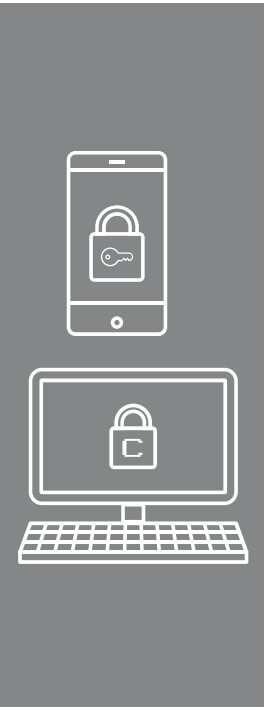


RECOMENDACIONES DE **CIBERSEGURIDAD** EN TIEMPOS DE **COVID-19**

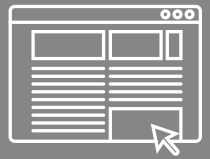
COVID-19

Abril 2020

ALGUNAS INDICACIONES PARA NUESTRA SESIÓN

Si tiene a la mano, puede ser mejor utilizar audífonos para tener un mejor audio.

Se recomienda tener apagada la cámara que transmite video y permanecer en la sesión solamente con audio, esto permitirá que la conexión a internet sea más estable.



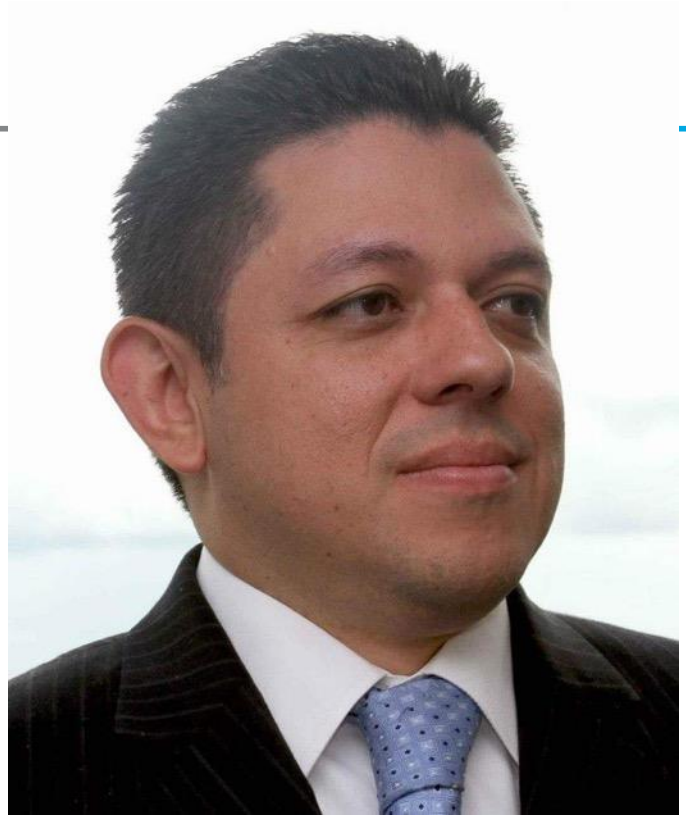
Solamente el expositor podrá compartir en la pantalla las presentaciones.

Todos los micrófonos, excepto los de los expositores, permanecerán cerrados durante la sesión.

Haremos las preguntas por escrito en el chat al final o durante la presentación. Podrán ser contestadas de forma privada o pública, ya sea de forma verbal o en el mismo chat.

Si por alguna razón se congela la presentación, pueden salir del link y volver a entrar.
Quien requiera más información puede enviarnos un correo electrónico a los datos de contacto que aparecerán al final.
La presentación y la grabación del evento estarán disponibles para ser consultadas o descargadas.

RSM



NUESTROS EXPOSITORES

Carlos Alberto Giraldo Díaz

- Socio de Consultoría de Riesgos de la Oficina de Colombia
- Más de 20 años de experiencia en proyectos relacionados con ciberseguridad, Sarbanes Oxley, auditoría de tecnología, auditoría interna, informes de control interno (SOC 1, SOC 2), planes de continuidad y consultoría de riesgos.
- Certificado CISA, CRISC, CISM, CBCP, CIA, PMP, ITIL, COBIT 5

NUESTROS EXPOSITORES

Victor Julián Morales Rivas

- Gerente / Consultor de Tecnologías de Información de la Oficina de Mérida de RSM México
- Vicepresidente de Ciberseguridad de CANIETI Sureste
- Expresidente de ISACA Capitulo Mérida

