Supervisión de amenazas físicas en el centro de datos

White Paper 102

Revisión 3

Por Christian Cowan y Chris Gaskins

> Resumen Ejecutivo

Las metodologías tradicionales para la supervisión del entorno de los centros de datos ya no son suficientes. Las nuevas tecnologías (como los servidores Blade) elevan las necesidades de refrigeración, y las nuevas leyes (como la Ley Sarbanes-Oxley) aumentan los requisitos de seguridad. Por lo tanto, el entorno físico del centro de datos debe controlarse más de cerca. Aunque existen protocolos bien conocidos para la supervisión de dispositivos físicos, como sistemas SAI, equipos de aire acondicionado de salas de ordenadores y sistemas de extinción de incendios, hay una serie de puntos de supervisión distribuidos que no suele tenerse en cuenta. En este documento se describen este tipo de amenazas, se sugieren estrategias para la implementación de dispositivos de supervisión y se ofrecen prácticas recomendadas para aprovechar los datos recopilados con el fin de reducir el tiempo de inactividad.

Contenido

haga clic en una sección para saltar a ella

Los documentos técnicos de APC by Schneider Electric son ahora parte de la biblioteca de documentos técnicos de Schneider Electric producido por Schneider Electric's **Data Center Science Center**
DCSC@Schneider-Electric.com

Schneider Electric

Introducción

Las técnicas habituales que se utilizan actualmente para supervisar el entorno de los centros de datos se remontan a la época de los sistemas mainframe centralizados y consisten, entre otras cosas, en recorrer las instalaciones con termómetros y tener en cuenta las sensaciones del personal de TI para intuir el entorno de la sala. Sin embargo, a medida que los centros de datos continúan evolucionando con tecnologías de servidor y procesamiento distribuido que elevan las necesidades de alimentación y refrigeración, el entorno debe controlarse más de cerca.

La creciente densidad de potencia y las fluctuaciones dinámicas de potencia son las dos causas principales que obligan a modificar la metodología de supervisión de los entornos de TI. Los servidores Blade tienen densidades de potencia increíblemente elevadas y han provocado un cambio radical en la dinámica de alimentación y refrigeración de los entornos circundantes. Las tecnologías de gestión del suministro eléctrico han mejorado la capacidad de los servidores y los equipos de comunicaciones para alterar el consumo de potencia (y, por tanto, la disipación de calor) en función de la carga computacional. Esta cuestión se describe de forma detallada en el Documento técnico 43, *Fluctuaciones dinámicas de potencia en centros de datos y salas de red*.

Enlace al White Paper 43

Fluctuaciones dinámicas de potencia en centros de datos y salas de red

Aunque es habitual contar con funciones sofisticadas de supervisión y alerta en equipos físicos, como sistemas de alimentación ininterrumpida (SAI), equipos de aire acondicionado de salas de ordenadores (CRAC) y sistemas de extinción de incendios, no suelen tenerse en cuenta otros aspectos del entorno físico. La supervisión de los equipos no es suficiente: el entorno circundante debe considerarse de forma holística y supervisarse de forma proactiva en busca de amenazas e intrusiones. Entre dichas amenazas se encuentran temperaturas de entrada excesivas en los servidores, fugas de agua, acceso de personal no autorizado al centro de datos o acciones inadecuadas del personal del centro de datos.

Las ubicaciones de red remotas, como sucursales, armarios de red y puntos de venta locales incrementan aún más la necesidad de una supervisión automatizada en aquellas ubicaciones en las que resulta poco práctico y fiable destinar a personas para la comprobación de las condiciones ambientales como, por ejemplo, la temperatura y la humedad. Con la introducción del envío automático de mensajes a través de la red sin la intervención de los usuarios, los administradores de TI deben disponer de sistemas fiables para saber lo que está ocurriendo en todo momento.

Las tecnologías de hoy en día permiten configurar los sistemas de supervisión de una forma tan detallada como para satisfacer las necesidades particulares ambientales y de seguridad de cualquier centro de datos. Cada rack se puede considerar un mini centro de datos con sus propios requisitos, con una estrategia de supervisión que puede incluir múltiples puntos de recopilación de datos.

En este documento se abordan las amenazas físicas que se pueden paliar mediante estrategias de supervisión distribuida y se ofrecen pautas y prácticas recomendadas para la implementación de sensores en el centro de datos. También se examina el uso de herramientas de diseño de centros de datos para simplificar el proceso de diseño y especificación de estos sistemas de supervisión distribuida.

¿Qué son las amenazas físicas distribuidas?

Este documento se centra en un subgrupo de amenazas: *las amenazas físicas distribuidas*. Estas son de un interés especial porque requieren un diseño correcto y proyectado para defenderse contra ellas. Para identificar este subgrupo conviene describir brevemente la serie de amenazas a las que se enfrentan los centros de datos.

