Webcast PwC

Impacto COVID -19: Continuidad de operaciones mediante teletrabajo seguro

Business Security Solutions

18 Marzo 2020

pwc

Agenda

1. Contexto coronavirus, un rinoceronte gris
2. Grandes cuestiones a resolver…
3. Tipo de estructura de mi organización y necesidades
4. ¿Dónde me duele/dolerá más?
5. **BCP:** afrontando la incertidumbre en la coyuntura con el uso de best practices
6. War Room: Comité de Dirección
7. Necesidad de comunicación y concienciación directa y recurrente
8. Comunicación hacia los medios y RR. SS.
9. Establecer y gobernar el mapa de riesgos de mis proveedores
10. **El CIO** como garante de las TIC que soportan la operación
11. **El CISO** como guardián del ciber-riesgo y asesor en soluciones tácticas

Contexto coronavirus, un rinoceronte gris

*De **"Cisne Negro"** a **"Rinoceronte Gris"***

La pandemia del COVID-19 se puede considerar como un "**Cisne Negro" para China** (alto impacto, baja probabilidad), sin embargo para el **Europa,** debe considerarse como un **"Rinoceronte Gris"**... evento de alta probabilidad, con indicios claros pero peligro de no medición/diligencia respecto al impacto real:

...

- ***Impacto en cuenta de resultados***
- ***Absentismo laboral***
- ***Derrumbe confianza de empleados y clientes***
- ***No atención a tareas clave***
- ***Inapropiada gestión de la desinformación y fake-news***
- ***Disminución producción***
- ***....***

Grandes cuestiones a resolver…

Ante una situación como la que estamos viviendo, es necesario que **las organizaciones se (re)planteen una serie de cuestiones** para gestionar esta crisis y sus planes de contingencia asociados:

*Algunas preguntas obvias como: **¿qué tipo de estructura tiene mi compañía?,** ¿cuál es mi ámbito de actuación?, ¿impactos sobre mi modelo de negocio?, ¿cuál es mi nivel de manualización/digitalización interna/externa?.*

La salud de las personas lo primero / el negocio en segundo término, garantizando las nóminas y la cuenta de resultados.

*¿Disponen mis empleados de medios e instrucciones para continuar con la operativa y procesos de negocio?, ¿tengo identificados y bajo control mis **procesos críticos** y **funciones clave** en una crisis?*

*¿Conocen mis empleados y colaboradores los **medios y canales** por los que comunicarse y reportar incidencias? ¿Disponen de **información veraz, transparente y actualizada**?*

*¿Están mis **proveedores** preparados para cubrir demandas y necesidades?, ¿cuento con alternativas ante procesos críticos y/o en procesos de soporte?*

Tipo de estructura de mi organización y necesidades

Ahondando en las cuestiones corporativas, **cada organización debe analizar su situación y sus necesidades,** respondiendo a cada una de las siguientes cuestiones entre otras, cada una de ellas puede llevar un plan de acción/contingencia ad_hoc:

Tipos de empleados y sus necesidades	*Operativos, técnicos, autónomos, ETTs, proveedores, situaciones personales, movilidad, etc.*
Dispersión geográfica	*Local, nacional, comunitaria, multinacional, con dependencia de proveedores extranjeros.*
Nivel de manualidad procesos de negocio	*Cadenas de montaje con alto porcentaje de dependencia de mano de obra o supervisión humana (no remotizable), sectores de fabricación, industria, trasporte, investigación, turismo, facilities, retail, distribución. Cada uno de ellos con diferente mix IT, IoT y OT.*
Nivel de digitalización	*Herramientas de conectividad, sistemas de seguridad, medidas de teletrabajo, dependencia de proveedores, % digitalización de cadenas de montaje, plataforma digital para clientes.*
Cadena de valor/distribución	*Por sectores (primario, secundario, terciarios) por su dependencia de manualización de los procesos de negocio o por su dependencia de comercio electrónico (B2B, B2C, C2B, C2C), etc.*

¿Dónde me duele/dolerá más?

