Normativa de Seguridad de la Información

Aprobación del documento		
Cargo	Nombre	Firma
Responsable de Seguridad	Adolfo Trocolí Naranjo	 4fc1d694-884a-3c43-aa1c-066491d0a022 2025-04-04 11:52:51 UTC

Control de versiones			
Versión	Fecha	Responsable	Cambios
01	22/11/2024	Adolfo Trocolí	Versión inicial del documento.
02	28/02/2025	Adolfo Trocolí	Adecuación ENS.

Índice de contenidos

1 Objeto y ámbito de aplicación

La actividad de Olin Group, con un modelo de negocio en su mayoría digital y una gestión considerable de volúmenes de datos, así como herramientas específicas y gran variedad de dispositivos, conlleva que exista un Sistema de Información complejo donde la seguridad debe estar garantizada en todo momento. El usuario debe ser consciente de la importancia de dicha seguridad y disponer de unas normas de obligado cumplimiento respecto a su uso.

Por ello, con el fin de garantizar la correcta gestión del sistema, Olin Group acuerda aprobar las siguientes normas de utilización del Sistema de Información para garantizar el buen uso de los medios técnicos puestos a disposición de los usuarios.

Esta Normativa es de aplicación a todo el ámbito de actuación de Olin Group, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información.

La presente Normativa es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en Olin Group, incluyendo el personal de proveedores externos, cuando sean usuarios del Sistema de Información de Olin Group.

En el ámbito de la presente normativa, se entiende por usuario cualquier usuario perteneciente o ajeno a Olin Group, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con Olin Group y que utilice o posea acceso al Sistema de Información de Olin Group.

2 Vigencia

La presente Normativa de Seguridad de la Información ha sido aprobada por el Comité de Seguridad, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que Olin Group pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de Olin Group.

3 Revisión y evaluación

La gestión de esta Normativa de Seguridad de la Información corresponde al Comité de Seguridad, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.
- Revisar la presente Normativa anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), y si es necesario aprobar las modificaciones que puedan realizarse. Esta revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

4 Utilización del equipo informático y de comunicaciones

Olin Group facilita a los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos que Olin Group pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.

En general, el ordenador personal (PC) será el recurso informático que permitirá el acceso de los usuarios al Sistema de Información y servicios informáticos del Olin Group, constituyendo un elemento muy importante en la cadena de seguridad, razón por la que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.

Este apartado concierne específicamente a todos los equipos facilitados por Olin Group para su utilización por parte de los usuarios, incluyendo equipos de sobremesa,

portátiles y dispositivos móviles con capacidades de acceso al Sistema de Información de la organización.

4.1 Normas generales

- Los ordenadores personales deberán utilizarse únicamente para fines corporativos y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.
- Se garantiza el derecho a la intimidad en el uso de los recursos y dispositivos puestos a disposición del personal y los utilizados para la gestión del personal y la seguridad de las instalaciones y recursos, incluyendo los sistemas de videovigilancia y geolocalización que se habiliten.
- El personal tiene derecho a la "desconexión digital" fuera del tiempo de trabajo y horario laboral establecido dentro del marco de sus tareas profesionales, tal como viene establecido en la política corporativa de "Desconexión Digital".
- Únicamente el personal autorizado, el Responsable del Sistema o quien este determine de forma explícita, podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad del Sistema de Información. Cuando se precise instalar dispositivos no provistos por la organización deberá solicitarse autorización previa al Responsable de Seguridad.
- Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa del Responsable de Seguridad. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.
- Salvo autorización expresa, los usuarios no tendrán privilegio de administración sobre los equipos.
- Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizará completado el mantenimiento o una vez resueltos aquellos.
- Si el personal de soporte técnico detectase cualquier anomalía que indicara una utilización de los recursos contraria a la presente norma, lo pondrá en

conocimiento del Responsable de Seguridad, que tomará las oportunas medidas correctoras.

