



www.oasiscom.com

Clasificación de la Información y Política de Dispositivos Móviles

Norma ISO/IEC 27001: 2013

Contenido

- ✓ Política del SGSI
- ✓ Objetivos del SGSI
- ✓ Clasificación de la información
- ✓ Política de Dispositivos Móviles

Política General del SGSI

1. OasisCom es una empresa de tecnología que brinda los servicios de desarrollo, implementación, soporte y prestación del servicio de facturación electrónica

2. Custodia y protege de riesgos externos y/o internos a sus principales activos de seguridad de la información.

3. Propende por el cumplimiento de los requisitos legales, estatutarios, reglamentarios y aquellos citados por el cliente.

4. Ofrece de este modo productos que cumplen con las expectativas del mercado, contando con personal competente.

5. Asegurando el cumplimiento y la mejora continua de su Sistema de Gestión de la Seguridad de la Información.



1. Desarrollar, implementar y ofrecer soporte al servicio de facturación electrónica



2. Garantizar que la plataforma para la prestación del servicio está disponible


3. Establecer los controles de seguridad de la información para la protección de los activos de información con base en la norma ISO/IEC 27001: 2013.

4. Hacer seguimiento a los controles de seguridad establecidos e implementados.



Objetivos del SGSI

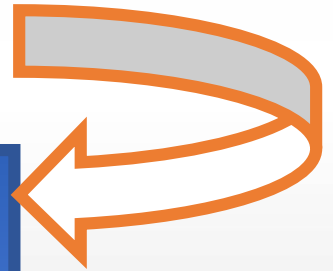
5. Identificar y hacer seguimiento al cumplimiento de los requisitos legales, reglamentarios, contractuales y estatutarios definidos por el Sistema de Gestión de Seguridad de la Información.



6. Contar con el personal y capacitarlo para que tenga el conocimiento requerido en los temas necesarios que permitan ofrecer una mejor prestación del servicio de facturación electrónica.

7. Hacer revisiones periódicas al Sistema de Gestión de Seguridad de la Información.

8. Gestionar las oportunidades de mejora que permitan la madurez del Sistema de Gestión de Seguridad de la Información.





Clasificación de la Información

La información de OasisCom se clasifica en **Privada**, **Restringida**, de **Uso Interno** y **Pública**.


Los documentos e información generada en OasisCom debe estar debidamente etiquetada dentro del documento con una de las clasificaciones según corresponda, a excepción de la información pública la cual no requiere etiqueta.





✓ Privada

- ☛ Información personal y laboral de los trabajadores de OasisCom.
- ☛ Esta es de uso exclusivo de las Gerencias y Talento Humano.




Expediente laboral (formatos de vacaciones, adelantos, incapacidades, hoja de vida, otros sí).

Datos personales (Información personal y familiar)



✓ Restringida

- ☛ Información correspondiente a la gestión de cada proceso.
- ☛ Esta es de uso y acceso sólo de los integrantes del proceso y clientes en ciertos casos.


- 
- ✓ Contratos de venta
 - ✓ Información de la ERP
 - ✓ Código Fuente
 - ✓ Actas de área
 - ✓ Información de gestión

**Información digital y
física.**



✓ Uso Interno


- ☛ Información de conocimiento para todo el personal de OasisCom.
- ☛ Acceso por OASISKB → (SIG) Sistema Integrado de Gestión.

- 
- ✓ Procedimientos
 - ✓ Formatos
 - ✓ Documentos organizacionales
 - ✓ Políticas



✓ Pública

☛ Información disponible para conocimiento del público en general.

- 
- ✓ Página Web
 - ✓ Manuales de Usuario
 - ✓ Políticas del Sistema Integrado de Gestión.



Etiquetado de la Información

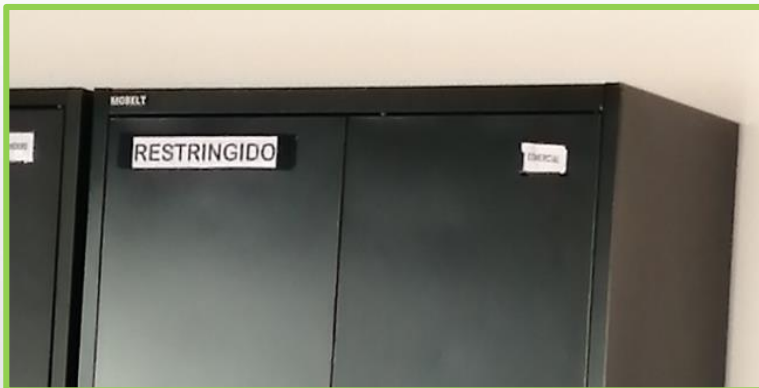
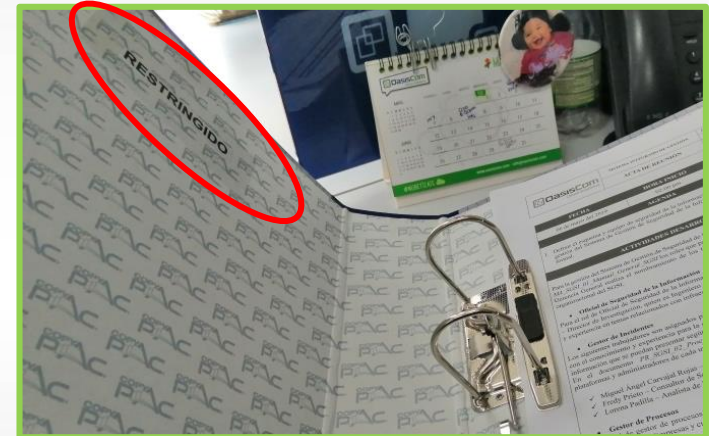
Digital

