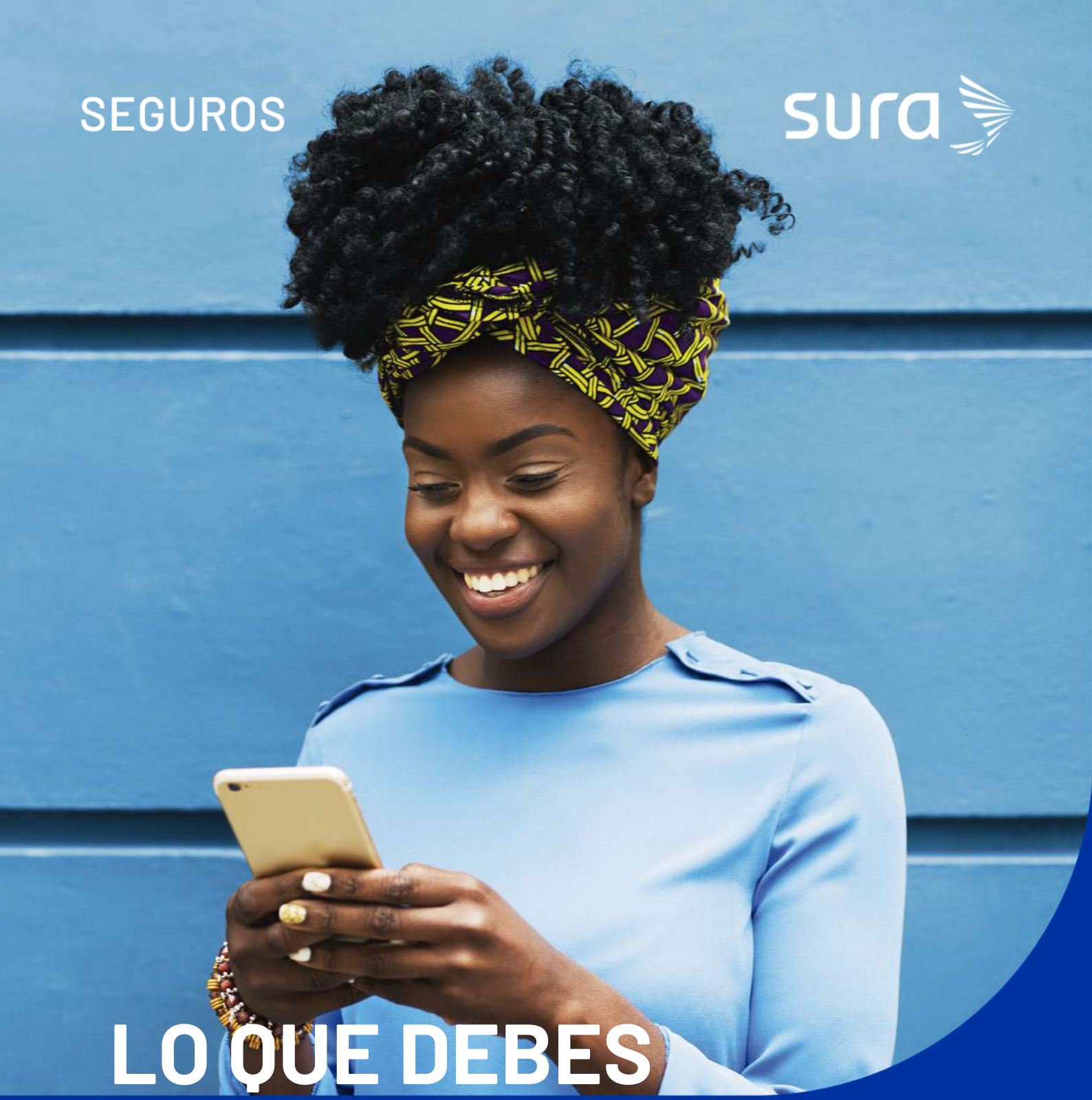
SEGUROS

sura



LO QUE DEBES SABER SOBRE CIBERSEGURIDAD

#asegúratedehacertuparte

INTRODUCCIÓN

Actualmente, la mayoría de los gobiernos y empresas del mundo están buscando garantizar el bienestar y la seguridad de sus ciudadanos, colaboradores y clientes. La preocupación colectiva en tiempos adversos hace que la información cobre un rol determinante. De esta manera, la proliferación de datos y contenidos puede provocar un aumento significativo en los ataques cibernéticos, y por eso se hacen más que necesarias las medidas de control y protección para los usuarios.

