Dequimsa
PINTURAS

POLÍTICA DE CIBERSEGURIDAD

DPQ-015, Rev 0, 15-feb-2026

CONTENIDO

		Página
1.	Objetivo	3
2.	Alcance	3
3.	Principios de ciberseguridad	3
4.	Compromisos de la organización	5
5.	Responsabilidades	6
6.	Controles de ciberseguridad	8
7.	Gestión de incidentes de ciberseguridad	10
8.	Capacitación y concientización	11
9.	Reporte de incumplimientos y denuncias	12
10.	Cumplimiento y consecuencias	12
11.	Revisión, aprobación y vigencia	13
12.	Tabla de cambios	13

1. OBJETIVO

Establecer los principios y lineamientos para proteger la información y los recursos tecnológicos de Desarrollos Químicos Mundiales S.A. de C.V. (Pinturas Dequimsa) contra accesos no autorizados, pérdida, alteración, divulgación, uso indebido, interrupciones y otras amenazas de ciberseguridad.

La presente política tiene como finalidad preservar la confidencialidad, integridad y disponibilidad de la información, así como promover una cultura de prevención y responsabilidad en materia de ciberseguridad entre el personal, contratistas, proveedores y demás personas que tengan acceso a la información o a los recursos tecnológicos de la organización.

2. ALCANCE

Esta política aplica a todo el personal de Desarrollos Químicos Mundiales S.A. de C.V. (Pinturas Dequimsa), así como a contratistas, proveedores, prestadores de servicios y terceros que, por motivo de sus actividades, tengan acceso a información, sistemas, equipos, redes, aplicaciones o cualquier otro recurso tecnológico de la organización.

Su aplicación comprende, entre otros:

- Información física y electrónica generada, recibida, procesada o almacenada por la organización.
- Computadoras, servidores, dispositivos móviles y demás equipos de cómputo.
- Redes, sistemas, aplicaciones, plataformas y servicios tecnológicos.
- Correo electrónico, servicios de almacenamiento y herramientas de colaboración.
- Dispositivos de almacenamiento externo y medios removibles.
- Información relacionada con clientes, proveedores, personal, productos, procesos, calidad, producción, mantenimiento, laboratorio, seguridad, medio ambiente y el Sistema de Gestión.
- Información y recursos tecnológicos proporcionados por terceros cuando sean utilizados para actividades de la organización.

El cumplimiento de esta política es obligatorio de acuerdo con las responsabilidades y nivel de acceso que correspondan a cada persona.Esta política no forma parte del contrato de trabajo de ningún empleado y podemos modificarla en cualquier momento. La ignorancia o la mala interpretación de las reglas no es excusa para su violación.

3. PRINCIPIOS DE CIBERSEGURIDAD

La ciberseguridad en Desarrollos Químicos Mundiales S.A. de C.V. (Pinturas Dequimsa) se fundamenta en los siguientes principios:

3.1 Confidencialidad

La información deberá ser protegida contra accesos, divulgación o utilización no autorizados, permitiendo su acceso únicamente a las personas que cuenten con la autorización correspondiente y lo requieran para el desarrollo de sus funciones.

3.2 Integridad

La información deberá mantenerse completa, exacta y protegida contra modificaciones, alteraciones o destrucciones no autorizadas, procurando que los datos utilizados para la operación y toma de decisiones sean confiables.

3.3 Disponibilidad

Los sistemas, equipos y la información deberán mantenerse disponibles para las personas autorizadas cuando sean necesarios para realizar las actividades de la organización, considerando medidas para prevenir y recuperar la información ante fallas o incidentes.

3.4 Acceso basado en responsabilidades

Los accesos a información, sistemas y recursos tecnológicos deberán otorgarse de acuerdo con las funciones y responsabilidades de cada usuario, evitando accesos innecesarios o superiores a los requeridos para el desempeño de sus actividades.

3.5 Prevención y gestión de riesgos

La organización promoverá la identificación, evaluación y tratamiento de los riesgos que puedan afectar la información y los recursos tecnológicos, priorizando medidas preventivas para reducir la probabilidad y el impacto de incidentes de ciberseguridad.