RSM

Agenda

1. Panorama del ciber riesgo en tiempos de COVID-19

2. Riesgos y vulnerabilidades a la seguridad de la información

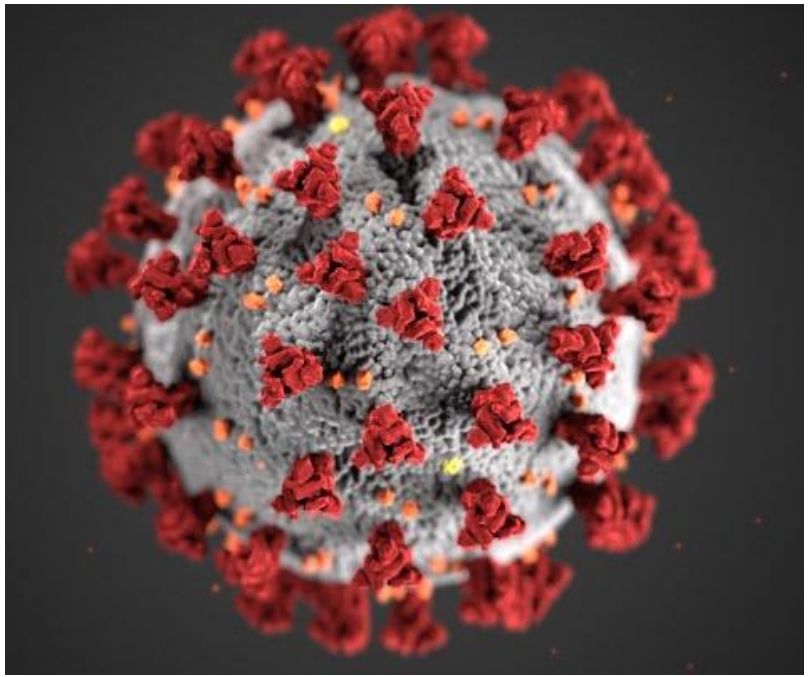
3. Trabajo remoto o Tele trabajo

4. Recomendaciones de seguridad para la empresa y los colaboradores

PANORAMA DEL **CIBER RIESGO** EN **TIEMPOS** DE **COVID-19**

RSM

INTRODUCCIÓN



La pandemia del COVID-19 ha generado cambios profundos y acelerados en la **manera de trabajar y hacer negocios**. En muchas áreas de la vida, incluyendo la educación, la vida social y comunitaria y por supuesto el trabajo y los negocios, las **tecnologías** han estado permitiendo la continuidad. Esto ha modificado la forma como vemos y usamos las **herramientas tecnológicas**.

En este contexto una de las preocupaciones necesarias que no debemos pasar por alto es la **seguridad de la información**, ya que de golpe en todo el mundo la mayoría estamos trabajando de manera remota o "**home office**".

Esto genera **oportunidades** pero también **vulnerabilidades** y **amenazas** que deben ser gestionadas adecuadamente por el bien de todos.

«Trabajar desde casa o estudiar con los programas en línea no son nuevos. Sin embargo, la migración casi instantánea de millones de usuarios desde redes empresariales y universitarias que se monitorean y protegen de cerca, a redes Wi-Fi domésticas en gran parte no supervisadas y a menudo inseguras, ***crea una oportunidad inmensa para los cibercriminales****«*

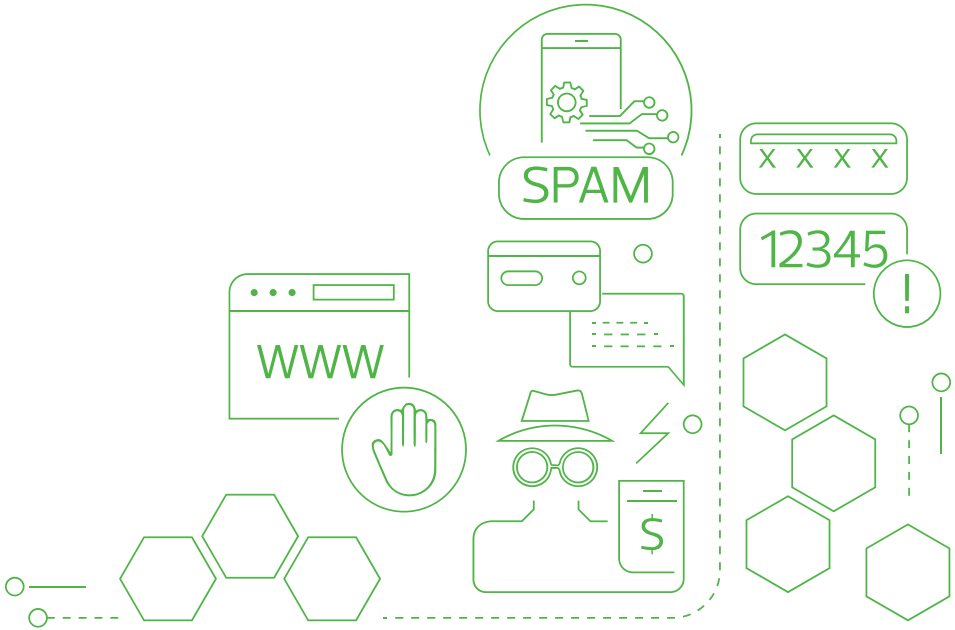
Chris Hazelton
Director de soluciones de seguridad
de Lookout.

