

DESDE LA RESPUESTA A LA CRISIS HASTA LA TRANSFORMACIÓN

EL PAPEL DE LA DIGITALIZACIÓN EN LA PANDEMIA DE LA COVID-19 Y EN EL FUTURO

La pandemia de la COVID-19 ha puesto de manifiesto la importancia de contar con una estrategia de trabajo a distancia bien pensada. Hemos decidido compartir nuestra experiencia con el cambio al trabajo desde casa, predecir el papel que desempeñarán los lugares de trabajo flexibles en el futuro y ofrecer consejos sobre cómo crearlos. Este manual puede servir de inspiración a los CISOs, CIOs y directores de IT, así como a los CEOs ilustrados que quieran descubrir la eficacia de la digitalización.



CONTENIDO

PARTE 1 **3**

CASO PRÁCTICO DE ESET 3

INFORMACIÓN DE PRIMERA MANO 4

PLANIFICAR, PLANIFICAR Y VOLVER A PLANIFICAR 5

INCLUSO LAS EMPRESAS TECNOLÓGICAS PUEDEN TENER PROBLEMAS TECNOLÓGICOS 7

LA SEGURIDAD ES LO PRIMERO 8

LA CRISIS COMO CATALIZADOR 9

PARTE 2 **10**

NUEVAS AMENAZAS PRESENTES EN EL JUEGO 10

AMENAZAS EN LA WEB 11

AUTORIDADES FALSAS 12

APLICACIONES PELIGROSAS 13

COVID-19: CIBERATAQUES EN CIFRAS 14

PARTE 3 **15**

MANTENER EL RUMBO:
6 PUNTOS DE PARTIDA PARA EL FUTURO 15

1. EVALÚA CÓMO LA CRISIS HA AFECTADO A TU EMPRESA 16

2. REVISAR EL ANÁLISIS DE IMPACTO Y EL PLAN DE CONTINUIDAD DE LA ACTIVIDAD 17

3. SI TU EMPRESA ES NUEVA EN LA DIGITALIZACIÓN COMIENZA CON PEQUEÑOS PASOS 18

4. EXAMINAR LA PREPARACIÓN DE TUS PROVEEDORES 19

5. ADAPTAR LAS SOLUCIONES DE SEGURIDAD A LOS CAMBIOS 20

6. CAPACITA A TUS EMPLEADOS Y EMPATIZA CON ELLOS 22

CONCLUSIÓN **24**

NO HABRÁ UN BUEN NEGOCIO SIN UNA BUENA IT 24

PARTE 1

CASO PRÁCTICO DE ESET:

Cómo hemos superado la pandemia de la COVID-19 y qué hemos aprendido de ella

La pandemia de la COVID-19 ha sido una experiencia nueva para la humanidad. Así que también ha sido nueva para ESET: habíamos preparado varios planes de crisis en el pasado, pero ninguno de ellos podía reflejar todos los retos que la pandemia ha traído. Desde el principio de la crisis, dos cosas fueron esenciales: mantener a nuestros empleados a salvo y trabajar a distancia para mantener el negocio en marcha. He aquí cómo lo logramos.



PARTE 1

INFORMACIÓN DE PRIMERA MANO

La falta de información causa problemas: al principio, muchos de nuestros empleados entraron en pánico. En cuanto supimos que la situación era grave, creamos una dirección de correo electrónico especial a la que nuestros empleados podían enviar preguntas de forma anónima.

Además, nuestros empleados se mostraron muy activos a la hora de buscar información sobre la COVID-19. Vimos varios casos en los que consultaban fuentes poco fiables y descargaban archivos que podían dañar sus ordenadores. Por ello, les proporcionamos una lista de medios de comunicación y fuentes expertas fiables, recomendando, por ejemplo, los estudios realizados por la Organización Mundial de la Salud (OMS) o la Universidad Johns Hopkins (JHU). Además, compartimos algunos consejos sobre cómo ser productivo mientras se trabaja desde casa y aconsejamos a los directivos sobre cómo gestionar sus equipos a distancia.

Dado que algunos de nuestros empleados no poseen dispositivos de la empresa, también elaboramos sencillos carteles con todo tipo de información relevante, desde cómo lavarse las manos hasta qué herramientas online utilizar y cómo pedir ayuda. Esta fue sólo una de las pocas medidas offline que aplicamos.

CARTELERÍA PARA LOS TRABAJADORES, CON MEDIDAS Y RECOMENDACIONES PARA LA PANDEMIA

Plan de Continuidad Empresarial para Enfermedades Epidémicas: **Coronavirus**

Nivel de riesgo actual: **Nivel 2 - CASO CONFIRMADO EN ESET**

INFORMACIÓN SOBRE EL CORONAVIRUS: MANTÉN LA CALMA Y NO ENTRES EN PÁNICO

MEDIDAS ADOPTADAS

- Se pidió a los miembros del equipo de los compañeros afectados que se pusieran en contacto con el servicio de atención al cliente durante dos semanas. En caso de enfermedad, se les pide que se ausenten y que se pongan en contacto con el médico por teléfono.
- ESET seguirá las instrucciones de su autoridad local.

¿TE SIENTES MAL?

- Si tienes síntomas como secreción nasal, dolor de garganta, tos y fiebre, debes informar a tu superior y quedarte en casa. Si tienes fiebre (>38°C), ponte en contacto con tu médico por teléfono.

REDUCE LOS DESPLAZAMIENTOS

- Por favor, considera la posibilidad de cancelar o posponer los viajes al extranjero.
- En caso de regresar de viajes desde países con un brote de coronavirus, por favor, informa a tu supervisor inmediatamente.

MINIMIZA LOS RIESGOS

- Lavarse las manos con frecuencia.
- Mantener el distanciamiento social.
- Posponer o cancelar reuniones o cambiarlas a llamadas / videoconferencias.
- Evitar tocarte los ojos, la nariz y la boca.
- Fortalecer tu sistema inmunológico: duerme lo suficiente (al menos 7 horas). Llevar una dieta rica en frutas y verduras. Realizar ejercicio físico con regularidad.

Busca "coronavirus" en la intranet y obtén las últimas actualizaciones relacionadas con el trabajo y con ESET.

Si tienes alguna duda respecto a la presencia del coronavirus, ponte en contacto con nosotros en health@eset.com



PARTE 1

PLANIFICAR, PLANIFICAR Y VOLVER A PLANIFICAR

La situación se estaba agravando gradualmente en todo el mundo, por lo que estábamos actualizando nuestro plan de continuidad de negocio para la gripe pandémica en consecuencia. Teníamos algunos planes de reserva del pasado, como el de la crisis del gas de 2009, pero estaban anticuados. En nuestro nuevo plan de crisis, tuvimos en cuenta tres etapas diferentes.

NIVEL 1: SUPERVISIÓN

La primera etapa se aplicó cuando la pandemia ya estaba presente en algunos de los países donde hay oficinas de ESET. En ese momento, también buscamos formas de proteger a los empleados que se encontraban en viajes de negocios o estaban programados para ello, creando, por ejemplo, una lista negra de países de riesgo. En el caso de las conferencias organizadas por ESET, también creamos una lista de programas alternativos que pudieran sustituir inmediatamente el discurso de un ponente enfermo, como pausas más largas para el café, cuestionarios de ESET o paneles de debate.

NIVEL 2: USO LIMITADO DE OFICINAS

La siguiente fase reflejaba el momento en que se preveía que podría haber un empleado infectado o cuando el gobierno pudiera presentar una normativa que pudiera afectar a varios equipos. También empezamos a ofrecer seminarios web organizados con psicólogos. Nuestro departamento de RRHH desempeñó un papel crucial en este aspecto.

NIVEL 3: CIERRE DE LA OFICINA

En la última etapa se tuvo en cuenta que podría haber una cuarentena forzosa, o que la dirección podría decidir que toda la empresa trabajara a distancia, que es lo que realmente ocurrió.



PARTE 1

PLANIFICAR, PLANIFICAR Y VOLVER A PLANIFICAR

Al principio de la crisis, también establecimos un Comité de Salud, formado por cinco personas: el Director de Continuidad de Negocio de ESET, el Director de Recursos Humanos, nuestro Director de Operaciones, así como el Director de Soporte de IT y el Director de Instalaciones. Su responsabilidad era supervisar la situación de forma regular, los siguientes pasos y las comunicaciones, realizar evaluaciones de riesgo y ayudar a la dirección de nivel C a tomar decisiones importantes. En cuanto a nuestras oficinas internacionales, recomendamos a quiénes debían discutir los impactos de estas decisiones, y les alertamos de que estaban obligados a informar al Comité de Salud.