3.6 Uso responsable de los recursos tecnológicos

Los recursos tecnológicos proporcionados por la organización deberán utilizarse de manera responsable, segura y exclusivamente para actividades autorizadas, de acuerdo con las funciones del usuario y los lineamientos establecidos.

3.7 Responsabilidad compartida

La ciberseguridad es responsabilidad de todas las personas que tengan acceso a la información o a los recursos tecnológicos de la organización. Cada usuario deberá contribuir a la protección de la información y reportar oportunamente cualquier situación que pueda representar un riesgo o incidente.

3.8 Mejora continua

La organización promoverá la revisión y mejora continua de sus medidas de ciberseguridad, considerando los cambios tecnológicos, nuevos riesgos, incidentes ocurridos, requisitos aplicables y necesidades de la organización. Trata de personas: es el delito que, por medio de la captación, el transporte, el traslado, la acogida o la recepción de personas, recurriendo a la amenaza o al uso de la fuerza, explota a mujeres, niños y hombres con numerosos propósitos, incluidos el trabajo forzoso y la explotación sexual.

4. COMPROMISOS DE LA ORGANIZACIÓN

Desarrollos Químicos Mundiales S.A. de C.V. (Pinturas Dequimsa) establece los siguientes compromisos para proteger la información y los recursos tecnológicos necesarios para el desarrollo de sus actividades:

4.1 Identificar y evaluar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información y de los recursos tecnológicos de la organización.

4.2 Implementar y mantener medidas de seguridad acordes con los riesgos identificados, las necesidades de la organización y los recursos disponibles.

4.3 Proteger la información contra accesos, divulgación, modificación, pérdida, destrucción o uso no autorizado.

4.4 Establecer mecanismos para controlar y administrar los accesos a sistemas, equipos, aplicaciones e información, de acuerdo con las funciones y responsabilidades de cada usuario.

4.5 Mantener medidas para prevenir, detectar, atender y recuperar la información y los recursos tecnológicos ante incidentes de ciberseguridad, fallas o interrupciones.

4.6 Mantener respaldos de la información que, de acuerdo con su importancia y nivel de riesgo, sean necesarios para apoyar la continuidad de las actividades de la organización.

4.7 Promover la identificación y atención oportuna de vulnerabilidades, amenazas y situaciones que puedan comprometer la seguridad de la información.

4.8 Proporcionar capacitación y concientización al personal sobre el uso seguro de la información y de los recursos tecnológicos, de acuerdo con sus funciones y nivel de acceso.

4.9 Establecer medidas de seguridad aplicables a proveedores, contratistas y terceros que tengan acceso a información o recursos tecnológicos de la organización, de acuerdo con los riesgos asociados.

4.10 Cumplir con los requisitos legales, reglamentarios, contractuales y otros requisitos aplicables relacionados con la seguridad y protección de la información.

4.11 Investigar y gestionar los incidentes de ciberseguridad de manera oportuna, estableciendo las acciones necesarias para contener sus efectos, recuperar la operación y prevenir su recurrencia.

4.12 Revisar periódicamente esta política y las medidas de seguridad implementadas, considerando cambios en los procesos, tecnologías, amenazas, riesgos e incidentes ocurridos, con el propósito de promover la mejora continua.

4.13 Proporcionar los recursos necesarios, dentro de las posibilidades de la organización, para mantener y mejorar las medidas de seguridad de la información.

5. RESPONSABILIDADES

La protección de la información y de los recursos tecnológicos es responsabilidad de todas las personas que tengan acceso a ellos. Las responsabilidades se establecen de acuerdo con las funciones y el nivel de autoridad de cada puesto.

5.1 Dirección

Corresponde a la Dirección:

a) Aprobar la Política de Ciberseguridad y proporcionar el respaldo necesario para su implementación.
b) Promover una cultura organizacional orientada a la protección de la información y la gestión de los riesgos de ciberseguridad.
c) Proporcionar, de acuerdo con las necesidades y posibilidades de la organización, los recursos necesarios para implementar y mantener las medidas de seguridad.
d) Revisar los resultados relevantes relacionados con la gestión de riesgos e incidentes de ciberseguridad y apoyar la toma de decisiones correspondientes.