INCIDENCIA DEL COVID-19 EN CIBERSEGURIDAD

Aumento de vulnerabilidades por uso de terminales / redes no corporativos	• Aumento del riesgo por uso de terminales / redes, sistemas de compartir archivos no corporativos y fuera del control del área de TI. • Con la descentralización se difumina el perímetro de seguridad.
Aumento de las amenazas	• Aumento de los ataques provenientes de hackers, grupos activistas y crimen organizado que tratarán de aprovecharse las debilidades indicadas.
Incremento de la presión y estrés de los colaboradores	• En condiciones de aislamiento las empresas deben implementar mecanismos para monitorear las necesidades de apoyo, concienciación y psicológicas de sus colaboradores. • Se pueden aumentar factores de estrés como incertidumbre laboral, desmotivación, angustia o tedio que cada persona podrá sobrellevar de diferente manera.

RSM

SUPLANTACIÓN DE IDENTIDAD (PHISHING) - ¿QUÉ ES?



- Es un método mediante el cual alguien finge ser una persona o compañía reconocida para engañarnos y que le proporcionemos información de cualquier tipo.
- Utilizan el correo electrónico o mensajes de texto (smishing) con links a sitios web inseguros de donde obtienen la información.

RSM

RIESGOS Y VULNERABILIDAD A LA SEGURIDAD DE LA INFORMACIÓN

TOP 10 FRAUDES QUE USAN COVID-19

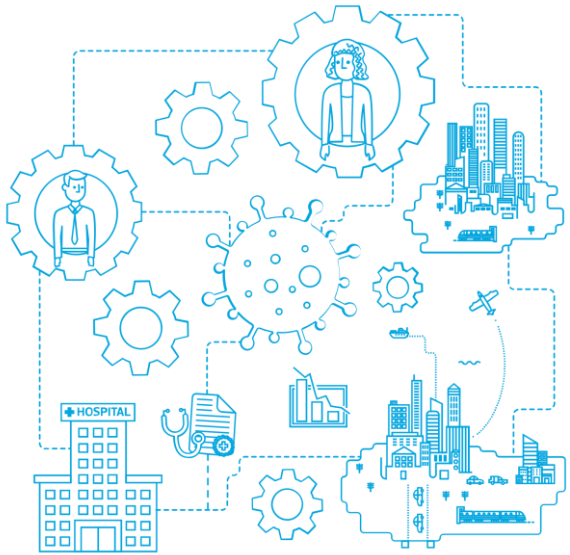
1. Mensajes con consejos para frenar el coronavirus (WhatsApp), varios de ellos con enlaces maliciosos.
2. Manda “Ayuda” a profesionales de salud al teléfono/email XXXX (redes sociales). Es una estafa a través de ayudas económicas.
3. Corona-phishing (correo electrónico, suplantando a una entidad como la OMS o entidades de salud locales)
4. Corona-smishing (SMS haciéndose pasar por el ministerio de trabajo o entidades similares)
5. Estafas en la venta de material sanitario (compras online)
6. Coronaware (ransomware) A través de un video o documento con instrucciones sobre como protegernos del virus
7. Mensaje de que el Gobierno reparte donaciones o subsidios por la crisis, el cual contiene un enlace malicioso
8. Ofertas de trabajo fraudulentas (robo de datos personales, incluso piden pago por adelantado)
9. Soporte técnico fraudulento (teléfono) Robo de datos personales o instalación de software malicioso
10. Lleva mejor la cuarentena con “servicios gratuitos” (falsos cupones). Un ejemplo de mensaje es el siguiente: “*Disfruta de todos nuestros servicios de streaming de películas y series de forma totalmente gratuita*”.

Fuente: OSI – Oficina de seguridad del internauta (España)

RSM

PRINCIPALES VULNERABILIDADES DE LA INFORMACIÓN

Los riesgos a que está expuesta la información son muchos. Podemos agruparlos de muchas maneras, una de las cuales es la siguiente:



1. La pérdida o destrucción no autorizada
2. El robo, extravío o copia no autorizada
3. El uso, acceso o tratamiento no autorizado
4. El daño, la alteración o modificación no autorizada

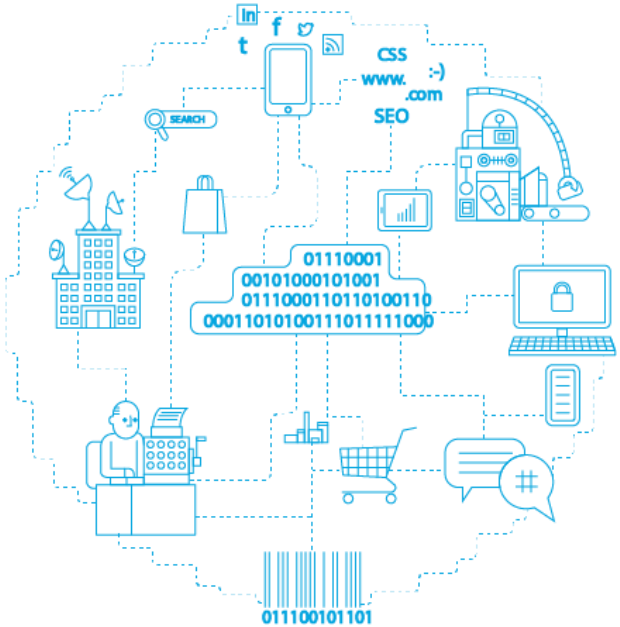
VULNERABILIDAD DE LA INFORMACIÓN ANTE EL COVID 19

PÉRDIDA O DESTRUCCIÓN NO AUTORIZADA

Se ha identificado que, a través de **correos electrónicos reconocidos como spam**, se incluyen comunicados engañosos en los que **suplantan páginas oficiales** para distribuir sitios web infectados haciendo uso de títulos llamativos.

