1. ***OBJETO***

Definir la política sobre manejo seguro de la información.

1. ***ALCANCE***

Esta política es aplicable a todas las actividades desarrolladas por Empleados, Visitantes, Contratistas, Asesores de Manufacturas Silíceas que tengan acceso a información o a los sistemas de información de Manufacturas Silíceas.

1. ***RESPONSABLES***

**Gerente General**

* Es responsable por la implementación y cumplimiento de este política

**Empleados, Visitantes, Contratistas, Asesores de Manufacturas Silíceas**

* Son responsables por la cumplir con esta política.

1. ***DEFINICIONES***
2. ***GENERALIDADES***

Esta política está orientada a ilustrar a los empleados, contratistas y visitantes de Manufacturas Silíceas sobre las responsabilidades respecto a:

* Manejo y uso de la información que es uno de los activos más valiosos de la compañía.
* Proteger esta información de su pérdida, uso inadecuado.
* Manejar la información como sensible y crítica mientras no se indique lo contrario.

Los sistemas de información puestos a disposición de empleados, contratistas y visitantes incluyen computadores, servicios de comunicación, red de acceso a internet entre otras aplicaciones.

Todas las personas deben tomar las medidas apropiadas para proteger la información sin importar el medio en que es almacenada (físico o electrónico). Dichas medidas incluyen entre otras, restringir el acceso solamente a las personas que requieren dicha información para ejecutar sus funciones. La gerencia de Manufacturas Silíceas se asegurará que todos los empleados, contratistas y visitantes tengan pleno conocimiento de esta política.

Como toda política, no logra cubrir todas las situaciones posibles, por lo que se debe entender la filosofía sobre la cual se basa y en caso de dudas puede preguntar a la gerencia o a su supervisor inmediato para aclaración.

Esta política contiene las siguientes secciones: Ninguna expectativa de privacidad, Vigilancia, Protección de la Propiedad Intelectual, Protección de la Información de los Activos, Uso Aceptable de los Servicios de Comunicación Electrónica y Actividades prohibidas / Acoso / Comportamiento ofensivo. Algunas de las secciones pueden contener descripciones, definiciones o fundamentos que pueden ser reconocidos por el tipo de fuente cursiva

Todos los empleados tienen la obligación de reportar cualquier posible violación de esta política de tal manera que se puedan tomar acciones correctivas a la menor brevedad posible.

1. ***DESCRIPCION DE LA POLITICA***
   1. ***Información sensible definida por Manufacturas Silíceas***

Una información se considera sensible si por si sola o junto con otra puede dañar la posición competitiva de la compañía, crear un problema de responsabilidad legal para la compañía o causar un perjuicio a los empleados si es divulgada a personas no autorizadas. Dentro de la información sensible se cuenta la información confidencial (procesos de manufactura, reportes financieros), información privada (historias clínicas, salarios) y cualquier información catalogada como secreta.

* 1. ***No Expectativas de Privacidad***

Los sistemas de información y los privilegios de acceso para empleados, contratistas y visitantes están diseñados para facilitar la realización de sus funciones, por lo tanto están obligados a mantener con carácter confidencial cualquier información sensible que reciban o desarrollen.

De igual manera autorizan para que las personas designadas por la gerencia tengan acceso a revisar toda la información que hayan creado, tengan almacenada, envíen o reciban en los sistemas de información de la compañía. Se entiende que estas monitorias se pueden hacer de forma manual o automática.

* 1. ***Monitoreos***

Manifacturas Silíceas tiene el derecho de acceso a todas las comunicaciones transmitidas a través de sus sistemas de información. Todos los empleados, visitantes o contratistas que usen los sistemas de información de la compañía deben saber que sus comunicaciones pueden ser grabadas o monitoreadas y que Manufacturas Silíceas puede elaborar y distribuir reportes de dichas comunicaciones a quienes considera necesario.

* 1. ***Protección de la Propiedad Intelectual***

Toda la información creada por empleados, consultores, contratistas y proveedores es propiedad intelectual de Manufacturas Silíceas a menos que la gerencia determine lo contrario y constituye un activo valioso de la compañía.

Manufacturas Silíceas tiene la obligación de asegurar que todas las leyes son obedecidas por quienes usan sus sistemas de información en actividades relacionadas con los negocios de la compañía.

