POLÍTICA DE PRIVACIDAD

1. INTRODUCCIÓN

Esta política tiene como finalidad establecer normas para el uso correcto de la información que se ingresa, procesa, transmite, transporta y almacena en el **Grupo Empresarial Nitrofert**, incluyendo los archivos de los usuarios, así como el uso de los servicios de correo electrónico, las bases de datos manejadas, así como el registro y monitorización de actividades por parte de colaboradores y/o contratistas que hagan uso de la información corporativa. Se alinea con la Ley Estatutaria 1581 de 2012 y los decretos reglamentarios 1377 de 2013 y 886 de 2014 sobre la protección de datos personales.

2. ALCANCE

La Política de Privacidad aplica a todo el equipo humano vinculado a cada una de las Compañías que conforman el Grupo Empresarial Nitrofert (Nitrofert, Nitrocaribe, Intefert), y a todas las partes relacionadas y grupos de interés, entendidos éstos como clientes, proveedores, distribuidores, contratistas, accionistas, inversionistas y en general a todos aquellos con quienes directa o indirectamente se establezca alguna relación comercial, contractual o de cooperación.

3. RESPONSABLES

La Gerencia de TI en apoyo con la gerencia de Talento Humano tienen la responsabilidad de implementar esta política, así como el seguimiento, monitoreo, control y mejora de la misma.

4. COMPROMISOS

a. Las credenciales de usuario se utilizarán como base para cargar el respectivo perfil de cada uno de los colaboradores, los cuales serán responsables de la seguridad de sus contraseñas y cuentas, así como del uso indebido de sus credenciales y de los actos cometidos con ellas. Se implementará la autenticación multifactor para el acceso a sistemas críticos.

b. Ningún colaborador o persona que labore en la compañía está autorizado para revelar información a terceros con respecto al direccionamiento de la

red, tecnología empleada en la organización o procedimientos internos. Lo anterior siguiendo las directrices y lineamientos del Reglamento Interno de Trabajo, inciso 27 del artículo 51 e inciso 40 del artículo 53.

c. El uso del correo electrónico corporativo está limitado al servicio de los intereses de la compañía y no para uso personal.

d. Cada vez que un colaborador requiera levantarse de su puesto, oficina o estación de trabajo deberá habilitar el bloqueo de pantalla para evitar intrusiones internas. Y en caso de que sospeche de que está siendo monitoreado o que detecte algún comportamiento sospechoso de su sistema informático o de comunicaciones, comuníquese inmediatamente con el área de TI.

e. En el momento en que un colaborador deje de pertenecer a la compañía, su cuenta y accesos serán puestos en suspensión inmediatamente.

f. Cada usuario es responsable del estado y del uso de sus archivos. Cualquier información que éste considere sensible o vulnerable debe ser asegurada y/o encriptada. Se utilizará cifrado de datos tanto en tránsito como en reposo para proteger la información confidencial.

g. La información que se capture, procese e imprima, o de la cual se genere una salida ya sea por medio físico o electrónico es de propiedad de la compañía y no de los responsables de la misma. Se clarificarán los derechos de los usuarios respecto a su información personal, incluyendo el acceso, rectificación y eliminación de datos.

h. Los colaboradores deben tener extrema cautela al abrir archivos adjuntos a su correo electrónico recibidos de remitentes desconocidos ya que pueden incluir bombas lógicas, troyanos o cualquier tipo de virus.

i. El área de TI se reserva el derecho de intervenir las redes y los sistemas de información periódicamente para asegurar el cumplimiento de esta política. Se realizarán evaluaciones de impacto de privacidad para identificar y mitigar riesgos.

j. Es tarea del área de TI revisar periódicamente el comportamiento de la red y la realización de monitoreo del tráfico de esta y el escaneo de puertos de los sistemas informáticos, con el fin de verificar la existencia del establecimiento de conexiones remotas, la ejecución de procesos peligrosos en background,

ataques tipo spoofing o de las capturas de sesiones que en algún momento puedan violar las políticas de privacidad de la compañía.

5. USO INACEPTABLE

a. Está prohibido el uso de computadoras de terceros dentro de la compañía, que no cuenten con un sistema operativo, paquete de ofimática y antivirus debidamente licenciado, excepto cuando éstas pertenezcan a personal de outsourcing y sea estrictamente necesario su uso.

b. Está prohibido presentar, alojar o transmitir información, imágenes, textos que en forma indirecta o directa se encuentren relacionadas con actividades sexuales y mucho menos con menores de edad.

c. Está prohibido el acceso a personal no autorizado a las dependencias administrativas de la compañía sin acompañamiento.

d. Está prohibido anunciar, enviar, presentar o transmitir contenido de carácter ilegal, atentatorio a la dignidad del ser humano, que tenga la potencialidad de ser peligroso, genere pánico económico, social, de salubridad, o que ponga en cualquier tipo de riesgo a la compañía, etc.

e. Está prohibido vulnerar derechos de propiedad industrial, derechos de autor, o copyright protegidos por las leyes nacionales, extranjeras y acuerdos o tratados internacionales sobre la materia que comprometan a la compañía.

f. Está prohibido enviar correo electrónico basura, Spam indiscriminado, o encadenado no autorizado o consentido previamente por los destinatarios, que en algún momento pueda llegar a generar un atentado contra la disponibilidad de la información o del servicio de correo corporativo.

g. Está prohibido para todos los colaboradores descargar o instalar aplicaciones o programas no autorizados por el área de TI en las estaciones de trabajo.

h. Está prohibido intentar acceder sin autorización a los sitios o servicios de la compañía o de terceros, mediante la utilización de herramientas intrusivas (hacking), descifre de contraseñas, descubrimiento de vulnerabilidades o

cualquier otro medio no permitido o legítimo utilizando la infraestructura tecnológica de la compañía.

i. Está prohibido influir injusta, ilegal o en forma indebida o inadecuada directa o indirectamente en los sistemas, redes, aplicativos, y demás elementos involucrados en la transmisión o recepción de información, incluyendo las terminales o estaciones de trabajo de los usuarios.

j. Está prohibida cualquier forma de asedio ya sea por teléfono, correo electrónico o lenguaje.

k. Está prohibido brindar información personal sobre los clientes de la compañía y de sus actividades por cualquier medio.

6. ENTRADA EN VIGOR

Esta política se expide el 14 de octubre de 2022 y es actualizada el 20 de mayo de 2024, derogando cualquier disposición anterior a ella. Será publicada y difundida a todo el personal, de tal forma que se asegure su conocimiento y participación, en aras del cumplimiento de la misma.