POLÍTICA INTEGRAL DE CALIDAD, MEDIO AMBIENTE,
SEGURIDAD Y SALUD OCUPACIONAL Y SEGURIDAD DE LA INFORMACIÓN

Somos una empresa importadora y comercializadora de productos químicos para minería e industria con más de 20 años de experiencia brindando como valor agregado a nuestros clientes productos de calidad certificada y asesoría técnica a través de un equipo de colaboradores y socios de negocio altamente capacitados y preparados para asumir los retos y exigencias del mercado

Actualmente CHEMSUPPLY S.A.C, asume el compromiso de cumplir con los requisitos de sus partes interesadas y legislación aplicable vigente en materia de calidad, seguridad, salud ocupacional y medio ambiental y seguridad de la información, entre otros que la organización suscriba. Para ello se han establecido los siguientes compromisos:

EN GESTIÓN DE LA SEGURIDAD Y SALUD OCUPACIONAL:

1. Proporcionar condiciones de trabajo seguras y saludables para la prevención de lesiones y deterioro de la salud relacionados **con el trabajo presencial y remoto** y que sea apropiada al propósito, tamaño y contexto de la organización y a la naturaleza específica de sus riesgos para la SST y sus oportunidades para la SST.
2. Cumplir los requisitos legales y otros requisitos.
3. Chemsupply se compromete en eliminar los peligros y reducir los riesgos de Seguridad y Salud en el Trabajo.
4. Promover la mejora continua del sistema de gestión de la SST.
5. Promover la consulta y participación de los trabajadores, a través de sus representantes.
6. Monitorear la salud de sus colaboradores a través de profesionales en medicina ocupacional y la realización de exámenes médicos ocupacionales anuales.
7. Apoyar permanentemente en la atención privada de salud (Eps) en favor de sus colaboradores.
8. Desarrollar capacitaciones permanentemente a favor de sus colaboradores para mitigar riesgos de accidentes dentro y fuera del centro laboral.
9. Proporcionar los EPP correspondientes a cada colaborador de acuerdo a sus actividades a ejecutar, y supervisar el uso correcto de los mismos y conservación.
10. Capacitar constantemente para la manipulación correcta de productos MAPTEL y supervisar el cumplimiento de los procesos y procedimientos vinculados de estos productos.
11. Supervisar y controlar el cumplimiento de los requisitos de SST necesarios en el desarrollo de trabajo de los proveedores de servicios.
12. Contar con fichas de datos de seguridad de los diferentes productos que se comercializa, generando un archivo interno que este a disposición de las partes interesadas.
13. Cumplir con las buenas prácticas de almacenamiento

EN GESTIÓN DE LA CALIDAD:

14. La búsqueda permanente de cubrir la plena satisfacción de nuestros clientes, cumpliendo con el contexto de la organización, sus necesidades y expectativas.
15. Promover un Marco de Referencia, para el establecimiento de los Objetivos del Sistema de Gestión Integrado.
16. Cumplir los requerimientos de calidad de nuestros clientes en cuanto a las características técnicas de los productos que comercializamos sustentado en sus respectivos certificados de análisis.
17. Cumplir con los compromisos de entrega a nuestros clientes asegurando los tiempos y lugar de entrega.
18. Cumplir con la política de stocks de seguridad de la compañía para asegurar el abastecimiento oportuno a nuestros clientes.
19. Cumplir con los requerimientos de asesoramiento técnico y atención post venta en nuestros clientes, asegurando el cumplimiento de objetivos técnicos y logrando la preferencia de nuestros clientes.
20. Nos comprometemos en integrar nuestros procesos con los de nuestros clientes reduciendo errores y agilizando su atención.
21. Promover el compromiso de nuestro personal en el aseguramiento de la calidad y la mejora continua a través de la capacitación constante.
22. Cumplir con los requisitos legales y de nuestra organización que sean aplicables.

