Seguros Venezuela y ESET comparten consejos para proteger sistemas y datos

Empresas y colaboradores deben blindarse para evitar riesgos de delitos informáticos en teletrabajo

Frente al auge del **teletrabajo**, que significa asumir y cumplir desde casa con las responsabilidades usuales de las labores que se hacen en la oficina, los expertos en seguridad informática recomiendan que tanto las empresas como sus colaboradores amplíen sus medidas de protección de datos y sistemas informáticos.

El gerente de Soporte y Capacitación de **ESET** en Venezuela, Carlos López, explica que los riesgos en el área de **ciberseguridad**, como pérdida de información o ataques de malware, son los mismos que si se trabaja desde casa o desde la sede de la empresa, si no se toman acciones como la utilización de redes VPN o la instalación de programas antivirus.

"En el modo de **teletrabajo** tenemos los mismos riesgos que cuando estamos directamente en nuestra oficina, lo que tenemos que hacer es trasladar nuestros controles de seguridad de los colaboradores desde la compañía a la casa.Se trata de ampliar nuestro 'anillo de seguridad'", señaló López.


Fotografía: Freepik

Cinco consejos para estar protegidos:

1 Encriptar los datos. Cuando no se cuenta con conexiones que encriptan o "cifran" datos, como contraseñas, es fácil para terceras personas ajenas a la organización obtener usuarios, claves o puertos de conexión, con herramientas que se pueden conseguir en internet para el análisis de tráfico de red.

2 Usar conexión VPN. "Una de las cosas que se requieren es que las empresas cuenten con conexión VPN, que cifra la información que transita del computador personal del trabajador hasta la red de la compañía", indicó López.

3 Activar antivirus. "Además de VPN, la organización de procurar la instalación de antivirus para evitar el malware tanto en dispositivos de la empresa como los de uso personal".

4 Sólo habilitar recursos y usuarios necesarios. En los a equipos solo se deben habilitar los recursos que requieran y a los usuarios estrictamente necesarios, para no aumentar los riesgos en cuanto a ciberseguridad. Pero esta seguridad debe extenderse una vez culmine la cuarentena.

5 Proteger con aplicaciones de seguridad. Cuando se trabaja desde casa los equipos personales o corporativos deben estar protegidos con aplicaciones de seguridad, que el equipo de informática de cada empresa debe configurar para que la protección sea eficaz.

Delitos cibernéticos

Para empresas que poseen grandes bases de datos de clientes y proveedores, como bancos, **aseguradoras** y prestadores de servicios, es muy importante la protección de esa información, ya que puede ser

Área de seguridad informática de Seguros Venezuela se activó para resguardar actividad del teletrabajo, y así minimizar riesgos de delitos informáticos a que están expuestas las empresas que forman parte del sistema financiero

sustraída por ciberdelincuentes para cometer fraude.

El gerente de Soporte y Capacitación de ESET explica que de los ciberataques se derivan delitos como la extorsión, que ocurre cuando el atacante pide un "rescate monetario" por la información sustraída; el "**phishing**" que es el envío de correos maliciosos para tratar de engañar a usuarios y que estos descarguen malware para robar datos y producir daños.

