1. Objetivo

GNS se compromete a proteger la privacidad de los Datos empresariales y personales de sus Trabajadores, Clientes, Socios Comerciales y demás personas identificables. Por lo tanto, GNS ha implementado un programa de protección de datos a fin de establecer y mantener altos estándares para la recopilación, uso, divulgación, almacenamiento, seguridad, acceso, transferencia o cualquier otro tipo de procesamiento de Datos. La presente Política de Protección de Datos constituye la base de dicho programa y describe el enfoque adoptado por GNS en el tratamiento de Datos.

2. ALCANCE

Todos los empleados, contratistas, consultores, temporales y demás trabajadores de GNS y sus subsidiarias deben cumplir con esta política, incluido todo el personal afiliado a terceros que pueda tener acceso a cualquier recurso aplicable de GNS, incluidos los servicios basados en la nube, alojados dentro o fuera de GNS.

La presente Política de Protección de Datos se aplica al tratamiento de Datos por parte de GNS, ya sea por medios electrónicos o manuales (es decir, en formato impreso, papel o analógico). Todas las entidades y trabajadores de GNS deberán cumplir esta Política de Protección de Datos.

La presente Política se aplica a todos los Datos que se creen, recopilen, procesen, utilicen, compartan o destruyan por o para GNS.

3. DEFINICIONES

Derechos ARCO: Acceso, Rectificación, Cancelación y Oposición.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de Datos Personales**.**

Aviso de Privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus Datos Personales, donde se informa de la existencia de las Políticas aplicables, forma de acceso y finalidades del Tratamiento.

Dato Personal o Semi Privado: Cualquier información que identifique directa o indirectamente a un individuo, como nombre, correo, teléfono, fecha de nacimiento, otro.

Dato sensible o Privado: Información que afecta la intimidad del Titular. Revela origen racial o étnico, orientación política, religiosa o filosófica, pertenencia a organizaciones, vida sexual, información biométrica.

Encargado: Persona natural o jurídica que trata Datos Personales por cuenta del responsable**.**

Información estructurada: Datos que se han organizado y formateado de manera que sean fácilmente legibles y accesibles.

Información no estructurada: Datos que no están organizados de una manera predefinida o no siguen un formato específico, lo que hace más difícil su análisis y procesamiento

PIA: Evaluación de Impacto de la Protección de Datos. ayuda a identificar y minimizar riesgos de privacidad en el procesamiento de datos.

Responsable: Persona física o jurídica, autoridad, servicio u otro organismo que decide sobre la base de datos y/o el tratamiento de datos.

SGSI: Sistema de Gestión de Seguridad de la Información.

Titular: Persona a la que se refieren los datos a recopilar y procesar. Cuenta con derechos en relación con sus datos personales, incluyendo los ARCO.

Transferencia: Envío de información a un responsable del Tratamiento, que se encuentra dentro o fuera del país.

Transmisión: Envío de información a un Encargado del Tratamiento, que se encuentra dentro o fuera del país.

Tratamiento: Recolección, almacenamiento, uso, circulación o supresión de Datos.

4. DECLARACIÓN DE LA POLÍTICA

Esta política rige la protección de Datos en GNS y tiene alcance a todos los países donde se prestan los servicios por parte de la organización.

4.1. Garantías Adecuadas para el Tratamiento de Datos

La presente Política de Protección de Datos tiene por objeto proporcionar garantías adecuadas para el tratamiento de los Datos confiados a GNS y transferidos desde países que exigen tales protecciones. De este modo, GNS podrá transferir los Datos a cualquier lugar del mundo en que sean necesarios para posibilitar y respaldar sus procesos comerciales internos o habilitar la funcionalidad de servicios y productos.