Fundamental **comprender cuáles son los procesos críticos** en el modelo operativo de mi compañía, y las **acciones para reducir el impacto** (que seguro habrá) en **ámbitos clave** de **interés** para **el Comité de Dirección**:

Económico

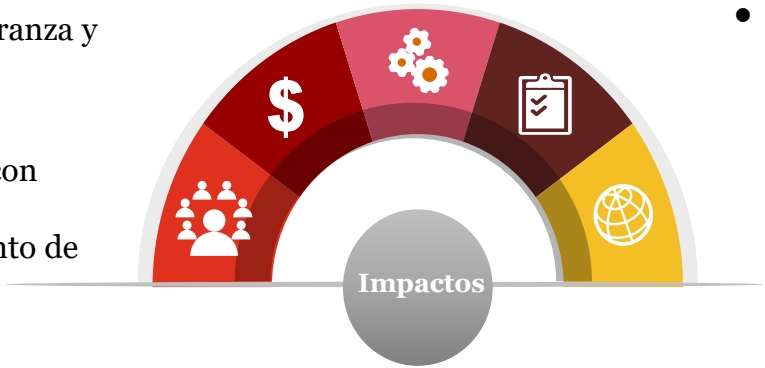
- Garantizar un mantenimiento de los flujos de caja y cuenta de resultados
- Proteger la tesorería
- Evitar riesgos de cobranza y mora

Comercial

- Reforzar comunicación con clientes
- Asegurar el mantenimiento de la operativa con impacto comercial

Operaciones

- Evitar retrasos operacionales
- Garantizar recursos necesarios para asegurar la contingencia
- Proteger las funciones clave
- Reforzar comunicación con empleados y colaboradores



Legal

- Revisar contratos con proveedores, colaboradores y empleados
- Asegurar los aspectos relacionados con Riesgo Laboral

Reputacional

- Asegurar la información de calidad para la toma de decisiones
- Comunicar mensajes claros y transparentes hacia empleados y clientes

BCP: afrontando la incertidumbre en la coyuntura con el uso de best practices

Best Practices

ISO 22301: Continuidad de Negocio

PwC BCP Framework

- Gobierno
- Análisis de impacto
- Situación de crisis
- Planes de contingencia
- Aprendizaje y mejora continua

Gestión de Crisis

Detección de señales → Preparación y prevención → Gestión, Control y Contención → ... Recuperación → Aprendizaje

Retroalimentación

Falta de planificación anticipada

Tardar en responder

Errores comunes en la Gestión de una crisis

No saber manejar Medios y RRSS

Descoordinación

Mentir

Improvisación
Descoordinación
Rumores
Falta de foco
Contradicciones
Desconfianza

Situación de contingencia desconocida

Agentes externos

- Actualización online de avance pandemia en fuentes reputadas
- Medición de RRSS

Alta Dirección

WAR ROOM

Procesos

Tecnología

Escenarios Contingencia

Comité de Dirección, C-Suite, CIO y CISO

Personas (empleados)

Comunicación y concienciación

Instalaciones

Monitorización

Proveedores y colaboradores

War Room: Comité de Dirección

Gestionar la crisis para librar batalla a batalla hasta ganar la guerra

La Alta Dirección es el pilar fundamental en la gestión de situaciones complejas y debe **transmitir serenidad y asegurar la continuidad** de la operativa del negocio **en un escenario incierto**.

Gobierno

- Crear una **War Room** para el Comité de Dirección responsable de la toma de decisiones y de diferentes subcomités
- La información es vital tanto a nivel de estamentos (OMS, CSIC, Gobierno, etc.), RRSS e interna (CAU, HelpDesk)
- Establecimiento **Subcomités de Crisis:** proporcionar información hacia el Comité de Dirección y ejecución Planes de acción y Contingencias ad_hoc
- Definir el **POSICIONAMIENTO ESTRATÉGICO** de la compañía ¿Qué queremos ser/estar en el S/M/L plazo?

Premisas de actuación

- **Transmitir seguridad y confianza** a los stakeholders mediante mensajes cercanos y transparentes
- **Garantizar** las **necesidades técnicas y sanitarias** de los actores que dan continuidad a los procesos críticos
- **Potenciar** el desarrollo de **medidas de reestructuración y flexibilidad** para dar continuidad al resto de procesos
- **Esponsorizar consejos y medidas de trabajo seguro** (teletrabajo, higiene, sistemas de reporte excepcionales,etc.)