5.2 Responsable de Tecnologías de la Información

Corresponde al responsable de las tecnologías de la información:

a) Implementar y mantener las medidas técnicas de seguridad definidas por la organización.
b) Administrar los accesos a sistemas, equipos, aplicaciones y recursos tecnológicos de acuerdo con las autorizaciones establecidas.
c) Mantener actualizados los sistemas, aplicaciones y mecanismos de protección tecnológica, de acuerdo con las necesidades y riesgos identificados.
d) Coordinar la realización y recuperación de los respaldos de información establecidos por la organización.
e) Monitorear, atender y dar seguimiento a eventos e incidentes relacionados con la seguridad de los recursos tecnológicos.
f) Mantener identificados los activos tecnológicos bajo su responsabilidad y apoyar la evaluación de los riesgos asociados.
g) Coordinar, cuando sea necesario, la atención de incidentes con proveedores externos o especialistas.

5.3 Responsables de los procesos

Corresponde a los responsables de los procesos:

a) Identificar la información y los recursos tecnológicos utilizados en sus procesos que sean relevantes para la operación.
b) Determinar y comunicar las necesidades de acceso de los usuarios bajo su responsabilidad.
c) Informar oportunamente los cambios de puesto, bajas, movimientos o modificaciones de funciones que requieran ajustar los accesos a información y sistemas.
d) Participar en la identificación y evaluación de los riesgos de ciberseguridad relacionados con sus procesos.
e) Asegurar que el personal bajo su responsabilidad conozca y cumpla los lineamientos aplicables de ciberseguridad.
f) Reportar oportunamente cualquier incidente, vulnerabilidad o situación que pueda comprometer la seguridad de la información o los recursos tecnológicos.

5.4 Personal, contratistas y terceros

Toda persona que tenga acceso a información o recursos tecnológicos de la organización deberá:

a) Cumplir esta política y los procedimientos, instructivos y demás lineamientos de seguridad que le sean aplicables.
b) Utilizar de manera responsable los equipos, sistemas, cuentas, aplicaciones y demás recursos tecnológicos proporcionados por la organización.
c) Proteger sus credenciales de acceso y evitar compartir contraseñas, cuentas o mecanismos de autenticación.
d) Evitar acceder, copiar, modificar, divulgar o utilizar información para fines distintos a los autorizados.
e) Mantener bajo su responsabilidad los equipos, documentos y medios de almacenamiento que le sean asignados.
f) Reportar inmediatamente cualquier incidente, comportamiento inusual, pérdida de información, equipo, credenciales o cualquier situación que pueda representar un riesgo de ciberseguridad.
g) Participar en las actividades de capacitación y concientización que la organización establezca.

5.5 Recursos Humanos

Corresponde a Recursos Humanos:

a) Apoyar la comunicación de las responsabilidades de ciberseguridad aplicables al personal desde su incorporación a la organización.
b) Informar oportunamente al responsable de Tecnologías de la Información y a los responsables correspondientes sobre las altas, bajas o cambios de puesto que puedan requerir la creación, modificación o cancelación de accesos.
c) Apoyar la coordinación de las actividades de capacitación y concientización en materia de ciberseguridad.

5.6 Responsable del Sistema de Gestión

Cuando corresponda dentro de sus funciones, el responsable del Sistema de Gestión deberá:

a) Promover la integración de los requisitos y controles de seguridad de la información con los procesos del Sistema de Gestión de la organización.
b) Apoyar la identificación, evaluación y seguimiento de los riesgos relacionados con la seguridad de la información.
c) Dar seguimiento a las acciones de mejora derivadas de incidentes, evaluaciones, auditorías o revisiones relacionadas con la ciberseguridad.

5.7 Proveedores y prestadores de servicios tecnológicos

Los proveedores y prestadores de servicios que tengan acceso a información, sistemas o recursos tecnológicos de la organización deberán cumplir con los requisitos de seguridad establecidos por Dequimsa de acuerdo con la naturaleza del servicio y los riesgos asociados.

Cuando corresponda, dichos requisitos deberán establecerse mediante contratos, acuerdos, procedimientos u otros medios documentados. El Departamento de Recursos Humanos es el responsable de difundir esta política, a través de la entrega del documento físico a todos los colaboradores que ingresen a Desarrollos Químicos Mundiales, S.A. de C.V.