4.2. Cumplimiento de la Legislación Aplicable

GNS cumplirá las leyes y requisitos locales de protección de datos aplicables en todos los países peros sin limitarse a donde se prestan los servicios:

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México)
- Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Ley N.º 8968 Costa Rica).
- Ley de Protección de Datos Personales (Decreto N.º 144 El Salvador).
- Ley Nº 81 de 2019 sobre Protección de Datos Personales y el Decreto Ejecutivo N.º 285 de 2021 (Panamá).
- Leyes Federales Sectoriales HIPAA, GLBA, COPPA (Estados Unidos)
- Ley de Transparencia y Acceso a la Información Pública (incluye aspectos de protección de datos personales y Hábeas Data)
- Ley Estatutaria 1581 de 2012 (Colombia)

Cuando la legislación aplicable en materia de protección de datos establezca un nivel de protección de los Datos Personales superior al establecido en la presente Política de Protección de Datos, prevalecerán los requisitos de la legislación aplicable en materia de protección de datos. Cuando la legislación aplicable en materia de protección de datos establezca un nivel de protección de los Datos Personales inferior al establecido en la presente Política de Protección de Datos, prevalecerán los requisitos de la presente Política.

Cuando los Trabajadores de GNS tengan motivos para creer que la legislación aplicable impide a GNS cumplir con sus obligaciones en virtud de la presente Política de Protección de Datos, informarán inmediatamente a la VicePresidencia de atención al cliente, y/o al Departamento administrativo de GNS – protecciondedatospersonales@gns-latam.com. En caso de conflicto entre la legislación aplicable y la presente Política de Protección de Datos, el Departamento Jurídico de GNS tomarán una decisión responsable sobre las medidas a adoptar para resolver dicho conflicto y consultarán a la autoridad reguladora pertinente en caso de duda.

4.3. Principios de Privacidad

A continuación, se exponen los principios de alto nivel en los que se basan las prácticas de GNS a la hora de recopilar, utilizar, divulgar, almacenar, proteger, acceder, transferir o procesar de cualquier otro modo los Datos.

Equidad

GNS tratará los Datos Personales de forma lícita, justa y transparente.

Limitación de la finalidad

GNS sólo recopilará Datos Personales para un fin o fines específicos, explícitos y legítimos. Todo tratamiento posterior deberá ser compatible con dicha(s) finalidad(es), a menos que GNS haya obtenido el consentimiento de la persona o que el tratamiento esté permitido por la ley.

Proporcionalidad

GNS sólo tratará los Datos Personales que sean adecuados, pertinentes y no excesivos para la finalidad o finalidades para las que se recopilaron.

Integridad de los datos

GNS mantendrá los Datos Personales exactos, completos y actualizados en la medida en que sea razonablemente necesario para los fines para los que se tratan.

Conservación de datos

GNS conservará los Datos Personales en un formato que permita su identificación personal durante un plazo no superior al necesario para cumplir con la finalidad, u

otras finalidades permitidas, para las que se obtuvieron los Datos Personales. Los datos personales tratados para cualquier fin no se conservarán más tiempo del necesario para dicho fin. Existe una excepción para los datos de investigación.

Seguridad de los datos

GNS implementará las medidas técnicas y organizativas apropiadas y razonables para salvaguardar los Datos Personales contra la destrucción accidental o ilícita o la pérdida accidental, la alteración, la divulgación, el uso o el acceso no autorizados. GNS instruirá y exigirá contractualmente a los terceros que procesen Datos Personales por cuenta de GNS, si los hubiere, que: (a) los procesen únicamente con fines compatibles con los propósitos de GNS para el procesamiento; y (b) implementen las medidas técnicas y organizativas adecuadas para salvaguardar los Datos Personales.

Derechos de las personas

GNS procesará los Datos Personales de manera tal que se respeten los derechos de las personas en virtud de la legislación aplicable en materia de protección de datos.

Responsabilidad

GNS implementará las políticas, procesos, controles y demás medidas necesarias para poder demostrar que el tratamiento de los Datos Personales se realiza de conformidad con la presente Política de Protección de Datos y con la legislación aplicable en materia de protección de datos.

