmente conocida como MIGESA, para implementar sus soluciones de Symantec. “MIGESA es un partner comercial”, dice. “Nos apoyan, nos brindan las mejores respuestas, y escogieron Symantec”. Si bien MIGESA proporciona consultoría y soporte cada vez que el Municipio lo necesita, los ingenieros de Symantec también trabajaron directamente con Navarro en la creación e implementación de soluciones de Symantec.

“Tengo una alianza con ambas partes”, afirma. “Ambos vinieron y crearon una estrategia para ayudarme a lograr la protección que necesitaba”.

DESCRIPCIÓN GENERAL DE LA SOLUCIÓN

Principales Desafíos

- Garantizar la seguridad de la red.
- Controlar el uso de Internet y la mensajería instantánea de los empleados.
- Reducir el tiempo que demora el departamento de TI en la corrección de virus.
- Reducir el spam y el tiempo que demora el departamento de TI en eliminarlo.
- Garantizar la disponibilidad de los datos, si el hardware falla.

Solución

Proporcionó protección de la red, redujo el spam, garantizó protección de datos.

Productos de Symantec

Symantec™ Endpoint Protection
Symantec Backup Exec™ 11d
Symantec™ IM Manager
Symantec™ Premium AntiSpam

Partner de Symantec

Microsistemas Gerenciales, SA de CV (MIGESA), www.migesa.com.mx

Entorno Tecnológico

- Aplicaciones: SIMUN(solución del Gobierno de ERP, producida localmente en Nuevo León); Microsoft Exchange 2003; software 072 (alerta a la comunidad de problemas en 72 horas); VoIP
- Bases de datos: Oracle8; Microsoft SQL Server
- Servidores: seis servidores HP HP ProLiant BL460c servers in una sistema SAN ejecutando Microsoft Windows Server 2003 y dos servidores estratos ejecutando Linux
- Almacenamiento: HP EVA 4000 sistema de SAN
- Biblioteca de cintas: HP StorageWorks MSL2024

Resultados Comerciales

- Un incidente de programa malicioso cada seis semanas, mientras que antes se producían cinco por semana.
- Una reducción superior al 99% en el tiempo que el departamento de TI destina a la corrección de programas maliciosos, es decir, se pasó de 80 horas por semana a una hora cada seis semanas.
- En un año se planea recuperar la inversión realizada en Symantec Endpoint Protection.
- 100% de precisión en restauraciones de datos.
- 71% menos de spam en los buzones de los usuarios.
- Aplicación de políticas de Internet y mensajería instantánea