Las amenazas a las que se enfrentan los centros de datos se pueden clasificar en dos grandes categorías dependiendo de si afectan a la red y al software de TI (amenazas **digitales**) o si afectan a la infraestructura física de soporte del centro de datos (amenazas **físicas**).

Amenazas digitales

Las amenazas digitales son, por ejemplo, piratas informáticos, virus, cuellos de botella en la red y otros ataques accidentales o maliciosos a la seguridad o al flujo de datos. En el sector y en la prensa se concede mucha importancia a las amenazas digitales, por lo que la mayoría de los centros de datos dispone de sistemas sólidos mantenidos activamente, como cortafuegos o antivirus, para defenderse de ellas. En el Documento técnico 101, *Principios básicos de la seguridad de red*, se describen las medidas básicas de protección frente a las amenazas digitales. En este documento no se abordan las amenazas digitales.

Enlace al White Paper 101
Principios básicos de la seguridad de red

Amenazas físicas

Entre las amenazas físicas para los equipos de TI se encuentran, p. ej., los problemas de alimentación y refrigeración, la malicia o el error humano, los incendios, las fugas y la calidad del aire. Algunas de ellas (incluidas las amenazas relacionadas con la alimentación y algunas relacionadas con la refrigeración y los incendios) se supervisan de forma rutinaria a través de diversas funciones integradas en los dispositivos de alimentación, refrigeración y extinción de incendios. Por ejemplo, los sistemas SAI supervisan la calidad de la alimentación, la carga y el estado de las baterías; las unidades PDU supervisan las cargas de los circuitos; las unidades de refrigeración supervisan las temperaturas de entrada y salida y el estado de los filtros; los sistemas de extinción de incendios (impuestos por las normativas de construcción) supervisan la presencia de humo o calor; etc. Estos métodos de supervisión suelen acatar protocolos bien conocidos automatizados por sistemas de software que recopilan, registran, interpretan y muestran la información relevante. Las amenazas supervisadas de este modo, a través de una funcionalidad preconfigurada e integrada en los equipos, no requieren ninguna planificación ni pericia especial por parte del usuario para ser gestionadas con eficacia siempre que los sistemas de supervisión e interpretación estén bien diseñados. *Estas amenazas físicas supervisadas automáticamente son un componente crucial de un sistema de gestión exhaustivo, pero quedan fuera del ámbito de este documento.*

Sin embargo, para ciertos tipos de amenazas físicas (y se trata de amenazas serias) el usuario no tiene a su disposición soluciones de supervisión prediseñadas e integradas. Por ejemplo, la amenaza de unos niveles deficientes de humedad puede darse en cualquier lugar del centro de datos, por lo que el número y la ubicación de los sensores de humedad requieren una importante consideración para gestionar esta amenaza. Estas amenazas pueden estar **distribuidas en cualquier parte del centro de datos, en ubicaciones variables que dependen del diseño de la sala y de la colocación de los equipos**. Las amenazas físicas distribuidas objeto de este documento se clasifican en las siguientes categorías generales:

- Amenazas para los equipos de TI relativas a la calidad del aire (temperatura, humedad)
- Fugas de líquidos
- Presencia humana o actividad inusual
- Amenazas para el personal relativas a la calidad del aire (sustancias extrañas en el aire)
- Peligros por humos e incendios procedentes del centro de datos[1]

[1] La detección básica de humo/incendios exigida por las normativas de construcción se rige por normas legales y de seguridad específicas y no entra dentro del ámbito de este documento. Este documento aborda la detección de humos *suplementaria* específica de los peligros del centro de datos más allá de lo que exigen la normativa de construcción.

En la **Imagen 1** se ilustra la diferencia entre amenazas digitales y amenazas físicas, así como la diferencia entre las amenazas físicas con supervisión de alimentación/refrigeración preconfigurada e integrada en los equipos y las amenazas físicas distribuidas (objeto de este documento), que requieren tareas de evaluación, decisión y planificación para determinar el tipo, la ubicación y el número de sensores de supervisión. Este último tipo de amenazas físicas es el que representa un mayor riesgo de ser descuidado debido a la falta de conocimientos y experiencia en el diseño de una estrategia de supervisión eficaz.

Imagen 1

Amenazas para el centro de datos

En la **Tabla 1** se resumen las amenazas físicas distribuidas, su repercusión en el centro de datos y los tipos de sensores utilizados para supervisarlas.