Los ciberdelincuentes tienden a aprovecharse de temas actuales y de alto flujo de búsqueda de información, lo cual lleva a una gran probabilidad de que se descargue un archivo malicioso, con una apariencia de contenido que alude a temas de interés común.

Otra de las amenazas a las cuales nos vemos enfrentados actualmente son las noticias falsas. WhatsApp y otras redes sociales son los medios más usados para difundir rumores en forma de testimonios atribuidos a autoridades o personajes reconocidos en el asunto que se esté tratando.

CONSIDERACIONES

Durante periodos de crisis, se reducen los niveles de alerta y protección de los usuarios finales y de esta situación se aprovechan los ciberdelincuentes para ejecutar ataques cibernéticos con el fin de obtener información privilegiada o vanagloriarse de esta. Por tal motivo, es importante saber cómo identificar cuando una situación puede comprometer o no la seguridad de la información.

Mientras estamos más conectados a internet, los riesgos cibernéticos aumentan. En una situación de trabajo remoto las medidas y los controles para protegernos de los ciberdelincuentes deben ser mayores, pues el acceso a la información es mucho más sencillo, considerando que en los hogares y sitios públicos, por lo general, no contamos con medidas de seguridad eficientes.

Los ciberdelincuentes disponen de una variedad de programas informáticos para obtener datos privilegiados como cuentas bancarias, redes sociales, datos médicos y demás, utilizando también técnicas de manipulación o ingeniería social para obtener información de las personas o de las empresas y, en muchos casos, suplantar su identidad.

Aunque para los cibercriminales siempre es un buen momento para ejecutar ataques cibernéticos, las situaciones de crisis o los temas coyunturales incrementan su actividad, aprovechándose de la vulnerabilidad de las personas.

ALGUNOS DE LOS ATAQUES CIBERNÉTICOS MÁS COMUNES SON:

- **Ingeniería social:**
  Se busca manipular a las personas por medio de información confidencial que se obtiene a través de correos electrónicos, mensajería instantánea como WhatsApp y redes sociales.
- **Malware:**
  Es un método de manipulación y chantaje por medio de softwares maliciosos, en el que se busca tener un control total o parcial de los dispositivos de las víctimas.
- **Phishing:**
  Es uno de los fraudes más comunes en Internet y se lleva a cabo a través de la creación de páginas web falsas y de la alteración del destinatario de los correos electrónicos.

En situaciones de alerta, los ciberdelincuentes han visto la oportunidad de engañar a las personas para suplantar la identidad de industrias en especial relacionadas con el tema de atención médica, por ejemplo, en momentos de crisis de salud han suplantado destinatarios de la Organización Mundial de la Salud (OMS). Igualmente, han recibido correos electrónicos y mensajes invitando a cooperar con iniciativas relacionadas, prácticas o ejercicios de meditación estando en cuarentena y similares. Cualquier tema relacionado con los momentos de crisis puede ser objeto de engaño para las personas.

Estos son algunos ejemplos de lo que podríamos recibir en nuestra bandeja de entrada:

Correos que afirman tener vacunas para la cura de enfermedades. Este caso proviene de un supuesto médico quien redacta el correo y hay un enlace al final del mensaje. Al pasar el mouse sobre el enlace, es posible visualizar la página a la cual hace el direccionamiento e identificar que el sitio web es de dudosa procedencia. Adicionalmente, es importante revisar si el emisor del mensaje es conocido o familiar.

Cabe resaltar que los avances médicos [Office1] [Office2] se pueden consultar en las páginas oficiales de la OMS o de los entes gubernamentales en salud, todos estamos expuestos a una situación de alta incertidumbre en donde no hay entidades no gubernamentales que tengan de primera mano esta información.

Correos de centros de investigación: en este tipo de contenido puedes estar siendo invitado a participar en una investigación cuyo fin es desarrollar vacunas o medicamentos, y para la cual te solicitan realizar un pago en monedas digitales o criptomonedas. Ten en cuenta que, actualmente, son los institutos educativos y del sector salud los responsables de estas investigaciones. Si recibes un correo puedes verificar la participación a través de su página web, en lugar de realizar cualquier pago o de abrir un enlace malicioso.

TE SUGERIMOS LAS SIGUIENTES LÍNEAS DE ACTUACIÓN:

Correo electrónico: debes mantenerte alerta, evitar abrir correos sospechosos, no descargar ningún archivo adjunto ni hacer clic en enlaces cuyo remitente no reconozcas, especialmente aquellos que prometen contenido exclusivo. Ten precaución con las descargas que realizas, dado que los archivos adjuntos aparentar ser confiables, pero pueden tener virus informáticos que comprometen tu información.

