En virtud del fuerte compromiso de **HIGH NUTRITION COMPANY S.A.S.** con el adecuado tratamiento de datos personales, garantizando además de la salvaguarda y seguridad de la información, en ejercicio del Habeas Data, la empresa establece la presenta Política aplicables para la seguridad de la información en la organización.

1. OBJETIVO

La presente Política establece las directrices generales para la Seguridad de la Información al interior de **HIGH NUTRITION COMPANY S.A.S.**, con el objetivo de brindar las condiciones de seguridad necesarias que impidan la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento a la información que es tratada por **HIGH NUTRITION COMPANY S.A.S**.

2. ALCANCE

Esta Política de Seguridad de la Información será aplicada en todos los aspectos administrativos, de gestión, logísticos y de control fijados por la empresa, que deben ser cumplidos por los directivos, funcionarios, contratistas, terceros que presten sus servicios, empleados de terceros proveedores que estén regulados por términos contractuales, y en general todas aquellas personas que tengan algún tipo de relación con la manipulación de información en **HIGH NUTRITION COMPANY S.A.S.**

3. POLÍTICAS ESPECÍFICAS PARA EL TRATAMIENTO DE DATOS PERSONALES.

3.1 INSTALACIÓN DE SOFTWARE

Propósito: Minimizar el riesgo de exposición y de infección por malware, evitando a su vez posibles sanciones por el uso de software sin licenciar.

Política

Los trabajadores no deben instalar software en los dispositivos de la compañía sin la respectiva autorización. Las peticiones de instalación de software deben ser

aprobadas por la Gerencia de Operaciones y el proceso de instalación debe ser realizado por el área de sistemas.

Todo software que sea instalado debe tener licenciamiento comercial o en su defecto la licencia debe provenir del área de sistemas. En caso de que se requiera la instalación de un software (open source, free o trial), se debe recurrir al área de sistemas quien junto con la Gerencia de Operaciones tomaría la decisión que corresponda.

3.2 USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

Propósito: Minimizar el riesgo de exposición de información de la empresa o de infección por malware contenido en dispositivos externos de almacenamiento (Discos Duros externos, USBs, CDs, Diskettes, Teléfonos Celulares, Reproductores Multimedia, etc).

Política

Está prohibido el uso de dispositivos de almacenamiento personales dentro de la infraestructura tecnológica de **HIGH NUTRITION COMPANY S.A.S.** En caso de requerirse un medio extraíble, se debe solicitar apoyo al área de sistemas, quien hará el manejo con un dispositivo corporativo.

Una vez se termine de realizar la labor requerida con el dispositivo se eliminará toda la información contenida en el mismo y realizará una limpieza con un software de antivirus.

3.3 USO DEL INTERNET EMPRESARIAL Y POLÍTICA DE MONITOREO

Propósito: El propósito de esta política es definir los estándares para el monitoreo y limitación de la navegación por Internet desde cualquier dispositivo en la red empresarial. Estos estándares están diseñados para asegurar que los empleados utilicen el Internet de forma segura y responsable.

Política

La Gerencia de Operaciones está en potestad de monitorear todas las comunicaciones entrantes y salientes dentro de la red de la organización. Esto incluye conocer la IP de origen, la fecha, la hora, el protocolo, el servidor o dirección de destino y los datos comunicados.

La Gerencia de Operaciones puede bloquear los sitios de Internet que se consideren inapropiados para el ambiente empresarial. Se considera una falta disciplinaria bajo cualquier circunstancia el acceso a páginas y sitios web de contenido sexual explícito o pornografía, sitios de juegos, apuestas o de deportes, sitios relacionados con sustancias ilícitas, sitios de citas, redes sociales (Whatsapp, Facebook, Instagram, Twitter, entre otros), sitios de fraude, contenidos SPAM o en relación a delitos tipificados por la ley colombiana, contenido racista o de alguna forma ofensivo y discriminatorio, contenido violento, emisoras, sitios dedicados a compartir videos y todo contenido que no esté relacionado con el desarrollo de las finalidades de la empresa, sin que medie previa autorización de la Gerencia de Operaciones .

Así mismo está totalmente prohibido el uso de la infraestructura empresarial para realizar ataques informáticos o similares. Además, está prohibido el uso del Internet en horas no autorizadas para acceder a contenido multimedia no asociado a la labor del empleado.
Cualquier intento por evadir los controles técnicos impuestos, será considerado en sí mismo una falta disciplinaria.

3.4 MANEJO DE CLAVES

Propósito: El propósito de esta política es establecer un estándar de generación de contraseñas seguras, la protección de dichas contraseñas y su frecuencia de cambio.

Política
Todas las contraseñas de nivel de sistema (root, administrador, usuarios de Windows, bases de datos, etc.), deben ser cambiadas al menos cada tres (03) meses.

Todas las contraseñas de nivel de usuario (correo, cuentas personales), deben ser cambiadas al menos cada seis (06) meses.

