Data-A

Águilas News

Diciembre 2020

Videoseguridad: Un aliado en la lucha contra la emergencia sanitaria.

5 Estrategias para prevenir los ciberataques en tiempos de trabajo remoto.

VIDEOSEGURIDAD, UN ALIADO EN LA LUCHA CONTRA LA EMERGENCIA SANITARIA

Por: Pedro Duarte / Seguridad en América

Los gobiernos y las instituciones deben aprovechar las tecnologías que mejoren sus capacidades de identificación y respuesta en momentos críticos.

En medio de todos los problemas sociales, económicos y climáticos que afligen al mundo, nos enfrentamos a una emergencia sanitaria provocada por la pandemia del COVID-19, una situación que ningún gobierno contemplaba y para la cual no estábamos preparados con planes de contingencia de seguridad. Para América Latina, la presión de esta situación sin precedentes plantea una grave amenaza para la salud y, ciertamente, un gran desafío para las ciudades en todos los frentes.

La presión pone a prueba y expone, lo mejor y lo peor, de las acciones de seguridad ciudadana, el trabajo coordinado entre las instituciones gubernamentales, la labor del sector salud y los servicios de emergencia, así como las operacioens de seguridad pública en el marco de los asentamientos urbanos deficientemente planificados, y una región con algunas de las ciudades más pobladas pero dispares del mundo.

A medida que la pandemia evoluciona, los planes de respuesta de los gobiernos cambian a diario para identificar rápidamente a las personas con síntomas relacionados, ya que esto es fundamental para contar con planes de respuesta eficaces que limiten la propagación del virus y eviten que los hospitales y las instalaciones de atención médica se vean desbordados. México se enfrenta a un momento crucial. Debe elegir acciones para aplanar la curva de infección, y minimizar así no sólo la mortalidad, sino también la gran crisis económica.

Frente a esta necesidad urgente, los gobiernos y las instituciones deben aprovechar las tecnologías que mejoren sus capacidades de identificación y respuesta en momentos críticos.

LA VIDEOVIGILANCIA ANTE EL COVID 19

Especialmente centradas en las tecnologías que permiten reconocer situaciones y personas con precisión y rapidéz, las soluciones de videovigilancia se convierten en un eslabón clave para la implementación de estrategias de seguimiento, protección y prevención. Ejemplos de esto son situaciones en las que hay grandes multitudes y dificultades para el distanciamiento social, como los hospitales y centros de atención médica, salas de espera, etc.

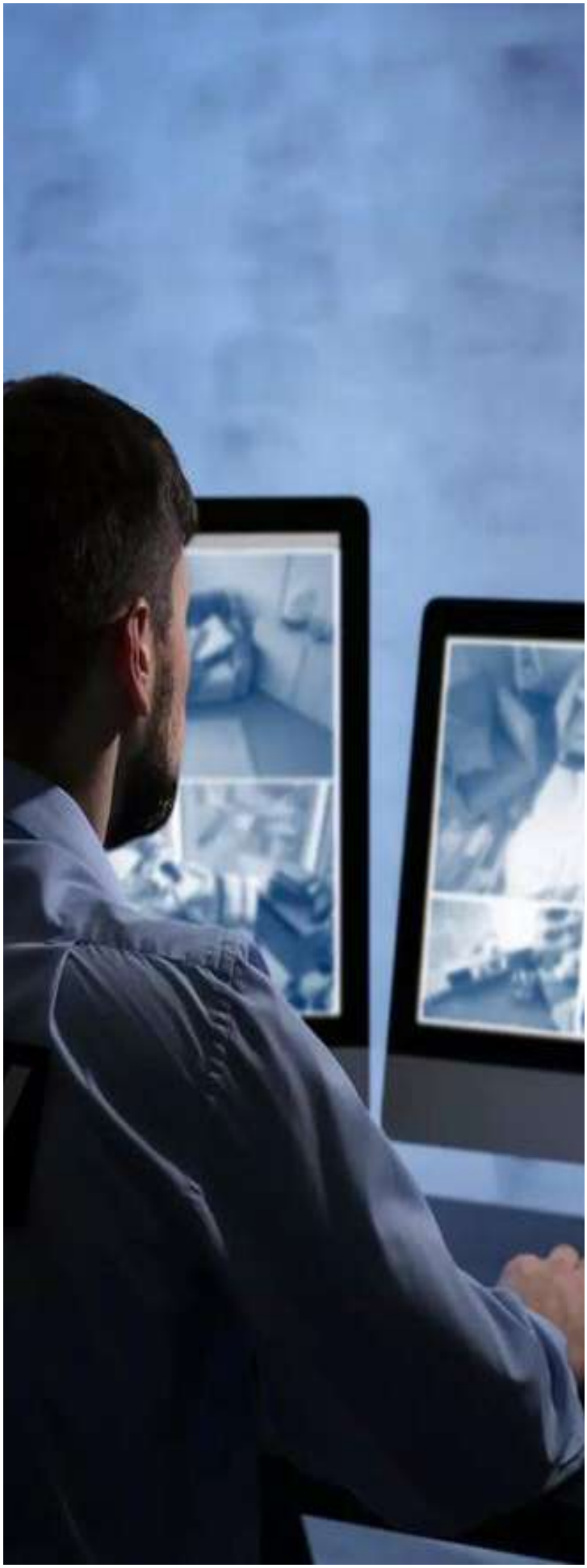
Es en estos lugares donde las cámaras de videovigilancia con inteligencia artificial aumentan el conocimiento y el contexto del sitio que protegen, lo que las convierte en una herramienta que nos ayuda a responder rápidamente al identificar a las personas sospechosas de estar infectadas para separarlas de las zonas de gran afluencia de gente.