Búsqueda de información: consulta fuentes oficiales y revisa los archivos a descargar.

Mantener la salud cibernética: ten cuidado con la información que te llega y no la reenvíes sin validar su veracidad.

Protege la información: haz respaldo de tus datos frecuentemente para mantenerlos seguros.

OTRAS RECOMENDACIONES:

- Ten cuidado con la información que llega y no la reenvíes sin validar la veracidad de esta.
- Haz un respaldo frecuente de tus archivos para mantenerlos seguros.
- Evita dar clic a enlaces enviados por mensajería instantánea. Tampoco los compartas.
- El exceso de información puede llevar a una desinformación, confía en fuentes de organizaciones públicas y gubernamentales.
- Estar en casa hace que cambien los hábitos, las interacciones y rutinas, por eso es momento de reflexionar y replantearte nuevamente lo esencial. Desconectarse es también estar conectado.
- Que la ansiedad por conocer no limite tu juicio y capacidad crítica para identificar destinatarios, fuentes y contenidos falsos.
- No dudes en preguntar y consultar todas las inquietudes que tengas respecto a tu vida diaria en los diferentes medios de los sistemas de salud. Una buena decisión se centra en una buena fuente de información.
- Si nos enfrentamos a un momento de alta incertidumbre, donde hay más preguntas que respuestas, debemos comunicarnos entre los más cercanos y acudir a las fuentes gubernamentales para resolver las inquietudes.
- Ten precaución con la ejecución o apertura de archivos adjuntos, especialmente si tienen la extensión ".exe", ".js" o ".xlsx".
- En este momento. las compañías (aerolíneas, bancos, clínicas, supermercados) están usando sus redes sociales oficiales para comunicarse con sus clientes. Si tienes dudas con alguna en particular, síguelas y escríbeles.
- Recuerda que los corres de entidades financieras nunca te piden información de tu cuenta bancaria o claves de acceso a través de formularios web o un correo electrónico.
- Si recibes un correo electrónico sospechoso de una persona desconocida, elimínalo.
- Revisa el origen y el contenido de los correos electrónicos para identificar direcciones erróneas, dominios incorrectos (esto es lo que hay después del @), URL con etiquetas engañosas (puedes verificarlo con .com .org) y otras señales (idiomas del correo, nombre del remitente conocido).

- En el caso de recibir un correo electrónico de un remitente desconocido o que tiene información que no esperabas, no lo abras y elimínalo inmediatamente. Tampoco respondas o reenvíes correos sospechosos. Si deseas reportar un fraude, puedes tomar una captura de pantalla desde tu celular o computador.

- Usa otros canales de comunicación como redes sociales, llamadas telefónicas, mensajes vía WhatsApp en caso de que debas hacer algún cambio o validación de estado de vuelos, reservas, citas médicas, exámenes médicos, domicilios, entre otros.

- En caso de que hayas abierto un correo fraudulento, te aconsejamos cambiar las contraseñas de todas tus cuentas desde otro dispositivo.

- En redes sociales, sigue las cuentas oficiales de las instituciones o empresas, es importante verificar la fuente real de la información.

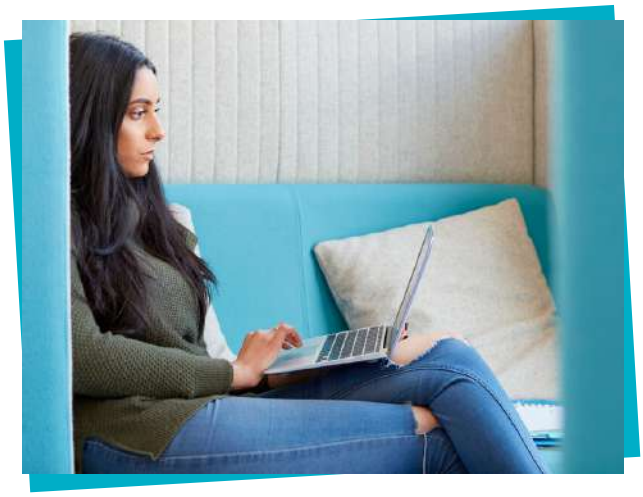
- Si algo es demasiado bueno para ser verdad, desconfía, realmente no lo es.

