COMPLIANCE

DENOMINACIÓN: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CÓD.: GRP-POL-CPL-04

ELABORADO POR:	REVISADO POR:	APROBADO POR:
COMPLIANCE OFFICER	DIRECCIÓN DE SEGURIDAD CORPORATIVA COMITÉ DE CUMPLIMIENTO	PRESIDENCIA – CONSEJO DE ADMINISTRACIÓN

ace
avintia compliance & ethics
management system

CONTROL DE VERSIÓN DEL DOCUMENTO		
Nº	FECHA	CONTROL DE CAMBIOS
v_01	11/11/24	Generación inicial del documento

ÍNDICE

I. OBJETO

La presente Política de Seguridad de la Información (en adelante, también, la "Política") tiene por objeto determinar la posición de Grupo Avintia (en adelante, también, el "Grupo" o la "Organización") y de todas sus sociedades en la protección de la seguridad de la información corporativa, considerada como un activo crítico para la Organización. Desarrolla el apartado "5.8 Seguridad de la información" del Código Ético y de Conducta, y forma parte del sistema ace | avintia compliance & ethics management system.

La información es un activo crítico para todas las sociedades de Grupo Avintia y, por tanto, debe gozar de las medidas de seguridad necesarias para evitar cualquier tipo de amenaza relacionada con fraudes, sabotajes, extorsiones, espionaje industrial, violaciones de intimidad, interrupciones de servicio, desastres naturales o, incluso, errores humanos, entre otros.

La presente Política define las principales pautas para la formulación de procedimientos de seguridad de los sistemas de información, en base a los siguientes pilares:

- La protección de la información permite el desarrollo de las actividades de negocio de Grupo Avintia;
- La información del Grupo debe ser protegida en base a su susceptibilidad, valor y criticidad;
- Todos los empleados y colaboradores tienen la responsabilidad de proteger la información que se les ha confiado;
- Las medidas de protección deben desarrollarse en línea con las correspondientes evaluaciones de riesgo;
- Para determinar qué medidas de protección son necesarias, se deben garantizar los principios generales de seguridad de la información, especialmente la confidencialidad, la integridad y la disponibilidad de la información, y se debe clasificar la misma en distintos niveles (confidencial, restringida, de uso interno y pública).

II. ÁMBITO DE APLICACIÓN

La Política de Seguridad de la Información de Grupo Avintia resulta de aplicación a Corporación Grupo Avintia, S.L. y a todas sus sociedades filiales y mayoritariamente participadas en las que, de forma directa o indirecta, ejerza un control efectivo, así como a la Fundación Avintia.

Quedan, por tanto, obligados a cumplir con las disposiciones de esta Política los administradores, representantes, directivos y empleados de todas las sociedades indicadas,

incluido el personal de empresas externas que presten servicios en las mismas, así como todas las personas vinculadas a la Fundación.

Las uniones temporales de empresas, entidades participadas en las que el Grupo no tenga un control efectivo y demás figuras de colaboración en las que la Compañía sea parte deberán estar alineadas con las pautas de comportamiento establecidas en esta Política.

La presente Política tiene rango de alto nivel, en dependencia directa del Código Ético y de Conducta del Grupo.

III. PRINCIPIOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información de Grupo Avintia se rige por los siguientes principios generales:

- **Confidencialidad**. El acceso a la información del Grupo (servidores, datos, programas informáticos, etc.) solo estará disponible para las personas autorizadas en cada caso. La Organización garantizará el nivel necesario de secreto de la información y de su tratamiento, con el objetivo de prevenir su divulgación no autorizada.

- **Integridad**. La información se almacenará en lugares seguros donde no pueda ser alterada o manipulada, evitando asimismo su pérdida o destrucción, ya sea accidental o intencionada.

- **Disponibilidad**. La información estará disponible para las personas autorizadas en cualquier momento en que la necesiten. La Organización articulará mecanismos de recuperación de la información en caso de incidentes.

- **Autenticidad**. La Organización dispondrá de medidas que permitan garantizar la autoría de la información.

- **Resiliencia**. El Grupo implementará planes de contingencia, continuidad de negocio y recuperación ante desastres que le permitan resistir y recuperarse frente a cualquier imprevisto, evento o perturbación que pueda afectar a la seguridad de su información y a sus actividades.

- **Universalidad**. La presente política resultará de aplicación en todos los estadios por los que pasa la información (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción) y en todos los sistemas de procesamiento de la información (análisis, diseño, desarrollo, implantación, explotación y mantenimiento).