Necesidad de comunicación y concienciación directa y recurrente

Trazar y ejecutar acciones de comunicación y de concienciación para **informar a empleados, clientes y proveedores de la situación y las acciones tomadas por la Organización ante una situación de contingencia.**

*Proporcionar instrucciones claras y medios a **todos los actores** para que su trabajo diario sufra el menor impacto posible.*

*Cada interlocutor requiere **mayor o menor información** con **mayor o menor detalle***

ACTOR

- **Emisor** — *Alta dirección, mandos intermedios, personas con responsabilidad y poder en la organización*
- **Receptor** — *Empleados internos, clientes y proveedores/colaboradores*

MEDIO

- **Canales disponibles en mi empresa** — *Intranet, correo corporativo, RR. SS., página web, cartelería, video conferencias, reuniones, etc.*

MENSAJE

- **Transparente, creíble, preciso** — *Combatir rumores con información clara, veraz y necesaria. Fuentes oficiales.*
- **Tranquilizador** — *Evitar el tono alarmista.*
- **Recurrente** — *Comunicaciones recurrentes y continuas con información actualizada.*
- **Dinámico y competente** — *Satisfacer la solicitud de información.*

Comunicación hacia los medios y RR. SS.

Gestionada por **expertos en comunicación. Si no comunicas, comunicarán por ti**

Las **personas** siempre son **lo primero**

Aseguramiento de la **continuidad de las operaciones**

Mensajes claros y firmes ante eventos concretos

Cadencia periódica

EMPRESAS

y suspenden las entregas a domicilio

Las supermercados garantizan el abastecimiento de alimentos por el coronavirus

El coronavirus impone el teletrabajo a decenas de miles de trabajadores en 24 horas: Bancos, operadoras, constructoras, pymes...

cierra temporalmente su sede europea por el coronavirus

CRISIS CORONAVIRUS

suspende la puesta en marcha de su nuevo

traslada de a a 100 empleados del área de mercados como prevención por el coronavirus

Establecer y gobernar el mapa de riesgos de mis proveedores

Tener claro el **mapa de mis proveedores esenciales y críticos** en una situación de pandemia, **así como las acciones a realizar y los compromisos y deberes regulatorios. Especial atención en los procesos de soporte, que en un escenario como este son prioritarios:**

Identificar **proveedores críticos y esenciales** en la continuidad de mis operaciones y abastecimiento

Identificar **proveedores de soporte que pasan a ser significativamente vitales** en esta situación de crisis (servicios de seguridad, de limpieza, ETTs, etc)

Conocer los riesgos de todos ellos para los servicios que me prestan

Restringir el acceso innecesario a las instalaciones para reducir los riesgos

Realizar **llamadas de seguimiento** continuo para estar al corriente de sus situaciones

Para proveedores críticos/esenciales/de soporte, **trazabilidad de cumplimiento** de sus normas internas y normas de nuestra Organización

...

Identificar **proveedores alternativos** en caso de indisponibilidad de abastecimiento de los principales

El CIO como garante de las TIC que soportan la operación

Riesgos a monitorizar (entre otros)

- Ausencia de equipos correctamente dimensionados para gestión de incidencias / gestión del cambio a nivel IT y OT.
- Cuello de botella en comunicaciones. No garantía en el *performance* de componentes front-office.
- Obsolescencia de sistemas para el acceso remoto; aumento de caudal en concentradores VPN.
- Log-in de usuarios y logging de operaciones.
- Ausencia de buenas prácticas y protocolos de conexión remota.
- Indisponibilidad de herramientas colaborativas.
- Indisponibilidad de Firma Electrónica.
- Indisponibilidad del CAU (Centro de Atención al Usuario) y call-centers.
- Gestión de credenciales, personas clave y protocolos no documentados.

Rol en contingencia

- KPIs de performance de sistemas/red/comunicaciones y teletrabajo. Atención 24x7.
- Garante de provisión de información a la Alta Dirección para la toma de decisiones, y sistemas de analítica sobre la misma.
- Mensajes botton up y top down en los planes de comunicación y concienciación tecnológica.
- Continuidad y contingencia tecnológica. Gestión y resolución de incidencias e incidentes.
- Monitorización de proveedores tecnológicos y no tecnológicos con acceso tecnológico.
- "Generador" de soluciones work-around, cuyo riesgo debe ser conocido y asumido, por ejemplo, maximización de entornos Cloud - Shadow IT - vs On-Premise..; gestión de entornos colaborativos SaaS (entornos colaborativos, CRM, ERP, ...).