EN GESTIÓN AMBIENTAL:

23. Contribuir con la protección del medio ambiente, incluida la prevención de la contaminación y uso sostenible de recursos; tomando en cuenta los impactos ambientales de nuestras actividades.
24. Dar cumplimiento de las indicaciones establecidas en las hojas MSDS de cada uno de los productos químicos comercializados.
25. Cumplir con los requisitos legales nacionales e internacionales de los entes correspondientes.
26. Aplicar la mejora continua a su sistema de gestión ambiental para el logro y cumplimiento de sus objetivos ambientales.

EN GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:

27. La información de Chemsupply debe clasificarse en 03 niveles (Confidencial, Uso Interno y Pública), además de etiquetarse y gestionarse en función de su valor, nivel de sensibilidad, requisitos legales y criticidad para la organización.
    a. **Confidencial:** Información de alta sensibilidad que debe ser protegida por su relevancia. Esta información debe ser accedida sólo por personas que tengan una necesidad específica de conocerla o usarla por sus funciones. Se deberán utilizar controles de encriptación para protegerla tanto en su almacenamiento como en su uso.
    b. **Uso Interno:** Información que, sin ser reservada ni confidencial, debe mantenerse en el ámbito interno de Chemsupply y no debe estar disponible externamente, excepto a terceras partes involucradas, previo acuerdo de confidencialidad y conocimiento del propietario de esta.
    c. **Pública:** Información de uso común para toda la organización. Debe ser expuesta y de conocimiento para todos los colaboradores. Esta información no está sujeta a ningún tipo de tratamiento especial.
28. Respecto a lo relacionado al Control de Acceso, se deberán mantener controles como segregación de funciones, registros de logs de acceso y monitoreo de accesos a la información de Chemsupply para asegurar que solamente las personas que tengan una necesidad legítima de acceder a la información tengan dicho acceso.
29. Todos los colaboradores de Chemsupply deben proteger la información que se encuentre en medios físicos o digitales: USB, disco duro externo, DVD, Blu-ray, laptop, celular, tablets, entre otros. Para lo cual deberán cumplir con las buenas prácticas de Escritorio Limpio.
30. Todos los colaboradores de Chemsupply deben proteger la información del negocio, por ende, deberán cumplir con lo siguiente:
    d. No dejar documentos físicos ni medios digitales removibles a la vista o que sean de fácil acceso por terceras personas.
    e. Bloquear la sesión cuando no se esté usando la computadora, tanto en casa como en lugares públicos (“Windows + L” o “Ctrl + Atl + Supr”)
    f. No registrar las contraseñas o información de accesos en lugares que sean accesibles por personas no autorizadas. (Ejemplo: notas adhesivas, blocks, etc.)
    g. No abrir archivos, enlaces ni páginas sospechosas que se reciban por correo electrónico.
    h. Usar soluciones de cifrado de información y correos sensibles.
    i. No usar correos personales para compartir información corporativa.
    j. Trabajar la información en repositorios que cuenten con backup: Servidor de Archivos.
31. Todo equipo de cómputo corporativo de Chemsupply, debe contar con el disco duro encriptado, antivirus corporativo instalado, y controles de acceso a páginas web maliciosas o sospechosas habilitadas.
32. Todo equipo que no es propiedad de Chemsupply y requiera conectarse a sus sistemas y/o recursos, debe contar con la aprobación de su Gerencia y/o Jefatura inmediata y sujetarse a las políticas de seguridad de la información vigentes:
    k. Tener instalado en su equipo de cómputo un antivirus licenciado, ya sea corporativo o personal.
    l. Acceder a información y/o recursos de Chemsupply a través de equipos de cómputo con sistemas operativos vigentes y con soporte.
    m. Tener instalados en su equipo de cómputo todos los parches de seguridad permitidos.
    n. Tener instalado el software necesario para acceder a los recursos de Chemsupply, y que el acceso sea limitado y restringido a lo específico.
    o. Acceder a través del acceso remoto VPN - Forticlient a las aplicaciones de la compañía de acuerdo con su perfil.
33. En caso de pérdida o robo, el colaborador debe avisar lo más pronto posible al Área de Sistemas para que se puedan realizar las gestiones respectivas de bloqueo y borrado de información.
34. Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de Chemsupply y deben acatar las condiciones de uso establecidas para dichas conexiones.

