



[www.oasiscom.com](http://www.oasiscom.com)

## ¿QUÉ ES UNA VULNERABILIDAD?

Debilidad de un activo o control que puede ser explotado por una o más amenazas.

## ¿QUÉ ES UN EVENTO?

Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles o una situación desconocida que puede ser relevante para la seguridad.

## **¿QUÉ ES UN INCIDENTE?**

Toda acción que genere un impacto en la operación con respecto a la Seguridad de la Información teniendo en cuenta la confidencialidad, disponibilidad e integridad de los activos.

# ¿Qué deberíamos reportar?

“¿Se debe reportar  
terceros sin  
acompañamiento?  
¿Por qué?”





**¡SÍ!** Es una política del  
SGSI que todo visitante  
esté acompañado,  
además, estaría en riesgo  
la información tanto  
digital como física de  
OasisCom.



“¿Los  
visitantes  
pueden tener  
acceso a las  
redes  
privadas?”





**¡No!** las redes privadas de OasisCom son para uso exclusivo de los colaboradores, los visitantes deben acceder por la Red de Invitados, la cual tiene algunas restricciones de seguridad.



“¿Por qué debo bloquear mi equipo si tengo una contraseña genérica?”

"¿Realmente es necesario bloquear el equipo si este se encuentra dentro del área?"



- ✓ Recuerda que debemos tener una **contraseña personal** en nuestro equipo
- ✓ Estamos expuestos a **acceso no autorizado** por parte de terceros o de los mismo colaboradores de OasisCom.

“¿Los antivirus sin licencia son un riesgo para la seguridad de la información?”





**¡No!** Recordemos que todo software instalado en los equipos debe estar validado por el Oficial de Seguridad la Información.

Si el software no cuenta con una versión gratuita se debe adquirir la licencia por requisito legal.

“¿Es necesaria la restricción de acceso a bases de datos y ambientes de determinada área para algunos colaboradores de ésta?”

“¿La norma ISO 27001:2013 lo plantea así?”







**¡Sí!** La empresa es quien define estas restricciones basados en el conocimiento, experiencia y grado de responsabilidad del colaborador.

La norma sólo pide que se controle el acceso a la información por seguridad.



“¿El manejar un sólo usuario para todos los colaboradores de determinada área es un riesgo para la seguridad de la información?”





**iSi!** dado que a cualquier cambio realizado por medio de un usuario genérico no se le podrá llevar una trazabilidad de quién lo hizo.

Se debería usar la cuenta corporativa personal de cada uno.



“¿Dejar la llave en el escritorio representa un riesgo para la seguridad de la información?”



**¡Si!** Si guardamos información sensible dentro nuestros escritorios estamos expuestos a robo o alteración de la información sensible por parte de terceros.

- Información impresa
- Equipos

“¿Es un evento de seguridad que los clientes laboren en los puestos de trabajo que están libres sin el acompañamiento de un colaborador de OasisCom?”





**iSi!** Porque pueden tener acceso a los puestos de trabajo que manejen información sensible.

Deben estar acompañados e identificados.

Recordemos que OasisCom cuenta con los ambientes ideales para trabajo con clientes



“¿Quién debe hacer la gestión  
en AMEJ?”

“¿Debe ser la  
persona que lo  
reporta?”







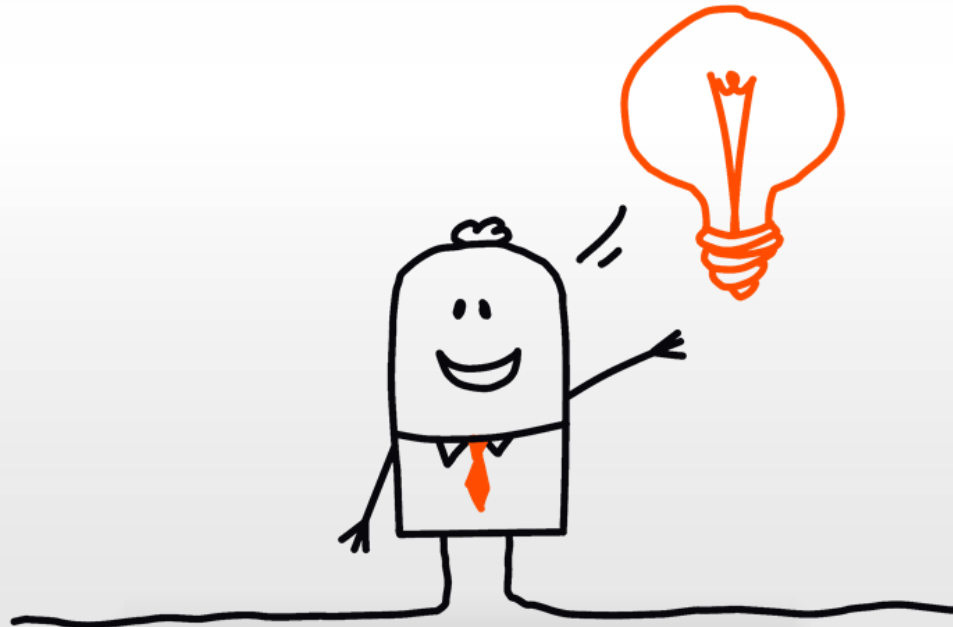
**¿Quién gestiona?**  
**Gestor de Incidentes.**

