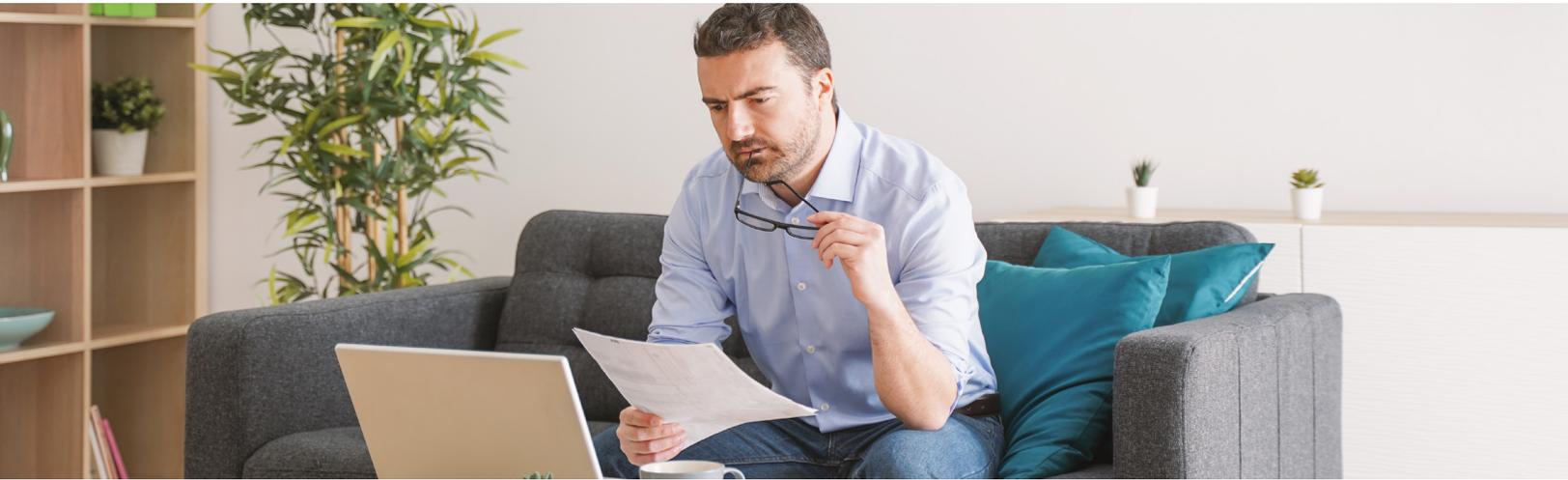


Soluciones para empleados remotos



Para limitar el número de empleados dentro de un lugar de trabajo durante cierto lapso de tiempo, muchas empresas están exhortando o exigiendo que los trabajadores no esenciales trabajen desde su casa. Sin embargo, también es importante para ellos proteger a esos empleados de cualquier riesgo, independientemente de dónde se encuentren, así como de resguardar los activos que se les otorga para trabajar desde casa. Cuando su personal no está protegido por la infraestructura de seguridad proveída en la oficina, existen elementos críticos a considerar tanto físicos, como de seguridad de la información.

Cuando se consideran los aspectos físicos del trabajo remoto, garantizar la seguridad del personal es un factor clave. Tal vez sea necesario comunicarse rápidamente con los empleados, ya sea que se encuentren en sus instalaciones o trabajando remotamente. El saber en dónde están sus empleados podría ser necesario debido a varias razones, por ejemplo, tener controles de seguridad durante desastres naturales o verificar su seguridad durante otros incidentes públicos importantes, como protestas masivas. Además, tiene el deber de proteger la información de su empresa y propiedad intelectual, así como otros materiales que pueden ser emitidos por trabajadores remotos. El espionaje comercial puede tener un impacto catastrófico en su negocio. Con más personas trabajando de forma remota, su empresa podría ser susceptible a ataques cibernéticos, donde los sistemas son pirateados y los datos confidenciales se descargan, copian o roban; además de la pérdida de activos físicos como computadoras, o la pérdida de información clave a través de ataques de ingeniería social hacia el personal que no tiene el conocimiento de cómo proteger la propiedad intelectual crítica de la compañía mientras trabaja desde casa.

