# WEBINAR

## Protege a tu personal para trabajar de forma remota

**Paul Rangel**
Especialista de Ciberseguridad
CISSP, CIAM, CAMS, CIMP

**Eduardo Palacio**
Arquitecto de Ciberseguridad

infosecurity® MEXICO

En alianza con

ISACA. Mexico City Chapter

ISACA. Guadalajara Chapter

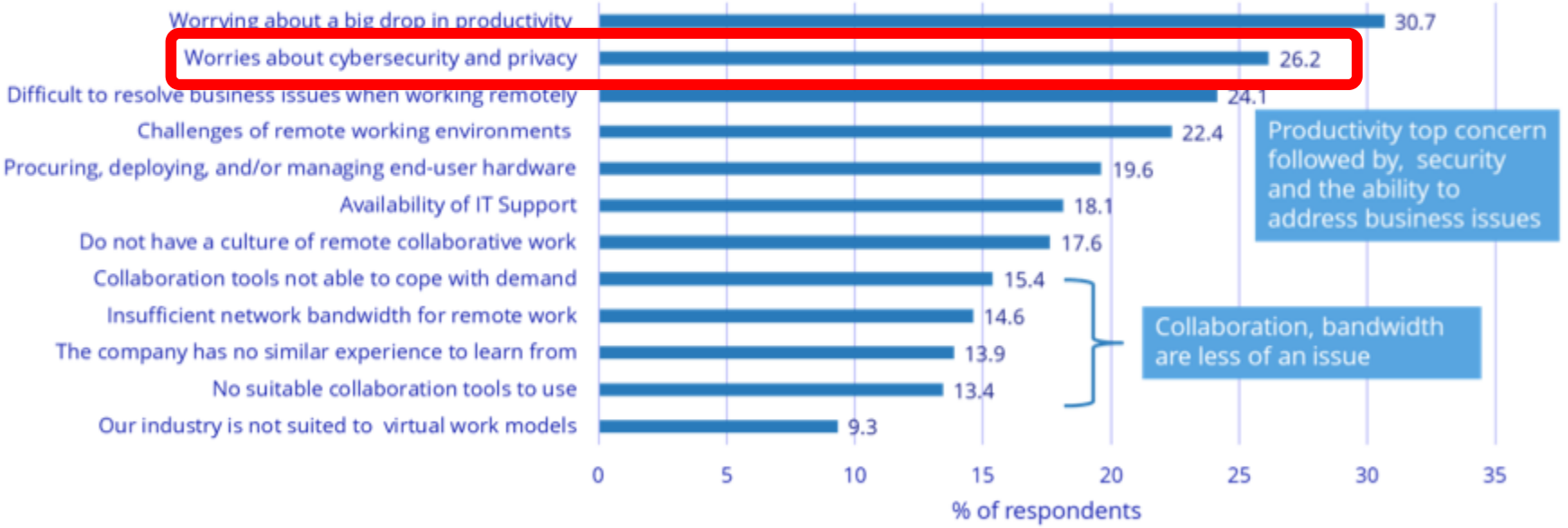
Organizado por Reed Exhibitions®

# IDC Survey Spotlight

## What are the biggest challenges to organizations globally in adjusting to remote work in the COVID-19 era?

Holly Muscolino

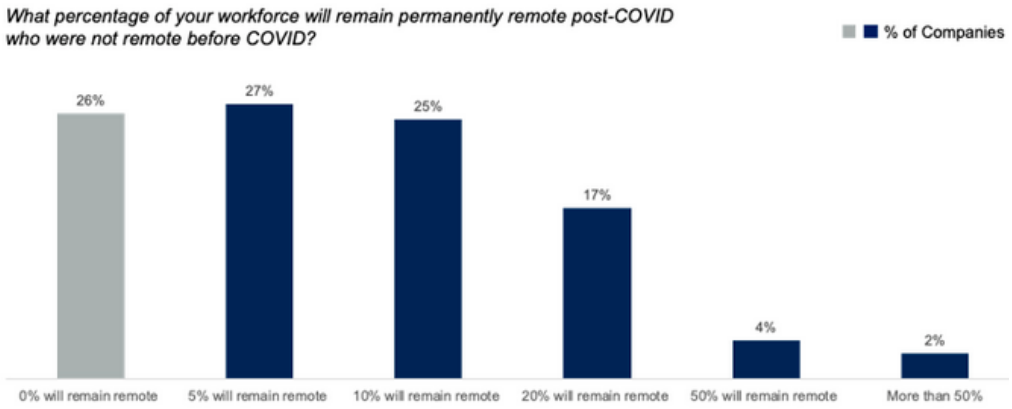
**Q. For supporting work-at-home/remote working, what are your organization's biggest challenges?**






