Compañía Guatemalteca de Níquel, S.A. (en adelante – Compañía) es una compañía dedicada a la extracción de mena de níquel para atender las necesidades del mercado internacional, que garantiza el uso eficiente de los recursos y la energía para lograr sus objetivos a largo plazo, desde la alta dirección acepta la presente Política de Seguridad de la Información.

PROPÓSITO

El propósito de la presente Política de Seguridad de la Información (en adelante - Política) es garantizar un nivel adecuado de protección de los recursos informáticos de acuerdo con las normas internacionales orientadas al Desarrollo Sostenible y lograr de esta manera una eficiente y alta calidad en las actividades de la compañía.

ALCANCE

La Presente Política se aplica a todos los procesos del negocio y todas las actividades que se lleven a cabo dentro de las instalaciones de la compañía o bajo su dirección; de esta manea es de carácter obligatorio para todos los colaboradores que participen en alcanzar los objetivos de la presente Política

OBJETIVOS Y VALORES

Los objetivos estratégicos de la Compañía en el ámbito del Seguridad de la Información son:

- Utilizar los principios básicos de las normas internacionales en el ámbito de TI ISO20000, ISO 27001 y también las mejores prácticas ITIL para la construcción de la infraestructura TI;
- desarrollar una infraestructura de tecnología de la información unificada que abarque el cableado, redes de comunicación y transferencia de datos, además de los sistemas de gestión de envíos, equipos de servidores, servicios básicos de información y los sistemas de seguridad para la información;
- Implementar y utilizar sistemas de información de acuerdo con los requisitos de la legislación acerca de temas de propiedad intelectual y concesión de licencias;
- Garantizar medidas de protección contra las amenazas a la seguridad de la información;
- seleccionar e implementar las medidas actuales de seguridad de la información, incluyendo todas las técnicas de software y herramientas de hardware para el sistema de gestión de seguridad de la información;
- Garantizar el nivel necesario de resistencia a los fallos para los servicios TI y la disponibilidad de los datos para los departamentos a cuenta de un mayor grado de reserva y resistencia a los fallos del software y hardware;
- Desarrollo y diseño centralizados para los sistemas de información, incluyendo todos los elementos que componen a estos sistemas de información; también los métodos y la tecnología de integración, composición y estructura de flujos de información, modelos de datos, mapas de cobertura funcional para los sistemas de información;
- Delimitarle el acceso de los usuarios a los recursos de información.

Las actividades de la Compañía en el ámbito de Seguridad de la Información se llevan a cabo en base a los siguientes valores:

- Perfeccionamiento: labor continua encaminada a mejorar el sistema integrado de gestión en todos los procesos de negocio de la compañía;
- Calidad: buena organización y eficacia del proceso de producción como consecuencia de una excelente labor por parte del colaborador y un balance en los intereses de todas las partes interesadas;
- Innovación: recursos y herramientas utilizadas por nosotros para alcanzar objetivos que cumplan con los criterios de las mejores prácticas mundiales.

PROCESO DE NEGOCIO RESPONSABLE

El proceso de negocio "Gestión de tecnologías de la información" se compromete con la eficacia y la mejora continua de los resultados y a asignar los recursos necesarios para el cumplimiento de la presente política.

PRINCIPIOS DE TRABAJO

Dentro de los marcos de las normas de sostenibilidad adoptadas internacionalmente y de los principios ESG, se adoptan los siguientes principios de trabajo:

- Definición de las funciones del proceso de gestión de tecnologías de la información de acuerdo con el manual PCF;
- Análisis de los requisitos legales en el ámbito de la gestión de tecnología de la información;
- Análisis del entorno, de las partes interesadas, de sus necesidades y expectativas;
- Definición de una lista para la documentación interna normativa;
- Establecer objetivos estratégicos y operativos;
- Análisis de riesgos;
- Análisis del desarrollo innovador;
- Planificación de actividades;
- Realización del plan sobre desarrollo sostenible;
- Realización de los planes operativos y estratégicos;
- Recopilación y análisis de los datos mediante indicadores de rendimiento;
- Implementación de medidas correctivas o de medidas para la mejora.

PRINCIPIOS DE CONTROL

El control en el ámbito de Seguridad de la Información se realiza mediante:

- Cumplimiento de la documentación normativa, de planificación y de informe;
- Resultados de evaluación de los riesgos a la seguridad de la información de acuerdo con las regulaciones e instrucciones establecidas por el SIG.

PRINCIPIOS DE INFORME

En el ámbito de Seguridad de la Información la Compañía utiliza los siguientes principios de informe:

- Sobre indicadores de rendimiento reales y su comparación con los objetivos planificados;
- Según los requisitos de la documentación interna normativa de los ciclos estratégicos y operativos de la compañía;
- Teniendo en cuenta todos los incidentes relacionados con la seguridad de la información y realizando las investigaciones con sus respectivos informes a todas las partes interesadas.

PRINCIPIOS DE LA MEJORA CONTINUA

Uno de los principios más importantes del SIG de la Compañia es el principio de la mejora continua dentro del ciclo de gestión. Para mejorar la capacidad para responder a contextos internos y externos cambiantes y crear nuevas oportunidades en el ámbito de Seguridad de la Información, la Compañía sigue los siguientes principios:

- Realización de capacitaciones sistemáticas y continuas del personal que interactúa con el proceso de gestión de tecnologías de la información;
- Mantener un funcionamiento eficaz del sistema de gestión de calidad, y su mejora continua a través de la mejora de los procesos tecnológicos y de gestión con el uso racional de los recursos de acuerdo con los requisitos de la norma 9001.
- Asignacion de responsabilidades y obligacipones claras para los trabajadores de todos los niveles, para el cumplimiento de los requisitos del sistema de gestión de la seguridad de la información

La presente política es autorizada por el director general de la Compañía y sus postualciones son revisadas periodicamente.

Director general interino

C. Gonzalez