También tuvimos que establecer normas para los viajes a otros países. En cuanto alcanzamos el nivel 2, cumplimos las recomendaciones del Ministerio de Asuntos Exteriores de la República Eslovaca y aconsejamos a nuestros empleados que no viajaran a ningún sitio.

ASÍ ES COMO EL CISO, DANIEL CHROMEK, ORGANIZÓ NUESTRO PLAN DE CONTINUIDAD EMPRESARIAL PARA LA GRIPE PANDÉMICA Y APOYÓ LAS COMUNICACIONES INTERDEPARTAMENTALES.

CARGO	RESPONSABILIDAD
COMITÉ DE SALUD <ol style="list-style-type: none"> 1. Gestor de la continuidad del negocio, 2. Director de recursos humanos, 3. Director de operaciones, 4. Director de apoyo informático y 5. Director de instalaciones 	Planificación de la respuesta, preparación de la comunicación, seguimiento de la situación, preparación de la información necesaria para las decisiones de la dirección de nivel C.
GERENTE DE RRHH EN LA OFICINA DE ESET	Comunicación a los empleados. Gestión del foco del contagio dentro de la oficina de ESET. Informar al comité de salud.
DIRECTOR NACIONAL EN LA OFICINA DE ESET	Decisiones sobre la oficina en posición de dirección de nivel C. Decide sobre el cierre de la oficina y aprueba los costes adicionales junto con: <ul style="list-style-type: none"> • Director regional y director de negocios / director de ventas (a quien corresponda) para las oficinas de S&M • Director de tecnología o arquitecto jefe de software para las oficinas de I+D
DIRECTOR REGIONAL PARA EMEA, APAC, NORAM Y LATAM	Decide el cierre de la oficina junto con el director nacional. Aprueba los costes adicionales.

PARTE 1

INCLUSO LAS EMPRESAS TECNOLÓGICAS PUEDEN TENER PROBLEMAS TECNOLÓGICOS

Se podría pensar que las empresas tecnológicas no pueden atascarse en la transición al trabajo a distancia... ya que son las expertas en IT. Mientras que no nos enfrentamos a ningún problema con respecto a la seguridad, sí experimentamos problemas en la organización.

En cuanto quedó claro que todos los empleados tendrían que trabajar a distancia, tuvimos que conseguir portátiles adicionales para varios empleados que habían estado trabajando en ordenadores de sobremesa, tras descubrir que, de hecho, no teníamos suficientes. Por tanto, nuestro equipo de IT tuvo que visitar varios almacenes y tiendas para conseguir todo lo que necesitábamos, lo que nos retrasó al principio. Finalmente, algunos de nuestros empleados tuvieron que llevarse a casa ordenadores de sobremesa enteros y otros accesorios. Además, todos los nuevos dispositivos tuvieron que configurarse muy rápidamente; al final, nuestros especialistas en IT gestionaron este esfuerzo en tres días, durante un turno de fin de semana largo. Lección aprendida: comprueba siempre si tienes el equipo técnico necesario para trabajar desde casa.

Una vez resuelto esto, también resultó que carecíamos de suficientes licencias VPN para que todos nuestros empleados pudieran conectarse a los sistemas internos desde casa. Por desgracia, nuestros proveedores tuvieron problemas para cubrir la demanda, y tuvimos que esperar más tiempo para que nos entregaran los servicios que necesitábamos. Esto demostró claramente que, aunque te esfuerces en crear el mejor plan de crisis, todo puede fracasar por la falta de servicios de un proveedor de los que depende tu empresa.



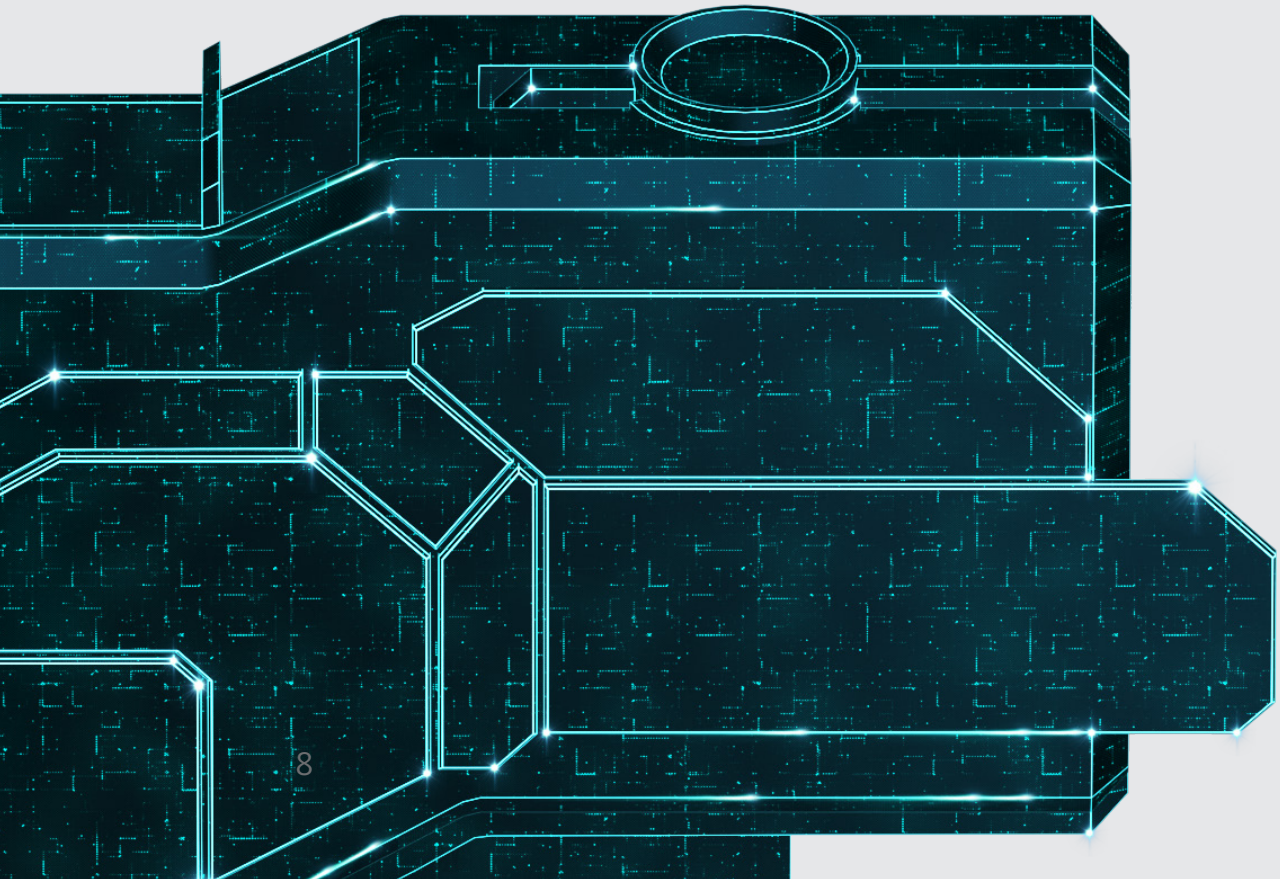
Daniel Chromek, CISO de ESET

De repente, la situación se agravó muy rápidamente, y el 80% de nuestros empleados necesitaban acceso remoto... Había que encriptar todos los discos duros de los ordenadores de sobremesa, y preparar rápidamente nuevos portátiles, lo que era bastante complicado.

PARTE 1

LA SEGURIDAD ES LO PRIMERO

Fuera de la red corporativa, los dispositivos son más vulnerables a los ciberataques. Para poder mantener a salvo tanto los dispositivos como todos los datos, nos centramos en capas de seguridad adicionales vitales para la protección de los equipos y la seguridad del correo: desde el [cifrado completo del disco](#) y [la autenticación multifactor](#) hasta la tecnología de [sandbox en la nube](#).



SOLUCIONES DE SEGURIDAD QUE UTILIZAMOS DURANTE LA CRISIS

[ESET Endpoint Security](#): plataforma de protección de equipos que combina una fuerte prevención de malware, exploits y ransomware reforzada por el aprendizaje automático.