Lorena Padilla  
Miguel Carvajal  
Fredy Prieto

**¿Quién reporta?**  
Todos los **colaboradores** de  
OasisCom.



A continuación veremos algunos activos y sus posibles afectaciones en cuanto a Seguridad de la Información:



# ANTIVIRUS

VULNERABILIDAD

No tener  
activo el  
antivirus.

EVENTO

Mensaje de  
alerta en el  
equipo.

INCIDENTE

Infección por  
virus en el  
equipo.

# EJEMPLO

Aparece un mensaje informando a cerca de la infección del equipo por un virus.



# ACTIVOS DE CÓMPUTO

## VULNERABILIDAD

Activos en mal estado que no cuenten con los controles definidos por la empresa.

## EVENTO

Alertas del equipo reportando su estado.

## INCIDENTE

Pérdida de la información almacenada en el equipo o pérdida total del activo.

## EJEMPLO

Equipo sin revisión de  
mantenimiento por un lapso de  
tiempo prolongado



Equipo que se recalienta, o su  
rendimiento no es el óptimo.

Pérdida total del equipo o de  
la información allí almacenada



# MANEJO DE INFORMACIÓN SENSIBLE

## VULNERABILIDAD

Falta de controles para el acceso a la información.

## EVENTO

Consulta de información sensible por parte de personal no autorizado.

## INCIDENTE

Divulgación o alteración de dicha información.

# EJEMPLO

- ✓ Archivadores abiertos
- ✓ Computadores desbloqueados.
- ✓ Aplicaciones de OasisCom sin restricción



Intruso en el computador y  
archivador

Pérdida de una hoja de vida o un  
contrato



# INFORMACIÓN Y/O ACTIVO

## VULNERABILIDAD

Falta de información o conocimiento para manipular un activo o manejar información sensible, debido a la falta de manuales, instructivos o procedimientos.

## EVENTO

Solicitud de manuales, instructivos o procedimientos para saber el adecuado manejo de la información y manipulación del activo.

## INCIDENTE

Daño o alteración en el activo y/o corrupción de la información.



- ✓ Falta de documentación
- ✓ Inducción incompleta al puesto de trabajo



Necesidad de capacitación  
en OasisKB.

Eliminación de archivos en OasisKB o  
corrupción de la información en  
OasisCom.



# CARNÉ CORPORATIVO Y PERMISOS

## EVENTO

Ceder el carné o permisos a terceros.

## INCIDENTE

Acceso a información sensible o zonas restringidas por parte de terceros.

## EJEMPLO

Tercero en las instalaciones de  
OasisCom portando las  
credenciales de un colaborador de  
la empresa.



Prestar el usuario para hacer  
alguna modificación a  
información sensible.

# COPIAS DE SEGURIDAD

## VULNERABILIDAD

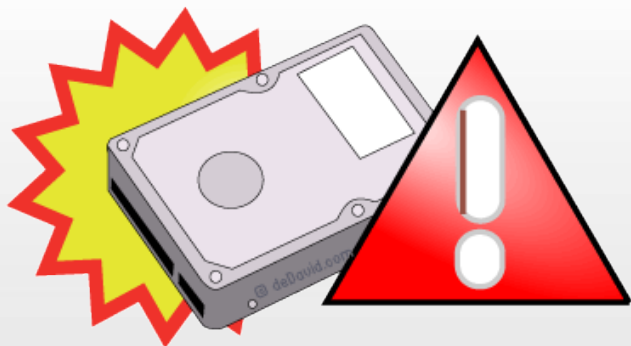
No realizar  
copias de  
seguridad.

## INCIDENTE

Perder información  
sensible o importante  
al no tener copias de  
respaldo.

## EJEMPLO

Almacenar información  
comercial, de proyectos o  
financiera en el equipo local.



Daño con pérdida  
total del disco duro  
del portátil.

# INFORMACIÓN VÍA CORREO

## EVENTO

Enviar correo electrónico revelando información sin autorización o de forma accidental.

## INCIDENTE

Repercusiones negativas sobre el alcance que puedan tener terceros sobre dicha información confidencial.

## EJEMPLO

Envío de un contrato vía correo electrónico a una persona equivocada por diligenciar mal el correo.



Secuestro de información  
Aprovechamiento de información  
para fines comerciales  
Suplantación de personal de  
OasisCom.