

Guía de buenas prácticas, **2024: SLED**

Administración estatal y local | Educación | Defensa/Aviación/Aeroespacial



El vertical SLED, tal y como lo define Convergent, engloba la administración estatal y local, la educación y la aviación/aeroespacial. Aunque cada uno de estos subverticales es sin duda distinto, hay más puntos en común que variabilidad en lo que respecta a la seguridad. Esto queda ejemplificado **por el reto de la escalada de riesgos físicos y cibernéticos** que obliga a priorizar la planificación de la seguridad y la mitigación de procedimientos para todas las entidades SLED.

El dedicado equipo SLED de Convergent ofrece **estrategias de protección de alta seguridad, implementación metódica de programas y soluciones integrales** centradas en impulsar tanto la seguridad como la eficiencia operativa en este sector. Con un profundo conocimiento de las amenazas del sector y los requisitos de cumplimiento normativo, y dotado de personal con subvenciones y recursos de financiación, Convergent puede desplegar sistemas integrados que funcionan dentro de las limitaciones de la planificación presupuestaria.

Incidentes y riesgos de seguridad del SLED

Los responsables de la seguridad en el espacio SLED se centran sobre todo en **mantener a salvo a los ciudadanos y en aprovechar toda la financiación disponible** para implantar sistemas que faciliten su capacidad para hacerlo.

Dicho esto, su mayor riesgo es adoptar una postura reaccionaria con respecto a la planificación de la seguridad. Este enfoque de tirita que aborda el incidente en lugar de la situación general es demasiado común. Por ejemplo, un centro de enseñanza primaria o secundaria puede sufrir un incidente de acoso escolar y reaccionar añadiendo cámaras y vigilancia. Una oficina de la administración local puede sufrir una oleada de robos y, por tanto, instalar un control de acceso. Un tiroteo puede dar lugar a la detección de armas.

En lugar de abordar la seguridad de forma fragmentaria, es importante tener una visión holística y considerar los objetivos a corto y largo plazo. La aplicación de un plan integral evita muchos incidentes individuales que conducen a la erosión de la marca, problemas de reputación y riesgos legales.

También es útil desglosar las cosas por subverticales SLED para facilitar valiosas perspectivas específicas de la empresa en cuestión.

La Administración estatal y local ahora y en el futuro

Los gobiernos estatales y locales dan prioridad a garantizar la seguridad de la comunidad y de sus empleados. Más allá de las implicaciones obvias, deben considerar las repercusiones en la percepción pública, la contratación y la retención. En concreto, los municipios gestionan una multitud de riesgos de seguridad, entre los que se incluyen:

- Delito
- Seguridad policial y exposición legal
- Migrantes y personas sin hogar
- Seguridad en el transporte y el tránsito

Sin embargo, hay otras cuestiones en juego. **El vandalismo contra la propiedad y las amenazas cibernéticas siguen siendo riesgos críticos para los municipios, con importantes consecuencias para los contribuyentes.** Todos los problemas de seguridad pueden verse exacerbados por unas comunicaciones deficientes dentro de los organismos y entre ellos que, en última instancia, dificultan la capacidad de la comunidad para gestionar los incidentes y aprovechar plenamente los recursos de financiación.

Educación

Planificación coherente

Como se ha señalado, el riesgo más grave para los centros de enseñanza primaria y secundaria **sigue siendo la ausencia de una planificación de la seguridad cohesionada y holística.** Demasiados distritos carecen de un plan maestro estratégico integral y compran arbitrariamente equipos de seguridad sin tener en cuenta cómo complementarán las tecnologías existentes. La falta de integración de dispositivos y equipos acaba creando un sistema dispar que no funciona como debería.

Este enfoque poco sistemático del diseño y la planificación de sistemas de seguridad se debe a menudo a una financiación estatal y local incoherente e inadecuada. Los centros de enseñanza primaria y secundaria dependen específicamente de las subvenciones estatales y federales para suplir los déficits presupuestarios, y el déficit de financiación suele aumentar con el paso del tiempo, lo que acelera los problemas de seguridad.

Comunicación

La seguridad en los centros de enseñanza primaria y secundaria también se ve afectada negativamente por la falta de protocolos de respuesta a emergencias y de una terminología coherentes y uniformes. Curiosamente, muchos distritos de todo el país siguen utilizando una terminología de respuesta a emergencias personalizada o única para los incidentes que se producen en el campus. **Esto puede crear problemas cuando varios distritos escolares bajo la jurisdicción de una agencia de respuesta policial tienen diferentes códigos de respuesta o, por el contrario, un distrito es atendido por múltiples jurisdicciones durante una emergencia.** Por ejemplo, el Distrito A puede utilizar el "Código Rojo" para un encierro y el "Código Amarillo" para un perímetro seguro, mientras que el Distrito B utiliza el "Encierro Forzoso" para un encierro y el "Encierro Suave" para un perímetro seguro. Esto puede crear una confusión masiva y un retraso en la respuesta durante un incidente crítico, en el que el tiempo es esencial.