Tabla 1

Amenazas físicas distribuidas

Amenaza	Definición	Repercusión en el centro de datos	Tipos de sensores
Temperatura del aire	Temperatura del aire en la sala, en los racks y en los equipos	Fallo de los equipos y reducción de la vida útil de los equipos si la temperatura se encuentra por encima del valor especificado o si fluctúa de forma drástica	Sensores de temperatura
Humedad	Humedad relativa en la sala y en los racks a una temperatura específica	Fallo de los equipos debido a la acumulación de electricidad estática en los puntos de humedad baja Formación de condensaciones en los puntos de humedad alta	Sensores de humedad
Fugas de líquidos	Fugas de agua o refrigerante	Daños en suelos, cableado y equipos Indicio de problemas en los equipos CRAC	Sensores de fugas de cable Sensores de fugas puntuales
Error humano y acceso del personal	Infracciones no intencionadas cometidas por el personal Acceso no autorizado o forzado al centro de datos con malas intenciones	Daño en equipos y pérdida de datos Tiempo de inactividad de los equipos Robo y sabotaje en los equipos	Cámaras de vídeo digital Sensores de movimiento Contactos para puertas Sensores de rotura de cristales Sensores de vibración
Humo/incendios	Incendio eléctrico o de materiales	Fallo de los equipos Pérdida de activos y datos	Sensores suplementarios de humo
Contaminantes peligrosos en el aire	Productos químicos, p. ej. hidrógeno de las baterías, y partículas, p. ej. polvo, en el aire	Situación peligrosa para el personal o falta de fiabilidad y fallo del sistema SAI debido a la fuga de hidrógeno Fallo de los equipos debido al aumento de electricidad estática y obstrucción de filtros/ventiladores por la acumulación de polvo	Sensores de hidrógeno/productos químicos Sensores de polvo

Ubicación de los sensores

Se pueden utilizar diversos tipos de sensores para obtener una advertencia anticipada de los problemas causados por las amenazas descritas con anterioridad. Aunque el número y el tipo específico de sensores puede variar en función del presupuesto, el riesgo de la amenaza y los costes empresariales de una brecha, hay un conjunto de sensores mínimo esencial que resulta conveniente para la mayoría de los centros de datos. La **Tabla 2** contiene las pautas de instalación de este conjunto de sensores básico recomendado.

Tabla 2

Normas de instalación de sensores básicos

Tipo de sensor	Ubicación	Práctica recomendada general	Comentarios	Normas del sector aplicables	Ejemplo
Sensores de temperatura	Rack	En la parte superior, central e inferior de la puerta frontal de cada rack de TI para supervisar la temperatura de entrada de los dispositivos instalados en el rack.	En armarios de red u otros entornos de rack abierto, la temperatura se debe supervisar lo más cerca posible de las entradas de los equipos.	Normas ASHRAE[2]	
Sensores de humedad	Fila	Uno por cada pasillo frío; se instala en la parte frontal de un rack del centro de la fila.	Como las unidades CRAC proporcionan lecturas de la humedad, puede que sea necesario ajustar la ubicación de los sensores de humedad basados en filas si están demasiado cerca de la salida de CRAC.	Normas ASHRAE	
Sensores de fugas de cable **Sensores de fugas puntuales**	Sala	Cable de fugas colocado alrededor de cada sistema CRAC, alrededor de las unidades de distribución de refrigeración, debajo del falso suelo y junto a cualquier fuente de fugas (p. ej., tuberías).	Sensores de fugas puntuales para supervisar el desbordamiento de fluidos en bandejas de recogida y para supervisar armarios, salas pequeñas o cualquier punto débil.	Ninguna norma del sector	
Cámaras de vídeo digital	Sala y fila	Colocación estratégica según la distribución del centro de datos para cubrir todos los puntos de entrada/salida y poder ver todos los pasillos calientes y fríos; todo el campo de visión necesario debe quedar cubierto.	Supervisión y grabación del acceso autorizado, no autorizado y fuera de horas mediante software de vigilancia por vídeo.	Ninguna norma del sector	
Interruptores de sala	Sala	Interruptor electrónico en todas las puertas de entrada para poder verificar a posteriori el acceso a la sala y limitar el acceso de personas determinadas en horas específicas.	Puede ser recomendable integrar los interruptores de sala en el sistema del edificio mediante una interfaz de comunicaciones.	HIPPA y Ley Sarbanes-Oxley[3]	

Además de los sensores esenciales incluidos en la **Tabla 2**, existen otros que pueden considerarse opcionales y que dependen de la configuración particular de la sala, el nivel de riesgo y los requisitos de disponibilidad. En la **Tabla 3** se enumeran estos sensores adicionales y se ofrecen pautas sobre prácticas recomendadas.

[2] Normas ASHRAE TC9.9 para Instalaciones de misión crítica, *Thermal Guidelines for Data Processing Environments*, 2004.

