



CONTROL A.18 CUMPLIMIENTO

NORMA ISO/IEC 27001:2013

Tabla de contenido

1. Cumplimiento de requisitos legales y contractuales.
2. Identificación de la legislación aplicable y de los requisitos contractuales y sus sistemas.
3. Derechos de propiedad intelectual
4. Protección de registros
5. Privacidad y protección de información de datos personales
6. Revisiones de seguridad de la información
7. Revisión independiente de la seguridad de la información
8. Cumplimiento con las políticas y normas de seguridad
9. Revisión del cumplimiento técnico

■ 1. Cumplimiento de requisitos legales y contractuales

Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.



■ 2. Identificación de la legislación aplicable y de los requisitos contractuales y sus sistemas

OasisCom realiza dicha identificación en el documento ***OR_SIG_07_Matriz_Requisitos_Legales***, en donde también se describen los controles para cumplir tales requisitos y el responsable. Esta matriz debe ser revisada cada seis meses por el responsable y actualizarla según se requiera.





3. Derechos de propiedad

■ Derechos de propiedad intelectual

OasisCom debe velar por el cumplimiento de la legislación relacionada con la **Seguridad de la Información**, entre ella la referente al uso legal del software, productos informáticos, derechos de autor y propiedad intelectual.



■ Derechos de propiedad intelectual

Cualquier violación a las políticas o directrices definidas, podrá ser sancionado según lo establecido en el documento ***PR_GTH_07_Procedimiento_Proceso_Disciplinario***, en la **ley de delitos informáticos 1273 del 2009** y demás aplicables.



■ Derechos de propiedad intelectual

Dentro de las cláusulas en los **contratos de venta** y los **contratos laborales** se encuentra definida la propiedad intelectual de OasisCom y su adecuado manejo.



■ Derechos de propiedad intelectual

Se debe reportar en la aplicación **AMEJ** de OasisCom las violaciones a la seguridad, confirmadas o sospechadas.

Como colaboradores somos responsables de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política.



■ Derechos de propiedad intelectual

El software que requiera adquirir OasisCom para el uso y buen funcionamiento de los procesos de la empresa debe tener licencia y ser adquirido siempre de fuentes conocidas y confiables, con el fin de asegurar que no se viola los derechos de autor.



■ Derechos de propiedad intelectual

Solo el **Gestor de Soporte Nivel 1** con previa autorización del Oficial de Seguridad de la Información está **autorizado para instalar el software** en los equipos de cómputo de la empresa.



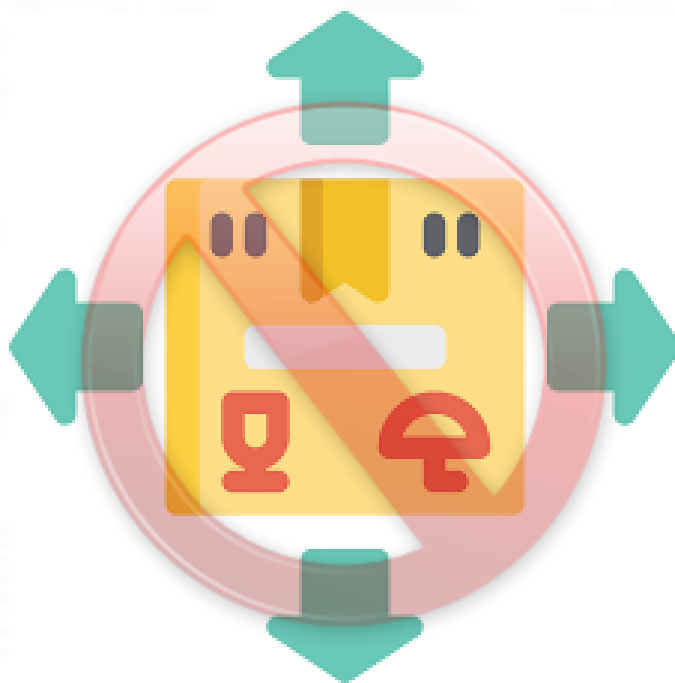
■ Derechos de propiedad intelectual

Con el fin de verificar el apropiado uso de software, OasisCom cuenta con la **autoridad y autonomía** para realizar auditorías periódicas sobre las estaciones de trabajo, con previa autorización del gerente inmediato.



■ Derechos de propiedad intelectual

No está permitido **distribuir copias** de esta política a **personas externas** a la empresa, sin la autorización respectiva por parte del Oficial de Seguridad de la Información.