Las desconexiones en la comunicación se agravan aún más cuando los distritos adyacentes y los primeros organismos de respuesta no colaboran entre sí a la hora de seleccionar y adquirir herramientas y tecnología de seguridad/respuesta a emergencias. A menudo, a los distritos se les vende la capacidad de una tecnología para comunicarse directamente con las fuerzas de seguridad a fin de agilizar la respuesta de emergencia. Sin embargo, esto exige que los primeros organismos de respuesta conozcan la tecnología en profundidad y dominen su capacidad para

gestionarla. Si varios distritos escolares bajo una misma jurisdicción policial no seleccionan un producto común, los organismos de primera intervención deberán manejar varios sistemas durante un incidente crítico. Por ejemplo, el Distrito A puede utilizar la Tecnología 1, que proporciona interoperabilidad con su despacho o PSAP. El despachador debe iniciar sesión y comunicarse directamente con el distrito a través de un canal o portal seguro. Mientras tanto, el Distrito B puede utilizar un sistema tecnológico diferente que requiera unas credenciales de acceso al portal URL totalmente distintas, con notificación a través de un canal diferente. Esto crea un gran potencial de error humano que puede producirse durante la respuesta a un incidente crítico.

Ciberamenazas

Mientras que la seguridad física sigue siendo un punto central para las escuelas K-12, la ciberseguridad es un riesgo de seguridad cada vez mayor en el espacio educativo. Esto abarca ransomware, violaciones de datos, ingeniería social, phishing y ciberseguridad básica. En esencia, dado que la tecnología de seguridad presenta acceso o entrada a Internet y a los sistemas electrónicos que contiene, la necesidad de dispositivos de "seguridad de la seguridad" es de vital importancia.



La educación en el futuro

Planificación coherente



Los centros de enseñanza primaria y secundaria de todo el país están empezando a **comprender el valor de desarrollar sus sistemas y operaciones de seguridad** basándose en evaluaciones de seguridad complejas, evaluaciones de riesgos para la seguridad de la empresa o planes maestros estratégicos. Identificar las necesidades, vulnerabilidades, activos, lagunas y amenazas de un distrito es esencial, pero aplicar estrategias de seguridad por capas que se centren en la capacidad de disuadir, detectar, retrasar y negar estas vulnerabilidades y amenazas es primordial. Y un enfoque metódico puede garantizar la capacidad de un distrito para

para alcanzar metas y objetivos de seguridad a corto y largo plazo.

Como la financiación adecuada es esencial para apoyar este enfoque, las escuelas K-12 se beneficiarán trabajando con socios de confianza para complementar los recursos internos de redacción de subvenciones. En particular, el equipo de Convergint SLED ofrece asistencia integral en materia de subvenciones y financiación. Esto incluye ayuda profesional para redactar y perfeccionar las propuestas de subvención.

Seguridad por niveles

La Partner Alliance for Safer Schools (PASS K-12) ofrece orientación y buenas prácticas para la seguridad escolar.

Siguiendo sus recomendaciones, muchas escuelas ya están adoptando un enfoque de seguridad por capas, y se espera que este enfoque gane más fuerza en los próximos años.

El refuerzo de cinco capas físicas puede hacer frente a una amplia gama de amenazas, ya que cada capa sucesiva proporciona componentes específicos para disuadir, detectar/retrasar y responder a comportamientos adversos en caso de que se eludan o vulneren otras capas.

Cada capa incluye componentes básicos de protección de la seguridad:

- Políticas y procedimientos
- Personas (funciones y formación)
- Arquitectura
- Comunicación
- Control de acceso
- Videovigilancia
- Detección y alarma

Y dentro de cada capa existen niveles de seguridad. En pocas palabras, **el primer nivel proporciona una buena protección de base, mientras que el último promete el enfoque más completo de la seguridad en el K-12.** Muchos centros educativos serán incapaces de aplicar medidas más allá del primer y segundo nivel, o puede que no tengan necesidad de hacerlo. Muchas escuelas serán incapaces de implementar medidas más allá del primer y segundo nivel o puede que no tengan necesidad de hacerlo.