- Los ordenadores personales de la organización deberán mantener actualizados los parches de seguridad de todos los programas que tengan instalados.
- Los usuarios deberán notificar al departamento de informática, a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo.
- El usuario debe ser consciente de las amenazas provocadas por malware. Muchas instancias de código malicioso requieren de la participación de los usuarios para propagarse, ya sea a través de memorias USB, mensajes de correo electrónico o instalación de programas descargados desde Internet. Es imprescindible, por tanto, vigilar el uso responsable los equipos para reducir este riesgo.
- El usuario será responsable de toda la información extraída fuera de la organización a través de dispositivos tales como memorias USB u otros que le hayan sido asignados. Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información sensible, confidencial o protegida.
- El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata al departamento de informática, al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por Olin Group estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente a la unidad responsable cuando finalice su vinculación con dicho puesto o función.

4.2 Usos específicamente prohibidos

Están terminantemente prohibidos los siguientes comportamientos:

- Utilización de cualquier tipo de software dañino.
- Utilización de programas que, por su naturaleza, hagan un uso abusivo de la red.
- Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por Olin Group, sin la previa autorización.

- Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.
- No conectar ni desconectar ningún dispositivo. Este trabajo lo realizará el Responsable del Sistema correspondiente.

4.3 Normas específicas para equipos portátiles

- Los equipos portátiles y móviles serán asignados por el Responsable del Sistema correspondiente.
- Este tipo de dispositivos estará bajo la custodia del usuario que los utilice, quién deberá adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.
- Cuando se trabaje en zonas no controladas se tomarán medidas para evitar que se pueda acceder a la información por parte de terceros (no mantenerlos a la vista, protectores anti reflectantes, evitar zonas públicas)
- La sustracción de estos equipos se ha de poner inmediatamente en conocimiento del Responsable del Sistema correspondiente para la adopción de las medidas que correspondan y a efectos de baja en el inventario.
- Los equipos portátiles y móviles deberán utilizarse únicamente para fines laborales, especialmente cuando se usen fuera de las instalaciones de Olin Group.
- Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas al Olin Group o no autorizadas para ello.
- Los usuarios de equipos portátiles deberán realizar conexiones periódicas a la red corporativa, según las instrucciones proporcionadas por La organización, para permitir la actualización de aplicaciones, sistema operativo y demás medidas de seguridad.
- Cuando la tipología de la información tratada así lo requiera, los ordenadores portátiles afectados deberán tener cifrado el disco duro, disponer de software que garantice un arranque seguro, así como mecanismos de auditoría capaces de crear un registro por cada fichero extraído del sistema por cualquier medio (red, dispositivos extraíbles, impresoras, etc.).
- Los usuarios no tendrán privilegio de administración sobre los equipos portátiles, teniendo prohibido realizar cualquier modificación

hardware/software sobre los mismos. Corresponderá al Servicio de Informática llevar a cabo estas modificaciones.

4.4 Uso de memorias externas

- Con carácter general, el uso de memorias externas en Olin Group no está autorizado. En su caso, la autorización deberá proporcionarla el Responsable del Sistema de la empresa correspondiente.
- En el caso de que a un usuario se le autorice el uso del interfaz USB de su puesto de trabajo, las memorias USB utilizadas serán las proporcionadas por Olin Group, que serán conformes a las normas de seguridad de la organización.
- Las memorias externas están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento. En el caso de uso con finalidad de realizar copias de seguridad debe ser autorizado por el Responsable del Sistema.
- La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento del Responsable del Sistema correspondiente, de forma inmediata.

4.5 Grabación de CDs y DVDs

- El uso de equipos grabadores de CDs y DVDs en Olin Group no está autorizado para la copia de información de la empresa a discos. En su caso, la autorización deberá proporcionarla el Responsable de Seguridad.