[3] Fiona Williams, directora general de los servicios de seguridad de Deloitte & Touche, afirma: "La seguridad física entra dentro de los requisitos de la ley Sarbanes-Oxley. Es un componente importante tanto del programa infosec como de los controles informáticos generales. Se encuentra dentro de las secciones 302 y 404, que requieren que la dirección evalúe y se asegure de que los controles internos están funcionando eficazmente". http://www.csoonline.com/read/100103/counsel.html (visitado el 5 de marzo de 2010)

Tabla 3

Pautas de instalación de sensores adicionales en función de la situación

Tipo de sensor	Ubicación	Práctica recomendada general	Comentarios	Normas del sector aplicables	Ejemplo
Sensores suplementarios de humo	Rack	"Detección de humo anticipada" (VESD) de rack para obtener una advertencia anticipada de los problemas en zonas muy críticas o en zonas sin sensores de humo propios.[4]	En caso de que los sistemas de detección suplementaria de humo de rack se salen del presupuesto, la colocación de sensores VESD en la entrada de cada CRAC ofrece cierto grado de advertencia anticipada.	Ninguna norma del sector	
Sensores de hidrógeno/productos químicos	Sala	Si el centro de datos tiene baterías VRLA, no es necesario colocar sensores de hidrógeno en la sala porque estas no emiten hidrógeno durante su funcionamiento normal (al contrario que las baterías de célula húmeda).	Las baterías de célula húmeda ubicadas en salas de baterías independientes están sujetas a una normativa especial.	Borrador de norma IEEE/ASHRAE[5]	
Sensores de movimiento	Sala y fila	Se utilizan cuando no es posible instalar cámaras digitales (práctica recomendada) por motivos presupuestarios (consulte la **Tabla 2**).	Los sensores de movimiento son una alternativa más asequible a las cámaras de vídeo digital para la supervisión de la actividad humana.	Ninguna norma del sector	
Interruptores de rack	Rack	En centros de datos de gran densidad de tráfico, utilice interruptores electrónicos en la puerta delantera y trasera de cada rack para poder verificar el acceso a posteriori y limitar el acceso a equipos críticos a personas determinadas en horas específicas.	Se recomienda integrar los interruptores de rack en el sistema del edificio mediante una interfaz de comunicaciones.	HIPPA y Ley Sarbanes-Oxley	
Sensores de vibración	Rack	En centros de datos de gran densidad de tráfico, utilice sensores de vibración en cada rack para detectar el montaje o desmontaje no autorizados de equipos críticos.	También se pueden utilizar sensores de vibración en todos los racks para detectar si alguien desplaza un rack.	Ninguna norma del sector	
Sensores de rotura de cristales	Sala	Utilice un sensor de rotura de cristales en cada ventana del centro de datos (ya sea exterior o interior).	Se recomienda la utilización combinada con cámaras de vigilancia por vídeo.	Ninguna norma del sector	

[4] Se de por sentada la existencia de un sistema de detección de incendios independiente para satisfacer los requisitos de las normativas de construcción.

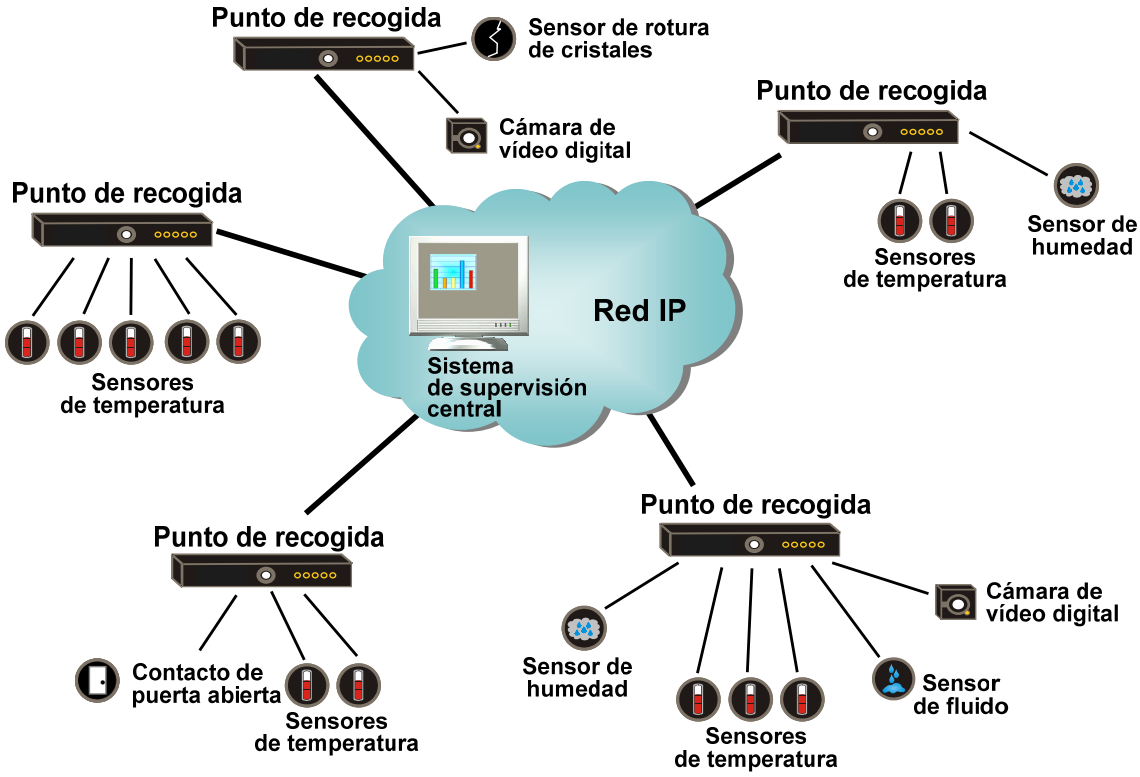
[5] IEEE/ASHRAE, *Guide for the Ventilation and Thermal Management of Stationary Battery Installations*, redactada para someter a votación a finales de 2006