35. Todo colaborador debe tener restringido el perfil de administrador local en su equipo de cómputo para evitar la instalación de software o sistemas no autorizados en el equipo y que no estén acorde a sus funciones y/o responsabilidades. Excepcionalmente, se asignará sólo a los usuarios que cuenten con el debido sustento asociado estrictamente a sus funciones, así como la autorización de su Gerencia inmediata.

36. Se deben identificar y evaluar los riesgos de seguridad a los cuales están expuestos los activos de información y activos digitales de Chemsupply, por lo menos una (01) vez al año o ante un cambio significativo en los procesos, organización o tecnología, para establecer los controles apropiados de seguridad que permitan mitigarlos.

37. Se debe realizar, por lo menos una (01) vez al año, un análisis sobre la red y los sistemas de Chemsupply, que permitan identificar vulnerabilidades a ataques externos o internos.

38. Se debe contar con un proceso de control de cambios en los sistemas, aplicaciones y recursos de Chemsupply, el cual incluya un análisis de impacto y riesgo del cambio, y una especificación de los controles de seguridad necesarios.

39. De igual manera, toda iniciativa o proyecto que contemple la implementación o adquisición de un servicio, sistema o software debe contar con la participación de Seguridad de la Información desde la concepción del requerimiento hasta su salida en vivo, a fin de cumplir con los requisitos mínimos de seguridad necesarios.

40. Se debe contar con un Plan de Continuidad del Negocio y un Plan de Recuperación ante Desastres, los cuales deberán ser revisados y actualizados periódicamente según lo definido por el negocio.

41. Los contratos con terceros deberán contemplar cláusulas de confidencialidad, protección de datos personales y antifraude con las empresas contratadas y sus funcionarios, para el manejo de la información de Chemsupply y/o uso de su propiedad intelectual.

42. Toda conexión de terceros a recursos y sistemas de Chemsupply, debe cumplir con todos los requisitos de seguridad de la información vigentes.

43. No se debe publicar NADA que pueda poner en peligro la privacidad de Chemsupply o de su personal, a través de redes sociales o algún otro medio.

44. Chemsupply debe hacer firmar a sus colaboradores un acuerdo de confidencialidad, no divulgación y tratamiento de datos personales, así como una autorización para auditar sus correos electrónicos en determinadas circunstancias (sospechas razonables de una falta laboral como competencia desleal, fuga de información, entre otras), en lo que se denomina “consentimiento informado”.

45. Se deben proteger los derechos de propiedad intelectual, los cuales abarcan derechos de copia (“*copyright*”), derechos de diseño, marcas registradas, patentes, licencias de código fuente, etc. de sistemas, recursos y desarrollos de Chemsupply.

46. Los datos personales (de colaboradores, clientes, proveedores) deben estar debidamente protegidos en todos los ambientes dónde residan, a fin de reducir los riesgos asociados a accesos indebidos, mal uso o divulgación no autorizada, etc.

47. Todos los colaboradores de Chemsupply deben recibir capacitación en materia de Seguridad de la Información, como parte de un Programa de Concientización, el cual deberá ser de carácter obligatorio.

48. Asimismo, cuando sea relevante, los terceros también deben recibir capacitación en materia de Seguridad de la Información.

49. Se deberá incluir como parte del proceso de inducción de todo nuevo colaborador, una capacitación de Seguridad de la Información.

50. Todo incidente de seguridad de la información deberá ser reportado y escalado, para investigar la causa y definir las acciones correctivas

51. Se deberán realizar copias de respaldo de la información del negocio de forma periódica, a fin de minimizar la pérdida de información crítica ante alguna contingencia o incidencia.

Todo esto en un marco de mejora continua de la eficacia de nuestro sistema de gestión de la calidad, gestión de seguridad y salud ocupacional y gestión ambiental.

Villa el Salvador, 25 de enero 2024