4.6 Impresoras en red y fotocopiadoras

- Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente, podrán instalarse impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente por parte del responsable del peticionario. En ningún caso el usuario podrá hacer uso de impresoras, fotocopiadoras o equipos de fax que no hayan sido proporcionados por Olin Group y, en su consecuencia, estén debidamente inventariados.
- Cuando se imprima documentación, deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.

- Conviene no olvidar tomar los originales de la fotocopiadora, una vez finalizado el proceso de copia. Si se encontrase documentación sensible, confidencial o protegida abandonada en una fotocopiadora o impresora, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. En caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento del Responsable del Sistema correspondiente.

4.7 Digitalización de documentos

- Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información sensible, confidencial o protegida.
- Conviene no olvidar tomar los originales del escáner, una vez finalizado el proceso de digitalización. Si se encontrase documentación sensible, confidencial o protegida abandonada en un escáner, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento del Responsable del Sistema correspondiente.
- En las cartas certificadas del juzgado se deberá anotar en el propio sobre cerrado la fecha de entrega, el cual será importante guardar y archivar. La persona receptora deberá entregarlo de forma inmediata al responsable.

4.8 Protección de equipos y puestos de trabajo

- Los puestos de trabajo del personal deben ubicarse preferentemente en ubicaciones que no queden expuestas al acceso de personas externas. No será de aplicación este punto en el caso de equipos que estén destinados al uso público.
- Los puestos ubicados en zonas de atención o tránsito de público, deben situarse de forma que las pantallas no puedan ser visualizadas por personas externas.
- Los puestos de trabajo permanecerán despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.
- Al finalizar la jornada de trabajo, los usuarios deben guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.

- Cada vez que un usuario se ausente de su lugar de trabajo debe bloquear su puesto de usuario, de forma que se proteja el acceso a las aplicaciones y servicios. Adicionalmente, los puestos de trabajo se configurarán para bloquearse automáticamente tras un periodo de inactividad.

4.9 Cuidado y protección de la documentación impresa

- La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que sólo tenga acceso a ella el personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y ser custodiada en armarios bajo llave.
- Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las máquinas destructoras de Olin Group, de forma que no sea recuperable la información que pudieran contener.
- Si, una vez impresa, es necesario almacenar tal documentación, el usuario habrá de asegurarse de proteger adecuadamente y bajo llave aquellas copias que contengan información sensible, confidencial, protegida, o crítica para su trabajo.
- Por razones ecológicas y de seguridad, antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo.

4.10 Protección de la dignidad de las personas

Está terminantemente prohibida toda transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.

5 Identificación y autenticación

- Los usuarios dispondrán de un código de usuario y una contraseña o bien una tarjeta criptográfica y/o certificado digital, para el acceso al Sistema de Información, y son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado. El código de usuario es único para cada persona en la organización, intransferible e independiente del PC o terminal desde el que se realiza el acceso.

- Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso o tarjeta criptográfica a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros.
- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.
- Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar al Responsable del Sistema correspondiente el incidente de seguridad.
- Si, en un momento dado, un usuario recibiera una llamada telefónica solicitándole su nombre de usuario y contraseña, nunca facilitará dichos datos y procederá a comunicar este hecho al Responsable del Sistema correspondiente, de forma inmediata.

5.1 Política de contraseñas

- Se deben utilizar contraseñas únicas para cada acceso.
- Las contraseñas de cuentas individuales son estrictamente personales.
- El tamaño mínimo de contraseña es de 10 caracteres, excepto en el caso de que esto no sea posible por motivos técnicos.
- Las contraseñas no pueden contener el nombre de la entidad, del empleado/a, de la fecha de creación, ni datos fácilmente relacionables con cualquiera de ellos.