- **Responsabilidad**. La seguridad de la información es responsabilidad de todas las personas de Grupo Avintia. Todos los empleados, directivos, administradores,

proveedores, colaboradores y terceras partes con las que se relaciona la Organización deberán conocer, cumplir, respetar y aplicar la Política en toda su extensión.

- **Control de terceros**. Los terceros ajenos a la Organización que accedan a la información del Grupo serán sometidos a las medidas necesarias que garanticen el cumplimiento de los principios anteriores.

- **Desarrollo**. Las medidas, directrices y contenidos de esta Política podrán desarrollarse en procedimientos y procesos que garanticen su operatividad, siempre y cuando se revisen y aprueben por las mismas vías.

- **Legalidad**. Sin perjuicio de lo dispuesto en los puntos anteriores, la Organización cumplirá con toda la normativa de aplicación en materia de seguridad de la información a nivel comunitario, nacional y autonómico.

IV. CLASIFICACIÓN DE LA INFORMACIÓN

La Política de Seguridad de la Información, sus procedimientos, procesos y medidas de desarrollo estarán encaminados a salvaguardar la confidencialidad de la información frente al posible acceso de terceros no autorizados. Este compromiso de confidencialidad viene determinado por la clasificación de la información en cuatro niveles:

NIVEL DE CONFIDENCIALIDAD	CLASIFICACIÓN
Alto	Confidencial
Medio	Restringida
Bajo	De uso interno
N/A	Pública

La clasificación de las distintas categorías de información de Grupo Avintia en cada uno de estos niveles se determinará en el procedimiento correspondiente. Dicho procedimiento incluirá, además, las medidas de seguridad adecuadas de aplicación para cada categoría.

V. USO DE RECURSOS DIGITALES Y DISPOSITIVOS ELECTRÓNICOS CORPORATIVOS

El uso de los recursos digitales y dispositivos electrónicos corporativos está sujeto a las siguientes normas y limitaciones:

- Los recursos digitales y dispositivos electrónicos que la Organización pone a disposición de sus empleados, directivos y otros profesionales son propiedad de la Organización. El uso de estos recursos y dispositivos está limitado únicamente a las tareas profesionales propias del puesto de trabajo o del servicio prestado, prohibiéndose su utilización para otros fines, como pueden ser: actividades particulares, comerciales, causas religiosas o políticas, trabajos independientes o cualquier otra actividad no relacionada con Grupo Avintia o sus sociedades, entre otros.

- A título enunciativo, pero no limitativo, se entienden por:

    - "**Recursos digitales**": cualquier elemento que esté en formato digital y que se pueda visualizar y almacenar en un dispositivo electrónico, y que pueda ser consultado de manera directa o por acceso a la red. A título ejemplificativo, pero no limitativo, son recursos digitales: la cuenta corporativa de correo electrónico, internet, las aplicaciones corporativas, los sistemas de comunicación electrónica y los servidores virtuales corporativos, entre otros.

    - "**Dispositivos electrónicos**": artefactos que utilizan componentes electrónicos organizados en circuitos y que realizan la función de controlar y aprovechar las señales eléctricas con la finalidad de realizar algún proceso informático. A título ejemplificativo, pero no limitativo, son dispositivos electrónicos: teléfonos móviles corporativos, ordenadores corporativos y televisores corporativos, entre otros.

- La Organización podrá supervisar, monitorizar, controlar y acceder a los recursos digitales y dispositivos electrónicos corporativos sin necesidad de previo aviso. Las evidencias podrán ser registradas y conservadas. Para ello, la Organización deberá cumplir con el procedimiento establecido al efecto, respetando los principios de idoneidad, necesidad y proporcionalidad, el derecho a la intimidad personal y el derecho a la protección de datos personales.

- El uso de los recursos digitales y los dispositivos electrónicos corporativos para fines ajenos a la actividad profesional podrá ser sancionado de conformidad con la normativa laboral y colectiva de aplicación, así como el procedimiento sancionador.

- Cualquier duda relacionada con el uso de los recursos digitales y dispositivos electrónicos se podrá dirigir al Departamento de Seguridad Corporativa o al

Departamento de Compliance, quienes realizarán las comprobaciones oportunas y aprobarán o denegarán el uso, según proceda.

VI. USO DE INTERNET

Internet es una vía estratégica para la consecución de los objetivos de negocio del Grupo. Por este motivo, la Organización establecerá los medios para su utilización como factor diferenciador que suponga una ventaja competitiva en el sector.

Grupo Avintia establecerá medidas que le permitan hacer frente a los riesgos de diversa índole derivados del uso de internet: revelación, enmascaramiento, acceso no autorizado, pérdida de integridad, denegación de servicio, daños a la imagen del Grupo, sustracción de servicios y recursos, etc.

