



# **CONTROL 12. SEGURIDAD DE LAS OPERACIONES**

**NORMA ISO/IEC 27001: 2013**

## ■ **Tabla de contenido**

### 1. Procedimientos operacionales y responsabilidades

1.1 Procedimientos de operación documentados

1.2 Gestión de cambios

1.3 Gestión de capacidad

1.4 Separación de los ambientes de desarrollo, pruebas y producción

### 2. Protección contra códigos maliciosos

2.1 Controles contra códigos maliciosos

### 3. Copias de respaldo

3.1 Respaldo de la información

## ■ **Tabla de contenido**

### 4. Registro (logging) y seguimiento

#### 4.1 Registro de eventos

#### 4.2 Protección de la información de registro (log information)

#### 4.3 Registros (Logs) del administrador y del operador

#### 4.4 Sincronización de relojes

### 5. Gestión de la vulnerabilidad técnica

#### 5.1 Gestión de las vulnerabilidades técnicas

#### 5.2 Restricciones sobre la instalación de software

### 6. Consideraciones sobre auditorías de sistemas de información

#### 6.1 Controles sobre auditorías de sistemas de información

## ■ 1. Procedimientos operacionales y responsabilidades



### Objetivo:

Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

## ■ 1.1 Procedimientos de operación documentados

OasisCom define y documenta en [\*PR\\_SGSI\\_03\\_Procedimientos\\_y\\_Políticas\\_Operacionales\*](#) sus procesos operacionales.

Allí podemos encontrar:

- ✓ Correo electrónico
- ✓ Reporte y gestión de incidentes
- ✓ Gestión de accesos y permisos
- ✓ Copias de seguridad
- ✓ Restablecimiento de OasisCom
- ✓ Restablecimiento de servidores
- ✓ Gestión de huellas
- ✓ Instalación y/o actualización de software

## ■ 1.2 Gestión de cambios

OasisCom define y documenta en *PR\_SIG\_05\_Procedimiento\_Gestión\_del\_Cambio* la debida gestión que se debe realizar para los cambios que se presenten en la organización:

1

**Identificar cambios**



2

**Analizar viabilidad**



3

**Analizar riesgos y  
requisitos de ley si aplica**



4

**Analizar el impacto  
del cambio**



## ■ 1.2 Gestión de cambios

5

**Establecer las recomendaciones pertinentes al caso**



6

**Planear ejecución del cambio**



7

**Ejecutar las actividades**



8

**Hacer seguimiento**



## ■ 1.2 Gestión de cambios

9

Verificar  
cumplimiento en la  
Seguridad de la  
Información



10

Comunicar  
cambio



11

Interrumpir el cambio  
(opcional)