IDC# US46243520 (April 2020)
Source: COVID-19 Impact on IT Spending Global Survey, N=582

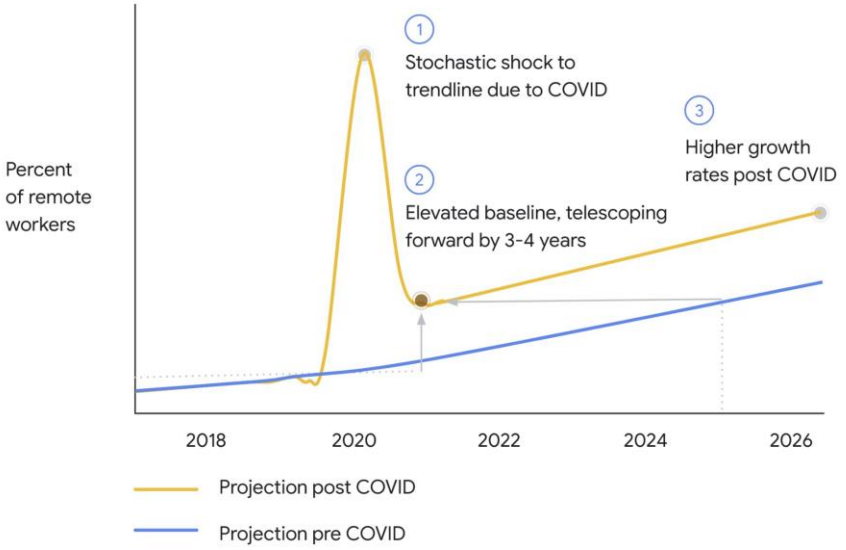
**Figure 1: 74% of Companies Plan to Permanently Shift to More Remote Work Post COVID-19**




Source: Gartner (April 2020)

~25% de las organizaciones tendrá a al menos 20% de sus empleados en trabajo remoto

El camino hacia el trabajo remoto se adelantará por 3-4
años en el mundo post-Covid




https://cloud.google.com/blog/products/chrome-enterprise/the-remote-work-revolution

# COVID-19

## Un reto de ciberseguridad

**Corona Lockdown: Work from home makes you vulnerable to cyber attacks**

By: Amitava Chakrabarty | Published: April 15, 2020 8:52:53 PM

Sniffing the opportunity at the time of lockdown, desperate cyber criminals are using coronavirus-themed emails and files as a lure for weeks.


**Trabajo en casa y ciberseguridad en tiem covid-19**

ESPECIAL

El *home office* podría atraer situaciones que vulneren a empresas durante la contingencia

TECNOLOGÍA

**El COVID-19 endurece las reglas de ciberseguridad en las empresas**

Ante una nueva normalidad de personas y máquinas más conectadas, expertos destacan la necesidad de nuevas regulaciones de ciberseguridad.

mar 19 mayo 2020 06:00 AM

threatpost | Cloud Security | Malware | Vulnerabilities | Waterfall Security Spotlight

**Malware Risks Triple on WFH Networks: Experts Offer Advice**

**Remote Working Is Transforming The Cyber Security Landscape in 2020**

COVID-19 Exploitations: Malicious Cyber Actors Strike with Pandemic-Related Scams

**Quarles & Brady LLP**

**La ciberseguridad cobra importancia en tiempos de Covid-19**

Por **Manuel Navarro** - 27 abril, 2020 0

# COVID-19 ha cambiado el panorama de seguridad

**14,000%**

incremento en spam y phishing relacionado a COVID-19

**84%**

incremento en el uso de herramientas de trabajo remoto desde inicio de Febrero

# Vectores de ataque

## Credenciales comprometidas

Acceso malicioso usando credenciales válidas que podrían haber sido adquiridas mediante phishing o robadas por ingeniería social

## Dispositivos comprometidos

Acceso remoto usando un dispositivo personal no administrado que está infectado con malware, está siendo spoofeado o algún otro indicador de riesgo

## Contexto

Uso de aplicaciones o sitios no autorizados usando redes inseguras con poca auditabilidad y riesgos de cumplimiento