Convergent proporciona a los administradores escolares herramientas que les permiten pueden utilizar para medir sus niveles de riesgo, identificar sus necesidades de seguridad y, tras tener en cuenta los recursos y la financiación disponibles, desarrollar planes de seguridad a medida que incorporen las mejores prácticas y procedimientos. Recuerde que, aunque los enfoques de seguridad de varios niveles pueden ser costosos, las directrices PASS incluyen recomendaciones y consideraciones prácticas de bajo coste o gratuitas.

Comunicación

Los centros de enseñanza primaria y secundaria se beneficiarán de la adopción de protocolos de respuesta a emergencias uniformes y coherentes que se adhieran a las mejores prácticas del sector, como el Protocolo de Respuesta Estándar (SRP) de la Fundación I Love U Guys. Adoptado por 36.000 escuelas de todo el país hasta la fecha, este SRP aprovecha la terminología común y la verborrea que es coherente para los primeros en responder, las escuelas y las comunidades. De este modo, cuando se produce un incidente, los organismos de primera intervención pueden comprender y gestionar la situación con mayor claridad. Se espera que, a medida que se corra la voz, más sistemas escolares se sumen a la iniciativa. Si un incidente sigue evolucionando, es posible que los distritos adyacentes también tengan que aplicar medidas reforzadas.

Ciberamenazas

En respuesta a la ciberamenaza, **es probable que los distritos escolares dediquen más recursos** a la concienciación, la formación y el refuerzo de los equipos. Este último debe comenzar con la evaluación de las cámaras y otros dispositivos de seguridad física que puedan tener credenciales de inicio de sesión predeterminadas, firmware obsoleto o visibilidad peligrosa en puntos de acceso abiertos/invitados.

Aviación Ahora

Los aeropuertos están experimentando un aumento de las violaciones del perímetro. Esto puede provocar el cierre del aeropuerto y multas de la FAA y la TSA, que pueden resultar muy costosas. En consecuencia, las instalaciones están reforzando la detección de intrusos con cámaras, radares, lidar y tecnologías de detección de vallas. La IA desempeña un papel en la gestión de falsas alarmas.



También hay una mayor conciencia de la amenaza interna, lo que ha llevado a la TSA a instituir mandatos de selección de empleados y formación especial. Esto incluye formación y protocolos cibernéticos para reforzar las mejores prácticas y las protecciones de dispositivos mediante software especializado.

La aviación en el futuro

Es probable que en el futuro el sector de la aviación adopte un sinfín de tecnologías para optimizar la seguridad, como PSIM y sistemas de megafonía más avanzados. Además de los requisitos de gestión de riesgos, también existe la necesidad de mejorar la eficacia operativa. Las tecnologías Lidar/sensores, por ejemplo, pueden contribuir tanto a la seguridad como a la gestión de los flujos (de puerta a puerta o de puerta a puerta) y ser una oportunidad para generar ingresos.

El coste de los ataques físicos o cibernéticos

Las entidades del SLED pueden sufrir importantes pérdidas **como consecuencia de una intrusión física o cibernética**, siendo las más preocupantes:

1. **Vida humana**

Obviamente, el resultado más ominoso de un ataque físico es la pérdida de vidas humanas. Lamentablemente, hay demasiados ejemplos de ello para nombrarlos en el espacio público.

2. Reputación/confianza

Las escuelas y las entidades públicas prosperan gracias a la confianza de la comunidad. La percepción de una falta de preparación ante un incidente de seguridad puede erosionar considerablemente su reputación. Esto puede incitar a los ciudadanos a cambiar de colegio, expulsar a alguien de su puesto o incluso mudarse.

Riesgos futuros más amenazadores

Al tiempo que gestionan las amenazas físicas, todas las entidades de la SLED deben prestar mucha atención a garantizar que las soluciones no creen otros problemas como el riesgo cibernético en el futuro. En concreto, deben establecerse protecciones para que los equipos de seguridad física no se conviertan en un vector de ciberamenazas. Muchos organismos públicos, distritos escolares, campus de seguridad y oficinas de la administración local carecen de personal para gestionar y mantener los sistemas de protección contra los ciberriesgos y otros riesgos. Por lo tanto, deben confiar en las salvaguardias de los proveedores. En última instancia, fortificar y simplificar la solución para el usuario minimiza el impacto en las operaciones diarias y optimiza las protecciones.

Contra medidas tecnológicas de seguridad

Muchos espacios públicos son intrínsecamente abiertos, por lo que es habitual que haya gente en ellos que no está necesariamente "invitada". Estas entidades suelen recibir visitantes, además de empleados, público en general y estudiantes. Aunque pueda parecer que el acceso abierto está reñido con la seguridad, **ambos pueden coexistir si la tecnología de seguridad está plenamente integrada en una plataforma sin fisuras** que admita una respuesta óptima y la elaboración de informes forenses.