[ESET Dynamic Threat Defense](#): sandbox en la nube que aprovecha múltiples modelos de aprendizaje automático para detectar y monitorizar las amenazas en los equipos y en los archivos adjuntos del correo electrónico; y detecta tanto las amenazas de día cero como las de ransomware.

[ESET PROTECT On-Prem](#): consola de administración que controla las capas de prevención, detección y respuesta de equipos en todas las plataformas: ordenadores de sobremesa, servidores, máquinas virtuales que no requieren intervención y dispositivos móviles gestionados, a través de un único panel de visualización.

[ESET Secure Authentication](#): una forma sencilla pero poderosa de implementar la autenticación multifactor diseñada para funcionar en todos los teléfonos, tokens HW, todas las VPN y servicios en la nube, con una función de autenticación push que es extremadamente fácil de usar.

[ESET Full Disk Encryption](#): potente cifrado gestionado de forma independiente a través de las consolas de gestión remota de ESET, aumentando la seguridad de los datos de las empresas para cumplir con la normativa.

PARTE 1

LA CRISIS COMO CATALIZADOR

A pesar de causar muchos problemas, la crisis nos hizo centrarnos en nuevos procesos y soluciones, que estamos seguros de que nos ayudarán en el futuro. Por fin hemos empezado a utilizar la firma electrónica, hemos alcanzado la madurez en nuestros procesos de contratación en línea y hemos potenciado nuestras capacidades de administración remota. No solo aprendimos a trabajar a distancia sin tener que cancelar ningún proyecto importante, sino también a ser más productivos. Esto es algo que nos ayudará a largo plazo.

Incluso antes de la crisis, sabíamos que nuestros empleados deseaban más flexibilidad, y la crisis nos ayudó a satisfacer sus necesidades. Creemos que un lugar de trabajo totalmente digitalizado es el futuro y, gracias a la pandemia, hemos dado varios pasos hacia él.

CRONOLOGÍA: NUESTRA RESPUESTA A LA CRISIS EN EL TIEMPO

ENERO

NÚMERO DE ARCHIVOS DE MALWARE DENUNCIADOS Y ELIMINADOS DE OUTLOOK: 6

1 DE FEBRERO

NIVEL 1: SEGUIMIENTO-NÚMERO DE PERSONAS EN LAS OFICINAS: 800

4 DE FEBRERO

CREACIÓN DE UN ESCRITORIO DE CORREO ELECTRÓNICO

10 DE MARZO

CREACIÓN DEL COMITÉ DE SALUD

12 DE MARZO

NIVEL 2-LIMITACIÓN DE USO DE LA OFICINA

15 DE MARZO

NIVEL 3-CIERRE DE OFICINAS

16 DE MARZO

LA ADQUISICIÓN DE TODOS LOS DISPOSITIVOS NECESARIOS RESTANTES

18 DE MARZO

CONFIGURAR CON ÉXITO TODOS LOS NUEVOS DISPOSITIVOS

ABRIL

NÚMERO DE ARCHIVOS DE MALWARE DENUNCIADOS Y ELIMINADOS DE OUTLOOK: 27

10 DE ABRIL

CASI TODO EL MUNDO TRABAJA A DISTANCIA - NÚMERO DE PERSONAS EN LAS OFICINAS DE ESLOVAQUIA: 25

PARTE 2

NUEVAS AMENAZAS PRESENTES EN EL JUEGO

¿Ética y moral? Nada para los ciberdelincuentes. Las crisis son ocasiones ideales para que inicien sus ataques. Aprovechan que los empleados están estresados, ansiosos y bajo presión, y que su empresa se apresura a introducir nuevas medidas para sobrevivir. “Los delincuentes han aprovechado rápidamente las oportunidades para explotar esta crisis adaptando sus modos de operar o desarrollando nuevas actividades delictivas”, afirma la Directora Ejecutiva de Europol, Catherine de Bolle, en un manual publicado recientemente.

Nuestras experiencias han confirmado las palabras de la Sra. de Bolle. Hemos recibido el doble de correos electrónicos de phishing de lo normal. Algunos de los remitentes incluso han utilizado nombres y contactos de empleados reales de ESET pidiendo a los destinatarios que paguen facturas fraudulentas, realicen ciertas tareas o compartan sus datos bancarios.



PARTE 2

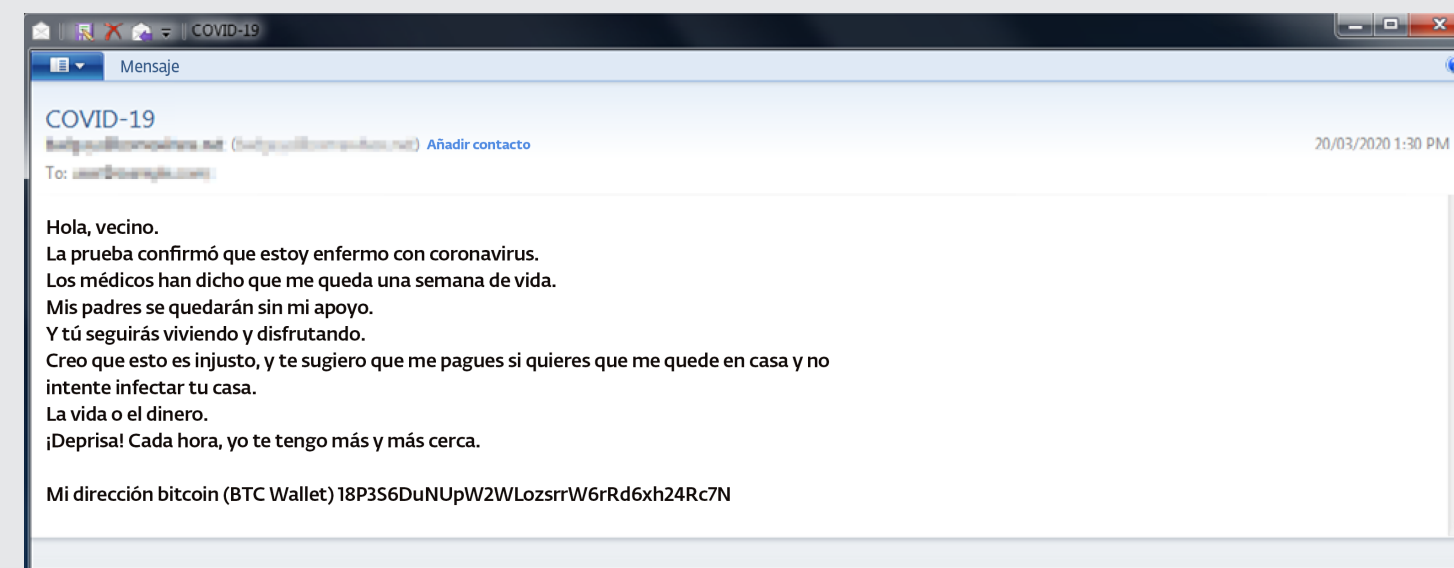
AMENAZAS EN LA WEB

El tema del coronavirus ha sido utilizado como señuelo en múltiples amenazas web. Según el Informe de Amenazas de ESET del primer trimestre de 2020, el número de sitios web fraudulentos bloqueados en el primer trimestre de 2020 aumentó un 21% en comparación con el cuarto trimestre de 2019.

Los ciberdelincuentes, por ejemplo, han aprovechado la gran demanda de material médico y han fundado falsas tiendas electrónicas con dicho material. Dejan que los usuarios paguen, pero o bien nunca reciben el pedido, o bien obtienen productos de baja calidad. Según Europol, las autoridades de todo el mundo se incautaron de unas 34.000 mascarillas quirúrgicas falsificadas solo entre el 3 y el 10 de marzo de 2020. Con la evolución de los hechos sobre el terreno, ESET se centró aún más en la concienciación del personal, informando regularmente a nuestros empleados sobre estas amenazas y estafas.

Los ciberdelincuentes llegaron a amenazar con infectar a los destinatarios del correo electrónico y a sus familias si se negaban a pagar el rescate. También aumentaron los llamados ataques de compromiso del correo electrónico empresarial (BEC), y las empresas se enfrentaron a un número todavía mayor de ataques de ransomware y malware.