* El uso y la divulgación no autorizados de información sensible o el uso información sensible de terceros se considera una violación de esta política.
* Copiar sin autorización programas de computador (software) es una violación de las leyes de derechos de autor. Todos los empleados, contratistas y visitantes deben cumplir con estas leyes y acuerdos de licencias aún con aquellas de dominio público (fee shareware).
* Todos los empleados, contratistas y visitantes deben saber verificar que el software bajo su control cumple con los acuerdos de licencias existentes. Si no están en capacidad de verificarlo, deben tomar acciones inmediatas para verificar el cumplimiento de los acuerdos de licencia o destruir la copia del software no autorizado. Cuando se recibe una actualización, la copia antigua no debe ser entregada a ninguna persona ni debe ser instalada en otro computador.
* Todos los empleados, contratistas y visitantes deben proteger la información sensible que reciban para evitar su mal uso, pérdida o comunicación no autorizada. La gerencia es responsable por divulgar este requerimiento a todos los obligados a cumplirlo.
  1. ***Protección de los activos informáticos***

La información es un activo valioso de Manufacturas Silíceas. Las medidas consignadas en esta política incluyen entre otras:

* La información sensible no debe ser transmitida a ninguna red externa a menos que vaya encriptada o protegida con contraseñas.
* Las contraseñas deben ser transmitidas separadamente del mensaje encriptado.
* La información sensible no debe ser discutida en sitios públicos tales como restaurantes, aeropuertos, oficinas de clientes etc.
* Los mensajes que contengan información sensible solamente deben enviarse a las personas que deben conocer dicha información. Cuando reenvie un mensaje debe asegurarse que no solamente el mensaje sino los archivos anexos deben también ser reenviados.
* Toda la información de Manufacturas Silíceas debe protegerse de ser divulgada a terceras partes. Esta autorización puede darse cuando existen razones que lo justifiquen y ha sido debidamente autorizado.
  1. ***Protección de la Información Ambiental***

El equipo y otros recursos para el manejo y uso de información electrónica son activos valiosos de Manufacturas Silíceas. Las medidas previstas por esta política son necesarias para su protección.

Manufacturas Siliceas puede hacer uso de los servicios de terceros, como las redes de comunicación o recursos de computación. El diseño, la gestión y el funcionamiento de estos servicios está fuera del control de Manufacturas Silíceas. Es necesario adoptar medidas especiales para asegurar que la información de medio ambiente Información de la compañía no se ve comprometida por las posibles deficiencias en operación de terceros.

* El acceso a todos los recursos del sistema de información de Manufacturas Silíceas información debe estar debidamente aprobado. Todos los empleados, consultores, contratistas y proveedores son responsables de la información obtenida a través del uso de su identificación de usuario (ID de conexión) y la contraseña. Está estrictamente prohibido el uso no autorizado de la identificación de otro usuario o contraseña, o haciéndose pasar por otro usuario.
* Todos los archivos electrónicos importados / descargados desde cualquier sistema externo deben ser examinados en busca de virus, utilizando el software anti-virus antes de ser ejecutado en cualquier recurso del sistema de información de Manufacturas Silíceas y no debe infringir los derechos de autor y las leyes de concesión de licencias de software.
* Sólo la importación / descarga de software debe hacerse desde un "sitio de confianza" en Internet. Un sitio de confianza es una ubicación de Internet que despliega el hardware, software y / o procedimientos que sean razonablemente a salvo de intrusos y mal uso; ofrece un nivel razonable de fiabilidad e integridad, son adecuados para desempeñar sus funciones y se adhiere destinados a las prácticas de seguridad generalmente aceptados.
* Todas las vulnerabilidades de seguridad y las deficiencias deben ser reportados inmediatamente.
* La identificación del usuario (ID de inicio de sesión) y contraseñas utilizadas en los recursos del sistema de información de Manufacturas Silíceas no se pueden utilizar en redes de proveedores de servicios de aplicaciones de terceros y los recursos del sistema de información. Esta declaración no se aplica al uso de servicios remotos de acceso telefónico portales o correo electrónico con cuentas / ID de inicio de sesión.
* Cualquier información confidencial, debe ser almacenada sólo en sitios de acceso controlado y / o directorios cifrados.
* El acceso remoto a los recursos del sistema de información debe ocurrir solamente a través de métodos aprobados.
* Todos los recursos del sistema de información utilizados para acceder a Internet deben ser a través de una pasarela segura aprobada. El enlace se puede configurar para incluir un "firewall", que se utiliza para la inspección de determinados tipos de actividad y que se puede utilizar para cortar la conexión se debe detectar una intrusión. El enlace se define como el hardware y software que permiten a los usuarios conectarse a una red a otra. Una pasarela segura limita el acceso entre las redes de acuerdo con las políticas y normas de seguridad locales, y hace cumplir una política de control de acceso entre dos o más redes. Está diseñado para evitar el acceso no autorizado a o desde una red en particular. Un servidor de seguridad es un componente o conjunto de componentes que restringe el acceso entre una red protegida y la Internet, o entre otros conjuntos de redes. Un dispositivo instalado en el punto donde las conexiones de red entran a un sitio que se aplica reglas para controlar el tipo de tráfico de red que entra y sale.
  1. ***Uso Aceptable de los Servicios de Comunicación Electrónica***