Necesidades en el corto plazo

- Consecuente balance entre partidas CAPEX / OPEX, posible incremento presupuestario. Incremento derivado de servicios "Pago por Uso" en entornos Cloud.
- Análisis de cobertura de licencias SW.

El CISO como guardián del ciber-riesgo y asesor en soluciones tácticas

Riesgos a monitorizar (entre otros)

- Ausencia de analítica de performance de servicios/servidores corporativos y comunicaciones.
- Monitorización de sistemas de seguridad propios. Incapacidad de cubrir el *performance* en cuanto a monitorización (WAF, IDS, IPS, …)
- Amenaza DoS/DDoS en concentradores VPN
- Uso de herramientas no corporativas con seguridad no garantizada: shadow IT.
- Ausencia de principio de mínimo privilegio y necesidad de conocer, con especial atención en accesos privilegiados.
- Limitaciones en el uso de 2FA. Seguridad en *end-points*; Incremento de dispositivos no plataformados (políticas BYOD - “Bring Your Own Device”).
- Uso de redes Wi-Fi personales sin hardening suficiente: aumento de pinchos y consumo de datos.

[Continúa en la presentación gestión de ciber-riesgo en teletrabajo]

Rol en contingencia

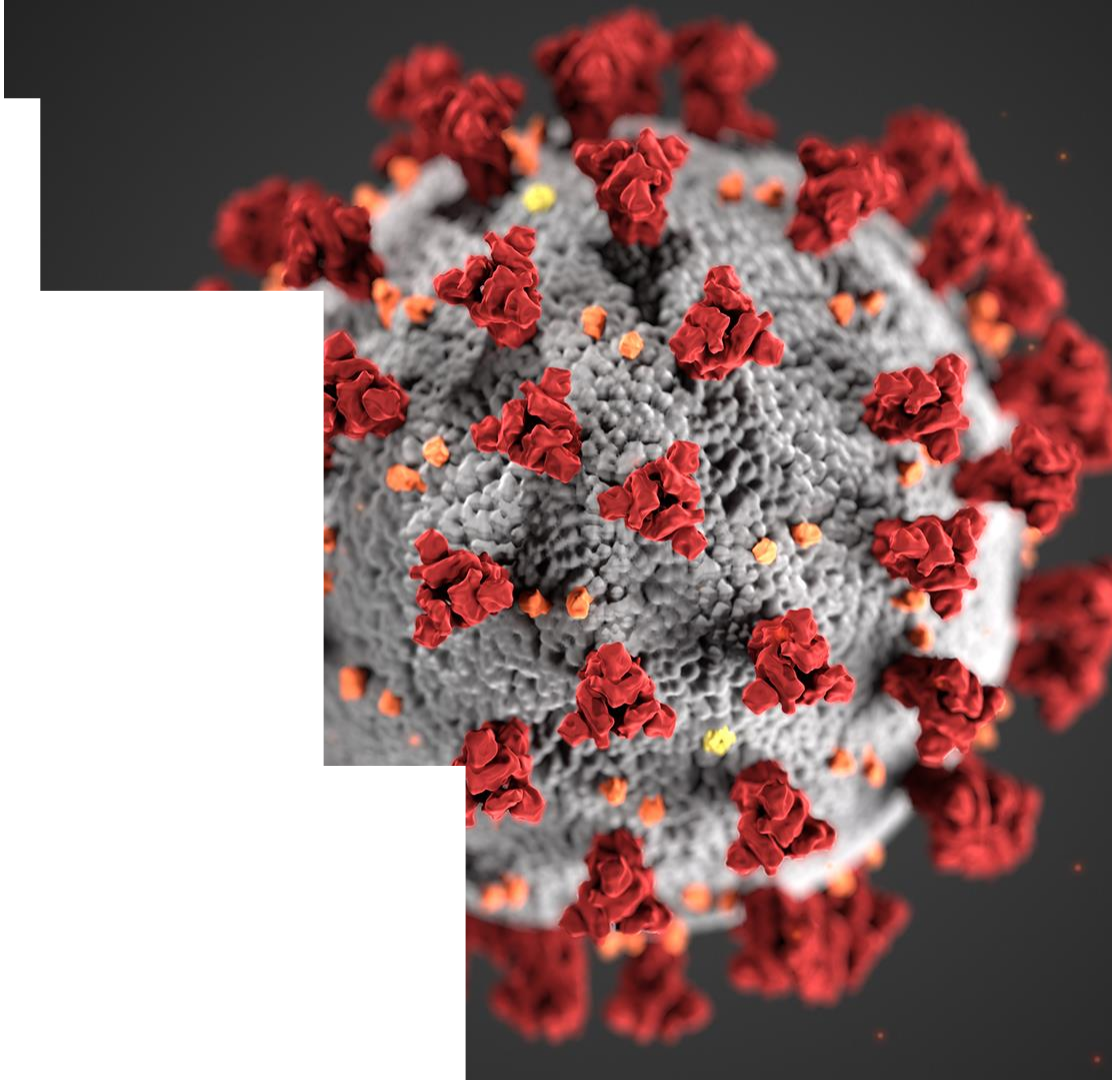
- Garante de la CID para sistemas de información y información de gestión en contingencia.
- Garante de buenas prácticas relativo a teletrabajo y uso de herramientas colaborativas, etc.
- Gestión y resolución de incidencias e incidentes.
- Garantizar que los permisos de acceso están actualizados, así como sus políticas de seguridad vinculadas.
- Garantizar el acceso seguro de proveedores a infraestructura *on-premise* y Cloud.
- Legitimación en el tratamiento de datos personales (GDPR) gestionando la privacidad y confidencialidad técnica.
- Atención y entendimiento de capacitación y disponibilidad del SOC interno o externo e integración con CSIRT sectoriales y/o nacionales.