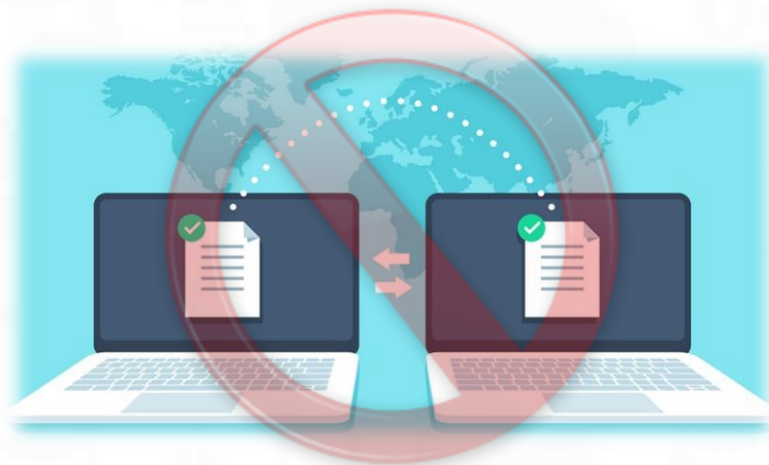
■ Derechos de propiedad intelectual

No se debe **duplicar**, **convertir** a otro formato o **extraer** de registros comerciales, ya sea video o audio, más allá de lo que permita la ley de derechos de propiedad intelectual y de autor.



■ Derechos de propiedad intelectual

No se debe **copiar** total ni parcialmente libros, artículos, reportajes u otros documentos diferentes de los permitidos por la ley de derechos de autor.



■ Derechos de propiedad intelectual

De acuerdo a los derechos de propiedad, hay determinados activos que deben ser protegidos. Estos activos se encuentran definidos en el documento ***OR_SGSI_04_Matriz_de_Riesgos_del_SGSI***.



■ Derechos de propiedad intelectual

El máximo de usuarios permitidos dentro de una licencia son los contratados en esta. Las plataformas no permiten el registro extra de usuarios.



■ Derechos de propiedad intelectual

Para garantizar el cumplimiento de lo establecido por los derechos de propiedad intelectual, el área de Infraestructura debe hacer una **revisión periódica** de que el software utilizado por la empresa para su operación de negocio se encuentra debidamente licenciado.



■ Derechos de propiedad intelectual

Los colaboradores y contratistas que trabajan para OasisCom no deben:

- Copiar el software suministrado en medios de almacenamiento.
- Transferir dicho software a otros computadores.
- Suministrar dicho software a terceras partes sin la autorización escrita del Oficial de Seguridad de la Información.



■ 4. Protección de registros

En OasisCom se debe velar por la protección de toda la documentación generada.

En el documento ***PR_SIG_01_***
Procedimiento_Gestión_Documental
se establece las directrices para la
clasificación, etiquetado y
almacenamiento de los registros.



■ 5. Privacidad y protección de información de datos personales

Para OasisCom es importante velar por la privacidad de la información de sus colaboradores y clientes.

Por esta razón define la política de privacidad y de protección de datos personales en la página web de la compañía <https://www.oasiscom.com> y por medio del documento [*PL_GTH_06_Política_Tratamiento_Datos_Personales*](#) el cual debe ser leído y firmado por los colaboradores de la empresa.



■ 6. Revisiones de seguridad de la información

Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.



■ 7. Revisión independiente de la seguridad de la información

Por medio de una **auditoría interna** se debe hacer una revisión al SGSI con el fin de asegurar la conveniencia, la adecuación y la eficacia continua de este evitando la materialización de algún riesgo en la seguridad de la información.

Esta revisión se debe hacer al menos una vez al año y está a cargo del equipo auditor de la norma ISO/IEC 27001: 2013

EQUIPO AUDITOR

- ✓ Daniela Martínez
- ✓ Lorena Padilla
- ✓ Miguel Carvajal
- ✓ Felipe Chisabo
- ✓ Fredy Prieto



■ 8. Cumplimiento con las políticas y normas de seguridad

El Gestor de Auditorías Internas junto con los gerentes deben hacer revisiones periódicas sobre el cumplimiento de las políticas, procedimientos y demás reglamentación de Seguridad de la Información que sea aplicable dentro del proceso a su cargo.



■ 8. Cumplimiento con las políticas y normas de seguridad

En caso tal de que sean encontradas no conformidades en las revisiones, los gerentes de cada proceso deben:

- Identificar las causas de la no conformidad.
- Evaluar la necesidad de acciones para lograr cumplimiento.
- Implementar las acciones correctivas apropiadas.
- Revisar la acción correctiva tomada, para verificar su eficacia e identificar cualquier deficiencia o debilidad.



■ 8. Cumplimiento con las políticas y normas de seguridad

Las **revisiones** deben quedar **documentadas** y las no conformidades registradas como oportunidad de mejora en la aplicación **AMEJ** de OasisCom, en la cual se debe hacer seguimiento de su cierre efectivo.



■ 8. Cumplimiento con las políticas y normas de seguridad

El Gestor de Auditoría Interna debe tener en cuenta estas revisiones y resultados como referencia para las revisiones independientes al Sistema de Gestión de Seguridad de la Información.



■ 9. Revisión del cumplimiento técnico

Se deben planificar las auditorías del SGSI a nivel técnico, las cuales se deben documentar y ser periódicas. Adicionalmente, se deben hacer por personas competentes o bajo la supervisión de estas.