Convergent aborda este reto mediante un enfoque consultivo de la evaluación de sistemas y necesidades, centrándose en la identificación de las mayores carencias y/o las mayores necesidades del cliente, aprovechando nuestras propias directrices y las mejores prácticas del sector como PASS para escuelas más seguras. Establecemos correspondencias con las alternativas tecnológicas adecuadas, aprovechando nuestra experiencia para determinar el enfoque más pragmático para llegar del punto A al punto B con un sistema de seguridad concreto.

El equipo de Convergent SLED identifica fácilmente las lagunas en la exposición al riesgo y sabe cómo encontrar las soluciones adecuadas. Y como somos agnósticos en cuanto a socios, nuestros clientes reciben opciones específicas para sus necesidades. En particular, nuestras soluciones se complementan con recomendaciones de procesos, como se ejemplifica a continuación:

Ejemplo 1

Desafío: Prevención de la delincuencia

Recomendación de equipos: LPRs, Cámaras,

Detalles: Convergent recomienda que en las solicitudes de licencia comercial se haga constar la obligación del propietario de cooperar con la policía en las investigaciones o de federar sus cámaras. Esto ayudará a agilizar la respuesta, la resolución de delitos y el conocimiento de la situación.

Ejemplo 2

Desafío: Seguridad de los agentes, relaciones públicas/gestión de la

percepción Recomendación de equipamiento: Cámaras corporales

Detalles: Convergent recomienda que todos los agentes lleven cámaras corporales para garantizar su capacidad de transmitir los detalles del incidente desde la perspectiva del agente. Esto reducirá las probabilidades de una denuncia falsa contra un agente de policía.

Ejemplo 3

Desafío: Gestión del bloqueo

Recomendación de equipamiento: Cámaras de seguridad, control de acceso y alarmas antipánico

Detalles: Convergent recomienda el control de acceso en los calabozos para enviar alertas al supervisor interno para que controle al preso en los intervalos requeridos. Las tarjetas de control de acceso auditarán sus entradas. El VMS puede integrarse en el control de acceso para ver los registros y garantizar la protección tanto de los presos como de los guardias.

Mejorar la eficacia del personal de seguridad/reducir costes

Eficacia de la mano de obra

El equipamiento de seguridad puede ser un multiplicador de fuerzas que mejore la eficacia global del plan de seguridad, pero también puede añadir una complejidad que no sea fácilmente absorbible por los recursos del cliente. En consecuencia, cualquier equipamiento añade un mandato para una evaluación exhaustiva. Por ejemplo, añadir más cámaras se traduce posiblemente en menos guardias in situ, lo que mejora la eficacia. Dicho esto, demasiadas cámaras requerirán operaciones de supervisión más sofisticadas, como un Centro de Mando y Control con todo el personal necesario.

Ningún equipo de un plan de seguridad debe considerarse una instalación aislada. Un sistema de detección de vapeadores en los baños de un colegio o un sistema de detección de tiradores en una instalación pública pueden parecer una solución convincente a un problema muy acuciante, **pero no serán óptimamente eficaces sin mantenimiento, pruebas, supervisión e integración** con el sistema en su conjunto. La integración es especialmente importante. Si un organismo tiene videovigilancia, un sistema de alarma y control de acceso, pero no se integran en un único panel, el personal de seguridad tendrá que trabajar en tres estaciones de trabajo distintas sólo para supervisar los sistemas. Esto es claramente ineficaz.

Reducción de costes

La rentabilidad de la inversión en tecnología depende de los gastos de capital iniciales y de los gastos de funcionamiento continuos. Es importante tener en cuenta no sólo los desembolsos iniciales, sino también el tiempo y los recursos necesarios para gestionar y mantener esos sistemas. El personal es una pieza fundamental de esta ecuación.

Cualquier decisión de inversión en tecnología debe tener en cuenta tanto las finanzas como los objetivos empresariales generales. Las entidades públicas suelen centrarse más en reducir los incidentes de seguridad que en maximizar los beneficios, pero también entran en juego otras necesidades empresariales. Todas ellas deben examinarse para obtener un mayor rendimiento de la inversión en tecnología de seguridad. Por ejemplo, la dirección de interfonía/comunicaciones masivas gestión de incidentes de seguridad, sino que también facilitan las capacidades de comunicación de difusión para la gestión de visitantes. Las ventajas van más allá de la seguridad.