4.4. Declaración General

4.4.1. Todos los ordenadores y portátiles deben bloquear su pantalla cuando no estén en uso para minimizar la pérdida o divulgación accidental de información. El personal debe ser consciente de que si no cierra la sesión y deja sus ordenadores/portátiles desatendidos puede ser considerado responsable de las actividades de otro usuario en su terminal y estar infringiendo esta política, la política de Protección de Datos y/o el requisito de confidencialidad con respecto a cierta información.

4.4.2. Todo el personal debe facilitar información exacta y actualizada sobre su empleo y mantener informada a la empresa de cualquier cambio en la

información que haya facilitado (cambio de dirección, número de teléfono de contacto, etc.)

4.4.3. Todos los datos personales se guardan en un armario o cajón cerrado con llave y, si son electrónicos, están protegidos por contraseña y se realizan copias de seguridad periódicas.

4.4.4. No se permite almacenar datos confidenciales o restringidos en un pen drive o en el disco duro local de los ordenadores portátiles de los empleados.

4.4.5. La información personal no debe divulgarse ni oralmente ni por escrito ni a través de páginas web ni por ningún otro medio, accidentalmente o no, a terceros no autorizados. Los documentos impresos sensibles y personales no deben dejarse en las impresoras ni en zonas públicas.

4.4.6. La información personal enviada a terceros autorizados debe enviarse utilizando la herramienta de cifrado aprobada por la VicePresidencia de atención al cliente.

4.4.7. El personal debe estar atento cuando acceda a información confidencial o restringida en pantalla para asegurarse de que nadie más, que pueda no estar autorizado, pueda leer la información.

4.4.8. El personal está obligado a utilizar un nombre de usuario seguro para acceder a la red y a los datos de la empresa y no se le permite instalar ningún software en los ordenadores / portátiles.

4.4.9. Se establece la prohibición del tratamiento de Datos Sensibles, salvo por las excepciones legales o con autorización expresa e informada del Titular, y la obligación de aplicar altos estándares de seguridad y confidencialidad, incluyendo la advertencia al titular de que no está obligado a autorizar su tratamiento.

4.4.10. Se establece la directriz para el tratamiento de Datos de Menores de Edad, asegurando el respeto de sus derechos fundamentales, el interés superior y la obtención de la autorización del representante legal (incluyendo el derecho del menor a ser escuchado).

4.5. Derechos de los titulares

Las personas naturales cuyos Datos Personales sean objeto de Tratamiento por parte de GNS, tienen los siguientes derechos, los cuales pueden ejercer en cualquier momento:

- Conocer los Datos Personales sobre los cuales GNS está realizando el Tratamiento.
- Solicitar, que sus datos sean actualizados, rectificados, suprimidos o cancelados.
- Solicitar prueba de la autorización otorgada para el Tratamiento de sus Datos Personales.
- Ser informado sobre el uso que se le da a sus Datos Personales.
- Presentar quejas por infracciones de la Ley de Protección de Datos Personales.
- Solicitar la supresión de sus Datos Personales y/o revocar la autorización otorgada para el Tratamiento. a solicitud de supresión no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la Base de Datos y/o Archivos, ni mientras se encuentre vigente la relación, en virtud de la cual fueron recolectados sus datos.
- Acceder de forma gratuita a sus Datos Personales, que hayan sido objeto de Tratamiento.
- Los derechos de los Titulares podrán ejercerse por el Titular, Causahabientes acreditados, Representante o apoderado.

Para ejercer estos derechos o cualquier otro que la ley establezca, la persona deberá presentar una solicitud en ejercicio y/o defensa de sus derechos. Dicha Solicitud podrá ser presentada a las direcciones de cada filial regional, o contactarse por medio escrito con las oficinas de Recursos Humanos de la organización. Se podrán establecer otros canales para tramitar estas solicitudes, lo que será informado oportunamente por GNS.