12

Cerrar cambio





## ■ 1.3 Gestión de capacidad

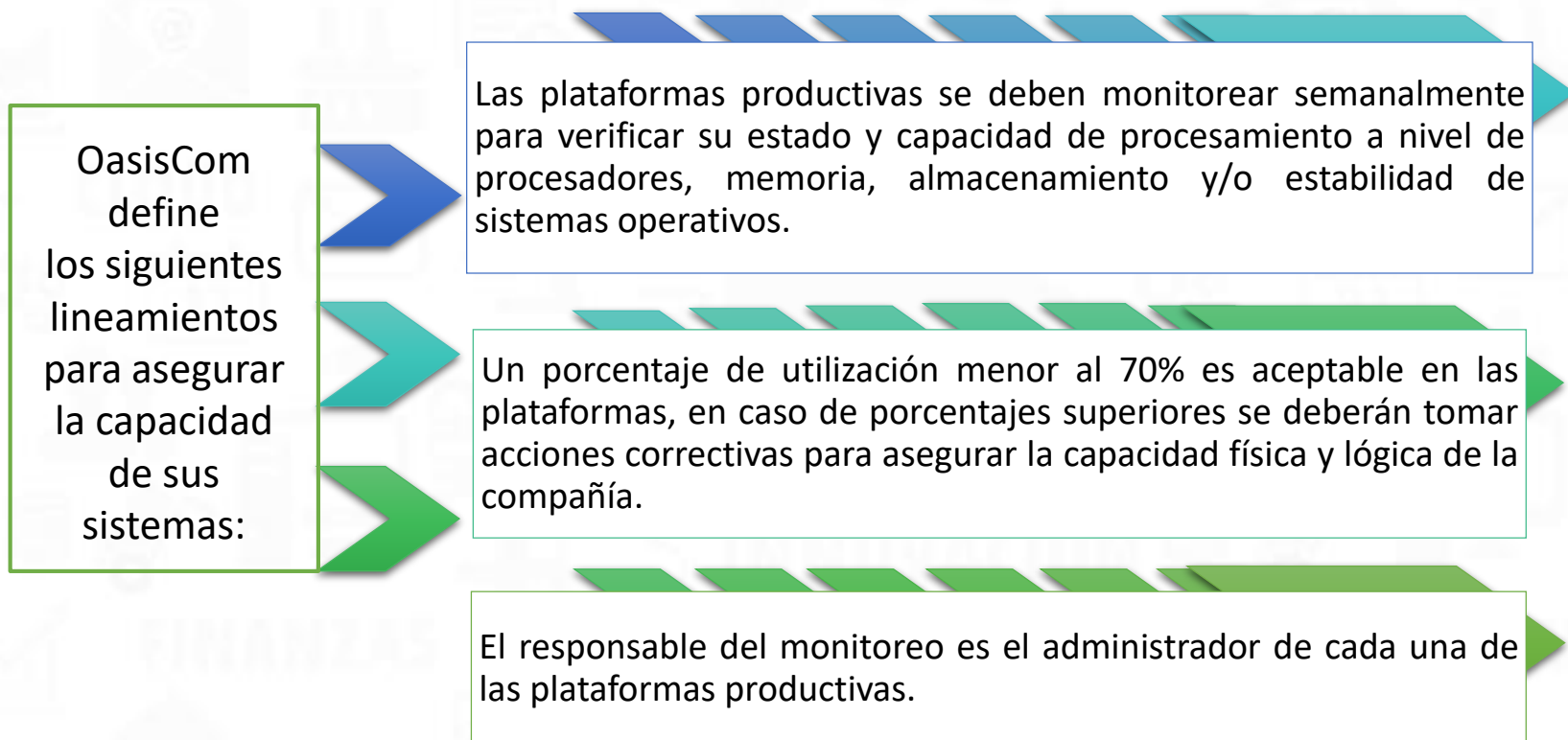
OasisCom define los siguientes lineamientos para asegurar la capacidad de sus sistemas:

Las plataformas que soporten la operación de la compañía deberán ser evaluados y dimensionados antes de hacer su despliegue.

Las plataformas productivas deben ser monitoreadas y evaluadas según su capacidad, implementando controles que se puedan desplegar antes de cualquier falla.

El dimensionamiento de las plataformas deberá tener en cuenta requisitos nuevos, procesos a soportar, tecnologías actuales y estimación de procesamiento de información.

## ■ 1.3 Gestión de capacidad



## ■ 1.3 Gestión de capacidad

OasisCom define los siguientes lineamientos para asegurar la capacidad de sus sistemas:

En los sistemas de almacenamiento, se hará una revisión mensual para eliminar información que no sea relevante para la operación de la compañía.

Cualquier ambiente, base de datos, archivos que se creen de manera temporal, deberán ser eliminados en cuanto se culmine con su utilización.

## ■ 1.3 Gestión de capacidad

OasisCom  
define  
los siguientes  
lineamientos  
para  
asegurar la  
capacidad de  
sus sistemas:

La utilización de canales de comunicación debe estar controlado para que aplicaciones, páginas, etc, que representen un consumo excesivo de ancho de banda sean restringidos o limitados para asegurar una óptima operación de los medios de comunicación.

La operación de las bases de datos (consultas) se deberán optimizar periódicamente para asegurar un óptimo desempeño de estas.

## ■ 1.4 Separación de los ambientes de desarrollo, pruebas y producción

OasisCom cuenta con cuatro ambientes con el fin de asegurar la calidad y la seguridad de los desarrollos:

### 1. Desarrollo

Se despliegan todos los desarrollos que han sido terminados por el equipo de calidad y puedan certificar que los desarrollos cumplen con la especificación del requerimiento.



### 2. Pruebas

Se valida el correcto funcionamiento del sistema luego de integrar todos los desarrollos aprobados por el equipo de calidad.



## ■ 1.4 Separación de los ambientes de desarrollo, pruebas y producción

### 3. PRE-PROD

Despliegue previo a la liberación de cada versión para validar el correcto funcionamiento del sistema en un ambiente similar al de producción y facilitar el despliegue al ambiente de producción.