Manufacturas Silíceas proporciona servicios de comunicaciones electrónicas en lo que requiera el desempeño y el cumplimiento de las responsabilidades del trabajo. Estos servicios, como el correo electrónico, mensajería de colaboración, correo de voz y acceso a Internet, tienen el propósito de aumentar la productividad y no para actividades no comerciales.

Si usted se está comunicando electrónicamente en el dominio público con declaraciones personales y / o dictámenes, o no está actuando dentro de las responsabilidades de su empleo o contrato de servicio que se le autoriza a hablar en nombre de Manufacturas Silíceas, la siguiente renuncia debe ser añadida a todo el correo electrónico (e-mail), dirigida a destinatarios fuera de la empresa:

***"Las opiniones expresadas son las del remitente, y no las de Manufacturas Silíceas"***

Es responsabilidad del usuario para añadir la renuncia a la comunicación electrónica. Si es factible, esta renuncia puede ser generada automáticamente por la tecnología de comunicación electrónica, por ejemplo, la tecnología de correo admite la generación automática de la excención de responsabilidad.

* Se permite el uso personal ocasional y razonable de los servicios de comunicación, siempre que ello no interfiera con el desempeño laboral. Estos servicios pueden ser utilizados fuera de las horas regulares de trabajo, siempre que dicho uso sea coherente con la conducta profesional. Es una violación de usar los servicios de comunicaciones electrónicas a revelar información corporativa sin autorización previa.
* Violaciones de Internet y el uso de correo electrónico incluyen, pero no se limitan a los juegos de azar o acceder, descargar, cargar, guardar, recibir o enviar material que incluya contenido sexual explícito u otro material utilizando vulgar, sexista, racista, amenazante, violento o lenguaje difamatorio.
  1. ***Actividades Prohibidas/ Acoso / Comportamiento ofensivo***

Esto complementa la prevención del acoso contenida en el Reglamento Interno de Trabajo.

* Las actividades ilegales no se llevarán a cabo con los recursos del sistema de información de Manufacturas Silíceas.
* Se prohíbe el lenguaje ofensivo , el chisme y el acoso de los demás , mientras que el uso de los recursos del sistema de información ( incluyendo servicios de noticias , grupos de discusión y tableros de anuncios ) .
* El acceso, visualización o difusión de material pornográfico en cualquier momento en los recursos del sistema de información está prohibido.
* Está prohibido en todo momento sobre los recursos del sistema de información de generar, acceder, mostrar o difundir cualquier material que viole o abogan por la violación de la política de Prevención del Acoso.
* En general, todos los empleados y todos los consultores, contratistas y proveedores que trabajan para Manufacturas Silíceas deben ser conscientes de la sensibilidad de los compañeros de trabajo. Por lo tanto, todos los empleados, consultores, contratistas y proveedores no deben difundir material en el lugar de trabajo que sus compañeros de trabajo podrían considerar ofensiva.
  1. ***Cumplimiento***

Las personas serán responsables por violaciones de política, lo que puede resultar en la terminación de empleo y / o acción legal.

Todas las violaciones sospechosas y conocido de esta Política deben ser reportados inmediatamente a la gerencia de la compañía

1. ***CONTROL DE CAMBIOS***

|  |  |  |
| --- | --- | --- |
| **FECHA** | **VERSIÓN** | **CAMBIO** |
| 01/01/2014 | 1 | * Versión original de la política. |

1. ***DOCUMENTOS DE REFERENCIA O RELACIONADOS***

* Reglamento Interno de Trabajo.