Todas las contraseñas utilizadas deben seguir las condiciones descritas a continuación: Contener al menos tres de los siguientes caracteres: Minúsculas, Mayúsculas, Números, Caracteres especiales (e.g. #$%&/(“!.;), la longitud de la contraseña debe ser de al menos ocho (08) caracteres, la contraseña no debe estar compuesta únicamente de palabras de diccionario ni de nombres de

familiares; se deben evitar contraseñas tradicionales como: password, 123456, qwerty, asdfg, etc.

Como base del adecuado manejo de claves y contraseñas se presentan una serie de recomendaciones para el manejo correcto de las mismas:

- Siempre utilice contraseñas diferentes para los servicios de la compañía y sus cuentas personales no relacionadas al ámbito laboral.
- No comparta sus contraseñas con ningún tercero, incluso si este pertenece a la organización.
- Las contraseñas nunca deben estar escritas en texto plano o block de notas (jamás archivos llamados claves.txt y en el escritorio).
- No revele las contraseñas por medios de comunicación desprotegidos como correo, mensajería instantánea, SMS, etc.
- Evite utilizar la opción de recordar o guardar contraseña en navegadores y programas internos.

3.5 USO DE CORREO ELECTRÓNICO Y COMUNICACIONES PERSONALES

Propósito: Prevenir daños y perjuicios en la imagen o el nombre de la organización por el manejo incorrecto de los servicios de comunicación, debido a la contaminación con listas negras.

Política

Los diferentes medios de comunicación disponibles para los trabajadores, no deben ser utilizados para la distribución de mensajes con contenido ofensivo, racista, discriminatorio, pornográfico, sexual, político u otros que atenten contra la normal convivencia. Los empleados que reciban comunicaciones con este contenido deben eliminarlo inmediatamente y reportar el incidente, a la Gerencia de Operaciones, si es de origen interno.

Utilizar los correos empresariales para comunicaciones personales está prohibido; en especial si es para la distribución de mensajes cadenas, spam o de alguna forma comerciales.
Los empleados no deben esperar privacidad alguna en contenido que almacenen o envíen como parte de los servicios de comunicación de la compañía. El no cumplimiento de las condiciones mencionadas anteriormente es considerado una falta disciplinaria y puede ser objeto de sanción.

3.6 CONFIDENCIALIDAD CON TERCEROS

Propósito: Establecer los requerimientos de confidencialidad en las relaciones con clientes, proveedores, contratistas; en particular con empleados y los terceros en general.

Política

Para el desarrollo de las relaciones contractuales, comerciales y laborales, se debe exigir a los terceros la aceptación de los acuerdos de confidencialidad definidos por la organización. En dichos acuerdos se establece el compromiso de salvaguardar la información, velar por su correcto uso, impedir el uso no autorizado de dicha información y guardar reserva. Se estipula, a su vez, la información que es objeto de protección dentro del acuerdo y su temporalidad.

Los acuerdos deben incluirse dentro de los contratos celebrados entre la organización y terceros, como parte integral del contrato o firmarse como un acuerdo independiente.
La aceptación de las condiciones de confidencialidad es indispensable para conceder al tercero el acceso a la información protegida.

3.7 LA SEGURIDAD FÍSICA Y AMBIENTAL

Propósito: Evitar el acceso físico no autorizado, evitar daños e interferencia para la información de la organización y las instalaciones de procesamiento de información.

Política

Los equipos de cómputo deben estar situados y protegidos para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado. El equipo deberá estar protegido contra fallas de energía y otras interrupciones causadas por fallas en el soporte de los servicios públicos. El cableado que transporta datos, energía y telecomunicaciones o el soporte de los servicios de información debe estar protegido contra la intercepción, interferencia o daños. Los equipos de cómputo deben tener un correcto mantenimiento para asegurar su continua disponibilidad e integridad.

Los equipos, la información o el software no podrán ser retirados de las instalaciones de la empresa sin la previa autorización. Se aplicará seguridad a los

activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

Los usuarios deben estar atentos, con los avisos emergentes en los equipos, de que el equipo cuenta con la protección adecuada.
Los usuarios que se retiren momentáneamente de su puesto de trabajo deberán bloquear o suspender de manera inmediata sus equipos de cómputo.

Los puestos de trabajo deben estar limpios de papeles, comidas y bebidas; y cuando un computador este desatendido deberá bloquearse la pantalla.

Cuando sea necesario, los documentos y cualquier medio de información deben estar asegurados (bajo llave) en archivadores apropiados, especialmente en horas fuera de las normales de trabajo.

3.8 REQUISITOS PARA EL CONTROL DE ACCESO

Propósito: Limitar el acceso de la información y a las instalaciones de procesamiento de la información.