### 4. PRODUCCIÓN

Este es el ambiente en el cual acceden todos los clientes de OasisCom.



## ■ 2. Protección contra códigos maliciosos



### Objetivo:

Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

## ■ 2.1 Controles contra códigos maliciosos

Se definen los siguientes lineamientos para asegurar el control contra códigos maliciosos:

- 1 Se prohíbe la instalación de software no autorizado por la compañía y/o por el Director de Infraestructura.
- 2 El Director de Infraestructura puede instalar cualquier tipo de software que requiera análisis, verificación y aprobación para su uso en las labores de la empresa.
- 3 El área de infraestructura debe hacer revisiones aleatorias periódicos a los equipos de los colaboradores para revisar y detectar el uso no autorizado.



## ■ 2.1 Controles contra códigos maliciosos

4

En todos los equipos debe estar siempre activo el firewall y el sistema de defensa por defecto del sistema operativo. Cada equipo debe tener instalado y activo el antivirus autorizado.

5

El antivirus debe estar configurado para hacer revisiones automáticas de cualquier archivo que se intente usar (local o de red) en el equipo y una revisión mensual para buscar posibles infecciones.

6

La actualización automática de las herramientas de protección debe estar siempre configurada y activa en cada equipo.

## ■ 2.1 Controles contra códigos maliciosos

7

Mediante la configuración de los permisos a nivel de firewall (FortiGate) se debe controlar la descarga de software

8

Mediante la configuración de los permisos a nivel del firewall (FortiGate) se debe controlar el acceso a sitios que se puedan considerar como maliciosos.

9

Los colaboradores de la compañía son conscientes que no deben descargar software o archivos que provengan de fuentes que sean o se sospeche que son maliciosas.

- Para los servidores de la compañía, se deben manejar las copias de respaldo para que en caso de una infección se pueda restablecer el sistema, de acuerdo con el siguiente procedimiento:


1. Identificar la información que se encuentra en la plataforma y que se debe respaldar.




2. El administrador de la plataforma debe programar y/o ejecutar la copia de seguridad de la información que se debe respaldar.



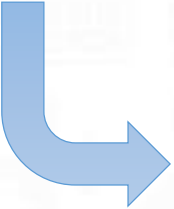
3. Comprobar que la copia de seguridad planeada/ejecutada culminó exitosamente, en caso de no ser así se debe corregir y generar la copia de seguridad.



**4.** Una vez se tiene la copia de seguridad, se debe comprimir usando WINRAR.



**5.** Una vez que la copia de seguridad esté comprimida, dicho archivo se debe almacenar en el lugar respectivo dentro de la plataforma designada para tal fin.



**3.** El administrador debe diligenciar el formato *FO\_SGSI\_03\_Formato\_Copias\_de\_Seguridad* de generación de copias de seguridad y almacenarlo en OasisKb.

### ■ 3. Copias de respaldo



#### Objetivo:

Proteger contra la pérdida de datos

## ■ 3.1 Respaldo de la información

OasisCom define y documenta en *PR\_SGSI\_03\_Procedimientos\_y \_Políticas \_Operacionales* los lineamientos para asegurar las copias de respaldo de la información sensible para la compañía.

Definir la información sensible de la cual se debe hacer copia de seguridad.



Identificar las ubicaciones donde se deben almacenar las copias de seguridad.



Comprimir las copias de seguridad usando WINRAR.



Almacenar el archivo en el lugar respectivo.



## ■ 4. Registro (logging) y seguimiento



**Objetivo:**  
Registrar eventos y  
generar evidencia.

## ■ 4.1 Registro de eventos

OasisCom define los siguientes lineamientos para asegurar el registro de eventos en sus plataformas:



1

Se hará uso de las **herramientas de trazabilidad** que cada una de las plataformas ofrezca, configurándolas de modo que dichos registros contengan la mayor cantidad de información relacionada con los **eventos más significativos** que en cada plataforma requieran seguimiento.



## ■ 4.1 Registro de eventos

2

En la medida en que cada plataforma lo permita, los registros de actividad deberán contener la siguiente información:

- ✓ Fecha y hora del evento
- ✓ Usuario que propicia el evento
- ✓ Tipo de evento
- ✓ Descripción del evento
- ✓ Respuesta de la plataforma al evento

### **Si lo permite la plataforma:**

- ✓ IP y/o equipo donde se origina el evento
- ✓ Herramientas usadas
- ✓ Cambios en información o configuración
- ✓ Códigos de error que se generen

## ■ 4.2 Protección de la información de registro (log information)

Se definen los siguientes lineamientos para asegurar la protección de los eventos generados en sus plataformas:

1

La responsabilidad sobre la información de los registros es del administrador de cada plataforma usada por la compañía.