6 Acceso de terceros a los edificios

Los terceros ajenos a Olin Group que, eventualmente, permanecieran en sus edificios, instalaciones o dependencias, deberán observar las siguientes normas:

- Toda persona no perteneciente a Olin Group que temporalmente deba acceder al Sistema de Información, deberá hacerlo siempre bajo la supervisión de algún miembro acreditado de Olin Group.
- Cualquier incidente que surja antes o en el transcurso del acceso a Olin Group deberá ponerlo en conocimiento del Responsable del Sistema correspondiente.
- Para los accesos de terceros al Sistema de Información de Olin Group, siempre que sea posible, se les crearán usuarios temporales que serán eliminados una

vez concluido su trabajo en Olin Group. Si, de manera excepcional, tuvieran que utilizar identificadores de usuarios ya existentes, una vez finalizados dichos trabajos, se procederá al cambio inmediato de las contraseñas de los usuarios utilizados.

- Tales personas, en lo que les sea de aplicación, deberán cumplir puntualmente la presente Normativa de Seguridad de la Información, así como el resto de normativa de seguridad de Olin Group.
- Para acceder a los edificios, instalaciones o dependencias del Olin Group deberá estar en posesión de la correspondiente documentación de identificación personal admitida en Derecho (DNI., pasaporte, etc.), debiendo estar incluido en la relación nominal proporcionada previamente por la empresa a la que perteneciere. La primera vez que acceda físicamente deberá identificarse al personal de Seguridad y solicitar la presencia de la persona responsable de Olin Group, que constituirá su enlace durante su estancia en él.
- Una vez en el interior de los edificios, dependencias o instalaciones de Olin Group, los terceros sólo tendrán autorización para permanecer en el puesto de trabajo que les haya sido asignado y en las zonas de uso común
- Los terceros atenderán siempre a los requerimientos que le hiciere el personal de seguridad de los edificios, instalaciones o dependencias a los que tuvieren acceso.

7 Uso del correo electrónico corporativo

El correo electrónico corporativo es una herramienta de mensajería electrónica, puesta a disposición de los usuarios de Olin Group, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas.

Se trata de un recurso compartido por todos los usuarios, por lo que un uso indebido del mismo repercute de manera directa en el servicio ofrecido a todos.

Por ello, se dictan las siguientes normas de uso:

7.1 Normas generales

- Todos los usuarios que lo precisen para el desempeño de su actividad profesional, dispondrán de una cuenta de correo electrónico, para el envío y recepción de mensajes internos y externos a la organización.

- Únicamente podrán utilizarse las herramientas y programas de correo electrónico suministrados.
- El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal, evitando el uso privado del mismo.
- Se deberá notificar al Responsable del Sistema correspondiente cualquier tipo de anomalía detectada, así como un alto volumen de correos no deseados (spam) que se reciban, a fin de configurar adecuadamente las medidas de seguridad oportunas.
- Se deberá prestar especial atención a los ficheros adjuntos en los correos recibidos. No deben abrirse ni ejecutarse ficheros de fuentes no fiables, puesto que podrían contener virus o código malicioso. En caso de duda sobre la confiabilidad de los mismos, se deberá notificar esta circunstancia al Responsable del Sistema correspondiente.
- Está terminantemente prohibido suplantar la identidad de un usuario de internet, correo electrónico o cualquier otra herramienta colaborativa.
- Para verificación y monitorización, La organización guarda datos de conexión y tráfico. En ningún caso esta retención de datos afectará al secreto de las comunicaciones.
- En caso de extinción de la relación laboral, independientemente del motivo, el trabajador/a deberá devolver inmediatamente todos los equipos y herramientas facilitadas, sin que la empresa tenga obligación alguna de custodiar, recuperar o facilitar acceso a información de carácter personal que pudiera haber sido indebidamente almacenada en dichos dispositivos o cuentas corporativas.