Política

Los cargos responsables de las áreas seguras de la empresa tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- El área de almacenamiento se cataloga como segura y debe permanecer cerrada y custodiada.
- El acceso a áreas seguras donde se procesa o almacena información confidencial y restringida, es limitado únicamente a personas autorizadas.
- El acceso a áreas seguras requieren esquemas de control de acceso, como tarjetas, llaves o candados.
- El responsable de un área segura reservará el derecho que la empresa tiene para el ingreso de cámaras fotográficas, videos, teléfonos móviles con cámaras, salvo se tenga una autorización expresa.
- Se utilizan planillas y/o registros electrónicos para registrar la entrada y salida del personal.
- Se restringe el acceso físico a dispositivos como: puntos de acceso inalámbricos, puertas de enlace a redes y terminales de red que estén ubicadas en las áreas seguras.

3.9 COPIAS DE SEGURIDAD

Propósito: Evitar la pérdida de información de la empresa.

Política

Las copias de seguridad de la base de datos del software ERP de la empresa se toman de forma automática dos (02) veces al día todos los días en los siguientes horarios: 6:00 p.m. y 12:00 p.m., las cuales se almacenarán en un disco duro externo a las 9:00 p.m. y serán custodiadas por **HIGH NUTRITION COMPANY S.A.S**.

Las copias de seguridad de los repositorios de la empresa se toman de forma automática todos los días a las 9:00 p.m. se encuentran alojadas en el NAS fuera de las instalaciones de la empresa pero bajo custodiada de **HIGH NUTRITION COMPANY S.A.S**.

Los funcionarios responsables de la gestión del almacenamiento y respaldo de la información proveen los recursos necesarios para garantizar el correcto tratamiento de la misma.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos tienen definidas las estrategias para la correcta y adecuada generación, retención, y rotación de las copias de respaldo de la información.
Los dueños o responsables de los activos de información tecnológicos y recursos informáticos velan por el cumplimiento de los procedimientos de respaldo de la información.

3.10 REGISTRO DE ACTIVIDAD Y SUPERVISIÓN

Propósito: Registrar eventos y generar evidencia.

Política

Se harán revisiones regulares y cuidadosas a los registros de eventos que se graban de las actividades de los usuarios, excepciones, fallas y eventos de seguridad de la información.

Los registros de información se protegerán contra la manipulación y el acceso no autorizado. Las actividades del administrador del sistema y de la red serán registradas.

Estos registros serán protegidos y regularmente revisados.

Los relojes de todos los sistemas de informática relevantes serán sincronizados a una fuente de tiempo de referencia única.

3.11 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN

Propósito: Garantizar que la seguridad informática sea implementada y aplicada de acuerdo con las políticas y procedimientos de la organización.

Política

Los sistemas de información son revisados regularmente a través de Auditorias para cerciorarse que se da cumplimiento a las políticas y normas de seguridad de la información de la empresa.

4 PROCESO PARA LA ATENCIÓN DE INCIDENTES

Toda vez que se presente algún incidente con la seguridad de la información tratada por **HIGH NUTRITION COMPANY S.A.S.**, deberá adelantarse el siguiente procedimiento:

1). **Reporte del Incidente:** Ocurrido el incidente de seguridad, la primera persona que tenga conocimiento del mismo y en el menor tiempo posible, deberá presentar un informe del mismo, el cual automáticamente se dirige al área de sistemas.

2). **Comunicación del Incidente ante la SIC:** Todo incidente de seguridad de la información, deberá ser reportado ante la Superintendencia de Industria y Comercio, específicamente ante el Registro Nacional de Bases de Datos -RNBD-.

3). **Reunión del comité de Seguridad de la información:** El área de Sistemas activará el equipo de trabajo de HIGH NUTRITION COMPANY S.A.S. (Gerencia de Operaciones, Dirección Financiera y Contable, Analista de Sistemas y otro(s) cargo(s) que la Gerencia de Operaciones considere de acuerdo al incidente), para reunirse de manera extraordinaria y desarrollar los siguientes ítems.

a. **Emisión del concepto técnico:** Evaluados los Hechos del caso se deberá dar un concepto técnico que determina todas las contingencias surgidas en el caso en concreto.
b. **Identificación de la falencia:** Como resultado del concepto técnico, se deberá identificar plenamente la falencia que dio pasó al incidente de seguridad de la información.
c. **Toma de medidas:** El comité deberá tomar las medias y los correctivos necesarios para evitar futuros incidentes.

5 MODIFICACIÓN DE LAS POLÍTICAS

HIGH NUTRITION COMPANY S.A.S. se reserva el derecho de modificar la presente Política de Seguridad de la información en cualquier momento, comunicando de forma oportuna a todas aquellas personas que estén relacionadas o que participen en la manipulación de la información de la empresa para su correcta implementación.

6 VIGENCIA

La presente Política rige a partir del día veintiuno (21) del mes de febrero del año dos mil veintitrés (2023)

Mario Alexander Villalobos Pinilla
Representante Legal