- Asegúrate de tener instalado un software contra virus informáticos en tu celular o computador personal.

- En caso de sentirte vulnerado, puedes realizar una denuncia ante las autoridades de tu país.

PREGUNTAS FRECUENTES

¿POR QUÉ ES IMPORTANTE ESTAR SENSIBILIZADOS SOBRE LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN?



Es importante que todos seamos conscientes de los riesgos a los cuales podemos vernos expuestos en internet. La información es uno de los activos más valiosos tanto para las empresas como para las personas, y especialmente ahora, todos podemos ser víctimas de amenazas cibernéticas, llegando a exponer fácilmente temas confidenciales.

¿ES CIERTO QUE LOS CIBERDELINCUENTES SÓLO ATACAN A LAS EMPRESAS GRANDES?

Tanto las personas, como las pequeñas y medianas empresas tienden a pensar que los ciberdelincuentes solo afectan a grandes compañías, motivo por el cual muchas veces no toman las precauciones necesarias.

Cualquier empresa o persona puede ser víctima de un ataque cibernético, por lo que es importante dejarse asesorar de un experto y trabajar para que no ocurra. Si sucede, es necesario aprender de la experiencia y salir fortalecidos. Cabe aclarar que, muchas veces, las pymes sirven de puente para acceder a otras empresas más grandes, al poseer información de interés para los ciberdelincuentes.

Recuerda: no importa tu tamaño, importa el tipo de información que manejas y el relacionamiento con otras entidades o aliados.

¿QUÉ MEDIDAS PUEDO IMPLEMENTAR PARA DISMINUIR LOS INCIDENTES CIBERNÉTICOS EN MODALIDAD DE TELETRABAJO?

- Tener una VPN para la conexión segura a los sistemas donde esta alojada la información. Preferiblemente VPN's probadas y actualizadas.
- Compartir las amenazas a las que todos podemos estar expuestos por medio de la navegación en internet, ingreso al correo electrónico o a links de noticias de interés.
- Hacer un buen uso de la información, por ejemplo: evitar descargar información confidencial en los computadores personales o enviarla a correos electrónicos distintos a los laborales

- Hacer respaldos de información constantes a un repositorio seguro en la nube y al cual solo tú tengas acceso.
- Mantener todos los sistemas operativos y las aplicaciones actualizadas.
- Revisar la seguridad de los accesos remotos a los sistemas de la compañía.
- Incentivar el uso de contraseñas seguras (mínimo 10 caracteres incluyendo caracteres especiales) e implementar un doble factor de autenticación a través de mensaje de texto, correo electrónico o llamada.

¿CÓMO IDENTIFICO CORREOS SOSPECHOSOS?

Revisa quien envía el mensaje, generalmente recibir un correo de una persona desconocida genera desconfianza.

Si recibes un correo de una persona que conoces, es fundamental evaluar si el asunto que comunica tiene sentido, si el texto es correcto y si el idioma concuerda con el nativo de la persona. También debes observar con detalle los enlaces del remitente (que la dirección asociada tenga una coherencia con su empresa o razón social) y tener en cuenta que, normalmente, ninguna empresa te pide alguna contraseña por medio de un correo electrónico. Si llegan a solicitar esta información, valídala por otro canal de comunicación.

Finalmente, recuerda que los correos maliciosos suelen utilizar tono de urgencia, exigiendo algún tipo de acción (como suministrar datos personales o alguna contraseña) y establecen una fecha límite para el suministro de datos.

¿CUÁLES SON LOS RIESGOS A LOS QUE ESTOY EXPUESTO DADO EL TRABAJO EN CASA?

Dada la crisis actual, el nivel de exposición y de riesgo de las empresas frente a fugas de información y accesos no autorizados a sus sistemas puede llegar a ser más probable.

Los espacios de oficina física son ambientes que por lo general se tienen controlados, pero en las instancias actuales se hace más difícil y lento activar el proceso de apoyo y de respuesta a incidentes de tecnología, haciendo que el robo de información sea un riesgo inevitable. Por dicho motivo, se vuelve indispensable contar con planes alternativos y herramientas confiables que permitan darle continuidad a su negocio.

LA SALUD ES RESPONSABILIDAD DE TODOS.
¡CONSERVEMOS LA CALMA, ACATEMOS Y AUMENTEMOS LAS MEDIDAS SANITARIAS!
ENTRE TODOS, PODEMOS SUPERARLO.

Para más información visita
www.segurossura.com/covid19

#asegúratedehacertuparte