Necesidades en el corto plazo

- Dimensionamiento a nivel de personal especializado.
- Consecuente balance entre partidas CAPEX / OPEX.
- Análisis de cobertura de licencias SW.

Coronavirus Digital
Marzo 2020

pwc



Índice

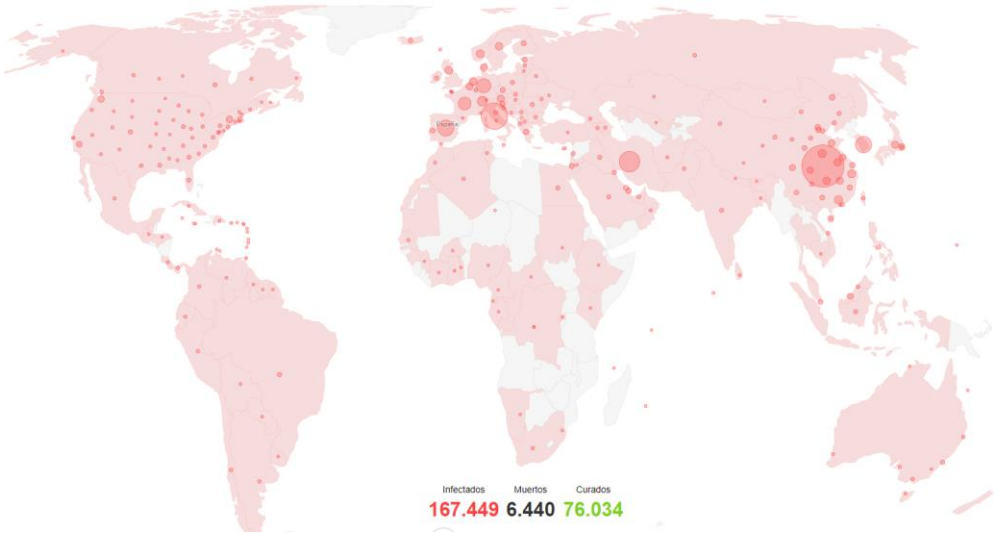
Una amenaza física con repercusiones en el entorno digital

Tormenta perfecta

- Miedo.
- Incertidumbre.
- Prisas.
- Desinformación / *Fake news*.
- Inquietud de los usuarios.
- Necesidad de información.

Nuestro equipo de Threat Intel está observando un aumento de campañas de phishing relacionadas con el COVID-19