A fin de ejercer los derechos, la persona deberá presentar mencionada solicitud, incluyendo:

I. Nombres y apellidos del titular del derecho y acreditación y en su caso de su representante.
II. Petición concreta.
III. Domicilio o dirección electrónica, para efectos de notificación.
IV. Fecha y firma del solicitante.
V. Documentos que sustenten la petición.
VI. GNS se compromete a atender y dar respuesta a la solicitud en los plazos establecidos por las leyes respectivas.

4.6. Consentimiento

Los Mecanismos de Autorización (Consentimiento) por parte de GNS, incluyen, pero no se limitan formato diligenciado de consentimiento informado, conversación telefónica/videoconferencia y conductas inequívocas, dejando claro que el silencio no se asimila a autorización.

4.7. Cifrado de Datos

4.7.1. Las implementaciones de cifrado deben cumplir lo descrito en el manual de políticas de seguridad de la información. Se prohíbe el uso de algoritmos de cifrados propietarios.
4.7.2. Las implementaciones de cifrado deben garantizar la autenticación de los pares antes de intercambiar las claves de sesión. Se requiere un cifrado autenticado.
4.7.3. Las claves compartidas con anterioridad para la autenticación basadas en una contraseña deben ser únicas y cumplir el procedimiento de Contraseñas (SI-PRO-003).
4.7.4. Los datos personales entran en las categorías de información confidencial, restringido o secreto.

4.8. Almacenamiento Electrónico de Datos

4.8.1. Los datos con clasificación confidencial o restringido solo deben almacenarse en la red empresarial en premisa o en nube y no en unidades locales para poder realizar copias de seguridad.

4.9. Traslado y Resguardo Temporal de Datos

4.9.1. No debe trasladarse fuera de las instalaciones o infraestructura tecnológica de GNS información con clasificación confidencial o restringida sin el permiso previo del Vicepresidente responsable y sólo debe hacerlo si está convencido de que se han tomado las medidas técnicas adecuadas para mantener la seguridad y confidencialidad de dicha información.

4.9.2. Antes de trasladar información fuera de las instalaciones de GNS, el líder/jefe/gerente responsable de área deberá crear y firmar una evaluación del impacto sobre la privacidad.

4.9.3. Si el traslado de datos es aprobado, se debe asegurar:

4.9.3.1. La información se guarda en un lugar seguro y bajo llave al que no pueden acceder personal autorizado.

4.9.3.2. Todo el material confidencial que deba eliminarse se tritura o, en el caso del material electrónico, se destruye de forma segura en cuanto desaparece la necesidad de conservarlo de acuerdo al procedimiento de borrado seguro.

4.9.3.3. La información no se transporta en bolsas o cajas transparentes o no protegidas.

4.9.3.4. La información no se lee en lugares públicos (por ejemplo, salas de espera, cafeterías, transporte público, etc.).

4.9.3.5. En la medida de lo posible, el personal accederá a la información a través de la intranet, wikis y/o sistemas autorizados por GNS utilizando sus credenciales autorizadas.

4.10. Requisitos de Implementación Criptográfica

4.10.1. Las implementaciones criptográficas de producción deben ser aprobadas por la VicePresidencia de atención al cliente.

4.10.2. Las claves criptográficas de desarrollo no deben utilizarse para ninguna aplicación, dispositivo o solución de usuario en ambientes de producción.

4.10.3. Las implementaciones criptográficas deben cumplir lo descrito en el manual de políticas de seguridad de la información.

4.10.4. Las claves criptográficas deben generarse mediante un sistema fiable y deben tomarse precauciones razonables para evitar que se pongan en peligro, se modifiquen, se pierdan, se divulguen o se utilicen sin autorización.