Protección en el sector financiero

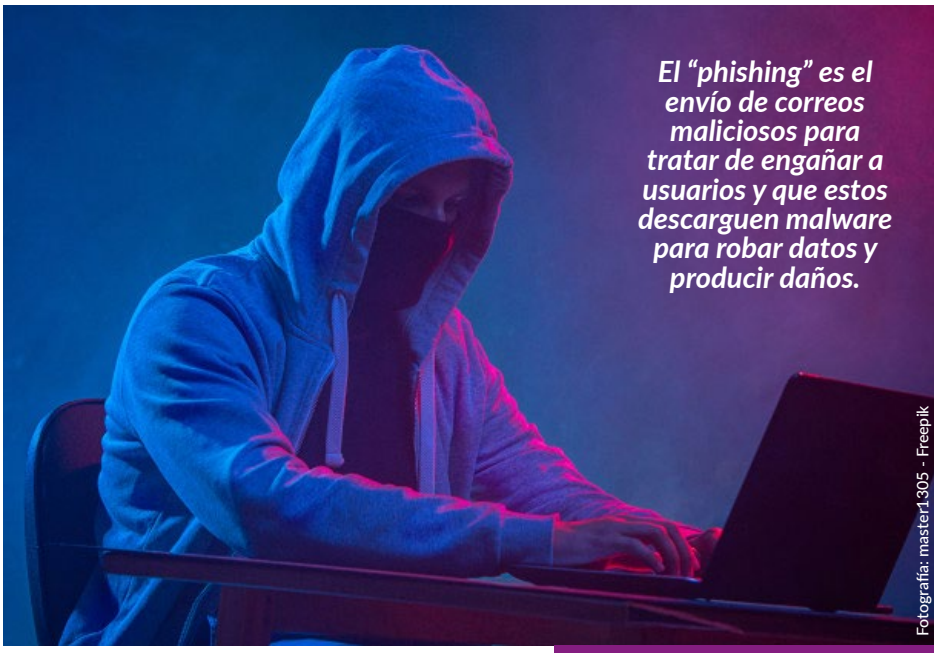
Un área extremadamente sensible en cuanto a la necesidad de proteger la data es el relacionado al de las aseguradoras. En tal sentido se consultó a la Oficial de Cumplimiento de **Seguros Venezuela** (SV), Marisol Pernía, para conocer la situación en la empresa al respecto.

"El teletrabajo surgió como una necesidad imperiosa de mantener la calidad de servicio a nuestros asegurados, intermediarios de seguros y proveedores de servicios de salud, durante y post COVID-19. Se designaron grupos de trabajo a distancia en diferentes áreas, con la finalidad de mantener la operatividad de la compañía. Para ello, se revisaron los protocolos de infraestructura de servicios y sistemas, y se asignaron los perfiles y recursos necesarios para tal fin", informó Pernía.

La funcionaria destacó la importancia del apoyo del área de seguridad informática para el resguardo de toda la actividad durante el teletrabajo, "lo cual permite minimizar los riesgos de delitos informáticos a que están expuestas las empresas que forman parte del sistema financiero, en estos tiempos en los que la disrupción de la información por teletrabajo, seminarios y reuniones web, redes sociales, son focos de riesgos de que sean utilizadas para cometer **delitos con fines económicos**".

Al respecto, en el marco legal venezolano, algunos de estos delitos están tipificados en la Ley Especial Contra Delitos Informáticos (G.O. No. 37.313 de fecha 30/10/2001), tales comoDelitos Contra los Sistemas que Utilizan Tecnologías de Información, acceso indebido, sabotaje o daño a sistemas, espionaje informático, falsificación de documentos, entre otros.

Pernía aseveró que las medidas de seguridad informática forman parte de las responsabilidades de los empleados de SV, en el buen uso de los recursos asignados, la política de confidencialidad de la información, documentos, la propiedad intelectual de los productos y servicios, con la finalidad de evitar los riesgos de delitos informáticos.



De los ciberataques se derivan delitos como la extorsión, que ocurre cuando el atacante pide un "rescate monetario" por la información sustraída.
Carlos López
Gerente de Soporte y Capacitación de ESET en Venezuela

Etiquetas: #teletrabajo #ciberseguridad

Editor: Comité de Prevención Laboral de Consumo de Drogas / Fondo Nacional Antidrogas (FONA) / Fundación Interamericana para el Desarrollo de la Gestión Social FIGSOCIAL.

Investigación: Comité de Prevención Laboral de Consumo de Drogas / Comstat Rowland Comunicaciones Estratégicas, C.A.

Diseño y diagramación: Zeca Marketing zecamarketing@gmail.com

Dirección: Av. Francisco de Miranda, Edif. Seguros Venezuela, Pisos 8 y 9. Urb. Campo Alegre, Edo. Miranda, Caracas 1060, Venezuela.
Telf.: (0212) 901.73.22 Fax: (0212) 901.74.00

Contacto: marisol.pernia@segurosvenezuela.com

Directorio telefónico y de contactos antidrogas: Oficina Nacional Antidrogas (ONA) (0212) 957.3400 / Fondo Nacional Antidrogas (FONA) 0212) 857.3477 / FIGSOCIAL (0212) 731.1980 / Fundación Humana 0212-284.6015 / Fundación José Félix Rivas (0212) 861.8710 / 76