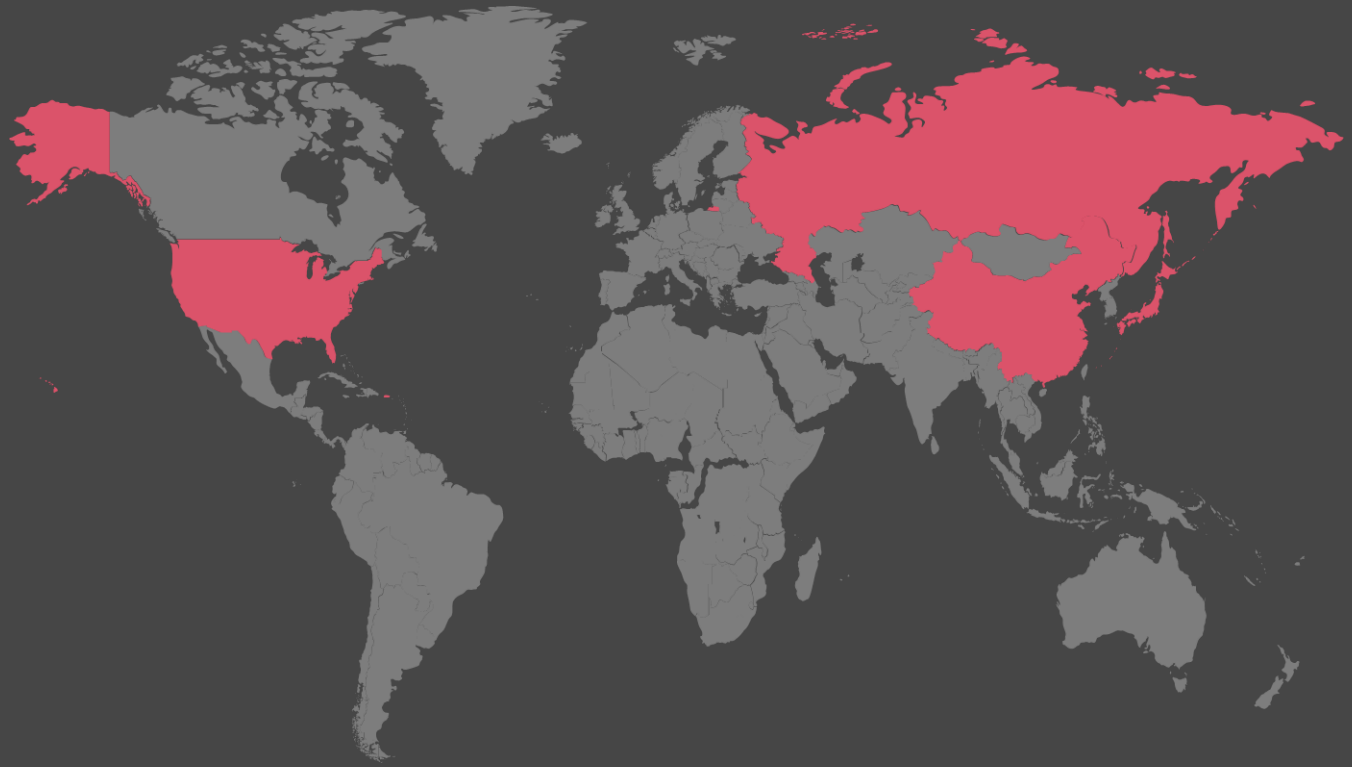
Problema Global



Ejemplos: COVID-19 como Vector de Ataque

- Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide. (*Recorded Future*)
- Chinese Hackers ‘Weaponize’ Coronavirus Data For New Cyber Attack: Here’s What They Did. (*Forbes*)
- Coronavirus Used in Spam, Malware, and Malicious Domains. (*Trend Micro*)
- Emotet Uses Coronavirus Scare in Latest Campaign, Targets Japan. (*Trend Micro*)
- The coronavirus scams are on the rise. (*Panda Security*)
- Y muchos más…

Origen de las campañas de phishing COVID-19



Marzo 2020

¿Quién no ha visitado una web como esta en estos días?

Campaña de spam de emails con **URLs maliciosas**

- Las URLs maliciosas alojan paneles **falsos** para seguir la evolución del COVID-19.
- Solicitan la **descarga de ficheros maliciosos** para su correcto funcionamiento.

Recomendaciones para vuestras organizaciones

Desde seguridad:

- **Acciones en el corto plazo dirigidas a reforzar la concienciación.**
- **Evitar abrir documentos y archivos adjuntos** en correos sobre COVID-19.
- Soluciones de seguridad especializas para **detectar y bloquear** spam, malware y dominios maliciosos.
- **Inspección** exhaustiva de los correos electrónicos.

Para los usuarios:

- **Evitar la difusión de mensajes no oficiales** y que puedan generar alarma social.
- Comprobar la **autenticidad** de la fuente.