Las soluciones de videovigilancia se convierten en un eslabón clave para la implementación de estrategias de seguimiento, protección y prevención.

De esta manera es posible limitar la propagación del virus y realizar un seguimiento oportuno, lo que se convierte en una pieza clave del rompecabezas para la contención en una situación de alto riesgo. Así, mediante el uso de evidencia registrada en video de alta calidad y herramientas como la búsqueda por apariencia y el reconocimiento facial, podemos determinar de manera eficiente todas las posibles instancias de contacto que una personas específica tuvo durante su paso por un lugar determinado.

Esto a su vez, nos permite identificar los lugares, el contacto con otros y superficies, de modo que, con base en esta evidencia registrada en video de alta calidad, podemos establecer claramente una potencial cadena de infección y tomar las acciones más efectivas orientadas a la contención.

Avigilon, una empresa de Motorola Solutiones, es líder mundial en soluciones de videovigilancia y, junto con Motorola, ha estado en la primera línea de la emergencia, trabajando con los gobiernos federales, del estado y locales de América Latina, para ayudar a salvar las distancias en cuanto a la disponibilidad de tecnología para las operaciones médicas y sanitarias necesarias para luchar contra la pandemia del COVID-19.



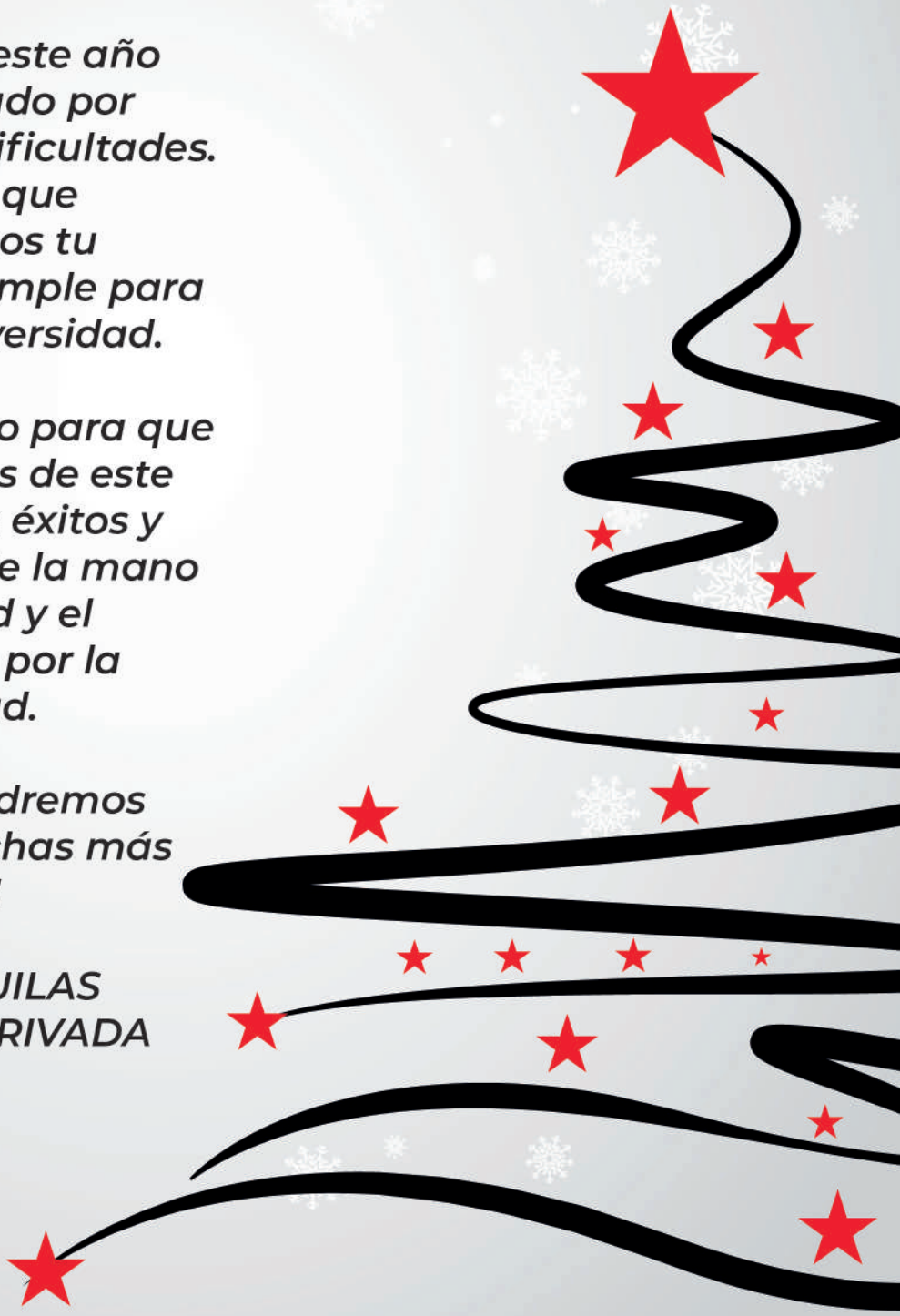
¡Feliz Navidad!