Recopilación de datos de los sensores

Una vez seleccionados y colocados los sensores, el siguiente paso es recopilar y analizar los datos que reciben los sensores. En lugar de enviar todos los datos de los sensores directamente a un punto de recogida centralizado, a menudo es mejor disponer de puntos de recopilación distribuidos por el centro de datos con capacidad de alerta y notificación. De este modo, no solo se elimina el riesgo de punto de fallo individual que implica el disponer de un único punto de recogida centralizado, sino que también es posible supervisar los puntos de uso de los armarios de telecomunicaciones y las salas de servidores.[6] Los puntos de recogida se comunican con el sistema de supervisión central a través de la red IP (**Imagen 2**).

Imagen 2

Recopilación de los datos de los sensores



Normalmente, los sensores individuales no se conectan de forma individualizada a la red IP, sino que los puntos de recogida interpretan los datos de los sensores y envían alertas al sistema central o directamente a la lista de notificación (consulte la sección siguiente). Esta arquitectura de supervisión distribuida reduce considerablemente el número de estaciones de red necesarias, rebaja los costes generales del sistema y facilita la gestión. Los puntos de recogida suelen estar asignados a zonas físicas del centro de datos y abarcan sensores de una zona limitada para reducir la complejidad de cableado de los sensores.

Acción "inteligente"

Los sensores proporcionan datos brutos, pero la interpretación de estos datos es igualmente importante a la hora de generar alertas, notificaciones y correcciones necesarias. A medida que las estrategias de supervisión se vuelven más sofisticadas y se multiplica el número de sensores instalados en el centro de datos, el procesamiento "inteligente" de esta cantidad potencialmente alta de datos es esencial. La forma más segura y eficaz de recopilar y analizar los datos de los sensores y desencadenar las acciones adecuadas es mediante el uso de "puntos de recogida", tal como se ha descrito en la sección anterior.

[6] Esta arquitectura de múltiples puntos de recogida, cada uno con capacidad de alerta y notificación para los sensores a los que da soporte, es lo que suele llamarse "inteligencia distribuida".

Es fundamental poder filtrar, correlacionar y evaluar los datos para determinar la mejor forma de reaccionar cuando se producen eventos que están fuera de los límites establecidos. Una reacción eficaz implica alertar a la persona adecuada por medio del método apropiado y con la información oportuna. Hay tres formas posibles de acción:

- Mediante **alertas** de condiciones fuera de límites que puedan poner en peligro dispositivos o racks específicos o el centro de datos en su conjunto
- Mediante la **acción** automática basada en alertas y en umbrales específicos
- Mediante el **análisis y la notificación** para facilitar mejoras, optimización y mediciones de fallos

Alerta

A la hora de configurar las alertas hay que definir tres aspectos: ***Umbrales de alarma*** (los valores que deben registrarse para que se activen las alarmas); ***métodos de alerta*** (cómo debe enviarse la alerta y a quién) y ***prioridad*** (¿es necesario asignar ciertos tipos de alarmas a un puesto distinto del escalafón empresarial para su resolución?).

Umbrales de alarma: es necesario determinar, para cada sensor, las condiciones de funcionamiento aceptables. Asimismo, se deben configurar umbrales para que se activen las alarmas cuando las lecturas sobrepasen las condiciones de funcionamiento establecidas. Lo ideal sería que el sistema de supervisión tuviese la flexibilidad necesaria para configurar varios umbrales por sensor a fin de alertar a distintos niveles (alerta informativa, de advertencia, crítica y de fallo). Además de los umbrales de valor único, debería haber condiciones de disparo como el rebase de los umbrales durante un periodo de tiempo determinado, el ritmo de ascenso y el ritmo de descenso. En el caso de la temperatura, una alerta sobre el ritmo de fluctuación ofrece una indicación de fallo más rápida que la lectura aislada de un valor de temperatura.

