Riesgo, resiliencia y seguridad en administraciones nacionales y locales

Tecnologías y prácticas recomendadas para mantener la continuidad operativa

Alcatel·Lucent Enterprise

Índice

La seguridad y la resiliencia son prioridades urgentes 3
Los riesgos son reales 3
La digitalización conlleva beneficios y riesgos 4
Nuevas formas de concebir los puntos de vulnerabilidad 4
Consideraciones y retos únicos 5
Enfoque integral y proceso normalizado 6
Cuatro pasos para aumentar la seguridad y la resiliencia 6
Reforzar la seguridad y la resiliencia 7
Protección de la seguridad ciudadana 7
Mayor fiabilidad en las operaciones 8
Aumentar la seguridad y la protección en edificios y espacios 8
Un socio para sus estrategias 9
Soluciones flexibles y totalmente conformes 9
Más información 10

La seguridad y la resiliencia son prioridades urgentes

En la actualidad, las administraciones nacionales y locales de todo el mundo se enfrentan a una policrisis, es decir, a una convergencia de riesgos cibernéticos y físicos que amenaza a los ciudadanos, los servicios fundamentales y los datos sensibles.

Los ciudadanos depositan ahora su esperanza y confianza en los servicios prestados a través de sitios web seguros; por otro lado, los empleados prevén trabajar desde casa o en la oficina, según sus necesidades y preferencias. Estas nuevas necesidades, junto con la proliferación exponencial de los dispositivos de la Internet de las cosas (IoT), amplían los límites de la red en un momento en que las tensiones geopolíticas y la polarización política aumentan el riesgo de ciberataques.

Además, la web oscura ha creado un mercado rentable para vender de forma anónima datos sensibles de las administraciones públicas, haciendo que los sistemas administrativos sean un blanco ideal para el robo de información. También constituye un refugio en línea para coordinar ataques contra las administraciones públicas.

El vandalismo, el terrorismo, los disturbios y la delincuencia también van en aumento, creando amenazas cada vez mayores para las infraestructuras civiles y de defensa y para la continuidad operativa. A ello hay que añadir los graves fenómenos meteorológicos y las catástrofes naturales, que hacen muy difícil, si no imposible, prestar servicios públicos y mantener a salvo a los ciudadanos cuando más lo necesitan. Además, con la inflación mundial tensando los presupuestos, la necesidad de iniciativas de digitalización que aumenten la agilidad operativa, la eficiencia y la productividad nunca ha sido mayor.

En conjunto, estos riesgos están dificultando más que nunca que las administraciones nacionales y locales cumplan plenamente la cada vez más estricta normativa sobre privacidad y soberanía de los datos. Como resultado, existen muchas posibilidades de demandas y multas por infracciones.

Ante esta nueva realidad, a las administraciones nacionales y locales se les quedan cortas sus anteriores estrategias de seguridad y resiliencia. Para mitigar estos riesgos, deben tomar medidas audaces y proactivas para mejorar su nivel de seguridad general. Se necesita un enfoque nuevo e innovador que responda mejor a las amenazas más importantes de hoy en día. Reforzando la seguridad, las administraciones nacionales y locales estarán mejor posicionadas para proteger a los ciudadanos y las operaciones y reforzar su resiliencia, de modo que puedan garantizar la continuidad operativa en cualquier circunstancia.

Los riesgos son reales

Por desgracia, a las administraciones nacionales y locales les resulta demasiado fácil retrasar las medidas de mitigación de riesgos, sobre todo cuando los incidentes de interés periodístico tienen lugar solo en lugares lejanos. Pero la realidad es que todo organismo público es un blanco potencial de ataques.

Una mirada a la realidad

- Los ciberataques contra la administración pública se dispararon un 95 % en el último semestre de 2022.[1]
- El ataque contra el gobierno de Costa Rica se consideró uno de los más costosos del año[2] , y el ransomware es uno de los métodos preferidos de ataque contra los servicios públicos[3].
- Para 2025, se calcula que el 30% de las organizaciones de infraestructuras críticas sufrirán una brecha de seguridad.[4]

[1] Los ciberataques contra la administración pública se dispararon un 95 % en el último semestre de 2022, según CloudSek. CSO United States, enero de 2023.

