Tecnología

Viajar 2.2
Cultura 2.3
Medio Ambiente 2.5
Pasatiempos 2.6
Clasificados 2.8

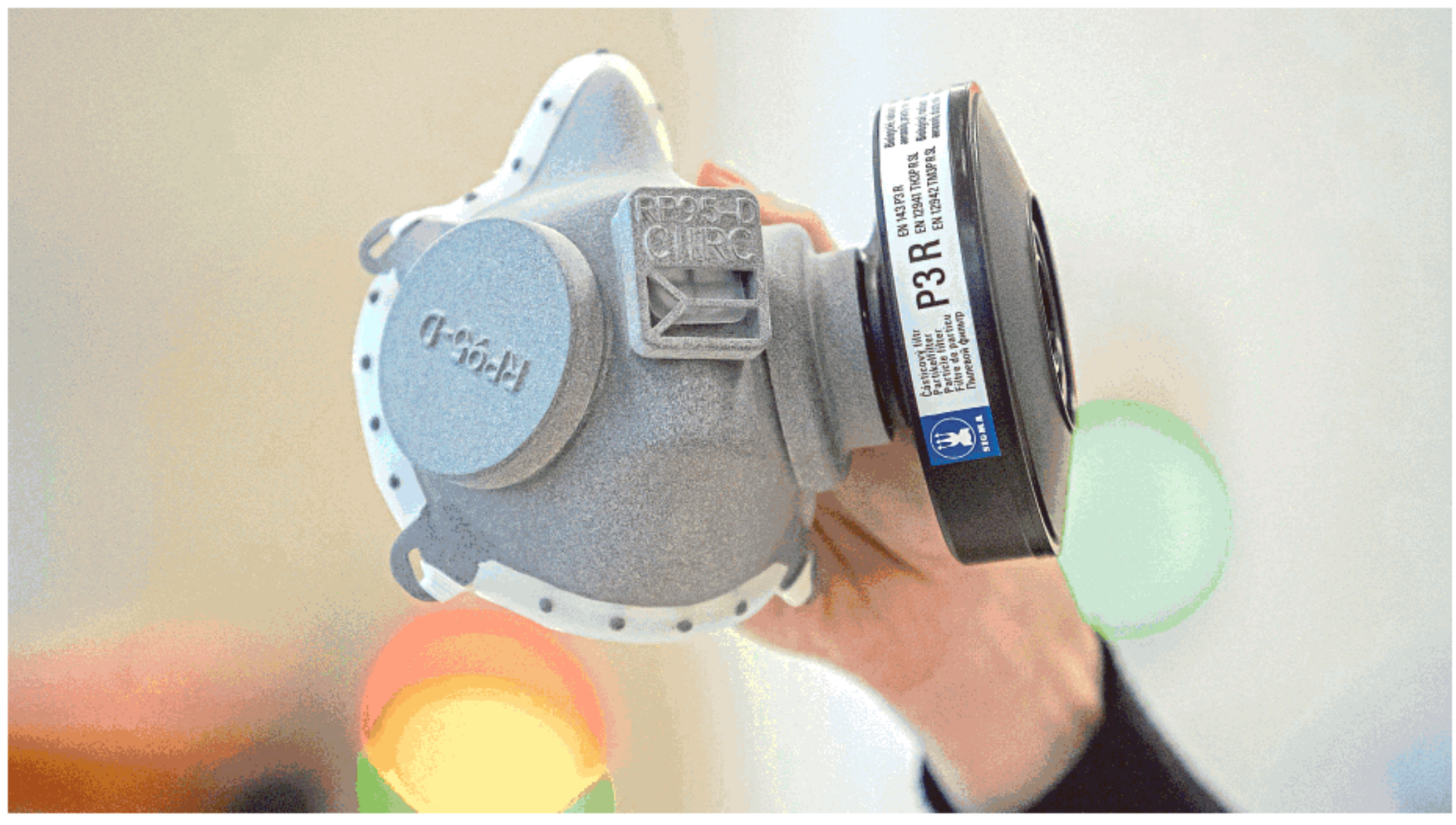
IBM LLAMA A SOLUCIONES POR CORONAVIRUS

El desafío para desarrolladores de IBM Call for Code 2020, que lanza en alianza con Naciones Unidas y este año aborda el cambio climático, agregó un apartado y llama a la comunidad a pensar soluciones al covid-19.