6. CONTROLES DE CIBERSEGURIDAD

Con el propósito de proteger la información y los recursos tecnológicos de la organización, se establecen los siguientes controles y lineamientos de ciberseguridad, los cuales deberán aplicarse de acuerdo con los riesgos identificados, la naturaleza de la información y las funciones de cada usuario.

6.1 Gestión de accesos

a) Los accesos a sistemas, aplicaciones, equipos, redes e información deberán otorgarse únicamente a las personas que los requieran para el desempeño de sus funciones.
b) Los permisos de acceso deberán corresponder al nivel de responsabilidad y necesidad de cada usuario.
c) Las cuentas de usuario deberán ser personales e intransferibles. No deberán compartirse contraseñas, cuentas o mecanismos de autenticación.
d) Los accesos deberán ser modificados o cancelados oportunamente cuando existan cambios de puesto, funciones o relación laboral o contractual.
e) Los accesos con privilegios administrativos deberán limitarse a las personas autorizadas y utilizarse únicamente cuando sean necesarios.

6.2 Contraseñas y autenticación

a) Los usuarios deberán utilizar contraseñas seguras y mantenerlas bajo su control.
b) Las contraseñas no deberán compartirse, anotarse en lugares visibles ni almacenarse de manera que puedan ser utilizadas por personas no autorizadas.
c) Cuando los sistemas disponibles lo permitan, deberán utilizarse mecanismos adicionales de autenticación, particularmente para accesos a información o sistemas de mayor riesgo.
d) Ante la sospecha de que una contraseña o mecanismo de autenticación haya sido comprometido, el usuario deberá reportarlo y realizar el cambio correspondiente de manera inmediata.

6.3 Uso de equipos y dispositivos

a) Los equipos y dispositivos proporcionados por la organización deberán utilizarse de manera responsable y segura.
b) Los usuarios deberán proteger los equipos bajo su responsabilidad contra pérdida, robo, acceso no autorizado o uso indebido.
c) No deberán instalarse programas, aplicaciones o herramientas que no hayan sido autorizados.
d) Los equipos deberán mantenerse con las medidas de seguridad y actualizaciones establecidas por el responsable de Tecnologías de la Información.
e) Los dispositivos personales que requieran conectarse a recursos de la organización deberán cumplir con los requisitos de seguridad establecidos para dicho acceso.

6.4 Correo electrónico, internet y comunicaciones digitales

a) El correo electrónico y los servicios de comunicación proporcionados por la organización deberán utilizarse de manera responsable y segura.
b) Los usuarios deberán verificar cuidadosamente el remitente, enlaces, archivos adjuntos y solicitudes inusuales recibidas por medios electrónicos.
c) No deberán abrirse archivos, enlaces o mensajes que presenten características sospechosas o que puedan representar un riesgo de seguridad.
d) Los usuarios deberán reportar mensajes sospechosos, intentos de fraude, suplantación de identidad o posibles campañas de phishing.

e) La información confidencial de la organización deberá compartirse únicamente mediante medios autorizados y con las personas que correspondan.

6.5 Software y dispositivos de almacenamiento

a) Únicamente deberá utilizarse software autorizado por la organización.
b) La instalación, modificación o eliminación de software en equipos administrados por la organización deberá realizarse de acuerdo con las autorizaciones y controles establecidos.
c) El uso de dispositivos de almacenamiento externo, como memorias USB, discos externos u otros medios removibles, deberá realizarse de manera controlada y considerando los riesgos asociados.
d) Cuando sea técnicamente posible, los medios de almacenamiento externos deberán ser analizados antes de utilizarse en equipos de la organización.

6.6 Protección y manejo de la información

a) La información deberá ser identificada y protegida de acuerdo con su importancia, sensibilidad y nivel de riesgo.
b) La información confidencial o de acceso restringido deberá mantenerse únicamente en medios y ubicaciones autorizados.
c) Los usuarios deberán evitar dejar información sensible expuesta en escritorios, pantallas, impresoras, equipos o espacios accesibles a personas no autorizadas.
d) La información deberá eliminarse o desecharse mediante métodos adecuados cuando haya concluido su periodo de conservación o cuando ya no sea necesaria, de acuerdo con los lineamientos aplicables.
e) La información de clientes, proveedores, personal, productos, procesos, fórmulas, laboratorio, calidad, producción, mantenimiento y demás información propiedad de la organización deberá utilizarse únicamente para fines autorizados.