	SISTEMA INTEGRADO DE GESTION	CODIGO	OR_SGSI_01
		VERSIÓN	2.0
	ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Página 1 de 2	
		USO INTERNO	

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

OR_SGSI_01

Física



Archivo Físico

Políticas de Dispositivos Móviles

Los equipos móviles (propiedad de OasisCom) utilizados dentro o fuera de empresa y en funciones propias de la compañía, deben ser exclusivamente utilizados para brindar apoyo a las actividades de esta y deben ser sujetos a un grado equivalente de protección al de los equipos que se encuentran dentro de las instalaciones de OasisCom.

1. Las computadoras personales institucionales no se deben utilizar en los hogares para conectarse a Internet u otras redes si no existen controles para los virus y firewall de la computadora personal, instalados y en constante funcionamiento.

2. Durante los viajes, los equipos (y medios) no se deben dejar desatendidos en lugares públicos. Las computadoras portátiles se deben llevar como equipaje de mano.

3. Los portátiles son vulnerables al robo, pérdida o acceso no autorizado durante los viajes. Se les deben proporcionar una forma apropiada de protección al acceso (ej. Contraseñas de encendido) con el fin de prevenir acceso no autorizado.

4. Los equipos de cómputo de OasisCom, así como la información almacenada en los mismos, son propiedad de empresa y pueden ser inspeccionados o utilizados de cualquier manera y en cualquier momento en que la compañía lo considere. Estos deben ser devueltos a OasisCom en el momento en que el usuario deje de tener relación laboral con la empresa o cuando esta lo requiera.

5. Un computador corporativo, equipo portátil, teléfono inteligente o cualquier otro sistema de cómputo usado para actividades de OasisCom que contenga información sensible, no se debe prestar a nadie y es responsabilidad exclusiva del colaborador que lo tenga asignado.

6. OasisCom prohíbe el almacenamiento de información de la compañía en equipos móviles personales, sólo se debe consultar en línea.

7. Todos los equipos móviles de propiedad de OasisCom y que se encuentren conectados a las redes de la empresa, deben estar registrados en el documento *FO_SS_03_Inventario_Hardware_Software_OasisCom* y aprobados previamente por el Oficial de Seguridad de la Información.

8. Si un trabajador requiere extraer de las instalaciones de OasisCom un equipo móvil, este debe ser llevado en una maleta ergonómica destinada para tal fin y debe ser transportado en un vehículo particular ya sea de propiedad del trabajador o de lo contrario se debe hacer uso del servicio de UBER, con el fin de minimizar el riesgo de robo o pérdida.

9. Las únicas personas autorizadas por OasisCom para instalar y realizar cambios al software y hardware de los equipos de la empresa son los técnicos de soporte con previa autorización del Oficial de Seguridad de la Información, motivo por el cual se prohíbe a los colaboradores y técnicos instalar algún software sin previa autorización del Oficial de Seguridad de la Información, con el fin de constatar la seguridad y legalidad de este.

10. A menos que sean específicamente autorizados por el Oficial de Seguridad de la Información, los colaboradores de OasisCom no deben utilizar herramientas de hardware o software que puedan ser empleadas para evaluar vulnerabilidades o comprometer la seguridad de los sistemas de información o la información de otros usuarios. Incidentes que involucren este tipo de herramientas y el intento no autorizado de comprometer las medidas de seguridad de los sistemas de información, serán considerados como faltas graves de las políticas de seguridad de la información de OasisCom y podrán ser denunciados legalmente.

11. El acceso de los usuarios a la red y a los diferentes servicios de red debe permitirse únicamente cuando sea formalmente autorizado por el gerente inmediato.

12. El acceso a los sistemas y recursos de información debe ceñirse al
PR_SIG_04_Procedimiento_de_Accesos_y_Permisos.

13. Todo dispositivo móvil autorizado por la empresa debe contar con un antivirus actualizado y vigente que lo proteja contra software malicioso.

14. En caso de pérdida de un dispositivo móvil, se deben reestablecer las contraseñas de las cuentas registradas en el dispositivo, con el fin de que todas las sesiones sean cerradas.

15. Es responsabilidad del trabajador que tenga asignado el dispositivo móvil, realizar periódicamente las debidas copias de seguridad de su información.

16. En la plataforma OASISKB (SharePoint) los trabajadores deben cargar los registros y documentos necesarios generados en sus procesos, con el fin de que estén disponibles en la nube y evitar pérdidas o modificaciones indebidas.

17. OasisCom da libre acceso a las aplicaciones y servicios que apoyen las labores de los colaboradores y que no afecten la seguridad de la información. Si un trabajador requiere acceso a otro tipo de servicio no autorizado, debe coordinarlo con el gerente de área siguiendo el PR_SIG_04_Procedimiento_de_Accesos_y_Permisos.

18. Cuando un equipo móvil se encuentre fuera de las instalaciones de OasisCom, se recomienda no conectarse a varias redes simultáneamente.

Actividad

Formar grupos de 3 personas

GRACIAS