FALSAS DONACIONES EN LA RED

La Organización Mundial de la Salud (OMS) advirtió que ciberatacantes están usando su nombre para engañar a usuarios y robar datos y dinero con falsas campañas de donaciones. Con técnicas *phishing*, atacantes envían correos electrónicos con adjuntos o *links* de dudosa procedencia. La OMS reiteró que sus donaciones son manejadas desde el Fondo de Respuesta Solidaria.

Respiradores impresos en 3D



Fotonoticia Investigadores de la República Checa desarrollaron un prototipo de respirador (CIIRC RP95) contra el covid-19 usando tecnología de impresión 3D. El instituto de informática, robótica y cibernética de la Universidad Técnica Checa, en Praga, está colaborando con el Ministerio de Salud del país para proveer una nueva categoría de respiradores para los hospitales. Aunque hay pocos impresos, están preparándose para producción masiva en las próximas semanas. FOTO: EFE

Teletrabajo puede abrir puertas a ciberataques

Expertos analizan que los usuarios son el 'eslabón más débil' y emiten recomendaciones a la hora de implementar estrategias de trabajo remoto.

YESHICA ORJUELA - REDACCIÓN TECNÓSFERA | @YeshicaT

A raíz de la emergencia sanitaria por la que esta atravesando el mundo, muchas empresas han tenido que pedirles a sus colaboradores trabajar desde casa. Sin embargo, ante la repentina decisión, no todas las compañías cuentan con las herramientas necesarias para garantizar el rendimiento del trabajador, pero sobre todo la seguridad de la información.

Un primer riesgo que corren las empresas es la falta de computadores propios para abastecer a todos sus empleados. Ello hace clave contar con una VPN (Red Privada Virtual) que permita el acceso remoto a programas y archivos, pero que además permite cifrar el contenido y contar con actualizaciones de seguridad.

Pero no se puede descartar que en caso de no contar con los dispositivos necesarios para suplir la demanda, las empresas se verán en la necesidad de usar los computadores de sus colaboradores, que no siempre cuentan con un antivirus con licencia, con las últimas actualizaciones del sistema o siquiera con una clave de acceso.

Cecilia Pastorino, especialista de seguridad informática de Eset Latinoamérica, cree que hay dos riesgos principales: la confidencialidad de la información y la disponibilidad de los servicios.

En el primer aspecto, explica que los hábitos inseguros en las comunicaciones remotas pueden habilitar que los atacantes tengan un camino adicional para acceder a la información confidencial de la empresa.

Por otra parte, en el segundo punto, señala que "cuando muchos trabajadores se conectan en remoto al mismo tiempo, se provoca que el sistema de red privado colapsé y que después nadie pueda hacer su trabajo de manera oportuna".

Riesgos comunes

A la hora de trabajar desde casa, es usual que los equipos (propios del trabajador o de la empresa) tengan acceso a sistemas a través de una red VPN, que cifra el tráfico desde el origen. Es decir, desde la computadora del empleado hasta la computadora de la empresa, la información está protegida por un *firewall* que bloquea el acceso no autorizado, y con protocolos IDS o IPS que permiten a los equipos técnicos el detectar y prevenir intrusos.

Según Alexander Ramírez, gerente de la firma de seguridad informática Frontech, otro riesgo es que "el trabajador puede acceder desde su computador a archivos maliciosos enviados por correo electrónico o redes sociales, los *malware* roban todo tipo de información, como las contraseñas, tanto del empleado como del empleador".

También es de considerar que en la mayoría de casos, los servicios de internet que no son lo suficientemente robustos para lidiar con las exigencias de las redes laborales, que tampoco están aseguradas.

Por eso, "el colaborador debe garantizar que la conexión a internet se haga directamente al *router* de su casa y no a través de una red wifi desconocida o de redes públicas", añade Ramírez.

> **En cada casa hay un *router*** que lleva años sin ser tocado. No se sabe qué nivel de actuación tiene, por lo que los equipos conectados son altamente vulnerables.
>
> **David Pereira,** EXPERTO EN CIBERSEGURIDAD

Por su parte, David Pereira, experto en ciberseguridad y CEO de la firma SecPro, señala que la VPN no es suficiente, "no basta con eso, hay que colocar otros mecanismos de seguridad adicionales; por ejemplo, herramientas de privacidad, de borrado seguro y de autentificación para mejorar la conexión", dice.

Desde la parte del acceso, un movimiento usual de los ciberacriminales es el de acceder a la red de wifi para invadir los otros dispositivos conectados a la red y de esta forma robar información.