[2] Los 13 ciberataques más costosos de 2022: una mirada retrospectiva. Security Intelligence, diciembre de 2022.

[3] Policy paper: National Cyber Strategy 2022. Oficina del Gabinete del Reino Unido, diciembre de 2022.

[4] Gartner predice que el 30 % de las organizaciones con infraestructuras críticas sufrirán una violación la seguridad en 2025. Gartner, diciembre de 2021.

A medida que crece la población de las ciudades,[5] aumentan los riesgos para la administración pública y los ciudadanos. Las Naciones Unidas aconseja a los Gobiernos que trabajen para que las ciudades y los asentamientos humanos sean más inclusivos, seguros, resilientes y sostenibles, como publica el Objetivo 11.[6]

Teniendo en cuenta todos estos factores, está claro que las administraciones públicas deben poner un foco renovado en el riesgo, la resiliencia y la seguridad para:

- **Garantizar la continuidad de los servicios críticos y proteger los datos sensibles**, sobre todo en momentos de crisis inesperadas
- **Minimizar los costes de los seguros de riesgos** implementando la protección adecuada para cada tipo de riesgo cibernético y físico que afronten
- **Reducir las pérdidas financieras** causadas por ataques cibernéticos y físicos, acciones judiciales de los ciudadanos y multas por violación de datos e incumplimiento de la normativa
- **Mantener su reputación y la confianza de los ciudadanos**, que pueden verse dañadas o perderse por completo debido a retrasos e interrupciones del servicio
- **Salvaguardar a los ciudadanos** proporcionando información importante relacionada con la salud, la seguridad y la protección

La digitalización conlleva beneficios y riesgos

En el mundo digital de hoy, las personas, los objetos y los procesos están conectados. Estas conexiones permiten a todas las administraciones públicas:

- Aprovechar la tecnología IoT y la información que esta proporciona
- Automatizar los flujos de trabajo para aumentar la eficacia y acelerar las respuestas a los ciudadanos
- Utilizar datos precisos y en tiempo real para aumentar la visibilidad y tomar decisiones fundamentadas
- Implementar aplicaciones para edificios inteligentes que permitan un funcionamiento más sostenible, rentable y resiliente

Aunque estas mejoras son esenciales para que las administraciones públicas alcancen sus objetivos, las tecnologías facilitadoras también introducen una nueva serie de riesgos cibernéticos y físicos a los que hay que hacer frente.

Nuevas formas de concebir los puntos de vulnerabilidad

Con la digitalización, los puntos de vulnerabilidad se exponen más fácilmente y las amenazas pueden propagarse rápidamente a los sistemas, dispositivos y aplicaciones interconectados:

- Un fallo en un sistema puede afectar a todos
- Los piratas informáticos pueden aprovechar las conexiones entre infraestructuras para ampliar su alcance
- Los virus pueden aprovecharse de las conexiones para propagarse por toda una organización

[5] Desarrollo urbano. Banco Mundial, abril de 2023.

[6] Objetivo 11: Lograr que las ciudades y los asentamientos humanos sean más inclusivos, seguros, resilientes y sostenibles. Naciones Unidas.

La digitalización también estrecha la conexión entre los riesgos cibernéticos y físicos. Por ejemplo, los actores maliciosos pueden piratear a distancia los centros de datos de las administraciones públicas o acceder físicamente a ellos poniendo en riesgo la cerradura electrónica de una puerta. Del mismo modo, las cámaras de seguridad pueden desactivarse, desconectarse o volver a conectarse a las señales de vídeo pregrabadas a través de un ataque cibernético o físico, lo que las hace inútiles desde el punto de vista de la protección en cualquiera de los casos.

La convergencia entre las TI y las tecnologías operativas (TO) crea nuevas oportunidades para los ataques. Así pues, los piratas informáticos pueden poner en peligro los sensores IoT para obtener acceso a la red y a los sistemas y recursos de información de gran valor conectados a ella. Por otra parte, pueden piratear directamente la red, utilizándola como puerta de entrada para atacar sistemas críticos de edificios, como ascensores, detectores de humo, alarmas contra incendios y sistemas de rociadores.