# En estos tiempos de incertidumbre, las organizaciones necesitan...

01

Habilitar y proteger a la fuerza de trabajo remota

02

Detectar y responder a las crecientes amenazas

03

Extender virtualmente al equipo de seguridad e incrementar rápidamente sus habilidades

# En estos tiempos de incertidumbre, las organizaciones necesitan...

01

Habilitar y proteger a la fuerza de trabajo remota

02

Detectar y responder a las crecientes amenazas

03

Extender virtualmente al equipo de seguridad e incrementar rápidamente sus habilidades

# Mejores prácticas protección de dispositivos móviles y endpoints

## 1 Dispositivos seguros

Cumplir con requerimientos mínimos de seguridad en los dispositivos móviles y endpoints que se conectan a la compañía (incluyendo BYOD)

Detección de dispositivos con malware o rooteos/jailbrake

## 2 Aplicaciones Autorizadas

Utilizar únicamente aplicaciones aprobadas por las compañías.

Distribución de aplicaciones correctas y seguras

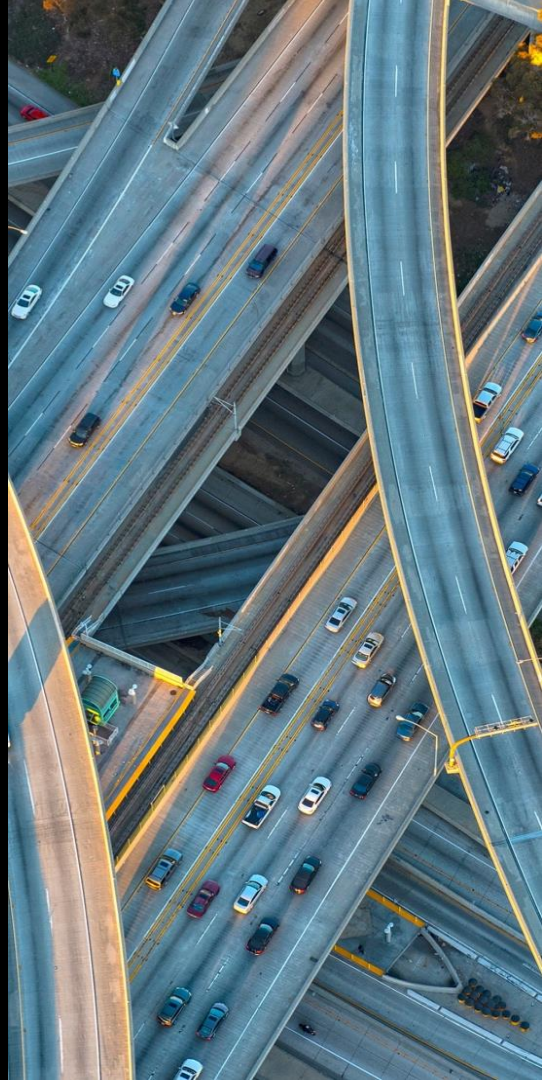
Bloquear accesos a sitios no autorizados

## 3 Proteger los datos

Distribuir y proteger documentos confidenciales de manera segura y por medios aprobados por la organización

## 4 Uso de Inteligencia Artificial

Facilitar la investigación de amenazas y posibles riesgos de seguridad



# Mejores prácticas acceso de los usuarios a las aplicaciones

## 1 Almacén de contraseñas

Utilizar soluciones seguras que permitan el almacenamiento de las contraseñas de acceso a las cuentas

## 2 Mejorar la experiencia del usuario

Facilitar la experiencia del usuario al ingreso a las aplicaciones sin poner en riesgo la seguridad

Autenticación solo cuando realmente sea necesario

## 3 Detección de Riesgos

Detectar riesgos en el acceso de los usuarios para verificar su autenticidad

Machine Learning

Segundos factores de autenticación

## 4 Ciclo de vida de las cuentas

Tener mecanismos automatizados para las Altas, Bajas y Cambios en las cuentas

Campañas de recertificación

# En estos tiempos de incertidumbre, las organizaciones necesitan...

01

Habilitar y proteger a la fuerza de trabajo remota

02

Detectar y responder a las crecientes amenazas

03

Extender virtualmente al equipo de seguridad e incrementar rápidamente sus habilidades

# Mejores prácticas de detección de riesgos y respuesta

## 1 Análisis de factores de riesgo

Recolectar, correlacionar y analizar atributos contextuales de:

-Usuario

-Dispositivo

-Actividad

-Ambiente

-Comportamiento

## 2 Contexto del análisis

Contextualizar las amenazas a partir de inteligencia de cibercrimen global

Bases de datos de reputación de Ips, URLs, ISPs, etc.