Uno de los primeros casos documentados relacionados con COVID-19 fue reportado el 3 de febrero de 2020, en la que apareció en el boletín especializado de *Check Point Research* informando que los ciberdelincuentes se encontraban **explotando el pánico mundial** sobre el brote del coronavirus para infectar a los usuarios japoneses con malware Emotet.

VULNERABILIDAD DE LA INFORMACIÓN ANTE EL COVID 19



PÉRDIDA O DESTRUCCIÓN NO AUTORIZADA

Esto lo hacen a través de correos electrónicos que pretenden ser un aviso sobre **medidas de prevención de infecciones**, sobre la fabricación de una vacuna para combatir al virus, hasta la navegación de mapas interactivos en los que se identifican las zonas de propagación, así introducen un malware a los equipos de cómputo de los usuarios.

De esta manera, se observa como el **software malicioso** está siendo propagado aprovechando la necesidad o **curiosidad** de las personas por consultar información respecto a la pandemia de COVID-19.

VULNERABILIDAD DE LA INFORMACIÓN ANTE EL COVID 19

ROBO, EXTRAVÍO O COPIA NO AUTORIZADA

Ofertas falsas

Los *scammers* (estafadores virtuales) envían **correos de spam** en búsqueda de que las víctimas crean que pueden ordenar **máscaras de protección** para mantenerse a salvo del nuevo virus. Lo que sucede es que las víctimas revelan información sensible, personal y financiera, a los atacantes.

EL PAÍS ESPAÑA

URGENTE La OMS advierte de que un desconfinamiento precipitado puede tener un "impacto mayor" en la economía

Las estafas por Internet aumentan un 70% durante la cuarentena

Las comunicaciones a Policía y Guardia Civil de posibles fraudes con material sanitario se multiplican

PATRICIA ORTEGA DOLZ

Madrid - 19 ABR 2020 - 17:56 CDT

Policía investigando delitos en Internet POLICÍA NACIONAL 07/04/2020 / EUROPA PRESS

NEWSLETTER

Recibe el boletín de Actualidad

TE PUEDE INTERESAR

Últimas noticias del coronavirus, en directo | La OMS advierte de que un desconfinamiento precipitado puede tener un "impacto mayor" en la economía

OFERTAS

escaparate | EL PAÍS

RSM

VULNERABILIDAD DE LA INFORMACIÓN ANTE EL COVID 19

ROBO, EXTRAVÍO O COPIA NO AUTORIZADA

Campaña en Colombia suplanta identidad del Ministerio de Salud

El Ministerio de Salud de Colombia, a través de su cuenta de Twitter advirtió la existencia de una campaña que circula por correo electrónico y por WhatsApp, suplantando la identidad del Ministerio de Salud, en la que envían un adjunto (archivo PDF) para distribuir un código malicioso que se instala en el dispositivo de la víctima. El objetivo de esta campaña **es robar información personal**, asegura el organismo de salud colombiano.

VULNERABILIDAD DE LA INFORMACIÓN ANTE EL COVID 19

USO, ACCESO O TRATAMIENTO NO AUTORIZADO

Una de las principales vulneraciones a los datos personales es la apropiación de la identidad de una persona, para hacerse pasar por ella, asumir su identidad frente a terceros públicos o privados, a fin de obtener ciertos recursos o beneficios a su nombre. El robo de identidad implica la obtención y uso **NO autorizado** e ilegal de **datos personales.**

VULNERABILIDAD DE LA INFORMACIÓN ANTE EL COVID 19

USO, ACCESO O TRATAMIENTO NO AUTORIZADO

Suplantación de identidad de la OMS

Como la **Organización Mundial de la Salud** (OMS), es la principal fuente de información sobre el brote de Coronavirus, se encuentra entre las autoridades cuya identidad se ha visto más suplantada en las últimas campañas de engaños. La forma de operar de los atacantes ha sido ofrecer información relevante acerca del virus, en un intento por lograr que potenciales víctimas hagan clic en los enlaces maliciosos. Comúnmente, dichos enlaces pueden instalar **malware**, robar información personal, o intentar obtener credenciales de ingreso y contraseñas.

VULNERABILIDAD DE LA INFORMACIÓN ANTE EL COVID 19

DAÑO, ALTERACIÓN O MODIFICACIÓN NO AUTORIZADA

Suplantación de sitios web

Se identificó que un sitio web de phishing se encontraba suplantando la identidad del sitio web de Wall Street Journal (WSJ) con supuestos reportes respecto a las últimas noticias acerca del COVID-19. En la dirección electrónica, se observa que comienza con ‘*worldstreet’*, y el logo que allí se muestra también dice *‘world street’*.