Las nuevas tecnologías también pueden utilizarse a favor y en contra de las organizaciones gubernamentales. Tomemos como ejemplo la inteligencia artificial (IA). La IA ayuda a prevenir las amenazas cibernéticas y físicas, a protegerse de ellas y a acelerar las respuestas a estas, pero también permite a los delincuentes descifrar las contraseñas de los sistemas públicos. En el futuro, podemos esperar una situación similar con la computación cuántica, que ayudará a las administraciones públicas a resolver problemas complejos pero también facilitará el descifrado de información sensible.

Consideraciones y retos únicos

Los riesgos específicos introducidos con la digitalización dependen de las tecnologías implementadas. Las redes y tecnologías de comunicación modernas conllevan tres riesgos principales:

- **Interrupciones**: Los fallos y averías de hardware y software pueden producirse en cualquier momento, sin previo aviso. Incendios, inundaciones, condiciones meteorológicas extremas y otros factores imprevistos también pueden causar averías, mientras que los cortes de electricidad pueden afectar a la calidad y estabilidad del suministro eléctrico, provocando fallos y anomalías.
- **Ciberataques**: Los datos confidenciales pueden perderse o ser robados, y las redes y sistemas pueden resultar dañados, lo que ralentizará y detendrá por completo los servicios y operaciones gubernamentales. Los ataques de ransomware pueden tomar redes y sistemas enteros como rehenes, haciendo inaccesibles los datos y las funciones críticas.
- **Obsolescencia**: Los proveedores de tecnología pueden poner fin al soporte de hardware y software, mientras que la escasez de la cadena de suministro puede hacer que sea logísticamente imposible o demasiado caro seguir utilizando soluciones. Los cambios en los requisitos normativos de conformidad también pueden dejar obsoletas las soluciones tecnológicas.

Cada uno de estos riesgos puede dar lugar a otros. Una avería o una tecnología obsoleta puede abrir la puerta a los ciberataques. Y estos, a su vez, pueden provocar una avería o poner de manifiesto que la tecnología se ha quedado obsoleta.

En conjunto, estos riesgos significan que las administraciones públicas deben mejorar su capacidad de prevención, protección y reacción ante las amenazas. No hacer nada ya no es una opción. Seguir utilizando redes y tecnologías de comunicación anticuadas y aisladas, mientras los riesgos siguen multiplicándose, no es un planteamiento viable desde ningún punto de vista.

Enfoque integral y proceso normalizado

Cada administración pública debe desarrollar un enfoque estratégico y táctico de la seguridad y la resistencia adaptado a su perfil de riesgo, ubicación geográfica, mandato, presupuesto y otros requisitos. Sin embargo, aunque los resultados de sus esfuerzos sean diferentes, es conveniente adoptar un planteamiento normalizado y compartir las prácticas recomendadas para obtener mejores resultados.

Un enfoque integral de la mitigación de riesgos permite a las administraciones públicas aumentar la seguridad y la resiliencia en tres áreas clave de su mandato, que incluyen:

- **Ciudadanos:** Para proteger la seguridad de las personas y los datos frente a las amenazas
- **Operaciones:** Para mantener la seguridad y fiabilidad de las funciones, transacciones y servicios en cualquier circunstancia
- **Edificios:** Para hacer más inteligentes y seguros los espacios y organismos públicos

Cuatro pasos para aumentar la seguridad y la resiliencia

Teniendo en cuenta las áreas anteriores, los siguientes pasos pueden ayudar a las administraciones públicas a determinar su perfil de riesgo y a elegir las soluciones de redes y comunicaciones adecuadas para su situación específica.

1. **Evaluar**: Identificar los riesgos cibernéticos y físicos, las áreas de exposición y las posibles consecuencias, así como las diferentes opciones de prevención, protección y reacción ante los ataques en cada caso. Comience con una auditoría y, a continuación, evalúe los riesgos y el potencial de pérdida de cada punto de vulnerabilidad detectado. Esto ayuda a determinar las acciones y soluciones adecuadas en cada caso.