6.7 Respaldos y recuperación de información

a) La organización deberá establecer mecanismos de respaldo para la información que, de acuerdo con su importancia y nivel de riesgo, requiera protección ante pérdida, daño, eliminación o indisponibilidad.
b) Los respaldos deberán protegerse contra accesos, modificaciones o destrucción no autorizados.
c) De acuerdo con el nivel de riesgo, deberán realizarse verificaciones de los respaldos para confirmar su disponibilidad y posibilidad de recuperación.
d) Cuando sea necesario, deberán establecerse mecanismos para recuperar la información y restablecer los servicios tecnológicos afectados por una falla o incidente.

6.8 Actualizaciones y protección contra software malicioso

a) Los equipos y sistemas deberán mantenerse protegidos mediante las herramientas de seguridad definidas por la organización.
b) Las actualizaciones de seguridad deberán aplicarse de acuerdo con las necesidades, riesgos y capacidades de los sistemas.
c) Los usuarios no deberán desactivar, modificar o evadir las medidas de seguridad instaladas en los equipos sin autorización.
d) Cualquier comportamiento inusual del equipo, detección de software malicioso o alerta de seguridad deberá ser reportado oportunamente.

6.9 Trabajo remoto y acceso externo

a) Cuando se autorice el trabajo remoto o el acceso a recursos de la organización desde ubicaciones externas, deberán utilizarse los mecanismos de seguridad establecidos.
b) Los usuarios deberán evitar utilizar redes públicas o dispositivos no confiables para acceder a información sensible, cuando existan alternativas seguras.
c) La información de la organización deberá mantenerse protegida durante su acceso, transferencia y almacenamiento fuera de las instalaciones.
d) Los equipos utilizados para trabajo remoto deberán mantenerse bajo condiciones razonables de seguridad y protección física.

6.10 Proveedores y terceros

a) Los proveedores, contratistas y terceros que tengan acceso a información o recursos tecnológicos deberán cumplir con los requisitos de seguridad establecidos por la organización.
b) Los accesos otorgados a terceros deberán limitarse al tiempo, sistemas e información necesarios para la prestación del servicio.
c) Los accesos deberán cancelarse cuando concluya la relación contractual o deje de existir la necesidad que los originó.
d) Cuando el nivel de riesgo lo requiera, deberán establecerse requisitos específicos de seguridad mediante contratos, acuerdos u otros documentos aplicables. Cualquier empleado que infrinja esta política se enfrentará a medidas disciplinarias, que podrían dar como resultado el fin de la relación laboral por mala conducta o falta grave.

7. GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

Desarrollos Químicos Mundiales S.A. de C.V. (Pinturas Dequimsa) deberá mantener un enfoque organizado para la identificación, reporte, atención, recuperación y seguimiento de los incidentes que puedan comprometer la seguridad de la información o de los recursos tecnológicos.

7.1 Todo el personal, contratista o tercero que tenga conocimiento de un posible incidente de ciberseguridad deberá reportarlo oportunamente al departamento de Recursos Humanos, ya sea de manera presencial, por teléfono o cualquier otro medio autorizado por la organización.

7.2 Se considerarán incidentes o posibles incidentes de ciberseguridad, entre otros:

a) Acceso no autorizado a información, sistemas, equipos o cuentas.
b) Pérdida, robo o extravío de equipos o medios que contengan información de la organización.
c) Divulgación, modificación o eliminación no autorizada de información.
d) Recepción de mensajes, enlaces o archivos que puedan representar intentos de fraude, suplantación de identidad o software malicioso.
e) Detección de software malicioso, comportamiento inusual o alertas de seguridad en los equipos o sistemas.
f) Uso indebido o sospechoso de cuentas, credenciales o recursos tecnológicos.
g) Interrupciones o fallas que afecten la disponibilidad de información o servicios tecnológicos.
h) Cualquier otra situación que pueda comprometer la confidencialidad, integridad o disponibilidad de la información.