Investigación de campañas de phishing, malware e ingeniería social en la Deep web.

## 3 Aplicación de Inteligencia Artificial

Análisis con IA de casos, observables, IOCs

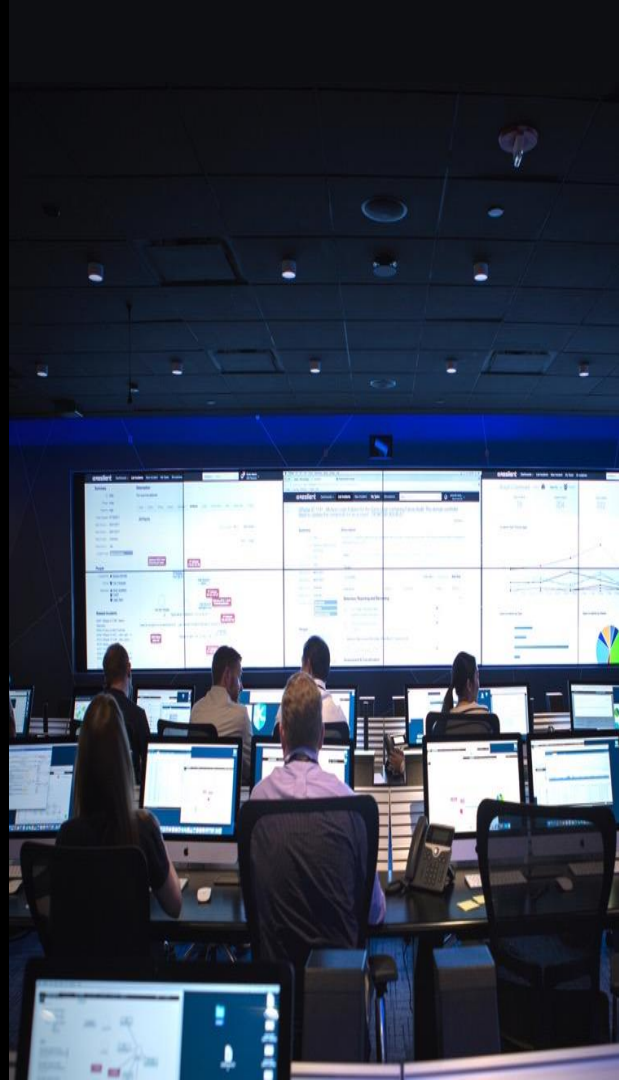
Optimización automática de políticas y reglas de detección

## 4 Integración Operativa

Automatización de alertamiento priorizable

Respuesta a incidentes auditable y automatizada

Visibilidad de casos, usuarios e impacto



# En estos tiempos de incertidumbre, las organizaciones necesitan...

01

Habilitar y proteger a la fuerza de trabajo remota

02

Detectar y responder a las crecientes amenazas

03

Extender virtualmente al equipo de seguridad e incrementar rápidamente sus habilidades

# Recomendaciones Generales

## 1 Internet Segura & Privacidad

Proteger a los usuarios contra correos electrónicos, sitios web, enlaces y dominios maliciosos, mitigando posibles impactos al negocio

## 2 Monitoreo de Perímetro

Monitorear y reportar el nivel de exposición a vulnerabilidades potenciales en Internet, de las aplicaciones y servicios de las Organizaciones

## 3 Simulación de Ciberseguridad

Probar controles, tecnología y gente, en relación al uso del trabajo a distancia

## 4 Seguridad del Trabajo a Distancia

Identificar las debilidades potenciales en los componentes de acceso remoto de la Organización

## 5 "Health-Check"

Proporcionar observaciones y recomendaciones sobre el uso de las tecnologías, el gobierno y las comunicaciones en comparación con las prácticas líderes de Ciberseguridad

## 6 Saneamiento de los Activos

Reintegrar los activos ("endpoints") utilizados en el trabajo a distancia al entorno corporativo y evaluar su apego a las políticas de seguridad y mejores prácticas

# ¡¡¡Gracias!!!

Síganos en:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions



IBM **Security**