CORREOS ELECTRÓNICOS DE EXTORSIÓN CON TEMÁTICA DE CORONAVIRUS



PARTE 2

AUTORIDADES FALSAS

Los empleados de ESET no fueron los únicos que se beneficiaron de la confianza depositada en la OMS. Lamentablemente, la organización fue una de las autoridades más suplantadas en las campañas de estafa, y desgraciadamente se convirtieron en una puerta a través de la cual los atacantes difundían noticias falsas, fingían tener información importante y pedían a los usuarios que hicieran clic en enlaces maliciosos; entre otros objetivos, los atacantes se proponían robar datos personales.

“

Los atacantes se aprovechan de que la gente está nerviosa y trabajando desde casa.

Daniel Chromek, CISO de ESET

SITIO WEB MALICIOSO QUE SE HACE PASAR POR LA OMS Y ATRAE A LOS USUARIOS PARA QUE DESCARGUEN PROGRAMAS MALICIOSOS

Aplicación de información de la COVID-19

Instala esta aplicación, para tener la última información e instrucciones sobre el coronavirus (COVID-19).

**Organización Mundial de la Salud.
Forma parte del Grupo de Desarrollo Sostenible de la ONU.**

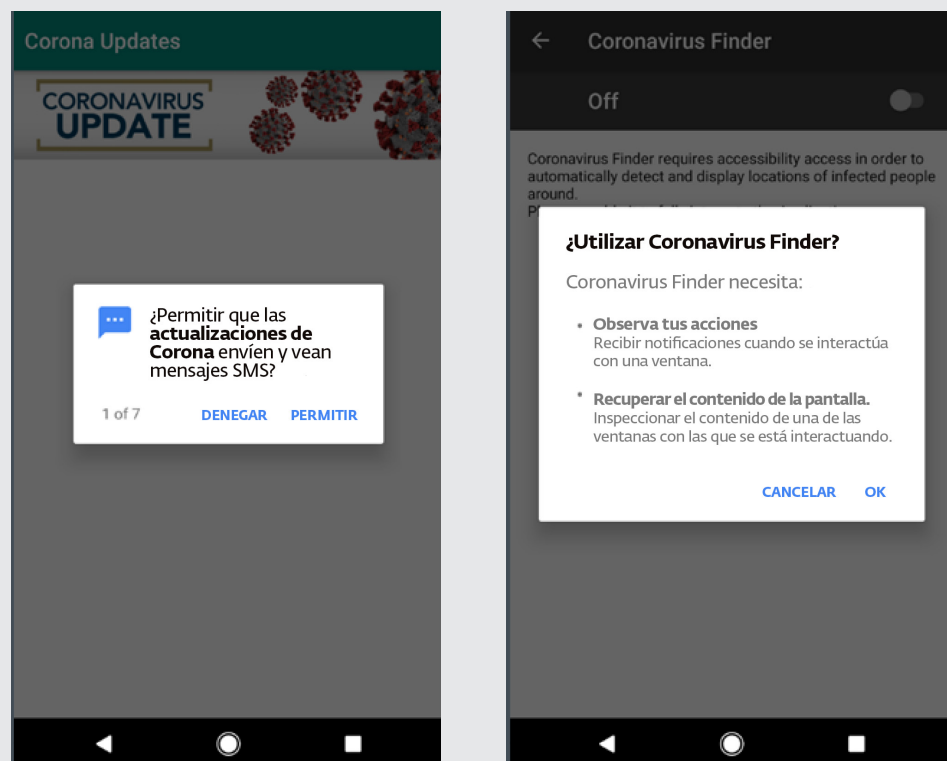
Descargar

PARTE 2

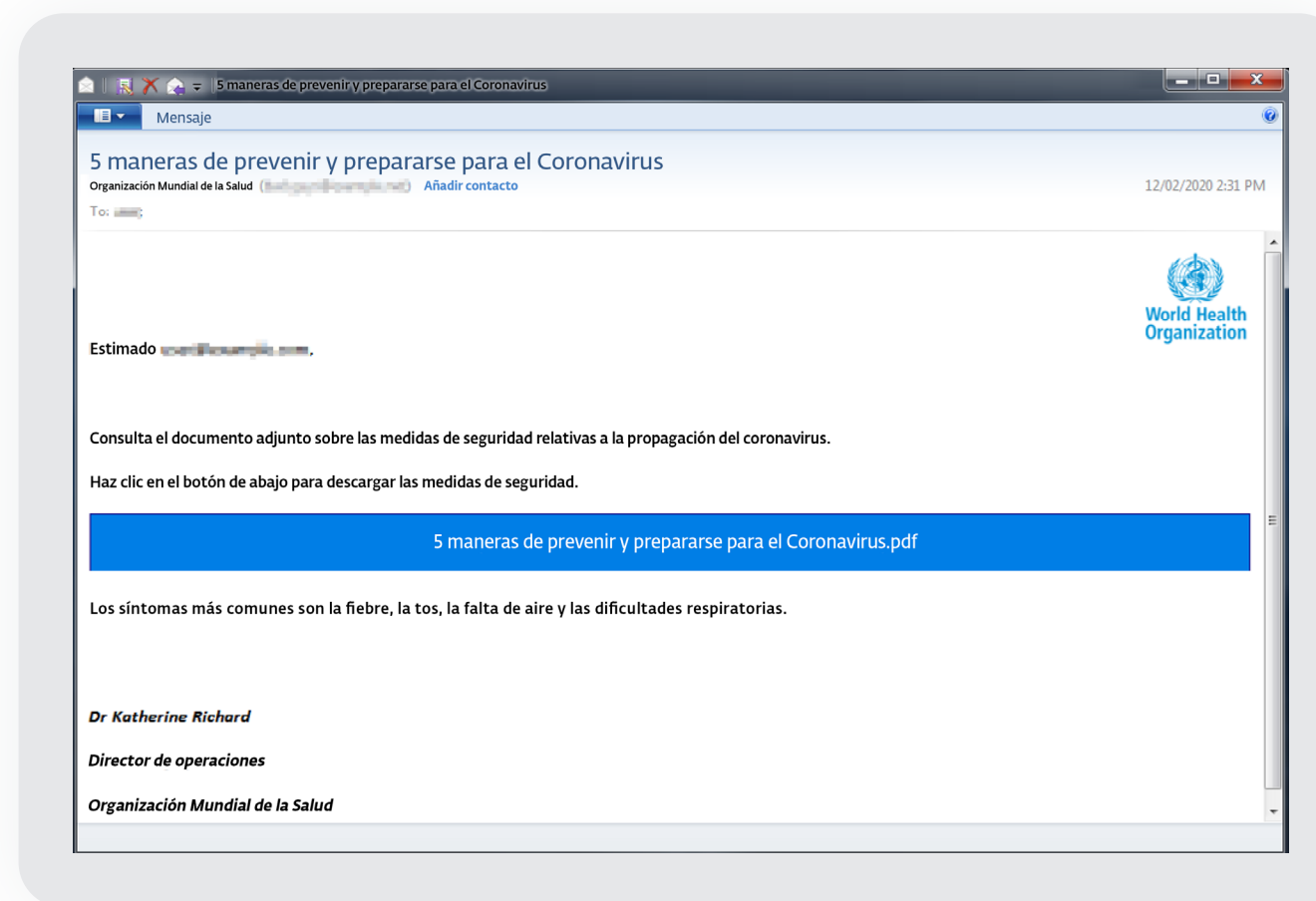
APLICACIONES PELIGROSAS

Además, aparecieron nuevas aplicaciones maliciosas que prometían a los usuarios la identificación de síntomas, el rastreo de contactos o la compensación financiera. Muchas de estas aplicaciones estaban infectadas por familias de troyanos bancarios, ransomware, spyware y adware.

EJEMPLOS DE SOLICITUDES DE PERMISOS DE MALWARE PARA ANDROID CON TEMÁTICA DE CORONAVIRUS



CORREO ELECTRÓNICO DE SPAM SUPLANTANDO A LA OMS.