Gestión del presupuesto de seguridad

La elaboración de presupuestos suele ser un reto para las entidades públicas, y las subvenciones son una solución excelente para financiar importantes desembolsos en materia de seguridad. Dicho esto, muchos clientes del SLED se sienten abrumados por el proceso de identificar oportunidades de financiación y pasar por el aro correspondiente. Por ello, Convergent ha creado un equipo de subvenciones y financiación con el único fin de orientar y ayudar a nuestros clientes en el proceso de obtención de fondos para gastos de seguridad.

Además, podemos apoyar el argumento de que otros departamentos comprometan recursos financieros y/o humanos para garantizar el éxito de los programas de seguridad. La financiación interdepartamental puede complementar las subvenciones, y el compromiso de los recursos humanos puede marcar la diferencia a la hora de obtener la aprobación de una subvención. Las organizaciones bien integradas son bien recibidas por los responsables de las subvenciones.

En última instancia, si el cliente puede ayudar a satisfacer las necesidades de otras partes de la organización más allá de la seguridad, es más probable que obtenga el apoyo interdepartamental necesario. Y esto sienta las bases para futuras relaciones, compromisos recurrentes y un enfoque más proactivo de las inversiones en seguridad.

Vehículos contractuales como opción

Los organismos estatales, municipales, de condado, de enseñanza primaria y secundaria y de enseñanza superior pueden aprovechar los vehículos contractuales para obtener lo último en tecnología innovadora a precios competitivos con el fin de aumentar la seguridad general. Los productos adecuados y los sistemas cuidadosamente diseñados pueden aumentar la eficiencia y mejorar las operaciones.

Los vehículos contractuales facilitan el proceso de compra y presupuestación mediante precios prenegociados para ofertas competitivas garantizadas por contratos de licitación. **Un Vehículo de Contrato es esencialmente un método racionalizado que tanto los gobiernos estatales como locales utilizan para comprar bienes y servicios, desde iPads hasta ascensores.** Los Contratos de Compra Cooperativa de Convergent garantizan nuestra capacidad para asegurar precios competitivos para nuestros clientes.



En última instancia, aprovechar el poder adquisitivo colectivo de múltiples organizaciones permite a las agencias garantizar precios competitivos para productos y servicios. Además, la agregación de las necesidades de todos los clientes permite la normalización de los productos y servicios, lo que redundará en una mayor coherencia y eficiencia en las adquisiciones. Los costes de administración se reducen al compartirse los esfuerzos entre entidades. Los vehículos contractuales de Convergent son numerosos, y todos ellos facilitan unas compras eficientes.

Utilizar la tecnología de seguridad para mejorar la competitividad de las empresas o marcas

La seguridad no se limita a un lado del balance. La seguridad es una propuesta vendible. Unos espacios públicos más seguros refuerzan la marca y la reputación de la ciudad. Esto, a su vez, atrae a empresas, residentes y visitantes. El valor también está ahí para las escuelas. **Los institutos y universidades aprovechan el tema de la seguridad como principal argumento de venta para captar estudiantes y asegurarse el apoyo de sus padres.** La conclusión: un programa de seguridad bien hecho puede marcar una diferencia significativa en la experiencia del cliente y, en consecuencia, prestarse a la promoción en apoyo de los resultados empresariales previstos.

Resumen de recomendaciones, 2024

Los responsables de la seguridad del SLED se esfuerzan continuamente por alcanzar objetivos a corto y largo plazo y, por tanto, estudian qué soluciones podrían integrarse en su plan actual respetando los presupuestos previstos. Es esencial empezar con el fin en mente. Por ello, **les instamos a dar un paso atrás y colaborar con un socio que entienda el espacio**. Disponer de un plan de seguridad holístico a 5 o incluso 10 años es muy valioso, incluso si algunos de los elementos incluidos en ese plan nunca se llevan a cabo. Hay que tener en cuenta todos los retos para descubrir todas las posibles soluciones. Una hoja de ruta estratégica elimina los riesgos inherentes a una respuesta reaccionaria y, en su lugar, garantiza un enfoque más medido de la gestión de amenazas. El primer paso hacia el éxito es una evaluación exhaustiva de la seguridad. No se trata de una gran partida presupuestaria y, a la larga, cosecha innumerables recompensas, empezando por un mejor control de los mayores riesgos para los clientes de SLED: la planificación reaccionaria y la incapacidad de lograr una verdadera integración para obtener los mejores resultados.

El equipo de Convergint SLED está preparado para ayudar a sus clientes, desde estudios exhaustivos de evaluación de sitios de gestión de riesgos de seguridad empresarial (ESRM) hasta soluciones creativas y tecnológicamente potentes para subvenciones y ayuda a la financiación. Nuestro éxito se evidencia en el éxito de nuestros clientes.