STAMFORD, Conn., March 10, 2020

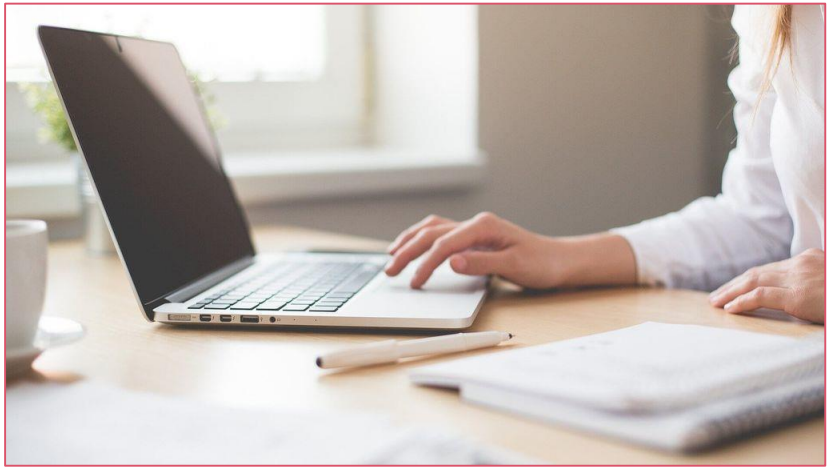
Gartner Says CIOs Should Focus on Three Immediate Actions to Prepare for Coronavirus Disruptions

1. Herramientas de colaboración digital con **controles de seguridad** y soporte de red.
2. Involucre a clientes y socios a través de canales digitales y mantenga actividades de ventas.
3. Establecer una **única fuente de verdad** para los empleados.

¿Cómo afecta a las empresas las medidas contra el COVID-19?

↑ Teletrabajo ↑ Superficie de exposición

- Redes WiFi domésticas.
- Equipos personales por falta de stock.
- Infraestructura VPN más compleja.
- Recursos sensibles ahora en remoto.
- Distintos perfiles de usuarios.



Recomendaciones para el trabajo remoto

Seguridad en los dispositivos

Seguridad en las comunicaciones

Recomendaciones para el trabajo remoto

Seguridad en los dispositivos

Administración remota

- Copias de seguridad periódicas.
- Actualización de software.
- Elevar el nivel de monitorización de eventos en equipos.

Configuración segura

- Contraseñas robustas
- Segundo factor de autenticación.
- Certificados digitales.
- Dispositivos cifrados.

Ojo con el uso personal de dispositivos corporativos que contienen acceso o datos relevantes de la organización

Recomendaciones para el trabajo remoto

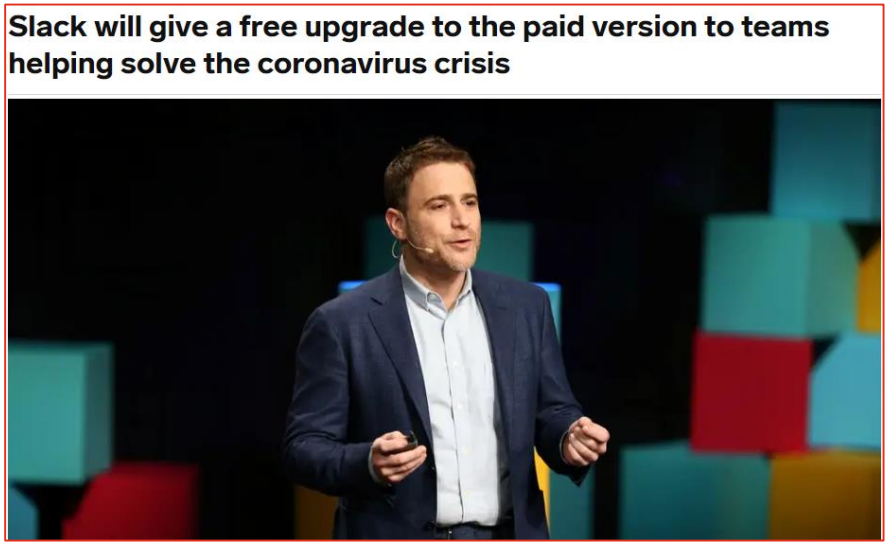
Seguridad en las comunicaciones

- Evitar aplicaciones de acceso excesivo remoto (RDP, Teamviewer, etc..)
- Entender **las implicaciones** de cada uno de los parámetros de la configuración de VPN (por ejemplo, *Split tunneling)*
- Proporcionar **herramientas corporativas** para compartir archivos, mensajería instantánea, etc.
- Mantener una monitorización proactiva de la infraestructura. Anomalías, posibles intrusiones, etc.
- Validar la **seguridad de los cambios** que se implementan en la infraestructura.