FUENTES DE IMÁGENES: INFORME SOBRE AMENAZAS DE ESET 2020

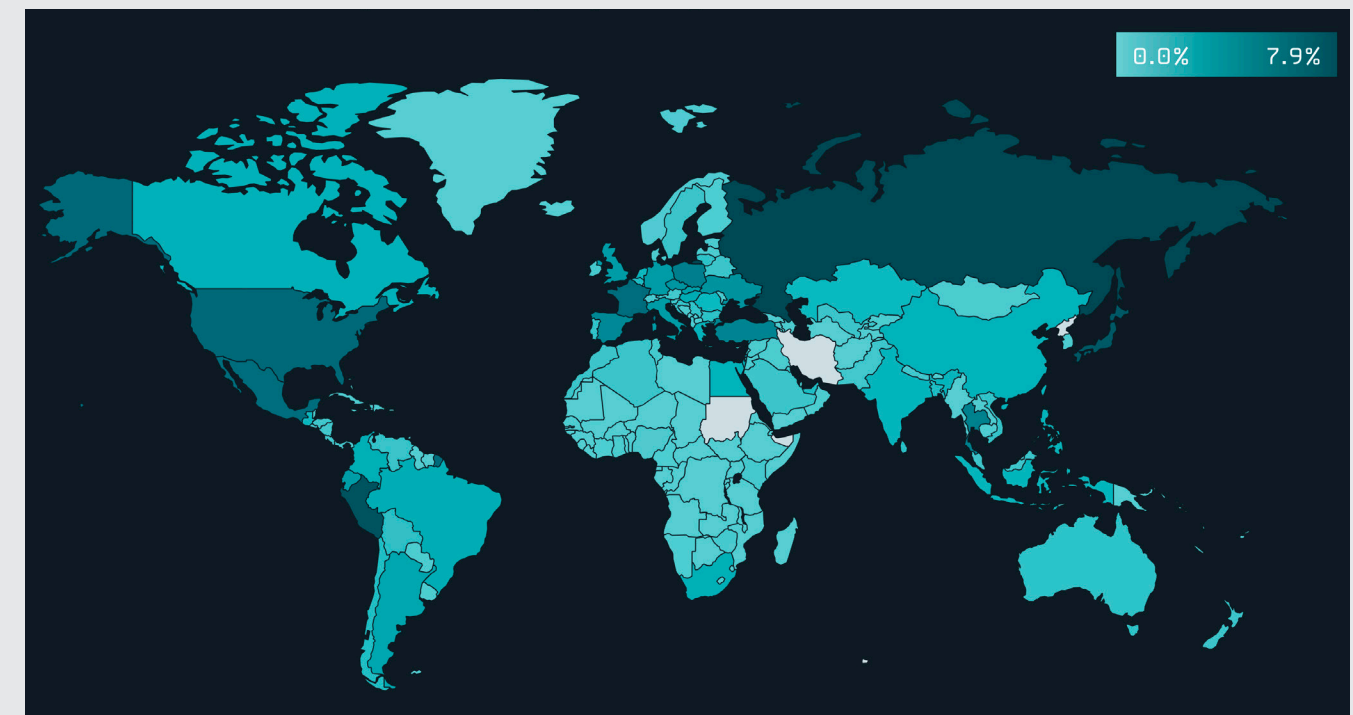
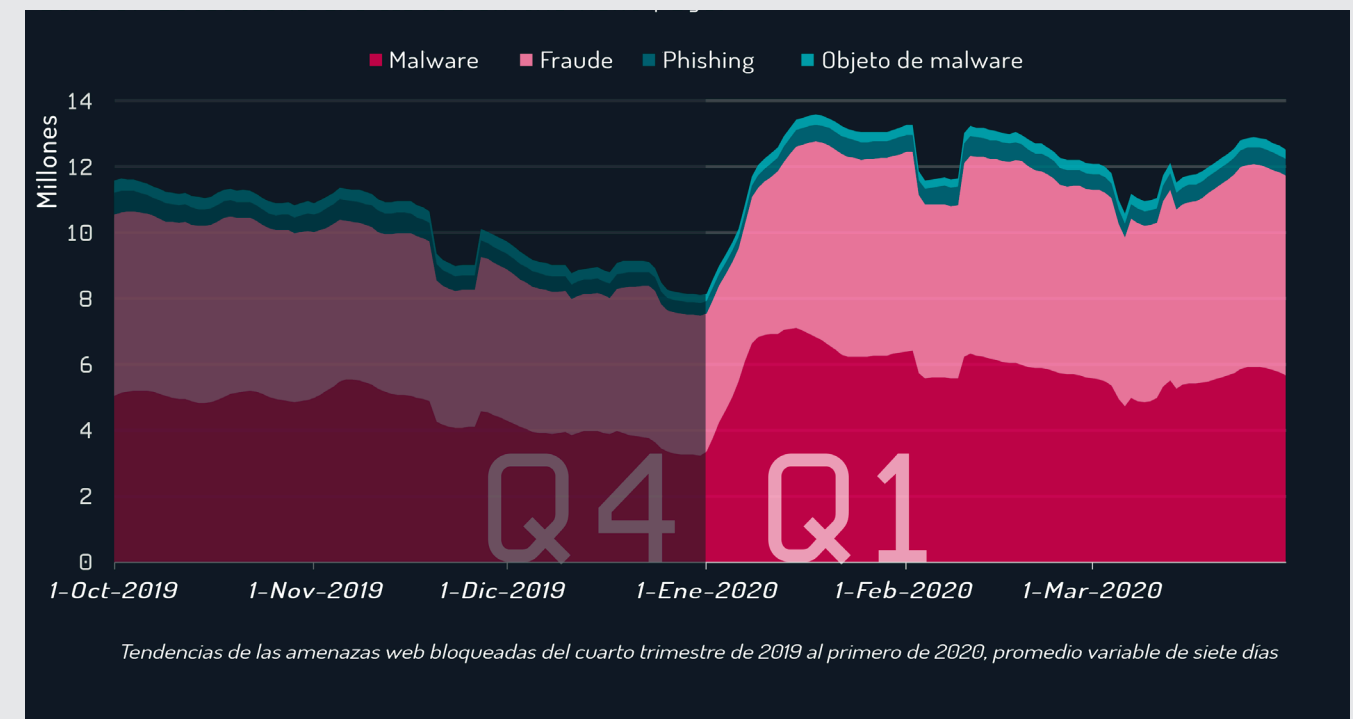
PARTE 2

COVID-19: CIBERATAQUES EN CIFRAS

- 18 millones de correos electrónicos diarios de malware y phishing relacionados con la COVID-19 fueron detectados por Google en la segunda semana de abril de 2020. De media, Google bloquea más de 100 millones de correos electrónicos de phishing al día.*
- Google detectó 240 millones de mensajes de spam relacionados con la COVID-19 diariamente durante el pico de la pandemia.
- 600 % es el crecimiento registrado de correos electrónicos de phishing relacionados con la covid-19 medidos en todo el mundo en el primer trimestre de 2020, según la investigación de KnowBe4.

* ESET es miembro fundador de la App Defense Alliance para proteger la Google Play Store, aportando sus galardonadas capacidades de detección y seguridad mejorada para el ecosistema Android. ESET también protege a los usuarios de Google Chrome, a través de un motor de ESET integrado en Google Chrome Cleanup, una herramienta de seguridad que alerta a los usuarios de Google Chrome de posibles amenazas; y también tiene una integración con Chronicle, una división de Google Cloud.