Los umbrales se deben fijar con cuidado para garantizar su máxima eficacia. Puede haber umbrales diferentes que disparen alertas distintas en función de la gravedad del incidente. Por ejemplo, el rebase de un umbral de humedad puede disparar el envío de un mensaje de correo electrónico al administrador de TI, mientras que la activación de un sensor de humo puede disparar una llamada automática al cuerpo de bomberos. Del mismo modo, cada nivel de umbral afecta a un puesto distinto del escalafón empresarial. Por ejemplo, el acceso no autorizado a un rack puede disparar una notificación al administrador de TI, mientras que la entrada forzada al centro de datos puede disparar una notificación al director de TI.

Los umbrales se deben ajustar de forma global a valores predeterminados y, luego, se deben personalizar en función de las especificaciones de los equipos de TI y de la ubicación de los sensores en relación con la ubicación de los equipos (por ejemplo, un sensor ubicado junto a la fuente de alimentación de un servidor debe reaccionar ante un valor más alto que un sensor ubicado junto a la entrada de aire de un servidor). La **Tabla 4**[7] muestra los umbrales recomendados predeterminados de temperatura y humedad, según la norma ASHRAE TC9.9. Además de estos umbrales, es importante supervisar el ritmo de fluctuación de la temperatura. Una fluctuación de temperatura de 5,6 °C (10 °F) en un periodo de 5 minutos puede ser indicio de un fallo del sistema CRAC.

[7] *ASHRAE TC9.9: recomendación para entornos de clase 1, que son los más controlados y más apropiados para centros de datos con operaciones de importancia crítica.*

Tabla 4

Umbrales recomendados de temperatura y humedad

Sensor	Umbral máximo	Umbral mínimo
Temperatura del aire	25 °C (77 °F)	20 °C (68 °F)
Humedad	55 % de humedad relativa	40 % de humedad relativa

Métodos de alerta: la información de alerta se puede enviar de formas muy distintas como, por ejemplo, a través de mensajes de correo electrónico, mensajes de texto SMS, capturas SNMP y notificaciones a servidores HTTP. Es importante que los sistemas de alerta sean flexibles y personalizables para poder proporcionar correctamente la cantidad adecuada de información al destinatario oportuno. Las notificaciones de alerta deben incluir varios datos, como el nombre definido por el usuario del sensor, la ubicación del sensor y la fecha/hora de la alarma.

Prioridad de la alerta: es posible que algunas alarmas requieran una atención inmediata. Un sistema de supervisión inteligente debe ser capaz de asignar alarmas específicas a un nivel superior de autoridad si el problema no se resuelve dentro de un periodo de tiempo específico. La priorización de las alertas contribuye a garantizar que los problemas se atajen a su debido tiempo antes de que se produzca un efecto “bola de nieve”.

A continuación se incluyen algunos ejemplos de alertas útiles y no tan útiles:

Sensor de temperatura n.º 48 por encima del umbral: no es muy útil, ya que no indica la ubicación del sensor n.º 48.

Peligro de sobrecalentamiento en el servidor web X: esta alerta es útil, ya que identifica el servidor específico.

Sensor de puerta activado: no es muy útil, ya que no identifica la puerta en cuestión.

Se ha abierto la puerta X en la ubicación Y, y se ha tomado una fotografía de la persona que ha abierto la puerta: es muy útil, ya que incluye la identificación de la puerta, la ubicación de la puerta y una fotografía del incidente.

Reacción ante los datos

La recopilación de los datos de los sensores es solo el primer paso, y si el responsable del centro de datos confía únicamente en una respuesta manual, los datos no se estarán aprovechando al máximo. Hay sistemas disponibles que actúan automáticamente en función de alertas y umbrales definidos por el usuario. Para implementar este tipo de automatización “inteligente” debe tenerse en cuenta lo siguiente:

Acciones de alerta: en función de la gravedad de una alerta, ¿qué acciones automatizadas deben realizarse? Estas acciones automatizadas pueden ser notificaciones personales o medidas correctivas, como la activación de puntos de contacto seco para conectar o desconectar ventiladores, bombas u otros dispositivos.

Visibilidad continua en tiempo real de los datos de los sensores: la posibilidad de saber las lecturas instantáneas de los sensores individuales es un requisito básico. Sin embargo, la posibilidad de conocer las *tendencias* de los sensores individuales en tiempo real ofrece una idea más precisa de la situación. La interpretación de estas tendencias permite a los administradores detectar problemas más amplios y correlacionar datos procedentes de varios sensores.