   Aunque la evaluación es el primer paso, no se trata de algo puntual. Para hacer frente al panorama de amenazas en constante cambio, es importante reevaluar periódicamente los riesgos y supervisar continuamente los recursos cibernéticos y físicos en busca de nuevos puntos de vulnerabilidad.
2. **Prevenir**: Elegir soluciones que ayuden a evitar, o contener, riesgos cibernéticos y físicos, tales como:
   - Desde un punto de vista cibernético, busque soluciones con funciones de seguridad integradas que no tengan que adquirirse por separado ni renovarse. Las soluciones deben tener en cuenta la seguridad en cada paso de la definición, desarrollo y entrega del producto, así como contribuir a un entorno tecnológico y arquitectura de confianza cero. También deben ser compatibles con la recuperación y las copias de seguridad automatizadas, así como proporcionar información con fines de auditoría.
   - Desde lo físico, identifique soluciones que aumenten la visibilidad y dificulten el acceso a los activos. Soluciones de videovigilancia, control de accesos, seguimiento de activos, detección de intrusiones y alarmas, servicios basados en la ubicación y reconocimiento facial son buenos ejemplos.
3. **Proteger**: Elegir soluciones que ayuden a protegerse de los riesgos cibernéticos y físicos, por ejemplo:
   - En el ámbito cibernético, asegúrese de que las soluciones están certificadas para cumplir las normas de seguridad, incluyen funciones de cifrado nativo y mecanismos avanzados de autenticación, y limitan la propagación de ciberataques y virus
   - Para aumentar la protección física, vaya más allá de la videovigilancia y tenga en cuenta el papel de las comunicaciones, las alertas y las notificaciones, así como las soluciones para proteger a los trabajadores en lugares aislados
4. **Reaccionar**: Elegir soluciones que permitan una recuperación eficaz en caso de violación de la seguridad, por ejemplo:
   - Las soluciones cibernéticas deben tener el respaldo de un equipo de respuesta a incidentes de seguridad de productos (PSIRT), proporcionar un registro de auditoría y procedimientos de recuperación, así como posibilitar la restauración de datos.
   - Las soluciones físicas deben ser compatibles con las operaciones de mando y control (C2) y las comunicaciones de carácter crítico.

Riesgo, resiliencia y seguridad en administraciones nacionales y locales

	1 Evaluar	2 Prevenir	3 Proteger	4 Reaccionar
Seguridad	✓	✓	✓	
Resiliencia	✓	✓		✓
Cibernética	• Identificación de riesgos • Evaluación • Asignación de activos • Valoración • Supervisión continua	• Segura por diseño • Evaluación de riesgos/auditoría • Asesoramiento preventa • Formación de usuarios • Detección de fraudes • Procedimiento de copia de seguridad • Configuración del registro de auditoría • Robustez en entornos adversos • Redundancia	• Certificación de seguridad • Cifrado • Autenticación	• PSIRT/CERT • Registro de auditoría • Gestión de incidencias • Procedimientos de recuperación • Restaurar
Física	• Identificación de riesgos • Evaluación • Valoración • Supervisión continua	• Videovigilancia • Control de acceso • Seguimiento de activos • Detección y alarma • Servicios basados en la ubicación • Reconocimiento facial • Redundancia	• Videovigilancia • Comunicaciones • Alerta y notificación • Protección para trabajadores aislados	• Control y mando • Comunicaciones de carácter crítico

La resiliencia y los mecanismos de respuesta ágil son clave para prosperar frente a los riesgos

«La resiliencia es algo más que la capacidad de recuperarse rápidamente. En el mundo empresarial, la resiliencia significa hacer frente a la adversidad y las crisis, así como adaptarse continuamente para seguir creciendo. Las organizaciones verdaderamente resilientes no solo se reponen mejor, sino que prosperan en entornos hostiles... La agilidad permite a las organizaciones responder de forma única a cada crisis, en lugar de aplicar soluciones inflexibles y universales.» ”

— McKinsey & Company

Reforzar la seguridad y la resiliencia

Las administraciones públicas que siguen el enfoque y proceso integral recomendado en el apartado anterior tienen nuevas oportunidades de aprovechar las soluciones de redes y comunicaciones para aumentar la seguridad y la resiliencia de los ciudadanos, operaciones, edificios y espacios.

