Servicios Postales Nacionales S.A.
Diagonal 25G Nº 95A - 55, Bogotá · Línea Bogotá: (57-1) 472 2000
Nacional: 01 8000 111 210 · Código Postal: 110911 · www.4-72.com.co

Oficina de Seguridad de la Información y Ciberseguridad
Gerencia de Riesgos y Cumplimiento

Circular No. 011

PARA: TODO EL PERSONAL DIRECTO Y MISIONAL

DE: PRESIDENCIA

ASUNTO: REGLAS Y/O REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PARA EL **"TRABAJO DESDE CASA"**

FECHA: 17 DE MARZO DE 2020

Contexto:

Teniendo en cuenta la Directiva Presidencial No. 02 de 2020 y las circulares 007, 008 y 010 de 2020 comunicada por la Presidencia de Servicios Postales Nacionales S.A., frente a las recomendaciones y medidas preventivas a nivel de salud, de ciberseguridad y de tecnología para prevenir el contagio del Coronavirus (COVID-19) y así habilitar la modalidad del trabajo desde casa, debemos advertirle que hay reglas de seguridad de la información, ciberseguridad y seguridad informática que se deben cumplir e implementar para evitar poner en riesgo la información personal de los empleados y de la entidad Servicios Postales Nacionales S.A., ya que trabajar desde casa implica que sus datos no están protegidos de la misma forma que sucede cuando se encuentra en las instalaciones de la entidad.

Por lo anterior, los empleados y funcionarios que trabajarán desde su casa deben cumplir con las siguientes reglas y/o requisitos de seguridad de la información y ciberseguridad para minimizar el riesgo de la pérdida de confidencialidad, integridad y disponibilidad de la información.

Reglas y/o Requisitos:

1. Asegurar las redes (inalámbricas o por cable) a las que se conecta en sus equipos de tecnología: Navegar en una red de wifi pública desde un parque o una cafetería puede ser un riesgo para su información privada, desde sus cuentas en el banco hasta las fotografías que envía a sus amigos. En este sentido, le resultará útil una Red Privada Virtual (VPN por sus siglas en inglés), que crea una red privada partiendo de una red pública.

   Esto se traduce en que sus actividades a través de la internet serán encriptadas y su información personal o la de su empresa no serán vulnerables para que cualquiera pueda interceptarlas.

2. Mantener sus dispositivos y equipos tecnológicos actualizados: Las ventanillas y los avisos de actualizaciones en sus equipos tecnológicos a veces pueden ser molestas. Y aún más cuando está en medio de algo importante desde su ordenador. En esos casos, aunque es válido dar clic en la opción de "Recordar más tarde", no es lo mejor. Posponer la actualización de sus aplicaciones puede jugarle una mala pasada.

   Es importante hacerlo inmediatamente, como una forma de prevenir ataques informáticos y cibernéticos en sus dispositivos. Las actualizaciones se encargan de corregir errores en sus dispositivos, agregar nuevas características y, entre otras cosas, arreglar esos huecos y debilidades en la seguridad informática que los hackers suelen aprovechar.

3. Tomar las medidas necesarias en caso de Robos o Perdidas: Estas situaciones pueden poner en riesgo su información y la de la empresa. Para empezar, debe denunciar el robo ante las autoridades policiales y a las siguientes instancias de SPN 4-72: Oficina de Seguridad de la Información y Ciberseguridad de la Gerencia de Riesgos y Cumplimiento al correo (ronald.cely@4-72.com.co) y al Jefe directo del área; ya que esto aumenta las posibilidades de que recupere lo perdido. Informe también, a su familia, a sus amigos sobre la pérdida.

   Siempre que pueda hacerlo, trate de rastrear el dispositivo a través de las opciones que las diferentes marcas ofrecen. Esta información de seguimiento también es vital para la policía. En caso de que el ladrón burle el sistema de bloqueo del dispositivo, usted debe entrar a los sitios web de las aplicaciones que usa, para cerras las sesiones y cambiar las contraseñas.

   Finalmente, si el dispositivo es irrecuperable, desactívelo. Aunque perderá contacto con él, evitará que el ladrón pueda acceder a sus cuentas o reutilizarlo.

4. Resguardar la Información que trabajara para la entidad SPN 4-72 en la Nube Corporativa (Microsoft OneDrive de Office 365): Algunas empresas prefieren que los documentos y archivos de trabajo sean almacenados en una nube y no en el equipo de trabajo. De igual forma deben tomarse medidas de seguridad informática para que la información ahí almacenada permanezca segura.

   Podemos empezar por utilizar contraseñas seguras intercalando letras mayúsculas, minúsculas y números. Otra opción es activar una verificación, para que cada vez que quiera acceder a la nube, sea enviado a su correo electrónico una notificación de que se accedió a la nube asignada.

5. Debe asegurarse contra Virus, Malware y Amenazas Cibernéticas Potentes: Cuando realizan trabajo desde casa, no se libra de los ataques cibernéticos que amenazan contra la confidencialidad, integridad y disponibilidad de la información, la cual es el activo más valioso y privilegiado de la entidad.

   Los malware como Viro Botnet y los ransomware Wannacry; así como los troyanos, podrían causarle estragos en su trabajo por la pérdida de información y otras tantas consecuencias nefastas.

   Para la protección básica contra estas amenazas, se debe contar con un antivirus activo y actualizado en sus equipos tecnológicos capaz de realizar análisis profundos a la

información y los sistemas que maneja, lo que facilita la detección, contención y eliminación de Virus y Malware conocidos y desconocidos.

Nota: Para cualquier apoyo requerido con base a las reglas de seguridad de la información y ciberseguridad para trabajo desde casa, requeridas por Servicios Postales Nacionales S.A., se puede contactar con la mesa de servicios de la Direccion Nacional IT y/o Oficina de Seguridad de la Información y Ciberseguridad.

Atentamente;

LUIS HUMBERTO JIMENEZ MORERA
Presidente
Servicios Postales Nacionales S.A

Proyectó, Revisó y Aprobó: Ing. Ronald Mauricio Cely Espitia – Gerente Oficial de Seguridad de la Información
Revisó y Aprobó: Orlando Bolivar Luna - Gerente de Riesgos y Cumplimiento
Revisó: Ing. Edgar Prieto – Director Dirección Nacional de IT
Aprobó: Isabel Cristina Vargas – Jefe Oficina Asesora Jurídica