VULNERABILIDAD DE LA INFORMACIÓN ANTE EL COVID 19

DAÑO, ALTERACIÓN O MODIFICACIÓN NO AUTORIZADA

Campañas de donación para vacunas en china

Otro tipo de engaño que se ha presentado es aquel que busca conmover al receptor para que éste colabore en la creación de una vacuna para los niños de China. De acuerdo con la Secretaria de Salud, no existe una vacuna disponible, y no se espera que llegue al público hasta el próximo año.

TRABAJO REMOTO O TELE TRABAJO

TRABAJO REMOTO O TELE TRABAJO

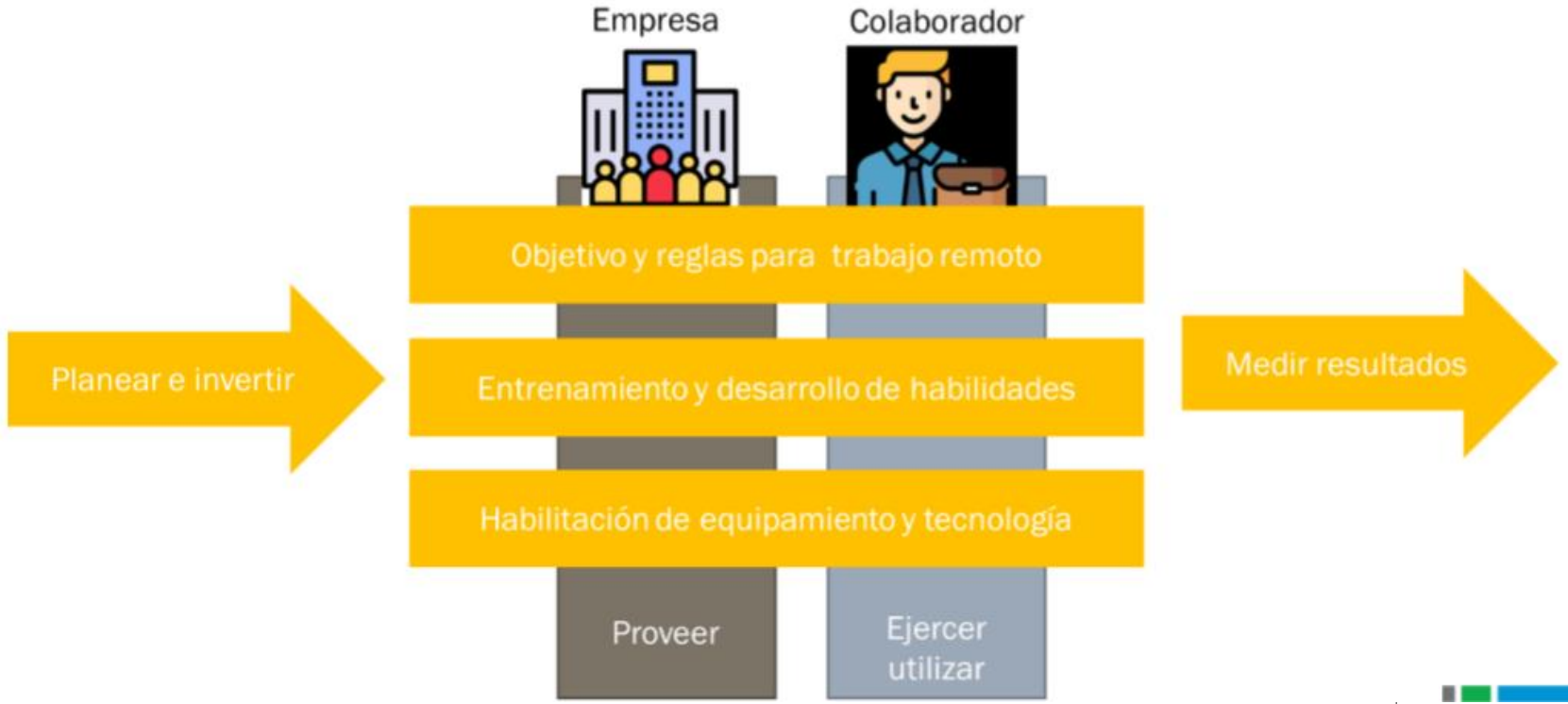
- El trabajo remoto o tele trabajo, es una modalidad en la cual el colaborador puede realizar su actividad profesional fuera de la oficina. Si bien generalmente está asociado con el home office, no está limitado únicamente al hogar; puede ser también en oficinas compartidas o cualquier espacio diferente al de la empresa.

- Sin lugar a duda, esta metodología ha tomado gran fuerza debido al crecimiento y las posibilidades que brinda Internet, especialmente en cuanto al desarrollo de nuevas tecnologías de la comunicación integradas en sistemas alojados en la nube.