Por lo general, explica Ramírez, los usuarios no saben que los *routers* deben actualizarse no solo para dificultar el acceso a los delincuentes, también para garantizar mayor rendimiento.

El atacante también puede bloquear la conexión para evitar que el usuario la use o crea un punto de acceso falso, que duplica el nombre de la red inalámbrica y desactiva la original. Así logra que los dispositivos se conecten a la nueva señal mientras tiene acceso a todo el tráfico generado, totalmente visible si no está encriptado.

Pereira expresa que "la protección de la red equivale a que el usuario tenga un equipo Wips (sistema de prevención de intrusión inalámbrica). Sin embargo, puede que lo tenga en tu oficina, pero no en la casa, lo que hace al usuario más vulnerable".

Recomendaciones

Pastorino, de Eset, recomienda, además del saludable hábito de tener copias de respaldo, las empresas se dediquen a diseñar un plan de seguridad, analizar el riesgo y tener una política que se acomode a cada organización.

Ramírez, de Frontech, manifiesta que los equipos deben contar con el sistema de doble factor de autentificación que requiere de un código obtenido a partir de una aplicación o SMS que llega al celular del colaborador y protege la información del computador de robo o pérdida.

Andrés Guzmán, CEO de Adalid, resalta que los usuarios deben estar atentos y tener cuidado para evitar caer en ningún tipo de información fraudulenta que les dé acceso a los criminales a la redes laborales o domésticas.

Cosas tan sencillas como no abrir mensajes ni correos electrónicos con link o archivos sospechosos. Si recibe una comunicación, trate de contactarse con la entidad o revisar página oficial y corroborar la información expuesta.

Los expertos coinciden en que la coyuntura del covid-19 va a generar un pico en los ataques y campañas de amenazas virtuales. Las firmas, que cuentan con sistemas propios dirigidos a las organizaciones para evitar riesgos, señalan que la prevención puede ser menos grave que corregir los errores.

Usuarios en *apps* de *streaming* aumentan

Hace seis días que millones de colombianos entraron en aislamiento preventivo con el fin de frenar la propagación del covid-19 en el país. Y aunque muchas personas continúan trabajando y estudiando desde sus hogares, el consumo de internet y de plataformas de contenido vía *streaming* sigue en aumento. De hecho, según Samuel Hoyos, presidente de Asomóvil, hay cerca de un 80 por ciento de los usuarios de internet utilizando la red, y esté valor porcentual seguiría en aumento.

Por ejemplo, Disney Plus, la nueva *app* de contenido bajo demanda de Disney, la cual venía teniendo un crecimiento normal por su lanzamiento, registró un 211 por ciento de aumento de suscriptores en Estados Unidos desde que la cuarentena preventiva se volvió una obligación en diferentes estados y desde que millones de estadounidense decidieran voluntariamente quedarse en casa.

Apple TV+, que desde hace meses aumentaba su número de usuarios en bajas proporciones, alcanzó un crecimiento del 10 por ciento. Y en HBO GO, el numero de inscritos creció en un 90 por ciento. El incremento de esta última plataforma se vio beneficiado también por el lanzamiento de la tercera temporada de la popular serie *Westworld*, la cual atrae un gran número de fanáticos.

Por su parte, Netflix registró un alza del 47 por ciento, un número alto teniendo en cuenta que es la plataforma que más usuarios registrados posee y que, según prensa especializada, estaba en un punto de saturación en el que su crecimiento sería lento.

En Colombia, este lunes, el Mintic presentó un nuevo decreto en el que especifica cuáles van a ser las medidas que se tomarán para garantizar el completo funcionamiento de las redes de telecomunicaciones en el país. En los artículos, se reconoce a las telecomunicaciones como un servicio público y, además, en el decreto se añade una nueva regla que les exige a todas las plataformas de *streaming* transmitir su contenido de video sobre formato estándar y no en alta definición o superior.

Así entonces, alineado a este esfuerzo, Netflix anunció que frente a la crisis mundial ha "desarrollado una forma de reducir el tráfico de la plataforma en las redes de telecomunicaciones en un 25 por ciento en Colombia, pero manteniendo la calidad de nuestro servicio", dijo Ken Florance, vicepresidente de Content Delivery de la plataforma. Así mismo, no se descarta que otras *apps* de contenido de video bajo demanda apliquen también medidas similares.

211 %
más suscriptores
LA PLATAFORMA DE 'STREAMING' DISNEY + TUVO UN CRECIMIENTO DEL 211 % EN ÚLTIMAS SEMANAS