Protección de la seguridad ciudadana

Gracias a las soluciones de videovigilancia de última generación, los funcionarios del Estado y la seguridad pública pueden ver en tiempo real los sucesos y emergencias a medida que se desarrollan, lo que aumenta significativamente el conocimiento de la situación. A continuación, pueden utilizar una plataforma de gestión de flujos de trabajo y orquestación de seguridad pública para compartir ese conocimiento y coordinar las respuestas. Los equipos de los distintos organismos y sedes de las administraciones públicas pueden compartir fácilmente observaciones e información contextual puntuales utilizando la combinación óptima de comunicaciones de voz, vídeo y texto para facilitar una toma de decisiones más eficiente, eficaz y colaborativa.

Los sistemas de notificaciones masivas pueden alertar rápidamente a las personas y los procesos de las emergencias para que puedan tomar las medidas adecuadas con mayor rapidez. Las llamadas de funcionarios sobre el terreno tienen acceso prioritario a los centros de contacto de la administración pública, y las funciones de preservación de llamadas mantienen a funcionarios y ciudadanos conectados con el personal del centro de contacto en cualquier circunstancia. Las soluciones de comunicaciones para trabajadores aislados, emergencias médicas y rastreo de contactos agilizan más las respuestas y aumentan la sensibilización sobre las situaciones potencialmente peligrosas.

Para ayudar a prevenir las emergencias y acelerar las respuestas, las soluciones de IA conectadas a múltiples fuentes de datos pueden utilizarse para identificar riesgos y sucesos potencialmente problemáticos, así como para automatizar los flujos de trabajo.

Mayor fiabilidad en las operaciones

Una red empresarial segura y resiliente da soporte a las comunicaciones de carácter crítico, así como a las tecnologías de IoT, ciberseguridad y seguridad física que son esenciales para un funcionamiento fiable.

Las soluciones de redes ideales incluyen funciones clave que protegen el acceso a la red y la información que esta transporta:

- **Código fuente y software reforzados en los conmutadores de red**: El código fuente es deliberadamente diverso, para que a los posibles atacantes les resulte mucho más difícil explotar los puntos de vulnerabilidad. Además, el código y el software se verifican y validan de forma independiente para garantizar su integridad y seguridad.
- **Macrosegmentación y microsegmentación**: En el contexto de la confianza cero, la segmentación recibe especial atención tanto a nivel macro como micro. La macrosegmentación divide la red en zonas distintas sobre la base de factores como la función, la aplicación o el grupo de usuarios, a fin de aislar los recursos y activo críticos del resto de la red. La microsegmentación adopta un enfoque más granular, segmentando la red a nivel de usuario o dispositivo para permitir un control más preciso sobre el acceso a la red y la imposición de directivas de seguridad.
- **Operaciones autónomas**: La automatización de la colocación de activos y recursos en macrosegmentos y la aplicación de directivas a nivel de usuario y dispositivo ayudan a reducir el riesgo de errores humanos, una causa común de las violaciones de la ciberseguridad.
- **Equipos robustos**: Los equipos de red pueden soportar condiciones duras, como temperaturas extremas y vibraciones intensas. El equipo admite redundancia de alimentación de dos fuentes para garantizar un funcionamiento continuo durante los cortes de energía. Un tiempo medio entre fallos (MTBF) elevado puede garantizar la fiabilidad, minimizando las interrupciones inesperadas y las alteraciones causadas por averías y fallos.

Las administraciones públicas también ganan flexibilidad para implementar soluciones de redes y comunicaciones tanto en sus instalaciones como en entornos de nube pública y privada. Estas opciones de implementación permiten aplicar estrategias de redundancia geográfica y espacial que son clave para mantener la continuidad operativa durante los fallos y emergencias, incluso en emplazamientos remotos.

Aumentar la seguridad y la protección en edificios y espacios

Se necesita una red multiservicio segura para dar soporte a las aplicaciones y procesos necesarios para protegerse de los riesgos y mantener la disponibilidad del servicio en todo momento. Además, para dar cabida al creciente número de dispositivos inalámbricos conectados a la red Wi-Fi, las administraciones públicas necesitarán una red inalámbrica robusta y fiable que funcione sin problemas ni congestiones que puedan reducir su eficiencia.

Las mismas soluciones avanzadas de videovigilancia que ayudan a proteger a los ciudadanos también ayudan a mantener seguros los edificios y espacios públicos. Estas soluciones se complementan con el seguimiento de activos, que agiliza y facilita la localización de personas y activos críticos en caso de imprevistos y emergencias.