- Esta modalidad obliga a que las empresas contemplen diversos panoramas, como la manipulación de información laboral en dispositivos que pueden no estar protegidos adecuadamente o el acceso remoto a información sensible. Estos casos, entre muchos otros, hacen que las organizaciones se planteen formas diferentes de gestionar la seguridad para minimizar los riesgos asociados con un ataque a la información más crítica

RSM

EL TRABAJO REMOTO ES UNA ALTERNATIVA BUENA CUANDO SE EJECUTA RESPONSABLEMENTE



TRABAJO REMOTO O TELE TRABAJO

ALGUNOS DOCUMENTOS QUE SE RECOMIENDA TENER DEFINIDOS E IMPLEMENTADOS PARA FORTALECER EL TRABAJO REMOTO

- Acuerdos laborales o cláusulas en el contrato de trabajo que contemplen la modalidad del trabajo remoto, según la legislación vigente aplicable.
- Clasificación de la información, que datos son de fácil acceso y cuales deben tener mayor nivel de protección
- Código de ética
- Programas de continuidad de negocios (BCP)
- Políticas internas de trabajo remoto que expliquen el qué, quién y cómo
- Política de sanciones a conductas inadecuadas
- Política de seguridad informática
- Política de confidencialidad y Acuerdos de confidencialidad firmados por los colaboradores.
- Política de uso de equipos de cómputo
- Política de contraseñas segura

RSM

RECOMENDACIONES

7 PILARES PARA LA SEGURIDAD

1 GESTIONAR ROLES

- Es vital cerciorarse de que el acceso a la información esté permitido únicamente para aquellos roles que realmente estén habilitados para ello.
- Los colaboradores deben estar al tanto de las políticas aplicables a su trabajo y, además, tener asignados los permisos necesarios para llevar a cabo sus tareas, puesto que dejar perfiles por defecto, sin control o sin políticas de acceso pueden generar problemas de seguridad.
- En la empresa se deben establecer las responsabilidades de acuerdo a los objetivos planteados, en relación a todos los aspectos del trabajo y del manejo de la información: quién debe crear, revisar, autorizar, respaldar…
- Aspectos como el control de las tecnologías, la realización de copias de seguridad, contar con procesos de recuperación, entre otros, son algunas de las tareas que deben tener un ejecutor y momento definido.

RSM

7 PILARES PARA LA SEGURIDAD

2 CONTROL DE DISPOSITIVOS

POR LA EMPRESA

- Considerar los equipos que serán utilizados y quiénes tienen acceso a ellos (ejemplo: equipos personales vs equipos de la empresa).
- Considerar software legal licenciado o libre, software para trabajo colaborativo (chat, videoconferencia,…), ofimática y aplicaciones
- Habilitar las políticas de las computadoras como si estuvieran en la oficina (ejemplo, cerrar sesión cuando no se este utilizando en la computadora)
- Cifrar los discos duros de las computadoras para asegurarse que si caen en manos equivocadas no se pueda acceder a los datos de la compañía.
- Controlar el uso de dispositivos externos como USB, discos duros o periféricos

POR EL COLABORADOR.

- Cuidar el equipo asignado en su caso protegiéndolo de accesos no autorizados, así como usos indebidos.
- Nunca pierda de vista su computadora o dispositivo o lo deje a la vista en el coche.
- Evita usar el dispositivo de la empresa para cuestiones personales o prestarlo a alguien mas.
- No descargar, ni utilizar software pirata o no licenciado en sus equipos propios o de la empresa.

RSM

7 PILARES PARA LA SEGURIDAD

3 PROTEGER CONTRA CÓDIGOS MALICIOSOS

POR PARTE DE LA EMPRESA.

- Importante contar con equipos de cómputo o escritorio virtualizado, que tengan antivirus, firewall activado, firmware y parches actualizados

POR PARTE DEL COLABORADOR.

- Mantener la computadora y dispositivos móviles actualizados con los últimos parches de seguridad y versiones de sistema operativos soportadas por los proveedores
- Realizar mínimo un escaneo completo de la computadora una vez a la semana
- Mantener habilitadas las medidas de seguridad que disponen los dispositivos

RSM

7 PILARES PARA LA SEGURIDAD

4 MONITOREAR EL TRÁFICO DE LA RED

POR LA EMPRESA

- Dado que hay dispositivos que están ingresando a la red por fuera del perímetro físico de la oficina, es necesario hacer un seguimiento de qué tipo de tráfico generan. Por ejemplo, dónde tratan de acceder, si hay intentos recurrentes y fallidos de ingreso a servidores o si, incluso, generan algún tipo de tráfico inapropiado, como la descarga de archivos desconocidos.
- Otro aspecto importante, es la posibilidad de hacer bitácoras de tráfico que permitan verificar el comportamiento de la red cuando se hace algún cambio, ya sea la inclusión de una nueva tecnología o algún servicio, logrando determinar el uso que hacen los usuarios que están por fuera de la red

RSM

7 PILARES PARA LA SEGURIDAD

5 CONEXIONES SEGURAS

POR PARTE DE LA EMPRESA

- Asegurar que se tenga acceso a internet.
- Habilitación de accesos remotos seguros a los aplicativos y datos de la empresa a través de VPN
- Habilitación de medios de autentificación multifactor

POR PARTE DEL COLABORADOR.