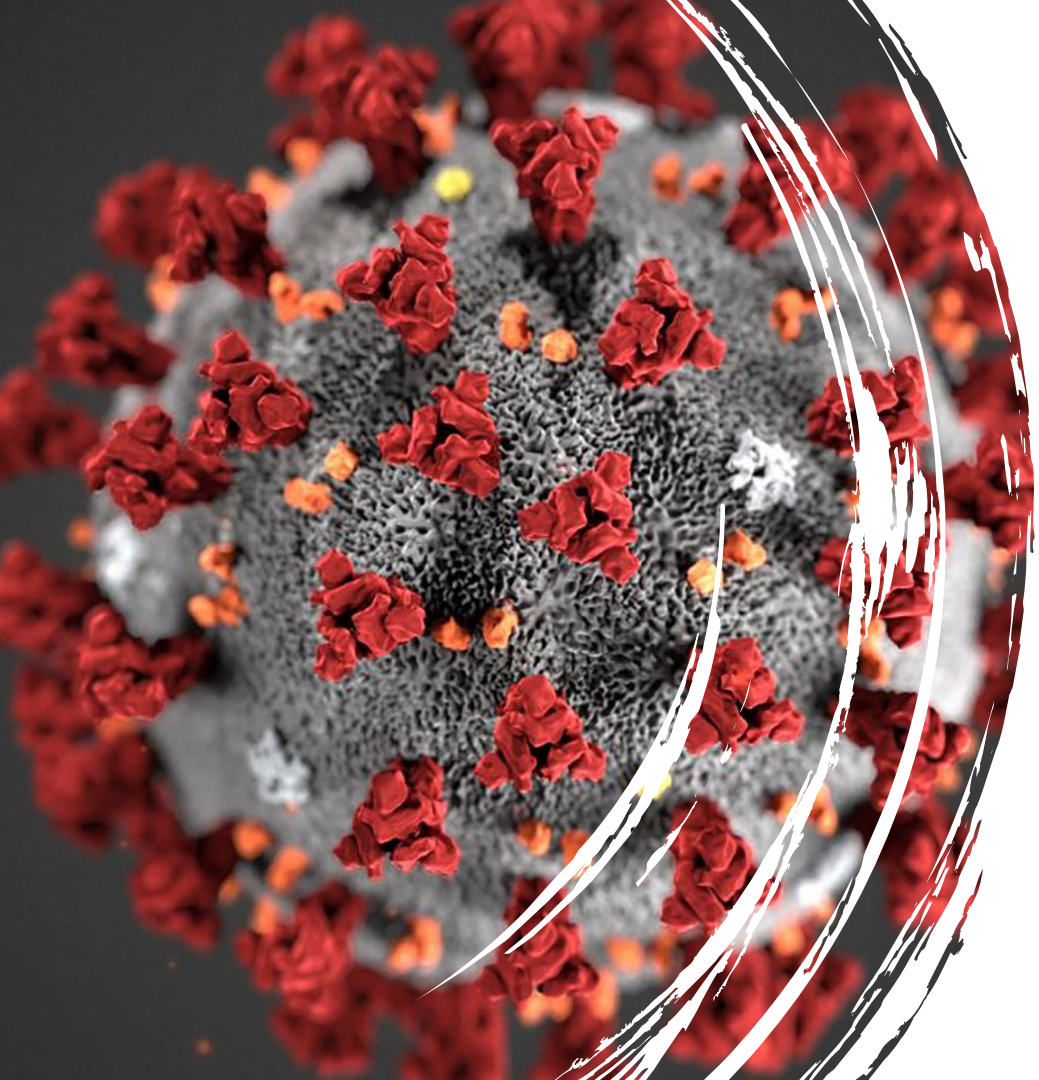
Iniciativas

Los gigantes tecnológicos ponen de su parte para favorecer entornos de trabajo seguros.

economiadigital.es



businessinsider.com



En nuestras manos está frenar el virus tanto físico como digital

#YoMeQuedoEnCasa

Pero seguro

Gracias

pwc.com