Internet es un recurso que el Grupo pone a disposición de sus empleados para un uso estrictamente profesional y relacionado con las funciones que desempeñen en la Organización. El Grupo se reserva el derecho a tomar medidas disciplinarias o judiciales, si procediera, en el caso de detectar el uso de internet para una finalidad distinta. A estos efectos, el Grupo informa a sus empleados de que el uso de internet estará sujeto a control y monitorización por parte de la Organización.

VII. USO DE CONTRASEÑAS

Todas las personas de Grupo Avintia son responsables de la seguridad de la información corporativa, en sus respectivos ámbitos de actuación.

La Organización asigna identificadores personales únicos y contraseñas para acceder a los diferentes recursos. El usuario autorizado es responsable de todas las acciones que se hayan realizado bajo la utilización de su identificador personal o contraseña. Las contraseñas individuales no deben ser compartidas o reveladas a personas distintas del autorizado.

El usuario autorizado es responsable de la renovación periódica de su contraseña, con el fin de protegerla de su revelación a personas no autorizadas.

VIII. USO DE SOFTWARE AUTORIZADO

Los empleados de Grupo Avintia y los colaboradores autorizados a acceder a sus sistemas solo podrán hacer uso de los programas informáticos, aplicaciones y funcionalidades autorizados por la organización, independientemente del dispositivo corporativo del que se trate (ordenador corporativo, teléfono móvil corporativo, etc.).

Los programas informáticos, aplicaciones y funcionalidades autorizados por la organización deberán utilizarse de conformidad con los términos uso determinados en la licencia correspondiente.

Queda prohibido descargar, instalar y hacer uso de programas informáticos, aplicaciones y funcionalidades no autorizados expresamente por la Organización o sin la licencia debida.

El software debe ser revisado y aprobado para su utilización antes de su instalación en los equipos de Grupo Avintia.

IX. ALMACENAMIENTO DE LA INFORMACIÓN

Las sociedades de Grupo Avintia disponen de servidores de almacenamiento en red. Estos servidores permiten disponer de un lugar de trabajo común donde almacenar la documentación y compartir la información.

Toda la documentación y la información generada durante el desarrollo de las actividades de los empleados es propiedad de la Organización, y por tanto está sujeta a los estándares y medidas de seguridad implementados por el Grupo.

La Organización pondrá en marcha controles adecuados de acceso a la documentación y a la información almacenada en los servidores. Los usuarios solo recibirán permisos de acceso a aquellas carpetas que resulten necesarias para el ejercicio de sus actividades. Cualquier otro tipo de permiso requerirá la aprobación de la Dirección de Seguridad Corporativa, previa justificación debidamente fundamentada por el solicitante. No se concederán permisos universales de acceso a todas las carpetas de los servidores, salvo causa debidamente justificada y sujeta a la aprobación de la Dirección de Seguridad Corporativa.

Como regla general, todos los empleados y colaboradores externos que tengan acceso a las redes corporativas de Grupo Avintia deberán trabajar en el servidor, guardando toda la documentación y la información en esta unidad de red. Se prohíbe el trabajo en la unidad local (escritorio o carpetas locales del disco duro).

Los usuarios no utilizarán dispositivos de almacenamiento externos para guardar información sensible para la Organización, como son los ficheros con datos de carácter personal. El riesgo de pérdida o sustracción de este tipo de información es máximo, y cada empleado es responsable de los datos sensibles que maneja en el ámbito de sus funciones, especialmente los de carácter personal. Asimismo, cualquier información confidencial o interna que se maneje deberá estar especialmente protegida, prohibiéndose asimismo su almacenamiento en dispositivos o servidores externos no autorizados por la Organización.

En aquellos casos en los que no resulte posible trabajar en el servidor o unidad de red corporativa durante la jornada laboral, se deberá archivar toda la documentación e información generada en los servidores en cuanto resulte posible.

Los empleados que trabajen fuera del alcance de los servidores corporativos deben solicitar la habilitación de una red privada virtual o VPN, que les dará acceso a la red corporativa.

La Organización se reserva el derecho a realizar controles aleatorios para verificar el cumplimiento de estas normas.

X. TELETRABAJO

En aquellos casos en los que se autorice el trabajo con acceso remoto (teletrabajo), los empleados deberán seguir las siguientes directrices:

- Los recursos digitales y dispositivos electrónicos facilitados por le Organización serán de uso exclusivo del trabajador y únicamente para el desempeño de sus funciones profesionales.
- El trabajador deberá proteger sus contraseñas de acceso y no compartirlas con ninguna otra persona, ni siquiera con los miembros de su familia.
- Los empleados se comprometen a no realizar actividades delictivas, ilícitas o que supongan incumplimientos del Código Ético y de Conducta o de cualquiera de las políticas de Grupo Avintia.
- Los empleados no utilizarán el acceso remoto para obtener un lucro personal ajeno a la Organización.
- Los empleados deberán proteger el buen funcionamiento del acceso remoto, deshabilitando el mismo al finalizar su jornada.