- Utilizar siempre una VPN para conectarse a la red interna de la compañía
- Acceder a las aplicaciones de la empresa solo desde la computadora o dispositivo configurado y avalado por la empresa
- Evitar el uso de redes públicas
- Procurar que la información sensible sea manejada en la red de la organización y no descargarla localmente al equipo

RSM

7 PILARES PARA LA SEGURIDAD

6 POLÍTICA DE SEGURIDAD

POR LA EMPRESA

- Definir las intenciones respecto a la seguridad de los recursos informáticos, determinar las obligaciones y responsabilidades de los usuarios respecto al uso de las tecnologías que tienen a su disposición.
- Habilitar a personal técnico o especializado para la respuesta inmediata a incidentes de seguridad
- Monitorear que se estén realizando de manera correcta los respaldos de la información y hacer prueba de restauración. (3-2-1)

POR PARTE DEL COLABORADOR.

- No dejar su sesión abierta en la computadora tanto en casa como en sitios públicos.
- Separar las cuentas personales y las de trabajo (no utilizar las mismas contraseñas)
- La información sensible como contraseñas y números de tarjetas de crédito no deben ser enviados a través de Internet.
- Usar contraseñas seguras y diferentes para diferentes cuentas (de preferencia autentificación multifactor)
- Si se requiere enviar información sensible, deberá encriptarse
- Estar atento a llamadas telefónicas, correos electrónicos o mensajes de texto inusuales

RSM

7 PILARES PARA LA SEGURIDAD

6 POLÍTICA DE SEGURIDAD

POR PARTE DEL COLABORADOR.

- No haga clic en los enlaces: escriba las URL
- Verificar los certificados de seguridad, especialmente para los sitios web de pago
- No se recomienda utilizar repositorios de datos personales y/o no validados por el área de TI de la empresa para almacenar información de la empresa, clientes o proveedores.
- Usar las cuentas de correo electrónico de la empresa en lugar de cuentas personales para correos electrónicos relacionados con actividades laborales
- Evita navegar por sitios no seguros
- No descargues archivos de origen desconocido ni bajar o ver películas o videos piratas o que sean gratis
- Realizar el respaldo de su información (3-2-1) de conformidad con las políticas y procedimientos aplicables
- Si identifica una situación inusual reportarla inmediatamente al área de tecnología de su empresa o a la mesa de ayuda.

RSM

7 PILARES PARA LA SEGURIDAD

7 CONCIENTIZACIÓN Y CAPACITACIÓN

POR LA EMPRESA

- Capacitación sobre herramientas colaborativas y de acceso remoto
- Concientización en temas de seguridad.
- Reglas aplicables al trabajo remoto.
- Reglas aplicables al manejo de la información.
- Capacitación sobre Políticas de uso de los equipos.
- Habilitar un canal de soporte para atender todas las necesidades de los colaboradores

POR EL COLABORADOR

- Participar en la capacitación y aprovecharla.
- Conocer y respetar las políticas que son aplicables.
- Entender que aunque esté por fuera de la oficina, el dispositivo desde el cual trabaja es una puerta a toda la organización y como tal debe garantizar un uso adecuado.

RSM

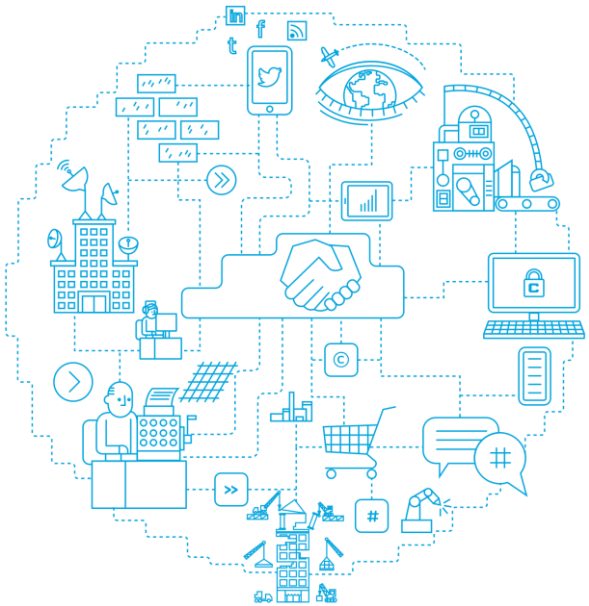
MARCO DE CIBERSEGURIDAD

Marco de ciberseguridad para **protección de activos digitales de acuerdo al** Instituto Nacional de Estándares y Tecnología (NIST) y la Agencia para la Seguridad de la Red y de la Información de la Unión Europea (ENISA).