Como su asesor en seguridad de confianza, G4S puede

proporcionar capacitación a los empleados, protecciones físicas, procesos de seguridad para empleados que trabajen remotamente y desarrollo de procedimientos; también soluciones para la seguridad de información para ayudar a proteger a sus trabajadores remotos. Los Analistas de Riesgos que trabajan en un Centro de Operaciones de Seguridad (SOC por sus siglas en inglés) pueden ayudar a monitorear la seguridad de sus empleados clave. Si la seguridad de un empleado está en riesgo, los analistas pueden informar al personal de emergencia. G4S ofrece herramientas de monitoreo de ubicación y una herramienta de recopilación por medio de inteligencia artificial aumentada que le avisa de inmediato cuando se producen incidentes que puedan afectar la seguridad de un empleado.

PREGUNTAS FRECUENTES

- ¿Cómo puedo proteger mejor la seguridad de mis empleados cuando no están en la oficina?
- ¿Cómo puedo proteger la propiedad intelectual de nuestra empresa cuando los empleados trabajan de forma remota?
- ¿Cómo puedo realizar una evaluación de mis trabajadores remotos?

G4S ha organizado soluciones fáciles de seguir en tres categorías: personas, proceso y tecnología. Esto le ayudará a personalizar la solución perfecta basada en sus necesidades y su presupuesto. También puede ayudar a su organización a desplegar una estrategia estructurada basada en los riesgos inmediatos que tenga su compañía y en sus objetivos a largo plazo.

PERSONAS



los operadores supervisarán la seguridad del personal clave, mientras que los profesionales de riesgo lo ayudarán a entender cómo el trabajo remoto afecta su perfil general de riesgo de seguridad.

PROCESO



una evaluación de riesgos puede ayudarlo a desarrollar reglamentos y procedimientos para reducir el riesgo a sus empleados remotos y organización.

TECNOLOGÍA



las herramientas de monitoreo de ubicación protegen a su personal en el campo, con el apoyo de herramientas como el servicio de inteligencia artificial aumentada (IAaS); los servicios de ciberseguridad reducen el riesgo de un ataque cibernético.



PERSONAS

Los operadores que trabajan en un centro de operaciones de seguridad supervisarán la seguridad de sus ejecutivos clave. Trabajan las 24 horas del día, los 7 días de la semana y, si se requiere, informarán al personal de emergencia si la seguridad de su empleado está en peligro. Los analistas de riesgos cuentan con títulos avanzados, son multilingües y, a menudo, ex-agentes policíacos con antecedentes privados y militares. Los asesores de riesgos realizarán una evaluación integral de sus trabajadores remotos y su entorno.



PROCESO

Realizaremos una evaluación de riesgos en la que consideraremos lo que se debe proteger (por ejemplo, su empleado, la propiedad intelectual de la empresa), de qué situación se debe proteger y cómo se puede proteger de manera más efectiva. Vincularemos nuestros conocimientos al valor de sus activos para garantizar que la organización no sufra daños. Si tiene un proceso de evaluación de riesgos ya existente, nos alinearemos con usted y le brindaremos soluciones para ayudar a proteger su organización.



TECNOLOGÍA

G4S ofrece herramientas de monitoreo de ubicación que brinda información práctica sobre la ubicación de su empleado clave y puede reducir el tiempo de respuesta de un centro de emergencias en caso de ser necesario. Puede rastrear y localizar fácilmente a sus empleados con tecnología GPS y supervisar, controlar y enviar oficiales desde un centro de comando. Puede ver el estado, la disponibilidad, la proximidad y el tiempo de llegada estimado al incidente. La herramienta de servicio de inteligencia artificial aumentada de G4S le alerta de inmediato cuando se producen incidentes que pueden afectar la seguridad de sus empleados. Si actualmente está abrumado por el gran volumen de información asociada con la pandemia, puede confiar en G4S para filtrar la información de eventos críticos en una imagen clara y relevante para que brinde mejores resultados y así proteger a su gente.

Para el personal clave, G4S puede recomendar soluciones cibernéticas para ayudar a proteger la información de su empresa cuando se tiene acceso a ella de forma remota. Los trabajadores remotos a menudo carecen de conocimiento sobre temas de ciberseguridad. Muchos empleados están trabajando desde casa por primera vez. No conocen las mejores prácticas que los trabajadores remotos experimentados conocen bien, como por ejemplo usar un VPN en redes públicas o no guardar información confidencial en sus dispositivos personales. Los empleados no informados son la causa número uno de las infracciones de seguridad cibernética y el riesgo aumenta exponencialmente cuando se trabaja de forma remota. G4S recomienda capacitación en ciberseguridad y una evaluación de riesgos acerca del tema para sus ejecutivos remotos con el fin de proteger su negocio de un espionaje comercial.

CONTÁCTENOS AHORA PARA UNA CONSULTA GRATIS DE VENTAS VIRTUAL.
WWW.G4S.COM/ES-AR