2

En cada plataforma se mantendrá registro de por lo menos los últimos tres meses de operación.

3

Si la plataforma cuenta con restricción de almacenamiento de los registros (capacidad) se hará depuración de los mismos mínimo cada tres meses.

## ■ 4.2 Protección de la información de registro (log information)

Se definen los siguientes lineamientos para asegurar la protección de los eventos generados en sus plataformas:

4

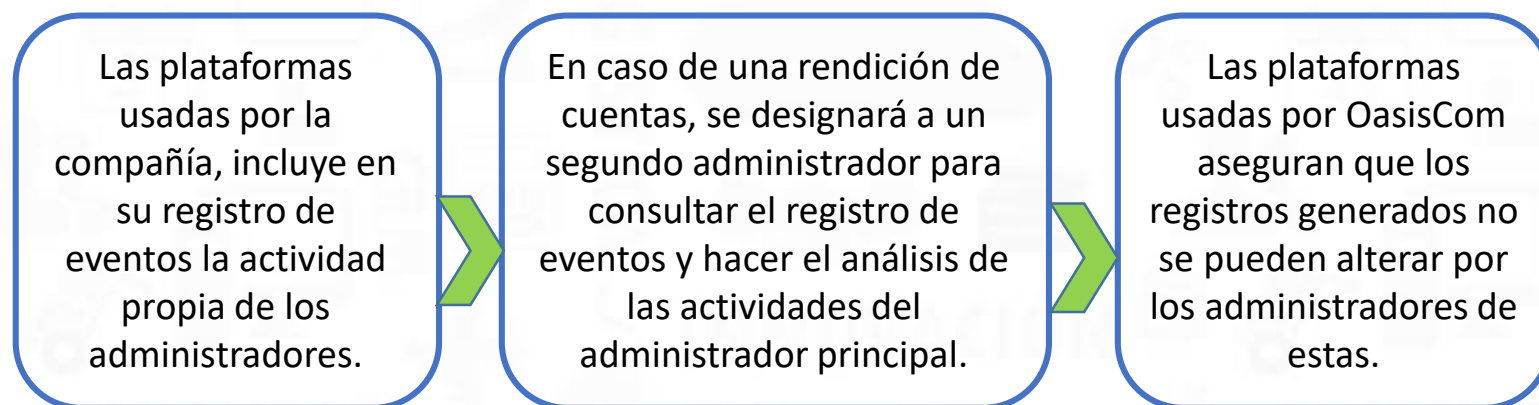
Las plataformas usadas por OasisCom aseguran que los registros generados no se pueden alterar por los mismos usuarios que lo generaron o por los administradores de la plataforma.

5

En caso de requerir la consulta sobre los registros, el administrador de cada plataforma será el único autorizado para realizar dicha labor e informar el resultado de la consulta.

## ■ 4.3 Registros (Logs) del administrador y del operador

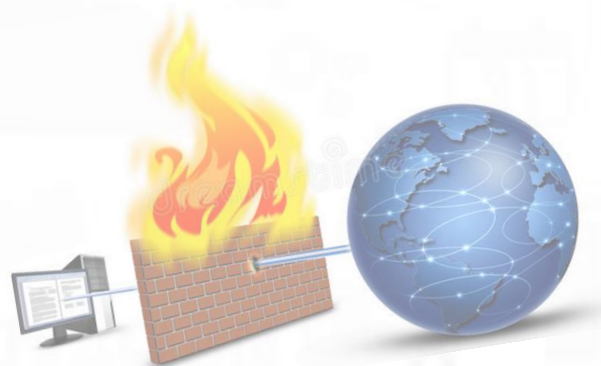
OasisCom define los siguientes lineamientos para llevar el registro de la actividad de los administradores de las plataformas usadas por la empresa:



## ■ 4.4 Sincronización de relojes

OasisCom define los siguientes lineamientos para asegurar la sincronización de relojes en todos sus sistemas de procesamiento:

- ✓ El firewall **sincronizará su fecha y hora** contra un servidor internacional “pool.ntp.org”.
- ✓ Se configura el Firewall FortiGate como **servidor horario**.
- ✓ Los sistemas de cómputo usados por la empresa, se configuran para sincronizar su fecha y hora usando el firewall FortiGate como servidor horario.