XI. DESARROLLO, MANTENIMIENTO Y EXPLOTACIÓN DE PROGRAMAS Y SISTEMAS INFORMÁTICOS

El procedimiento que regirá el desarrollo y mantenimiento de programas informáticos estará normalizado y formalizado, contemplando una segregación claramente establecida en cuanto a los distintos entornos que intervienen. Dentro de los procedimientos, se considerará en todo momento la participación activa de los usuarios tanto en la definición de las necesidades como en el desarrollo de las pruebas.

El acceso a la información se realizará sobre la base de las necesidades requeridas para cada uno de los puestos de trabajo desempeñados por los empleados, teniendo en consideración un adecuado nivel de segregación de funciones.

La información generada será protegida del acceso innecesario o no autorizada, por medio de controles que reduzcan el riesgo de utilización inadecuada, robo, alteración o destrucción.

Adicionalmente, Grupo Avintia establecerá normas que eviten la implantación de software ilegal y propiciará medidas concretas relativas a antivirus.

La actualización y modificación de los programas y aplicaciones de las sociedades del Grupo se llevarán a cabo dentro de un marco de controles que aseguren unos niveles adecuados de confidencialidad, integridad y disponibilidad de la información. Se evitarán aquellas actualizaciones que no resulten útiles o seguras.

Grupo Avintia determinará los procedimientos operativos y controles de acceso utilizados en cada momento para proteger el hardware, software y archivos de datos ante un acceso, divulgación, manipulación o destrucción no autorizados.

Los controles implementados en las telecomunicaciones del Grupo garantizarán la confidencialidad, disponibilidad e integridad en la transmisión a fin de prevenir que dicha información sea interceptada y manipulada por un tercero.

Las medidas implementadas estarán encaminadas al control de la información, del canal de transmisión y de las propias personas que intervienen a lo largo del proceso.

XII. ACUERDOS Y CLÁUSULAS DE CONFIDENCIALIDAD

Cualquier persona física o jurídica que vaya a disponer de acceso a información confidencial, restringida o de uso interno de Grupo Avintia deberá firmar previamente el acuerdo de confidencialidad o cláusula contractual correspondiente, extendido por la persona autorizada para habilitar dicho acceso.

El acuerdo o cláusula deberá definir de forma clara y exhaustiva las obligaciones y responsabilidades asumidas por el firmante a la hora de acceder a la información corporativa de la Organización.

Se incluyen en este punto los encargos de tratamiento de datos de carácter personal.

XIII. SERVICIOS DE OUTSOURCING

La Organización llevará a cabo una adecuada supervisión de todas las actividades que hayan sido externalizadas en terceras partes, al objeto de minimizar los riesgos derivados de estas operaciones (incumplimientos, pérdida de control, limitaciones de acceso, dificultades para implementar cambios, etc.).

De forma previa a la firma de estos contratos, el Grupo realizará la verificación y adecuación, si procede, de su clausulado en materia de confidencialidad y protección de datos, con el objeto de garantizar un nivel apropiado de seguridad de la información.

XIV. INCIDENTES Y BRECHAS DE SEGURIDAD

Un incidente de seguridad es cualquier evento que pueda afectar a la integridad, la confidencialidad o la disponibilidad de los datos o sistemas de la Organización. Puede tener un origen accidental o intencionado.

Una brecha de seguridad es un incidente de seguridad que afecta a datos de carácter personal. En general, se trata de un suceso que ocasiona la destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.

Todo el personal de Grupo Avintia es responsable de informar de cualquier incidente o brecha de seguridad al Departamento de Compliance, desde donde se coordinarán las actividades de respuesta.

XV. CONTROL DE FUGAS DE INFORMACIÓN

Grupo Avintia ha habilitado soluciones DLP (“Data Loss Prevention”) con la finalidad de identificar, monitorizar, detectar y prevenir la fuga de información considerada como confidencial, así como su uso no autorizado.

Este tipo de soluciones permiten prevenir las fugas o sustracciones de información a través de la identificación, monitorización y protección de los datos en uso, en movimiento o en reposo mediante técnicas de “deep packet inspection”, monitorización de sesiones, técnicas estadísticas y lingüísticas de análisis, monitorización del tráfico de red y análisis de seguridad contextual de las transacciones, junto con una definición centralizada de las políticas de detección, borrado o control de uso basadas en el contenido de la información.