4.11. Canales de comunicación

GNS proporciona canales específicos para las peticiones de datos personales como lo es protecciondedatospersonales@gns-latam.com

4.12. Actualizaciones a la Política

GNS podrá revisar y modificar periódicamente sus prácticas, políticas y procedimientos de protección de datos, incluida la presente Política de Protección de Datos. En caso de producirse cambios significativos, GNS deberá:

Tomar las medidas razonables para informar a todas las entidades de GNS, Trabajadores de GNS, Socios Comerciales y demás interesados afectados por las modificaciones.

Publicar en los sitios web pertinentes -tanto internos como externos, según corresponda los avisos pertinentes que hagan referencia a las modificaciones.

5. Cumplimiento de la Política

GNS se compromete a garantizar el cumplimiento de esta Política Global de Protección de Datos Personales y Privacidad por parte de todos los Trabajadores de GNS. Los Trabajadores de GNS deben cumplir esta Política Global. Los requisitos de cumplimiento de la política son los siguientes:

5.1. Fecha de entrada en vigor de la política.

Esta política entrará en vigor tras su aprobación definitiva.

5.2. Medición del cumplimiento

El cumplimiento de la presente Política Global de Protección de Datos Personales y Privacidad se verifica por diversos medios, incluidos los informes de las herramientas empresariales disponibles, las auditorías internas y externas, la autoevaluación y/o los comentarios al propietario o propietarios de la política. GNS supervisará el cumplimiento de la presente Política de forma continua. GNS verificará periódicamente que la presente Política Global de Protección de Datos Personales y Privacidad siga ajustándose a la legislación aplicable en materia de protección de datos y que se esté cumpliendo.

5.3. Excepciones al cumplimiento

Cualquier excepción a esta Política Global de Protección de Datos Personales y Privacidad requiere la aprobación por escrito de La VicePresidencia de atención al cliente y del líder del SGSI

Cualquier registro de excepciones debe archivarse de acuerdo con el Proceso de Gestión de Registros de GNS y no en el ordenador portátil de un individuo.

5.4. Incumplimiento

Se exige el cumplimiento de las políticas de GNS. Las desviaciones o el incumplimiento de esta Política, incluidos los intentos de eludir la política o el proceso establecidos mediante la elusión o la manipulación deliberada del proceso, el sistema o los datos, pueden dar lugar a medidas disciplinarias, incluido el despido, según lo permita la legislación local.

En algunos países, las infracciones de la normativa diseñada para proteger los Datos Personales pueden dar lugar a sanciones administrativas, penalizaciones, reclamaciones de indemnización o medidas cautelares, y/u otras acciones y recursos civiles o penales.

6. DOCUMENTOS RELACIONADOS

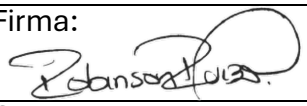
SI-MAN-002 Manual de Políticas de Seguridad de la Información
SI-PRO-019 Procedimiento de Transferencia de Información

7. CONTROL DE CAMBIOS

Fecha del Cambio	Motivo del cambio	Versión que cambia
14/12/2023	Creación del documento	1.0
11/10/2024	Revisión anual	2.0
06/11/2025	Inclusión de definiciones, derechos de titulares, canales de comunicación, creación de mecanismos para el consentimiento informado	3.0

14/07/2026	Migración a la estructura documental del SGSI. Corrección de referencias a documentos obsoletos por los vigentes (SI-MAN-002, SI-PRO-003, SI-PRO-016). Actualización de la Vicepresidencia responsable y de los aprobadores de excepciones. Alineación del esquema de clasificación a tres niveles. Actualización de documentos relacionados. Retiro de nombres de producto.	4.0

8. AUTORIZACIONES

Revisó	Aprobó
Nombre: Robinson Ruiz Muñoz	Nombre: Luis Enrique Rojas
Firma: 	Firma: 
Cargo: Líder del SGSI	Cargo: Vicepresidencia de atención al cliente

9. Apéndice: ISO 27001:2022 Alineación de Controles

Controles	A.5.31 Requisitos legales, estatutarios y reglamentario A.5.34 Privacidad y protección de la información

Tabla 1. Alineación de controles