7.3 Los incidentes deberán ser evaluados de acuerdo con su naturaleza, alcance e impacto, con el propósito de determinar las acciones necesarias para contenerlos, reducir sus efectos y recuperar la operación.

7.4 Durante la atención de un incidente, deberán preservarse, cuando sea posible y pertinente, los elementos o evidencias que permitan determinar su origen, alcance y consecuencias.

7.5 Cuando la naturaleza o gravedad del incidente lo requiera, la organización podrá solicitar el apoyo de proveedores especializados, autoridades competentes u otras partes pertinentes.

7.6 Los incidentes relevantes deberán documentarse y, cuando corresponda, deberán establecerse acciones para corregir las causas identificadas y prevenir su recurrencia.

7.7 La información relacionada con los incidentes deberá manejarse de manera confidencial y únicamente deberá ser compartida con las personas que tengan autorización o necesidad legítima de conocerla.

7.8 Los incidentes de ciberseguridad deberán considerarse como una fuente de información para la identificación de riesgos y para la mejora continua de las medidas de seguridad de la organización.

8. CAPACITACIÓN Y CONCIENTIZACIÓN

Desarrollos Químicos Mundiales S.A. de C.V. (Pinturas Dequimsa) promoverá la capacitación y concientización del personal, contratistas y terceros que tengan acceso a información o recursos tecnológicos de la organización, con el propósito de fortalecer una cultura de prevención y uso responsable de la información.

8.1 El personal deberá recibir información y capacitación sobre los principios, responsabilidades y lineamientos de ciberseguridad que sean aplicables a sus funciones y nivel de acceso.

8.2 Las actividades de capacitación y concientización podrán incluir, entre otros temas:

a) Protección y manejo adecuado de la información.
b) b) Uso seguro de contraseñas y mecanismos de autenticación.
c) Identificación de correos, mensajes, enlaces y archivos sospechosos.
d) Prevención de fraudes y suplantación de identidad.
e) Uso seguro de equipos, dispositivos y medios de almacenamiento.
f) Reporte oportuno de incidentes y situaciones de riesgo.
g) Uso responsable de los recursos tecnológicos de la organización.
h) Responsabilidades derivadas de esta política.

8.3 Las actividades de capacitación deberán considerar, cuando corresponda, las funciones, responsabilidades, nivel de acceso y riesgos asociados a los diferentes puestos.

8.4 Los nuevos colaboradores deberán recibir información sobre los lineamientos de ciberseguridad aplicables a sus funciones como parte de su incorporación a la organización, de acuerdo con los mecanismos establecidos internamente.

8.5 La organización podrá realizar actividades periódicas de concientización para reforzar buenas prácticas y mantener al personal informado sobre amenazas, riesgos o situaciones relevantes de ciberseguridad.

8.6 Los contratistas y terceros deberán recibir o conocer los lineamientos de ciberseguridad que les sean aplicables antes de acceder a información o recursos tecnológicos de la organización, cuando corresponda.

8.7 Recursos Humanos, en coordinación con los responsables correspondientes, apoyará la planeación y seguimiento de las actividades de capacitación y concientización en materia de ciberseguridad.

8.8 El personal deberá participar en las actividades de capacitación y concientización que sean establecidas por la organización y aplicar los conocimientos adquiridos en el desempeño de sus funciones. Ley Federal para Prevenir y Eliminar la Discriminación.

9. REPORTE DE INCUMPLIMIENTO Y DENUNCIAS

Desarrollos Químicos Mundiales S.A. de C.V. (Pinturas Dequimsa) establecerá medios para que el personal, contratistas y terceros puedan comunicar de manera oportuna cualquier incumplimiento, conducta o situación que contravenga la presente Política de Ciberseguridad.

9.1 Todo el personal, contratista o tercero podrá reportar cualquier incumplimiento a la presente política cuando tenga conocimiento de una situación que pueda poner en riesgo la seguridad de la información o el uso adecuado de los recursos tecnológicos de la organización.

9.2 Los reportes podrán realizarse al departamento de Recursos Humanos, de manera presencial, por teléfono o mediante cualquier otro medio de comunicación autorizado por la organización.

