POLÍTICA DE USO Y PRIVACIDAD DE LA INFORMACIÓN GRUPO CYGNUS

1.INTRODUCCIÓN

Actualmente la información es considerada un recurso estratégico que impacta en el cumplimiento de los objetivos y resultados de la organización y en la relación con nuestros clientes y colaboradores, que requieren de un esfuerzo constante por adaptarse y gestionar los riesgos derivados de un inadecuado uso de ésta.

Por ello, se elabora la presente política de uso y seguridad de la información para resguardar la confidencialidad, integridad y disponibilidad de ésta, así como proteger la infraestructura informática de las plataformas electrónicas que sustentan nuestros procedimientos administrativos y la relación con los clientes, reforzando el cumplimiento de los principios establecidos por nuestra compañía en base a lo dispuesto en la norma técnica de seguridad de la información y ciberseguridad conforme a la ley Nº 21.180 y tomando en consideración las recomendaciones expresadas en la norma ISO/IEC 27002:2013.

2.OBJETIVO

El objetivo principal de la presente política es definir y establecer un marco de gestión para controlar el uso, la seguridad y privacidad de la información de la organización.

3.ALCANCE

Se delimita su extensión a toda información relacionada a las sociedades de Grupo Cygnus, con independencia de la forma en la que se procese, quien acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente, y a todos los responsables que intercedan en cualquier fase del tratamiento de los datos de carácter restringido, confidencial e interno, quienes estarán obligados a mantener reserva respecto de éstos. De igual modo, tendrán la obligación de guardarlos y cuidarlos cuando corresponda, lo que subsistirá aún después de finalizar su relación laboral.

4.REFERENCIAS

La presente política responde a los estándares y directrices técnicas establecidas en:

- **Ley N° 21.180**

  Esta ley modificó la ley N° 19.880 para incorporar la digitalización y transformación del ciclo de los procedimientos administrativos. Este reglamento dictaminó seis normas técnicas sobre interoperabilidad, seguridad de la información y ciberseguridad, documentos y expedientes electrónicos, notificaciones, calidad y funcionamiento, y de autenticación.

- **Norma ISO/IEC 27002:2013**

  Normativa general que permite asegurar y proteger la información física y digital, brindando una serie de acciones para gestionar la seguridad de la información.

5.ROLES Y RESPONSABILIDADES

Todos los departamentos y colaboradores relacionados a Grupo Cygnus se deben comprometer a velar por la seguridad y compartir la responsabilidad de mantener la privacidad de toda información recogida en esta. Se identifican los siguientes equipos y principales responsabilidades asociadas:

- **Tecnología de la información**
    - Mantener actualizada la presente política de uso y seguridad de la información.
    - Integración de la privacidad por diseño en los sistemas.
    - Difundir la política de uso y seguridad de la información.
    - Control de ciberseguridad y seguridad de la información.
    - Supervisión del tratamiento de los datos.
    - Gestión del consentimiento.
    - Evaluación de impacto de privacidad.
    - Notificación de incidentes.

- **Recursos humanos**
    - Formación de empleados.
    - Difundir política de uso y seguridad de la información.
    - Seguimiento de las prácticas de seguridad.
    - Notificación de incidentes.

- **Comercial**
    - Procesamiento de solicitudes de los clientes.
    - Difundir política de uso y seguridad de la información.
    - Seguimiento de las prácticas de seguridad.
    - Notificación de incidentes.

- **Legal**
    - Permiso a los clientes para ejercer sus derechos.
    - Gestión del consentimiento.
    - Difundir política de uso y seguridad de la información.
    - Seguimiento de las prácticas de seguridad.
    - Notificación de incidentes.

- **Colaboradores**
    - Velar por la confidencialidad, integridad y disponibilidad de la información según las funciones que le han sido encomendadas.
    - Seguimiento de las prácticas de seguridad.
    - Notificación de incidentes.

Se identifica como responsable institucional de seguridad de la información, ciberseguridad, y activos de la información a quien asuma como encargado del Departamento de Tecnología de la Información. Actualmente es asumido por Héctor Ortega, y sus datos de contacto son los siguientes:

- **Correo electrónico**
  - hector.ortega@cygnus.cl
- **Número telefónico**
  - +56 9 8293 0262

6.PRINCIPIOS

Tomando en consideración las recomendaciones de seguridad de la información dispuestas en el estándar internacional ISO/IEC 27001, así como al cumplimiento de la legislación vigente, se establecen los siguientes principios básicos como directrices fundamentales:

- **Seguridad integral**

  La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.

- **Gestión de riesgos**

  La gestión de riesgos deberá ser parte esencial del enfoque colaborativo.