Sabemos que este año estuvo marcado por grandes retos y dificultades. Es por ello que agradecemos tu compromiso y temple para afrontar la adversidad.

Contamos contigo para que juntos hagamos de este 2021 un año de éxitos y satisfacciones, de la mano con la salud y el compromiso por la seguridad.

¡En equipo podremos consolidar muchas más metas!

GRUPO ÁGUILAS
SEGURIDAD PRIVADA



5 ESTRATEGIAS PARA PREVENIR LOS CIBERATAQUES EN TIEMPOS DELTRABAJO REMOTO

Por: Israel Austria / Noticias ALAS

Según la jefa de desarme de la ONU, Izumi Nakamitsu, la creciente dependencia digital aumenta la vulnerabilidad a los ciberataques, por lo cual en medio de la presente crisis se ha registrado un ataque de hackers cada 39 segundos y los ciberdelitos se han incrementado en un 600 %.

En América Latina, dos de cada tres ataques de este tipo son dirigidos a empresas, tal como lo revela el informe de este año del Panorama de Amenazas de Kaspersky. El reporte sitúa a Brasil con el mayor número de ataques (55.97 %), acompañado de México (27.86 %), Colombia (7.33 %), Perú (5.36 %), Argentina (1.87 %) y finalmente Chile (1.62 %).

Este panorama se presenta desafiante para todos los actores del ecosistema de seguridad, tanto integradores como clientes finales. ¿Cómo pueden enfrentar esta amenaza reinante? Hay una serie de estrategias para combatir ciberataques que se pueden adoptar:

1. Aislar la red del dispositivo de otras redes

Aislar la red de dispositivos, aquella donde se ubican las cámaras, micrófonos, altavoces, dispositivos de entrada / salida y otros IP asociados, es quizás la medida de configuración de seguridad más importante como estrategia para combatir ciberataques. Esto lo permite la arquitectura por niveles de un sistema de gestión de video (VMS).

De esta manera, con el servidor de grabación como punto de conexión entre el dispositivo y las redes del cliente, no hay un enrutamiento directo entre los dos segmentos de la red. Esto significa que un ciberataque en cualquiera de las redes no se propagará a la red de dispositivos ni fuera de ella. Fuera de aislar la red del dispositivo, todos los dispositivos deben utilizar contraseñas seguras no predeterminadas para mitigar otros problemas potenciales.

2. Controlar el tráfico de la red al segmentar VMS, clientes y redes comerciales

La segmentación es una de las estrategias más eficaces para combatir ciberataques, pero a menudo es pasada por alto. Las diferentes redes se pueden separar entre sí mediante un dispositivo de firewall o por un aislamiento total a través de una infraestructura de conmutación separada físicamente para diferentes sistemas. En la industria de VMS, el aislamiento total de las redes suele ser el enfoque estándar. Esto elimina todo tipo de amenazas que se originan en otras redes.