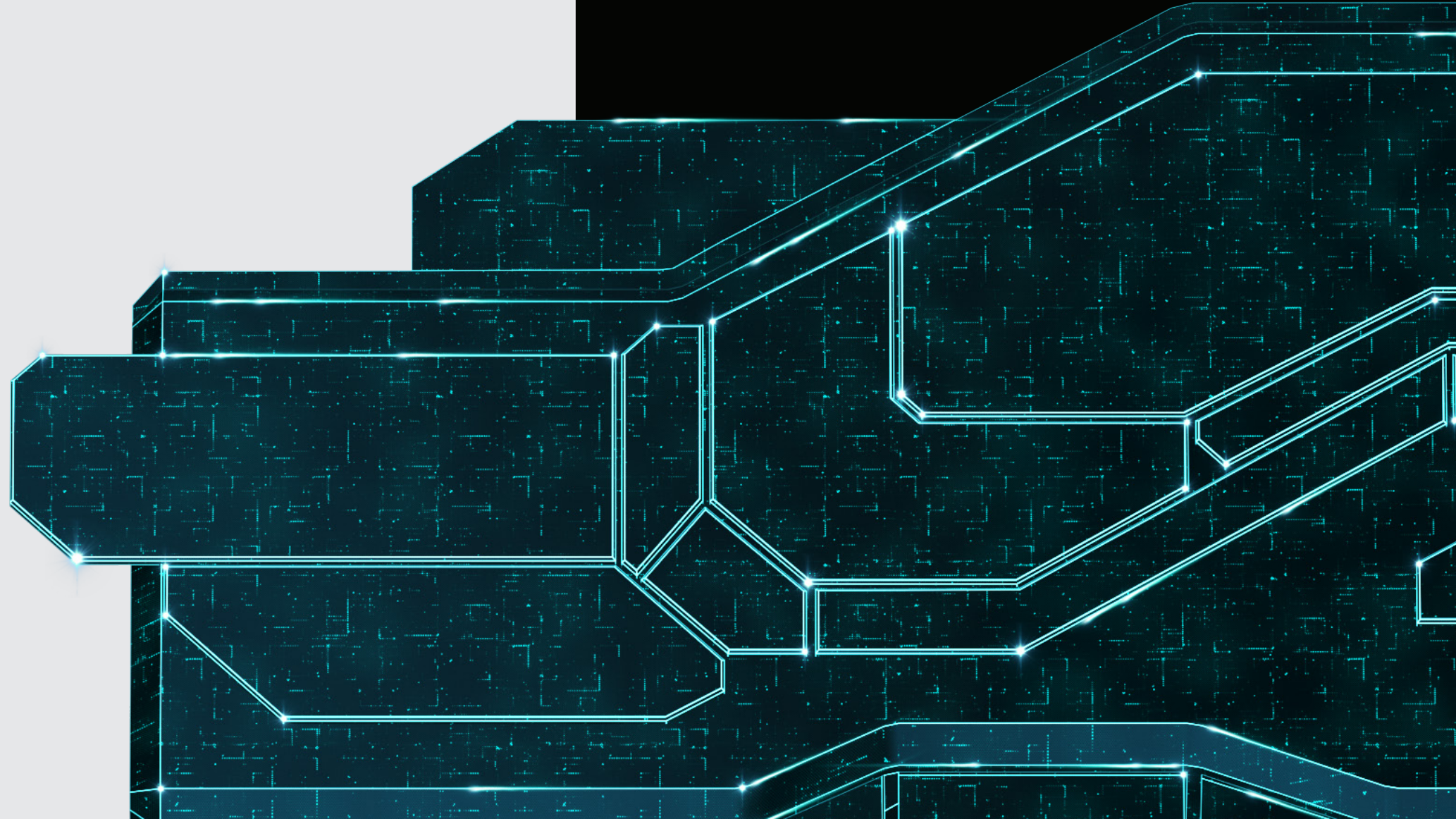
TENDENCIAS DE LAS AMENAZAS WEB BLOQUEADAS EN EL CUARTO TRIMESTRE DE 2019 AL PRIMER TRIMESTRE DE 2020, PROMEDIO DE SIETE DÍAS



PARTE 3

MANTENER EL RUMBO: 6 PUNTOS DE PARTIDA PARA EL FUTURO

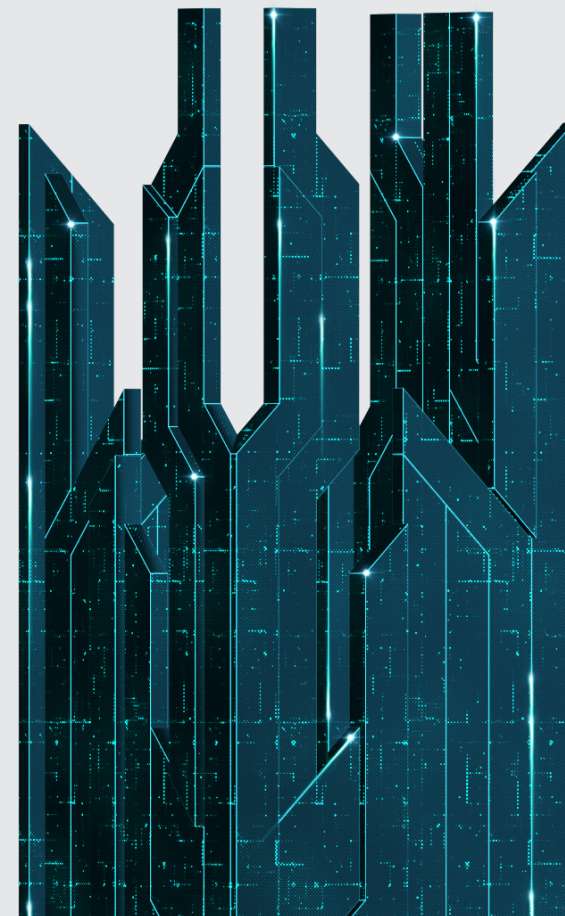
Albert Einstein tenía razón cuando dijo que “en medio de cada crisis, hay una oportunidad”. La crisis de la COVID-19 puede servir como inicio de una nueva realidad laboral. Los lugares de trabajo digitales y remotos son el futuro, y el futuro empieza ahora. ¿Cómo debemos proceder para gestionar entornos de trabajo seguros y flexibles?



PARTE 3

1. EVALÚA CÓMO LA CRISIS HA AFECTADO A TU EMPRESA

Puede que la crisis te haya hecho integrar finalmente nuevas herramientas y procesos en tu rutina y funcionamiento diarios. Para poder analizar qué soluciones podrían ser útiles en el futuro, he aquí algunas preguntas que debes hacerte.



PREGUNTAS QUE TE AYUDEN A DEFINIR QUÉ MEDIDAS (NO) MANTENER DESPUÉS DE LA CRISIS

- ¿Qué operaciones tuvieron que ser canceladas debido a la crisis y por qué?
- En comparación con la situación anterior a la crisis, ¿es tu arquitectura de IT ahora más capaz de satisfacer las necesidades de negocio de la empresa?
- ¿Habría resistido mejor la empresa la crisis si se hubieran digitalizado más procesos y operaciones?
- ¿Por qué sería ventajoso/desventajoso para la empresa seguir trabajando a distancia y buscar una mayor madurez digital?
- ¿Sería conveniente mejorar todavía más las nuevas políticas y procesos que tu empresa adoptó durante la crisis?
- En caso afirmativo, ¿qué herramientas y medidas apoyan esta forma de trabajo y serían también una buena inversión para el futuro?
- ¿Cómo percibe la dirección de la empresa las experiencias tanto de la crisis como de la digitalización?
- ¿Cómo perciben tus empleados esta modalidad de trabajo?

PARTE 3

2. REVISAR EL ANÁLISIS DE IMPACTO Y EL PLAN DE CONTINUIDAD DE LA ACTIVIDAD

La planificación y el establecimiento de prioridades son esenciales, no solo en tiempos de crisis. Teniendo en cuenta la experiencia de la crisis, en colaboración con el departamento de planificación de la continuidad, redefine qué departamentos necesitan aumentar su madurez digital, ya que se encuentran en el núcleo del negocio.

Ahora debes centrarte en los proyectos que te permitan trabajar a distancia. ¿Hay proyectos cruciales para la empresa que, hasta ahora, no podían transformarse o trasladarse al entorno digital? ¿O las soluciones que se te ocurrieron durante la crisis fueron insuficientes? Es el momento de asegurarse de que puedes ofrecer los mismos servicios con la misma calidad en línea.

El análisis del impacto en el negocio y la continuidad de la actividad de tu empresa deben reflejar la naturaleza crítica de determinados servicios, así como el papel de las IT. Es posible que la crisis haya demostrado que es necesario revisar algunos planes: comparte tus conclusiones con la dirección.

CÓMO HABLAR CO TU JUNTA DIRECTIVA SOBRE CIBERSEGURIDAD Y PRESUPUESTOS

A. LA CIBERSEGURIDAD ES LA CLAVE DE LAS NUEVAS OPORTUNIDADES DE NEGOCIO

Las soluciones digitales pueden aportar nuevas oportunidades de negocio. Pero también, una protección inadecuada de los datos puede dar lugar a enormes pérdidas de datos e ingresos, dañando la confianza general en la empresa, así como su reputación. Asegurar a los clientes de la empresa de que sus datos están bien protegidos aumentará la credibilidad de la empresa.

B. PRESENTAR PRUEBAS SUFICIENTES

Aportar estadísticas concretas sobre el aumento de la ciberdelincuencia y cómo un solo clic erróneo puede perjudicar a las empresas. Para demostrar lo peligroso que puede ser, por ejemplo, el phishing, haz una prueba con los empleados de la empresa: envíales unos cuantos correos electrónicos falsos y comprueba cuántos de ellos hacen clic en un enlace malicioso.

Además, intenta contratar a un informático y pídele que intente penetrar en la red de tu empresa.