- **Proporcionalidad**

  Deberá ser proporcional la aplicación de medidas de protección, detección y recuperación a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

- **Mejora continua**

  Las medidas de seguridad se revisarán y actualizarán periódicamente para adecuar su eficiencia y eficacia.

- **Alcance estratégico**

  La seguridad de la información deberá contar con el compromiso y apoyo de todos los niveles directivos de las sociedades de Grupo Cygnus de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.

7.POLÍTICAS DE SEGURIDAD

7.1 TRATAMIENTO DE LA INFORMACIÓN RESTRINGIDA

La información restringida se caracteriza por poseer repercusiones legales o de mercado si se revela a terceros, tales como propuestas comerciales, contratos, y/o decisiones estratégicas, entre otros. Por ello, se establece regular ejerciendo las siguientes acciones:

- Autenticación de accesos.
- Mantener registro en tiempo y ubicación de los dispositivos de la empresa desde donde los usuarios acceden.
- Sólo se podrán compartir con las personas que tienen autorización y requieren de esta información para cumplir con sus funciones laborales.

7.2 TRATAMIENTO DE LA INFORMACIÓN CONFIDENCIAL

La información confidencial incluye datos personales de nuestros clientes y empleados, tales como registros de clientes, datos de los empleados, transacciones financieras, de negocios, de proyectos, contratos, propuestas de proveedores, sistemas de trabajo, proyectos de inversión, marketing, planes de comercialización, información técnica, financiera o comercial, lista de clientes y proveedores, precios, esquemas, planillas, modelos, muestras, programas, software y documentación, entre otros. Estos documentos nos proporcionan ventajas estratégicas, financieras y operativas que se deben proteger, por ello, se establece regular ejerciendo las siguientes acciones:

- Restringir acceso según las funciones de los usuarios.
- Utilizar contraseñas seguras para prevenir accesos no autorizados.
- En el caso de poseer registros comerciales en papel, se deben almacenar en un archivador de seguridad y guardar la llave en una zona restringida.
- Incorporar en los cargos estratégicos y que tengan acceso a información confidencial de la compañía, acuerdos de confidencialidad que resguarden la información proporcionada.

7.3 TRATAMIENTO DE DATOS INTERNOS

Los datos internos son usados para nuestras actividades empresariales diarias tales como documentos generados por los empleados, notas de reuniones, decisiones importantes sobre el personal. Se establece regular ejerciendo las siguientes acciones:

- Evitar compartir con terceros.
- Establecer contraseña para acceder al equipo.
- Ir a una sala de reuniones privada.
- Borrar la información de la pizarra.
- Restringir el acceso a las notas realizadas salvo acceso compartido para terceros involucrados en el proceso.

7.4 TRATAMIENTO DE DATOS PERSONALES

El tratamiento de los datos personales se debe realizar de acuerdo con los fines específicos para los que se solicitaron en origen. Además, se debe informar a los interesados de forma sencilla y clara para que puedan comprender fácilmente:

- Finalidad de la actividad de tratamiento de sus datos personales.
- Identidad y los datos de contacto del responsable.
- Intención del responsable de transferir datos a un tercero.
- La posibilidad de ejercer los derechos sobre sus datos personales y cómo proceder.
- Todo derecho que se reconozca en la Constitución y las leyes vigentes.

7.5 TRATAMIENTO DE DATOS PÚBLICOS

Los datos públicos son aquellos que pueden ser visualizados por cualquier persona, aunque sólo deben ser divulgados por empleados autorizados, tales como valor bursátil, mpta de prensa del servicio, publicaciones en redes sociales, entre otros. Si bien, esta información se encuentra accesible a todos, se solicita adherirse a las siguientes prácticas:

- No comentar en redes sociales información de la operación de la empresa, exeptuando los eventos realizados de forma extraprogramáticas, donde se informe su autorización.
- No comentar entrevistas hasta que se hagan públicas.
- Seguir los procedimientos de comercio ético.

7.6 PUESTO DE TRABAJO

Se establecen los siguientes requisitos con el objetivo de mantener la seguridad en los puestos de trabajo:

- Bloquear la sesión de los equipos cuando el empleado deje el puesto, tanto por medios manuales (bloqueó por parte del usuario), como de forma automatizada mediante la configuración del bloque de pantalla.
- Recoger todo documento o soporte de información que por su clasificación sea confidencial o secreto. Procurar guardarlo bajo llave para que quede fuera de la vista.
- Mantener ordenado el puesto de trabajo y despejado de documentos o soportes de información que puedan ser vistos o accesibles por otras personas.