Sin embargo, más comúnmente, las redes se separan mediante un dispositivo de firewall y redes de área local virtuales (VLAN). Este enfoque hace que sea más difícil para los atacantes moverse de una red a otra si obtienen acceso. También mejora la administración de la red al concentrar las reglas del firewall en un solo lugar.

3. Utilizar Active Directory para la administración de usuarios y equipos

Active Directory (AD) es un sistema de administración de usuarios centralizado que autentica y autoriza usuarios y computadoras en un dominio. También asigna y aplica políticas de grupo para todos los equipos, incluida la configuración de seguridad.

La gestión de usuarios es un aspecto importante dentro de las estrategias para combatir ciberataques. Sin una base de datos de usuarios central, la administración de varias cuentas de usuario en diferentes sistemas puede resultar difícil y requiere mucho tiempo. Al utilizar un sistema centralizado como AD, los usuarios se pueden agregar y eliminar en un solo lugar, y el cambio se aplica en todo el sistema.

Esto evita que antiguos empleados y contratistas recuperen el acceso a sistemas en los que no se les fue revocado debido a un simple error humano. La estructura centralizada de AD simplifica muchas tareas de TI, minimizando los errores que ocurren en una configuración descentralizada.

4. Habilitar el cifrado en todas las etapas necesarias

Una de las estrategias para combatir ciberataques más importantes observadas tanto en la web como en el espacio VMS durante los últimos años es el cifrado. Cuando los datos son confidenciales y existe la posibilidad de acceso no autorizado, ya sea al escuchar el tráfico de la red o al acceder a los datos almacenados, el cifrado es la herramienta adecuada para protegerlos. Como regla general, los datos del dispositivo fluyen a través de varios pasos. Primero es recibido a través de la red por un servidor de grabación. Entonces puede que se grabe o no en el disco según la configuración del sistema. Las aplicaciones del cliente solicitan datos en vivo o grabados a pedido.

Finalmente, si se considera necesario, los datos se pueden exportar y entregar a las autoridades. Todas estas etapas plantean riesgos de ciberseguridad, así como riesgos de privacidad para los sujetos de los datos. El uso de cifrado en todas las etapas evita el acceso no autorizado.

5. Educar a los empleados sobre las amenazas a la seguridad

La educación y la conciencia son fundamentales como estrategias para combatir ciberataques, al enseñar a los empleados cómo identificar y contrarrestar una variedad de ciberamenazas. Considere la posibilidad de establecer una capacitación en concientización sobre ciberseguridad que cubra las brechas en la protección que muchas organizaciones deben mitigar, incluidas vulnerabilidades humanas, tecnológicas y físicas.

Los individuos maliciosos a menudo recurren a la ingeniería social porque encuentran que los objetivos humanos son los más fáciles de explotar y las recompensas son las mayores. La ingeniería social es un conjunto de tácticas que utilizan los atacantes para obtener información valiosa de otra persona. Esto se puede hacer de diversas formas, pero todas se basan en la tendencia natural de las personas a ser corteses y confiar unos en otros. A menudo, la víctima no tiene ni idea de que existe una amenaza.

RECOMENDACIONES DE SEGURIDAD

Al salir de compras

1. Lleva sólo el dinero necesario, y si puedes, paga tus compras con tarjetas bancarias.

2. Deja bien cerrado y en una zona iluminada tu vehículo. No dejes objetos de valor a la vista.

3. Realiza tus compras con tiempo, para evitar aglomeraciones que representen riesgo para tu salud.

4. No lleves niñas, niños o adultos mayores, embarazadas o personas vulnerables ante COVID-19.

5. Evita exhibir tus compras o regalos y adquiere tus artículos en lugares establecidos.

Al recibir tu aguinaldo

1. No comentes a extraños la cantidad ni la fecha en que recibirás tu aguinaldo.

2. Si te pagan en efectivo, acude a cobrar en grupo o con alguien de confianza.

3. No lleves el dinero en un solo sitio, como bolso o cartera, distribúyelo en las bolsas de tu ropa.

4. Cuando lo recibas, verifica que no haya nadie sospechoso a tu alrededor.

5. Mantente atento siempre que vayas a un cajero y nunca aceptes ayuda de extraños.

SEGURIDAD PRIVADA

SERVICIOS INTEGRALES

1. Seguridad Intramuros
2. Herramientas Tecnológicas
3. Traslado de personal VIP
4. Unidades K9
5. Seguridad Electrónica
6. Traslado de Mercancía en tránsito

A NIVEL NACIONAL

SEGURIDAD

PARA TU EMPRESA

COTIZA CON NOSOTROS

ventas@grupoaguilas.com