C. HAZ QUE LA CIBERSEGURIDAD SEA DIVERTIDA

Aporta ideas sobre cómo concienciar sobre la ciberseguridad en tu empresa creando materiales de formación interactivos. Se aprende a través del juego; la seguridad de los datos no es una excepción.

PARTE 3

3. SI TU EMPRESA ES NUEVA EN LA DIGITALIZACIÓN COMIENZA CON PEQUEÑOS PASOS

Si está claro que tu empresa aún no ha dado pasos significativos hacia la digitalización, el cambio no se producirá en un día. En cualquier caso, incluso los pequeños avances son importantes. Crea una estrategia de lugar de trabajo digital, empezando por pequeños pasos como la transición de la contabilidad corporativa hacia un entorno exclusivamente online. Esto te permitirá gestionar tus finanzas desde cualquier lugar y en cualquier momento, y si de repente toda la empresa necesita trabajar a distancia, la contabilidad digitalizada ya estará en marcha.

En general, encontrar soluciones que ayuden a eliminar el contacto físico entre las personas (cuando sea necesario) es la clave del éxito de la digitalización. Este es también un método adecuado para evitar las interrupciones del servicio por enfermedad.



PARTE 3

4. EXAMINAR LA PREPARACIÓN DE TUS PROVEEDORES

La mayoría de las empresas dependen de proveedores y servicios externos. Si no cumplen con sus obligaciones, es posible que no puedan resistir la crisis. Por eso es crucial saber hasta qué punto están dispuestos a cumplir sus obligaciones contractuales o incluso a ampliar su oferta hasta en tiempos de crisis.

Es útil tener varias soluciones para un mismo problema. Si una aplicación o servicio falla, debe haber una solución de respaldo, para que los empleados siempre puedan realizar cualquier tarea o comunicarse en línea.

PREGUNTAS QUE REALIZAR A TUS PROVEEDORES Y DISTRIBUIDORES

- ¿Dispones de un plan de continuidad empresarial para la gripe pandémica?
- ¿Has puesto a prueba tu plan de continuidad de negocio para la gripe pandémica en el último año?
- ¿Se ve afectado el proceso de nuestra empresa por el riesgo de altas tasas de absentismo entre tus empleados?
- En caso afirmativo, ¿aplicaste alguna medida para minimizar el riesgo de altas tasas de ausencia entre los empleados que prestan servicios a la empresa?
- ¿Tienes una lista de proveedores para los procesos críticos?
- ¿Se ve afectado el proceso que suministras a nuestra empresa por el riesgo de cortes de otros proveedores?
- En caso afirmativo, ¿habéis aplicado alguna medida para minimizar el riesgo de cortes en otros proveedores que participan en las entregas a nuestra empresa?
- ¿Tienes un plan de reanudación después de la crisis?
- ¿Está el personal formado para la gestión de la crisis?

PARTE 3

5. ADAPTAR LAS SOLUCIONES DE SEGURIDAD A LOS CAMBIOS

Aunque trasladar los procesos empresariales a Internet puede mejorar la continuidad de la empresa durante las crisis, también puede conllevar riesgos adicionales de ciberseguridad. Por lo tanto, tu función no solo debe ser garantizar una alta accesibilidad, sino también proteger los datos corporativos y personales en consecuencia. Una conectividad adecuada es también una necesidad, por lo que una red privada virtual (VPN) es esencial para contrarrestar los mayores riesgos de seguridad. Todos los empleados que trabajan a distancia deben tener una licencia VPN para poder conectarse de forma segura a la red corporativa.

Otra condición previa para un lugar de trabajo remoto y digitalizado eficaz es disponer de suficientes dispositivos que los empleados puedan utilizar desde casa. Pero, ¿qué ocurre si tu empresa no puede permitirse nuevos portátiles o tablets por el momento? Piensa en qué condiciones podrían utilizar los empleados sus dispositivos personales, como portátiles, smartphones, ordenadores de sobremesa y tablets. Lo más importante es que, como mínimo, cada dispositivo deberá estar protegido adecuadamente con una protección antimalware actualizada, utilizando una solución de protección de equipos multicapa completa de un proveedor fiable, no un antivirus gratuito.

PAQUETE DE INICIO DE CIBERSEGURIDAD PARA UN LUGAR DE TRABAJO DIGITALIZADO EFICAZ

- Entorno automatizado y estandarizado para facilitar la administración remota. Estandariza no solo las herramientas técnicas, sino también los procesos.
- Software fiable de protección de equipos, que puede utilizarse tanto para dispositivos corporativos como personales.
- Cifrado fiable del disco duro local.
- Seguimiento detallado de cada aplicación y de los datos.
- Contraseñas seguras respaldadas por MFA y políticas de grupo eficaces.
- Crear entornos híbridos combinando implementaciones de la nube para lograr una mayor eficacia.

PARTE 3

5. ADAPTAR LAS SOLUCIONES DE SEGURIDAD A LOS CAMBIOS

UTILIZAR NUEVAS APLICACIONES DE FORMA SEGURA PUEDE SER UN RETO, COMO LAS DE VIDEOCONFERENCIA. AQUÍ TIENES UNOS CUANTOS CONSEJOS SOBRE CÓMO REUNIRSE DE FORMA SEGURA.

- Asegúrate de que solo las personas autorizadas se unen a las reuniones. Crea grupos de usuarios o restringe el acceso por dominio de Internet.
- Establece contraseñas seguras para las reuniones y no incorpores la contraseña en el enlace de la reunión.
- Dejar que los participantes esperen en la sala de reuniones y aprobar la conexión para cada uno. Cuanto más grande sea la reunión, mayor será la posibilidad de que aparezca un invitado sin invitación.
- Encriptar el vídeo. Algunos servicios solo encriptan el chat.
- Limitar el intercambio de archivos por tiempo. No permitas que los archivos ejecutables sean intercambiados por los participantes.
- Elegir qué compartir en tu pantalla con los demás. Es posible que necesites compartir solo una aplicación, no todo el escritorio.
- Revisa tu entorno. Incluso los papeles en tu escritorio podrían incluir información sensible, revelando secretos corporativos.
- Comprueba la política de privacidad del servicio que utilizas. Puede ser que las aplicaciones gratuitas recojan y vendan tus datos para financiar la prestación del servicio: podrías convertirte en un producto.

PARTE 3

6. CAPACITA A TUS EMPLEADOS Y EMPATIZA CON ELLOS

Aunque la informática sea algo habitual para ti, no todo el mundo está tan familiarizado con el mundo digital. Organiza regularmente cursos y talleres de ciberseguridad. Además, asegúrate de que los empleados siempre puedan pedir ayuda: un correo electrónico especial para consultas anónimas es una buena solución.

Introduce la digitalización y las nuevas herramientas en línea como componentes útiles, no como una obligación. Las palabras importan: habla con claridad y utiliza un lenguaje sencillo, y si te cuesta explicarlo o tus empleados no captan la información, intenta cooperar con tu departamento de RRHH o los equipos de comunicación. Ten en cuenta que no existe ninguna pregunta que no sea importante.