Las administraciones públicas disponen ahora también de las capacidades de automatización necesarias para implementar y gestionar eficazmente soluciones de IoT para aplicaciones de seguridad y protección, como el control de accesos y el seguimiento de activos. Pueden incorporar de forma segura y automática un gran número de nuevos dispositivos IoT mediante la creación de huellas dactilares, la clasificación y la contenerización de dispositivos, evitando así el riesgo de que se introduzcan puntos de vulnerabilidad por causa de las distracciones del personal informático.

Un socio para sus estrategias

A medida que aumentan los riesgos para las administraciones públicas, también crece la necesidad de contar con un socio tecnológico experto.

Alcatel-Lucent Enterprise, empresa innovadora en tecnología desde hace más de 100 años, ha desarrollado un marco de riesgo, resiliencia y seguridad (RRS) que se ajusta a los requisitos de las administraciones públicas. El marco RRS incluye los procesos, las prácticas recomendadas y las soluciones que las administraciones necesitan para predecir, controlar, evitar y combatir la exposición a los riesgos cibernéticos y físicos.

El equipo de ALE, formado por especialistas en administraciones públicas con amplios conocimientos, colabora con los responsables de estas para ayudarlos a:

- Identificar su propio grupo de riesgos y elegir soluciones para afrontarlos
- Reducir la brecha entre la seguridad cibernética y física y la resiliencia
- Argumentar a favor de las aprobaciones presupuestarias

Soluciones flexibles y totalmente conformes

ALE integra la seguridad en sus soluciones de redes y comunicaciones desde las primeras fases de diseño. Para garantizar la máxima seguridad y resiliencia, las soluciones:

- Se elaboran con medidas de seguridad que cuentan con la confianza de las organizaciones públicas y de defensa de todo el mundo
- Se someten a pruebas con técnicas especializadas y específicas para la seguridad, como las pruebas de penetración
- Cumplen las normas mundiales, sectoriales y regionales en materia de seguridad y privacidad de los datos, incluidas las principales normas de seguridad del sector, como Common Criteria EAL2+
- Pueden implementarse en cualquier combinación de modelos locales y en la nube para satisfacer los requisitos más complejos.
- Son compatibles con los estándares abiertos, a fin de reducir la complejidad de la integración y las incompatibilidades entre soluciones y proveedores

Además de los modelos de compra tradicionales, ALE ofrece planes de suscripción para que los clientes puedan acceder a las últimas tecnologías y avances en seguridad sin renunciar a las limitaciones presupuestarias. También está disponible un paquete completo de servicios que presta apoyo a las administraciones públicas en cada fase de su transformación.

Experiencia y conocimientos

Los expertos y las soluciones de ALE cuentan con la confianza de organizaciones nacionales y locales de todo el mundo. Estos son solo algunos ejemplos:

- Metz Eurometropolis en Francia, donde ALE ayudó al área metropolitana a garantizar la continuidad de las comunicaciones y los servicios críticos, a poner rápidamente a disposición servicios de emergencia y a conectar de forma segura usuarios y objetos conectados a través de los edificios. .
- El Gobierno escocés, donde las soluciones de ALE proporcionan a más de 40 organismos públicos una infraestructura coherente, segura y fiable, control de acceso a la red y refuerzo de la seguridad de los datos.
- El Departamento de Defensa de los EE. UU., donde las soluciones robustas y modernas dan soporte fiable a las comunicaciones y aplicaciones de carácter crítico, al tiempo que cumplen todos los requisitos medioambientales y anticrisis, así como la Ley Federal de Acuerdos Comerciales (TAA) y los requisitos de certificaciones de defensa..
- Gwinnett County Public Schools en los EE. UU., donde las soluciones de ALE dan soporte, entre otras cosas, a la seguridad física, la videovigilancia, el servicio E-911 y la computación segura en un gran distrito escolar donde la seguridad y la protección son primordiales.

Más información

Si desea saber cómo Alcatel-Lucent Enterprise puede ayudar a su organización a mitigar los riesgos para aumentar la seguridad y la resiliencia, visite el sitio web o póngase en contacto con nosotros hoy mismo.

DID23061901ES (Diciembre de 2023)

Alcatel·Lucent Enterprise