XVI. FORMACIÓN Y CONCIENCIACIÓN

Grupo Avintia llevará a cabo acciones formativas encaminadas a garantizar que todos sus empleados conocen y aplican los principios básicos y medidas de seguridad de la información, profundizando en sus obligaciones y responsabilidades en este ámbito.

Todos los empleados convocados estarán obligados a completar estas acciones formativas en los plazos establecidos por la Organización.

XVII. ALTAS Y BAJAS DE EMPLEADOS

- **Alta de nuevos empleados**

Las altas de nuevos empleados en cualquiera de las sociedades de Grupo Avintia se llevarán a cabo de conformidad con el procedimiento específico establecido al efecto.

- **Baja de empleados**

Las bajas de empleados en cualquiera de las sociedades de Grupo Avintia se tramitarán de conformidad con el procedimiento específico establecido al efecto.

La gestión de los correos electrónicos de los empleados que causa baja se llevará a cabo de conformidad con las siguientes directrices:

1) Se deberá crear un mensaje de respuesta automática previo al bloqueo de la cuenta, informando acerca de la baja de su titular, y aportando una nueva dirección de contacto a la que remitir los correos electrónicos. Salvo causa debidamente justificada, los correos electrónicos no serán redireccionados.

2) Los correos necesarios para garantizar la adecuada continuidad de las actividades solo se podrán recuperar con carácter previo a la partida del empleado y en su presencia, salvo que la Organización y el empleado firmen un acuerdo expreso por el que este último otorgue su autorización para el acceso posterior a su baja. El acuerdo deberá especificar una fecha máxima para efectuar los accesos.

3) El día de la partida del empleado, su cuenta deberá de ser bloqueada, manteniendo el mensaje de respuesta automática. El período de bloqueo será de un mes, ampliable a tres por causa justificada y comunicada al ex trabajador.

4) Transcurrido el periodo de bloqueo, la cuenta deberá de ser eliminada.

No se autorizará ningún acceso a correos de ex empleados si no se cumplen los requisitos indicados.

XVIII. AUDITORÍAS

Con el fin de garantizar el cumplimiento de la presente Política, la Organización se reserva el derecho a realizar auditorías periódicas, llevando a cabo controles aleatorios para comprobar el nivel de almacenamiento en las redes locales, estadísticas de uso, accesos de usuarios, etc.

Todos los empleados del Grupo están obligados a colaborar si son requeridos en el ámbito de estas auditorías.

XIX. CUMPLIMIENTO Y VIGENCIA

Incumplimiento de la Política de Seguridad de la Información

Grupo Avintia espera que todos sus miembros actúen con absoluto respeto a las disposiciones contenidas en la presente Política, teniéndola siempre presente en el desempeño de sus actividades profesionales, y planteando al Compliance Officer cuantas cuestiones les suscite su aplicación en el día a día.

El incumplimiento de cualquiera de los preceptos contenidos en esta Política podrá dar lugar a la imposición por la Dirección de las sanciones disciplinarias que legal, reglamentaria o colectivamente se determinen, sin perjuicio de otras responsabilidades en que pudiera incurrir la persona incumplidora: penales, civiles, administrativas, etc.; y de las que responderá directa y personalmente, en su caso.

Informar de irregularidades: Canal ¡Dilo!

Grupo Avintia pone a disposición de todos sus miembros el Canal ¡Dilo! para que puedan comunicar al Comité de Cumplimiento cualquier irregularidad o acto contrario a la presente Política. El Canal ¡Dilo! garantiza la confidencialidad, la posibilidad de anonimato y la ausencia de represalias contra los denunciantes de buena fe.

https://grupoavintia.canaldenunciasanonimas.com/home

Entrada en vigor, actualización y formación

La presente Política entrará en vigor en el día de su comunicación a las personas incluidas en su ámbito de aplicación, permaneciendo vigente hasta su derogación expresa.

Los contenidos de esta Política serán actualizados para incorporar las novedades legislativas que procedan y las buenas prácticas que los más altos estándares en la materia determinen. Cualquier actualización del documento deberá ser comunicada a todas las personas incluidas en su ámbito de aplicación.

Todos los miembros de Grupo Avintia recibirán formación suficiente en las materias relacionadas con la presente Política.

La Política se publicará en la página web de Grupo Avintia y en su intranet, estando a disposición de cualquier persona.

Con la entrada en vigor de la presente Política de Seguridad de la Información de 2024 queda derogada la Política de Seguridad de la Información de 2020.