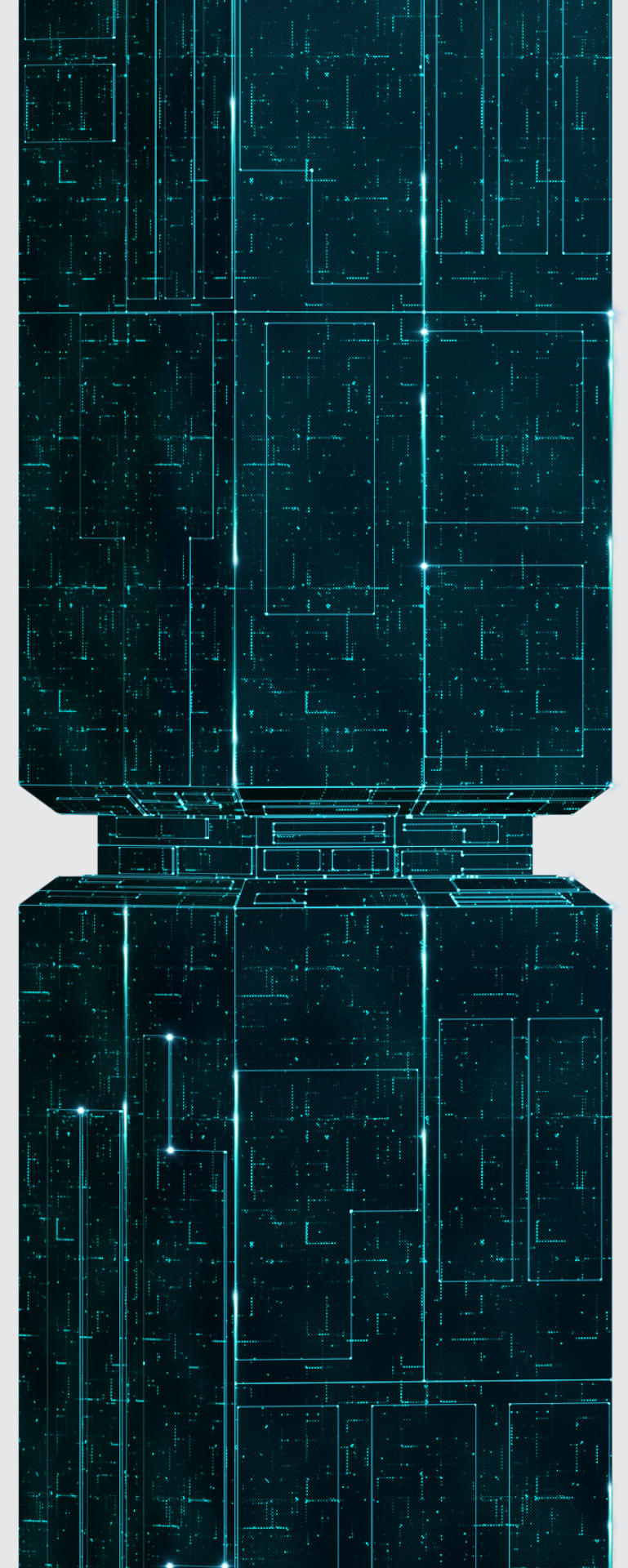
Intenta evaluar la eficacia de los empleados por tarea, no por hora. El mejor estimulante es la motivación: conoce bien a tus empleados y averigua qué tipo de tareas les gustan. Las tareas atractivas producen los mejores resultados y una alta productividad, y los empleados estarán más dispuestos a utilizar las nuevas herramientas digitales. Por último, pero no por ello menos importante, evalúa periódicamente los comentarios de los empleados y preocúpate por sus opiniones, problemas e ideas.

Además, cuando están estresados y trabajan a distancia, los empleados suelen leer y descargar información de fuentes poco fiables. Deben saber diferenciar entre los correos electrónicos normales y los de phishing. Un poco de formación sobre medios de comunicación también puede ahorrarte muchos problemas.

No te olvides del eslabón más débil de tu cadena de seguridad: el factor humano. Las instrucciones y la formación adecuadas de los empleados que ahora acceden a los sistemas críticos de la empresa desde su entorno doméstico, potencialmente desde dispositivos privados, deben ser implementados en tu empresa.

Los conocimientos sobre el malware, los virus y el phishing que se comunican de forma rápida y eficaz deberían ayudar a evitar una gestión negligente de las amenazas actuales que pueden amenazar la existencia de una empresa.

CONSEJO: LA FORMACIÓN EN CIBERSEGURIDAD DE ESET EVITARÁ QUE TUS EMPLEADOS PONGAN EN PELIGRO LA EMPRESA.



PARTE 3

6. CAPACITA A TUS EMPLEADOS Y EMPATIZA CON ELLOS

Te recomendamos que compartas los siguientes consejos de seguridad con tus empleados.

CÓMO DETECTAR FUENTES DE INFORMACIÓN SOSPECHOSAS

- No hay fecha de publicación.
- Falta el autor del artículo.
- La conexión no es segura (falta el icono del candado en el campo URL).
- El contenido es muy emotivo; aparecen muchos signos de exclamación.
- Se requiere una acción inmediata; por ejemplo, comprar algo o compartir algunos datos. El contenido está lleno de errores gramaticales.
- El contenido es gráfico.
- Aparecen frases como "Por qué los medios de comunicación no hablan de esto".

CÓMO EVITAR CAER DE LAS ESTAFAS DE PHISHING

- Evalúa la solicitud. ¿Es común o sospechosa?
- Si el remitente utiliza el nombre de un empleado de la empresa, ponte en contacto con él a través de otro canal fiable, o empieza a escribir un nuevo correo electrónico e introduce la dirección del remitente.
- No aceptes archivos y no hagas clic en nada de los correos electrónicos de desconocidos.
- Antes de hacer clic en un enlace de un sitio web, intenta buscar en Google el sitio web o incluso el nombre del remitente si el nombre no te resulta familiar.
- Busca errores gramaticales
- No envíes información sensible por correo electrónico. Si es posible, informa de los correos electrónicos sospechosos.

CONCLUSIÓN:

NO HABRÁ UN BUEN NEGOCIO SIN UNA BUENA IT

El futuro del trabajo es digital. He aquí por qué las empresas deben centrarse en la digitalización y en una gran infraestructura de IT, a partir de ahora.

LAS CIBERAMENAZAS SEGUIRÁN AUMENTANDO

El número de dispositivos en línea aumenta constantemente y las tácticas de los ciberdelincuentes mejoran continuamente junto con el uso de una sofisticada inteligencia artificial para mejorar la distribución y entrega de malware. Atrás quedaron los tiempos en los que los correos electrónicos de phishing eran muy fáciles de detectar.

El Informe de Preparación para la Ciberseguridad de Hiscox de 2019, que encuestó a unos 5.400 profesionales de Estados Unidos, Reino Unido, Alemania, Bélgica, Francia, España y Países Bajos, afirmó que alrededor del 61% de las empresas experimentaron un ciberataque en 2019, frente al 48% de 2018. "A nivel mundial, el coste medio de la pérdida asociada a un incidente cibernético ha pasado de 229.000 dólares a 369.000 dólares", señala el informe. Y las cifras van a aumentar en los próximos años.

LOS LUGARES DE TRABAJO FLEXIBLES ATRAERÁN EL TALENTO

Cada vez son más las personas que requieren flexibilidad en el trabajo, lo que puede conseguirse integrando soluciones

y herramientas en línea que permitan a los empleados trabajar a distancia.

Un lugar de trabajo digitalizado no solo permite mantenerse seguro y productivo en tiempos de crisis, sino que también ayuda a atraer más talento, atrayendo principalmente a los millennials (nacidos entre 1980 y finales de los 90), y la Generación Z (nacida entre finales de los 90 y 2010), que acaba de entrar en el mercado laboral. Un estudio del Centro de Investigación Pew de 2018 mostró que en 2016 los millennials se convirtieron en la generación más numerosa de la fuerza laboral estadounidense, por lo que es crucial satisfacer sus necesidades, que, entre otras, incluyen la flexibilidad de los horarios de trabajo.

Otra investigación llevada a cabo por PwC afirmaba que no solo los millennials, sino todas las generaciones de trabajadores, quieren más flexibilidad y un trabajo que les permita ocasionalmente trabajar desde casa. "Las similitudes en las actitudes de las distintas generaciones son sorprendentes", dice el estudio. Y así, cuando se aplican soluciones flexibles y digitalizadas, los empleados de todas las edades pueden estar más satisfechos, motivados y productivos.

CONCLUSIÓN:

NO HABRÁ UN BUEN NEGOCIO SIN UNA BUENA IT

PERMACE PROTEGIDO DE LA CRISIS

La crisis de la COVID-19 demostró que las empresas que fueron capaces de digitalizar sus procesos y activos resistieron la crisis mucho mejor que las que no estaban conectadas. Muchos expertos coinciden en que se avecinan más crisis e interrupciones, por lo que una plantilla remota y unos puestos de trabajo digitalizados y bien protegidos no solo serán una ventaja competitiva, sino también una necesidad.

Por lo tanto, las empresas deben darse cuenta de que las IT son su mejor aliado comercial y de que, en el futuro, no podrán operar sin profesionales de IT cualificados ni sin soluciones avanzadas de ciberseguridad. La crisis de la COVID-19 puede ser un momento decisivo, gracias a la cual la sociedad empieza por fin a percibir la digitalización de forma más positiva. Ya es hora.

SI QUIERES SABER MÁS SOBRE NUESTRA EXPERIENCIA, O NECESITAS AYUDA PARA ASEGURAR TU PERSONAL A DISTANCIA, HABLEMOS.

VISITA NUESTRA PÁGINA PARA **CONTACTAR CON NOSOTROS** DIRECTAMENTE, Y NOS PONDREMOS EN CONTACTO CONTIGO LO ANTES POSIBLE.