7.2 Usos especialmente prohibidos

Las siguientes actuaciones están explícita y especialmente prohibidas:

- El envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad, que contengan programas informáticos (software) sin licencia, que vulneren los derechos de propiedad intelectual de los mismos, de alerta de virus falsos o difusión de virus reales y código malicioso, o cualquier otro tipo de contenidos que puedan perjudicar a los usuarios, identidad e imagen corporativa y al propio Sistema de Información de la organización.
- El acceso a un buzón de correo electrónico distinto del propio y el envío de correos electrónicos con usuarios distintos del propio.

- La difusión de la cuenta de correo del usuario en listas de distribución, foros, servicios de noticias, etc., que no sean consecuencia de la actividad profesional del usuario.
- Responder mensajes de los que se tenga sospechas sobre su autenticidad, confiabilidad y contenido, o mensajes que contengan publicidad no deseada.
- La utilización del correo corporativo como medio de intercambio de ficheros especialmente voluminosos sin autorización, y el envío de información sensible, confidencial o protegida.

8 Acceso a internet y otras herramientas de colaboración

El acceso corporativo a Internet es un recurso centralizado a disposición de los usuarios de Olin Group, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional.

Olin Group velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso.

8.1 Usos específicamente prohibidos

Quedan prohibidas las siguientes actuaciones:

- La descarga de programas informáticos o ficheros con contenido dañino que supongan una fuente de riesgos para la organización.
- El acceso a recursos y páginas-web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.
- La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.).

9 Incidentes de seguridad

Cuando un usuario detecte cualquier anomalía o incidente de seguridad que pueda comprometer el buen uso y funcionamiento del Sistema de Información de Olin

Group o su imagen, deberá informar inmediatamente al Responsable del Sistema correspondiente, que lo registrará debidamente y elevará, en su caso.

10 Compromisos de los usuarios

Es responsabilidad directa del usuario:

- Custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad fijadas por Olin Group, para garantizar que aquellas no puedan ser utilizadas por terceros. Deberá cerrar su cuenta al terminar la sesión o bloquear el equipo cuando lo deje desatendido.
- En el caso de que su equipo contenga información sensible, confidencial o protegida, esta deberá cumplir todos los requisitos legales aplicables y las medidas de protección que la normativa que Olin Group establezca al respecto.
- Además de lo anterior, no se podrá acceder a los recursos informáticos y telemáticos de Olin Group para desarrollar actividades que persigan o tengan como consecuencia:
    - El uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones, para usos no profesionales.
    - La degradación de los servicios.
    - La destrucción o modificación no autorizada de la información, de manera premeditada.
    - La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.
    - El deterioro intencionado del trabajo de otras personas.
    - El uso del Sistema de Información para fines ajenos a los del Olin Group, salvo aquellas excepciones que contempla la presente Normativa.
    - Dañar intencionadamente los recursos informáticos del Olin Group, o de otras instituciones.
    - Incurrir en cualquier otra actividad ilícita, del tipo que sea.

11 Monitorización y aplicación de esta normativa

La organización, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

- Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
- Monitorizará los accesos a la información contenida en sus sistemas.
- Auditará la seguridad de las credenciales y aplicaciones.
- Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.

La organización llevará a cabo esta actividad de monitorización sin atentar contra los derechos constitucionales de los usuarios, tales como el derecho a la intimidad personal y al secreto de las comunicaciones, manteniéndose en todo momento la privacidad de la información manejada, salvo que, por requerimiento legal e investigación sobre un uso ilegitimo o ilegal, sea necesario el acceso a dicha información, salvaguardando en todo momento los derechos fundamentales de los usuarios.

Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca. El Responsable del Sistema correspondiente velará por el cumplimiento de la presente Normativa e informará al Responsable de Seguridad sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan código dañino. Igualmente, el sistema podrá registrar y dejar traza de las

páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar sobre usos prolongados e indebidos del servicio.

12 Incumplimiento de la normativa

Todos los usuarios de Olin Group están obligados a cumplir lo prescrito en la presente Normativa de Seguridad de la Información.

En el supuesto de que un usuario no observe alguna de los preceptos señalados en la presente Normativa, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.