9.3 Los reportes deberán ser tratados de manera confidencial y con respeto a las personas involucradas, procurando que la información sea conocida únicamente por quienes requieran intervenir en su atención.

9.4 La organización analizará los reportes recibidos y, cuando corresponda, determinará las acciones necesarias para su atención, incluyendo la participación de las áreas responsables o de personal especializado.

9.5 Cuando el incumplimiento reportado pueda constituir un incidente de ciberseguridad, se deberá atender adicionalmente conforme a lo establecido en el apartado 7 de la presente política.

9.6 No se deberán tomar represalias contra las personas que, de buena fe, comuniquen un posible incumplimiento o situación que pueda afectar la seguridad de la información.

9.7 Cuando corresponda, los incumplimientos podrán dar lugar a acciones de mejora, capacitación, medidas correctivas o las acciones administrativas aplicables de acuerdo con las disposiciones internas de la organización

10.CUMPLIMIENTO Y CONSECUENCIAS

El cumplimiento de la presente Política de Ciberseguridad es obligatorio para el personal, contratistas, proveedores y terceros a quienes les sea aplicable, de acuerdo con sus responsabilidades y nivel de acceso a la información y recursos tecnológicos de Desarrollos Químicos Mundiales S.A. de C.V. (Pinturas Dequimsa).

10.1 Las personas sujetas a esta política deberán conocer, comprender y cumplir los principios, responsabilidades y lineamientos aplicables a sus actividades.

10.2 El incumplimiento de las disposiciones establecidas en esta política será evaluado de acuerdo con la naturaleza, gravedad, impacto y circunstancias de la situación.

10.3 Cuando corresponda, la organización podrá establecer acciones de corrección, capacitación, restricción o retiro de accesos, medidas administrativas u otras acciones aplicables, de acuerdo con las disposiciones internas vigentes y con las obligaciones contractuales correspondientes.

10.4 Cuando un incumplimiento pueda representar un riesgo significativo para la información o los recursos tecnológicos de la organización, podrán implementarse medidas inmediatas para contener o reducir dicho riesgo.

10.5 Los proveedores, contratistas y terceros que incumplan los requisitos de seguridad que les sean aplicables podrán estar sujetos a las medidas establecidas en los contratos, acuerdos o disposiciones correspondientes.

10.6 La aplicación de medidas derivadas de un incumplimiento deberá realizarse de manera objetiva y proporcional a la situación identificada, procurando prevenir su recurrencia y fortalecer la seguridad de la información.

11.REVISIÓN, APROBACIÓN Y VIGENCIA

11.1 La presente Política de Ciberseguridad será revisada anualmente y, cuando sea necesario, actualizada para asegurar que continúe siendo adecuada a las actividades, necesidades y riesgos de Desarrollos Químicos Mundiales S.A. de C.V. (Pinturas Dequimsa).

11.2 La revisión podrá realizarse cuando se presenten cambios relevantes en la organización, los procesos, los recursos tecnológicos, los requisitos legales o contractuales, las amenazas de ciberseguridad, o cuando los resultados de incidentes, auditorías, evaluaciones o revisiones indiquen la necesidad de realizar modificaciones.

11.3 Las modificaciones a la presente política deberán ser revisadas y aprobadas por la Dirección, de acuerdo con los mecanismos establecidos en el Sistema de Gestión de la organización.

11.4 La política aprobada deberá comunicarse al personal, contratistas y terceros a quienes les sea aplicable, de acuerdo con sus responsabilidades y nivel de acceso a la información y recursos tecnológicos.

11.5 La presente política entrará en vigor a partir de su fecha de aprobación y permanecerá vigente hasta que sea sustituida o cancelada mediante una nueva versión autorizada.

11.6 La versión vigente de esta política será la única reconocida como aplicable dentro de la organización.

12.TABLA DE CAMBIOS

Revisión	Fecha	Modificación
0	15-feb-2026	Emisión del documento

ELABORÓ:	REVISÓ:	AUTORIZÓ:
Recursos Humanos	**Jefe de Sistemas de Gestión de Calidad y Seguridad**	**Director de Operaciones**