Los sistemas de alerta no solo deben proporcionar notificaciones básicas sobre la violación de los umbrales. Por ejemplo, algunos sistemas de supervisión permiten a los administradores adjuntar datos importantes a las alertas. Estos datos adicionales pueden ser grabaciones de vídeo o de audio, gráficos o mapas. Un sistema de alerta de este tipo permite a los administradores tomar decisiones con mayor conocimiento de causa gracias a los datos contextuales que acompañan a la alerta. En algunos casos, un exceso de información tal vez requiera la filtración de los datos útiles. Por ejemplo, en un centro de datos de gran densidad de tráfico sería muy molesto recibir una alerta cada vez que se detecta movimiento en el centro de datos. Puede haber casos en los que determinada información se bloquee o "enmascare" por motivos de seguridad. Por ejemplo, si en un vídeo se capta un teclado, puede bloquearse para que no se vea a las personas teclear sus contraseñas.
A continuación se incluyen algunos ejemplos de interpretaciones y acciones "inteligentes":

- Si se excede un umbral de temperatura, encender automáticamente un ventilador o CRAC.
- Ofrecer acceso remoto a racks específicos con cerraduras electrónicas en función de la cara que aparezca en la vigilancia de vídeo en tiempo real.
- Si se detecta agua en un centro de datos remoto, activar automáticamente una bomba de achique.
- Si se detecta movimiento en el centro de datos fuera de las horas habituales de trabajo, grabar un vídeo automáticamente y alertar a los vigilantes de seguridad.
- Si se detecta la rotura de un cristal fuera de horas de trabajo, avisar a los vigilantes de seguridad y disparar una alarma acústica.
- Si el interruptor de una puerta indica que la puerta de un rack ha permanecido abierta durante más de 30 minutos (lo que quiere decir que la puerta no se ha cerrado correctamente), enviar una alarma al administrador para que compruebe la puerta.

Análisis y notificación

Los sistemas de supervisión inteligente no solo deben incluir las tendencias a corto plazo de los datos de los sensores, sino también datos históricos a largo plazo. Los sistemas de supervisión de primera clase deben tener acceso a las lecturas de los sensores de semanas, meses o incluso años anteriores y permitir la elaboración de gráficos e informes a partir de estos datos. En los gráficos se deben poder representar varios tipos de sensores en el mismo informe para la comparación y el análisis. En los informes se deben poder incorporar lecturas mínimas, máximas y medias de los sensores durante el periodo de tiempo seleccionado abarcando diversos grupos de sensores.

La información histórica de los sensores a largo plazo se puede utilizar para muchos fines, por ejemplo, para demostrar que el centro de datos se encuentra al límite no por el espacio físico sino debido a una refrigeración inadecuada. Esta información se puede utilizar para extrapolar futuras tendencias a medida que se agregan equipos al centro de datos y puede ayudar a predecir el momento en el que el centro de datos alcanzará su capacidad máxima. El análisis de tendencias a largo plazo se puede utilizar en el nivel de racks para comparar el rendimiento de los equipos de distintos fabricantes ubicados en racks diferentes (cuál genera más calor o cuál trabaja a menor temperatura), lo que puede influir sobre futuras adquisiciones.

Las lecturas de los sensores capturadas por el sistema de supervisión se deben poder exportar a los formatos estándar del sector para poder utilizar los datos en programas de análisis y notificación estandarizados o personalizados.

Método de diseño

Aunque la especificación y el diseño de un sistema de supervisión de amenazas pueda parecer compleja, el proceso se puede automatizar con herramientas de diseño de centros de datos, como InfraStruXure Designer de APC. Las herramientas de diseño de este tipo permiten al usuario introducir una sencilla lista de preferencias a partir de la cual se coloca automáticamente el número apropiado de sensores y dispositivos de recogida. Los informes sinópticos contienen listas de piezas e instrucciones de instalación de los sensores recomendados. Estas herramientas de diseño de centros de datos utilizan algoritmos y reglas establecidas basadas en prácticas óptimas y estándares del sector para recomendar configuraciones específicas en función de la densidad, la distribución de la sala, las políticas de acceso de la sala y los requisitos de supervisión específicos del usuario.

Por ejemplo, las siguientes preferencias especificadas por el usuario pueden influir en el diseño del sistema de supervisión de amenazas en función del nivel de densidad de tráfico y acceso del centro de datos:

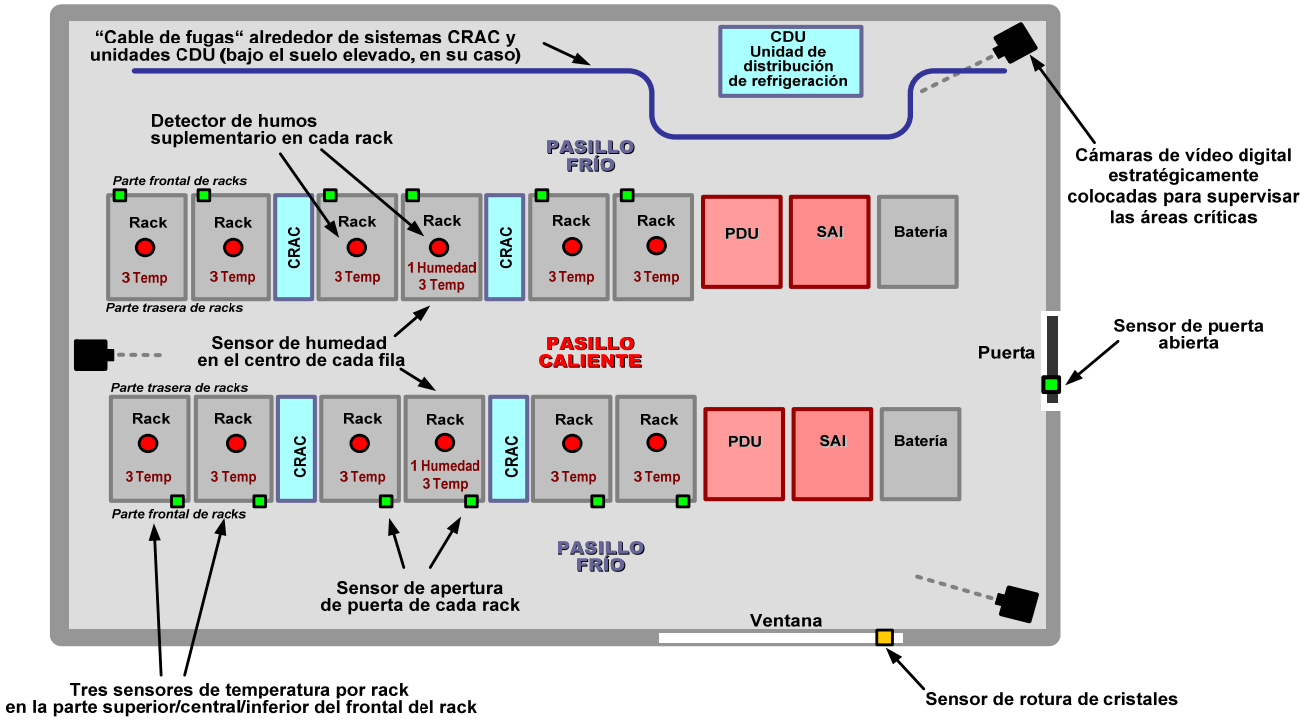
- **Gran densidad de tráfico/acceso**: si muchas personas tienen acceso al centro de datos, cada una de ellas con distintas funciones y aplicaciones, la herramienta de diseño sugerirá la instalación de interruptores de rack en cada rack para permitir el acceso solo a las personas que necesiten acceder al rack en cuestión.
- **Poca densidad de tráfico/acceso**: si al centro de datos solo tiene acceso un grupo reducido de personas, cada una de ellas con competencias sobre todas las funciones del centro de datos, la herramienta de diseño no sugerirá la instalación de interruptores de rack para controlar el acceso a los distintos racks, sino la instalación de un interruptor de puerta para impedir el acceso a la sala a las personas no autorizadas.

Ejemplo de distribución de sensores

En la **Imagen 3** se muestra un ejemplo de diseño de centro de datos en el que se ilustra la ubicación de dispositivos de supervisión de acuerdo con las prácticas recomendadas descritas en este documento.

Imagen 3

Ejemplo de distribución de sensores



Conclusión

La protección frente a las amenazas físicas distribuidas es fundamental para garantizar una estrategia de seguridad exhaustiva. Aunque la ubicación y la metodología de los equipos de detección requieren tareas de evaluación, decisión y planificación, hay disponibles prácticas óptimas y herramientas de diseño que facilitan la implantación eficaz de sensores.

Además de que el tipo, la ubicación y la cantidad de los sensores deben ser adecuados, también hay que instalar sistemas de software para gestionar los datos recopilados, registrar la información, realizar análisis de tendencias, enviar notificaciones de alerta inteligentes y tomar medidas correctivas de forma automatizada siempre que sea posible.

Si comprende las técnicas de supervisión de amenazas físicas distribuidas, el administrador de TI podrá llenar los vacíos críticos en la seguridad general del centro de datos y adaptar siempre la seguridad física a los objetivos de disponibilidad y la infraestructura en constante evolución del centro de datos.

Agradecimientos

Gracias a **Christian Cowan y Chris Gaskins** para la edición del contenido original de este documento técnico.

Recursos

Presione en el icono para dirigirse al recurso

Fluctuaciones dinámicas de potencia en centros de datos y salas de red
White Paper 43

Principios básicos de la seguridad de red
White Paper 101

Examinar todos los documentos técnicos
whitepapers.apc.com

Examinar todas las herramientas TradeOff Tools ™
tools.apc.com

Contacte con nosotros.

Si tiene algún comentario o sugerencia sobre el contenido de este White paper:

Data Center Science Center
DCSC@Schneider-Electric.com

Si es cliente y tiene dudas específicas sobre su proyecto de centro de datos:

Póngase en contacto con su representante de **Schneider Electric**
www.apc.com/support/contact/index.cfm