7.7 GESTIÓN DE ACTIVOS DE INFORMACIÓN

Se establecen los siguientes requisitos con el objetivo de mantener la seguridad en la gestión de activos:

- Tener identificados e inventariados los activos necesarios para la prestación de los procesos de negocio.
- Mantener actualizado el inventario de activos.
- Realizar la clasificación de los activos en función del tipo de información que se vaya a tratar, de acuerdo con lo dispuesto corporativamente.
- Asignar un responsable encargado de realizar la gestión propia de los activos de información durante todo el ciclo de vida, quién deberá mantener un registro formal de los usuarios con acceso autorizado a dicho activo.
- Para cada activo o elemento de información debe existir un responsable o propietario, el cual tendrá la responsabilidad de asegurar que el activo esté inventariado, correctamente clasificado y adecuadamente protegido.
- Actualizar de manera periódica las configuraciones de los activos para permitir el seguimiento de estos y facilitar una correcta actualización de la información.

7.8 GESTIÓN DE DISPOSITIVOS PERSONALES

En ningún caso se permitirá hacer uso de ordenadores personales (laptop o notebook). La empresa se compromete a entregar oportunamente estos dispositivos a todos los colaboradores que lo requieran para desarrollar sus funciones laborales. En aquellos casos, donde se permita a los

colaboradores utilizar sus dispositivos móviles personales (smartphone o tablet) para acceder a recursos tecnológicos o información de Grupo Cygnus y/o clientes de la empresa, el colaborador deberá tener en cuenta las siguientes consideraciones:

- Ser responsable de su equipo.
- En ningún caso se permitirá el acceso a la red interna de las oficinas de Grupo Cygnus.
- Recibir autorización de su responsable de área para utilizar las aplicaciones establecidas para su actividad laboral.
- Mantener actualizadas las aplicaciones establecidas como necesarias para su actividad laboral.
- Reportar al responsable de seguridad cualquier incidencia que pueda afectar a la confidencialidad, integridad o disponibilidad de estos dispositivos.

8.DEFINICIONES

- **Activo**

  Todo elemento lógico o físico, componente de hardware, equipamiento o sistema relacionado con la información, que permita su generación, almacenamiento, soporte, envío o intercambio.

- **Activo de información**

  Datos o información cuyo tratamiento es esencial para el funcionamiento y desarrollo de la organización que lo utiliza, genera, almacena, envía o intercambia. Debe ser protegido en su confidencialidad, integridad, disponibilidad u otros factores de importancia.

- **Ciberseguridad y seguridad de la información**

  Conjunto de acciones, políticas, medidas preventivas y reactivas destinadas a la prevención, mitigación, manejo, respuesta y estudio de las amenazas y riesgos de incidentes de seguridad. Además, permite la reducción de sus efectos y el daño causado antes, durante y después de su ocurrencia; respecto a los activos y activos de información y la continuidad de servicios, con el fin de proteger, preservar y restablecer la confidencialidad, integridad y disponibilidad de aquellos y de las plataformas electrónicas de la organización.

- **Confidencialidad**

  Atributo de los activos y los activos de información que asegura que estos sean conocidos y accedidos exclusivamente por quienes están autorizados para ello.

- **Acceso**

  Atributo de los activos y activos de información, relativo a su disponibilidad y utilización a requerimiento de una entidad o proceso autorizado.

- **Gestión de riesgo**

  Proceso estructurado y proactivo por el cual se identifican, evalúan, controlan y tratan los riesgos derivados de una o más amenazas determinadas.

- **Uso inadecuado de seguridad**

  Todo evento de seguridad o una serie de ellos, de carácter indeseado inesperado, que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas informáticos, los activos y activos de información, datos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y que puedan afectar al normal funcionamiento de estos.

- **Integridad**

  Atributo de los activos y activos de información relativo a la exactitud, autenticidad y completitud de estos.

- **Recursos tecnológicos**

  Software o conjunto de software, datos e infraestructura tecnológica que sustenta procesos o procedimientos.

- **Riesgo**

  Efecto de la incertidumbre sobre los activos de información y los objetos de una entidad, habitualmente expresado en relación con las consecuencias de un evento o incidente de seguridad y si probabilidad de ocurrencia.

- **Colaboradores**

  Funcionarios que acceden a los activos y activos de información que soportan procedimientos administrativos o procesos relacionados con estos.

9.INCUMPLIMIENTO DE LA POLÍTICA

El incumplimiento de alguna de las disposiciones de esta política podrá dar lugar a la responsabilidad y eventuales sanciones de conformidad a los deberes y obligaciones dispuestas en el reglamento interno de Grupo Cygnus, previa instrucción del correspondiente procedimiento disciplinario.

10.CONTROL DE CAMBIOS

Versión	Razón del cambio	Elaborado por	Fecha
1	Elaboración política	Valentina Gómez - procesos	Agosto 2023
2	7.8 Ajustes en definición	Héctor Ortega - tecnología	Octubre 2023

Eloisa Alvarez R.

Eloisa Álvarez Robledo
Gerente General Grupo Cygnus