## ■ 5. Gestión de la vulnerabilidad técnica



### Objetivo

Prevenir el  
aprovechamiento de las  
vulnerabilidades técnicas

## ■ 5.1 Gestión de las vulnerabilidades técnicas

Se definen los siguientes lineamientos para asegurar la gestión de vulnerabilidades técnicas en sus sistemas de procesamiento técnico.



- ✓ Se mantendrá actualizado el inventario de activos de información y el de Hardware y Software, que faciliten la gestión de la vulnerabilidad técnica.
- ✓ El **equipo de seguridad de la información** será el responsable de estar atento al reporte de cualquier vulnerabilidad técnica que pueda afectar cualquiera de los sistemas de procesamiento críticos de la compañía (con riesgos críticos).

## ■ 5.1 Gestión de las vulnerabilidades técnicas

Se definen los siguientes lineamientos para asegurar la gestión de vulnerabilidades técnicas en sus sistemas de procesamiento técnico.



- ✓ El equipo de seguridad de la información deberá **evaluar los posibles riesgos** que pueda materializar una vulnerabilidad identificada, y así plantear acciones para su gestión.
- ✓ Cuando una vulnerabilidad técnica sea reportada, se esperará a que el proveedor libere un parche y que algunos otros usuarios comenten sobre su **efectividad**, antes de desplegarla en los sistemas de procesamiento de la empresa.



## ■ 5.1 Gestión de las vulnerabilidades técnicas

Se definen los siguientes lineamientos para asegurar la gestión de vulnerabilidades técnicas en sus sistemas de procesamiento técnico.



- ✓ En los equipos de cómputo, las actualizaciones automáticas del sistema operativo y herramientas de seguridad (antivirus u otro), deberán estar siempre activas para **minimizar riesgos** por vulnerabilidades en dichas aplicaciones.
- ✓ Toda acción sobre detección y corrección de vulnerabilidades técnicas será **registrada** y se le hará **seguimiento** mediante el sistema OASISCOM en la opción **AMEJ**.

## ■ 5.1 Gestión de las vulnerabilidades técnicas

Se definen los siguientes lineamientos para asegurar la gestión de vulnerabilidades técnicas en sus sistemas de procesamiento técnico.



- ✓ Para minimizar una posible materialización de riesgos por vulnerabilidades técnicas, se **mantendrá siempre activo el Firewall** (FortiGate) para que realice las primeras inspecciones en los servicios usados por la compañía restringiendo el acceso a puertos, direcciones y aplicaciones permitidas por la empresa.
- ✓ Una vez al año se hará una revisión de hacking ético para **identificar posibles vulnerabilidades** y tomar las acciones respectivas para evitar la materialización de cualquier riesgo.

## ■ 5.2 Restricciones sobre la instalación de software

OasisCom define y documenta en [PR\\_SGSI\\_03\\_Procedimientos \\_y\\_Políticas \\_Operacionales](#) los lineamientos sobre las restricciones a la instalación y/o actualización de software:



- ✓ Están a cargo del Director de Infraestructura o Gestor de Soporte Nivel 1 con previa autorización del [Oficial de Seguridad de la Información](#).
- ✓ Los usuarios con derechos de acceso privilegiados pueden realizar la instalación y/o actualización de software siempre que sea [autorizado](#) por el Oficial de Seguridad de la Información.

## ■ 6. Consideraciones sobre auditorías de sistemas de información



### Objetivo

Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos (Operational Systems)

## ■ 6.1 Controles sobre auditorías de sistemas de información

OasisCom define su control en el documento [PR\\_SIG\\_03\\_Procedimiento\\_Auditorías\\_Internas](#).

Se realizan con el fin de verificar el correcto funcionamiento de los sistemas.

- El administrador de cada plataforma debe asegurar los accesos correspondientes para su revisión.
- En el [FO\\_SIG\\_13\\_Plan\\_Auditoría\\_Interna\\_Técnica](#) se define el alcance, sea controlado y las actividades a realizar.
- Las pruebas se deben limitar a acceso a software y datos únicamente para lectura y las que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales.
- Seguimiento de todos los accesos y registrarlos para producir un rastro de referencia.