RSM

ACCIONES DE CORTO PLAZO

Hay ciertas acciones no menos importantes que se deben de tomar en cuenta:



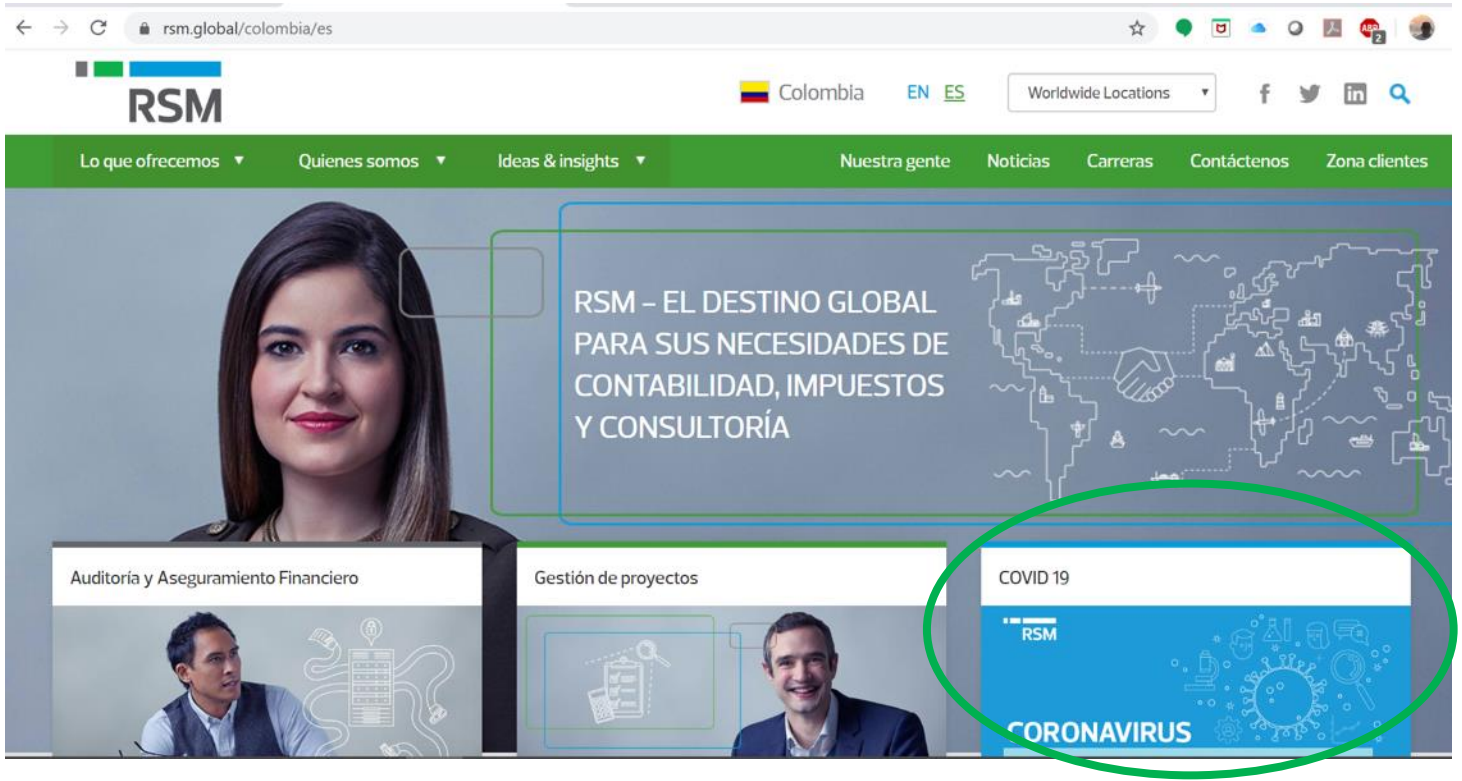
- Establezca una gestión virtual a puertas abiertas, escuche a sus colaboradores, no asuma que todos pueden cambiar a esta nueva dinámica de trabajo de manera efectiva, el hogar no es la oficina.
- Las áreas de TI deben ser mas cercanas, empáticas y con actitud de servicio hacia los colaboradores.
- Muchas empresas al igual que ustedes están experimentando lo mismo, por lo que el nivel de adaptación puede ser diferente, busque siempre se propositivo, hacer sinergias.
- El colaborador se siente mas productivo, vea que lo sea, ya que cuando regrese a la oficina ya no va ser igual.

¿DÓNDE PUEDO ENCONTRAR EL MATERIAL?

www.rsm.global/mexico

¿DÓNDE PUEDO ENCONTRAR EL MATERIAL?

www.rsm.global/colombia



RSM

Carlos Giraldo

Socio Consultoría de Riesgos de TI

Teléfono directo +57 (4) 2 666474 Móvil +57 315 5639280

Correo electrónico: carlosalberto.giraldo@rsmco.co

Julián Morales

Consultor de Técnologias de Información

Teléfono +52 (999) 9256680 Móvil +52 9999 551612

Correo electrónico: Julian.morales@rsmmx.mx

PREGUNTAS Y RESPUESTAS

Gracias por su tiempo y atención