

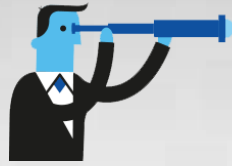


[www.oasiscom.com](http://www.oasiscom.com)

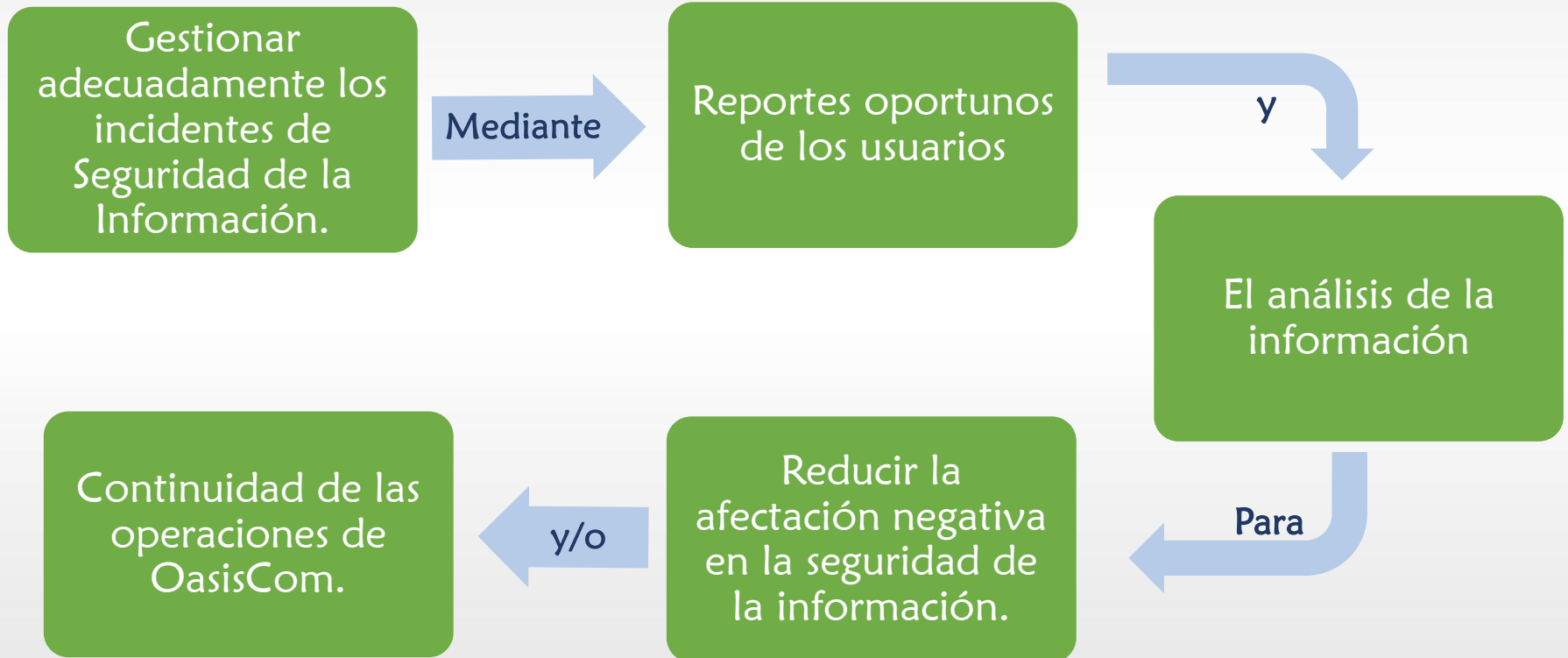
# Capacitación Procedimiento Gestión de Incidentes (SGSI)

Norma ISO/IEC 27001: 2013

- ✓ Objetivo del procedimiento  
Gestión de Incidentes
- ✓ Responsables del procedimiento
- ✓ Políticas
- ✓ Conceptos
- ✓ Roles que participan en el  
proceso
- ✓ Equipo de Seguridad de la  
Información
- ✓ Prevención de incidentes
- ✓ Política de comunicación
- ✓ Proceso para contacto con  
autoridades
- ✓ Reporte y registro de eventos
- ✓ Categorización de eventos
- ✓ Niveles de criticidad
- ✓ Tiempos de respuesta
- ✓ Procedimiento Gestión de Incidentes



# Objetivo del procedimiento





Reportar todo evento que pueda afectar la C, I y/o D de la información.

No poner a prueba las debilidades del SGSI.

Se debe dar prioridad a los incidentes en estado **Crítico** que afecten la operación de la empresa.

Quien incurra en alguna falta al SGSI se iniciará un proceso disciplinario.



EVENTO	DEBILIDAD	INCIDENTE
<p>Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad y disponibilidad de los datos.</p>	<p>Suceso identificado que <b>puede ser materia para que se materialice un riesgo y genere un incidente.</b> Una debilidad reportada con tiempo de antelación puede ser tratada y evitar posibles daños en la seguridad de la información.</p>	<p>Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una <b>probabilidad significativa de comprometer las operaciones del negocio</b> y amenazar la seguridad de la información.</p>

# Roles que participan en el proceso

## Oficial de Seguridad de la Información

- ✓ Orientar y dar adecuado tratamiento a los incidentes de seguridad de la información detectados o reportados.
- ✓ Debe hacer un seguimiento periódico a los incidentes de seguridad presentados.
- ✓ Debe mantener contactos apropiados con las autoridades y grupos de interés.





# Roles que participan en el proceso

## Colaboradores y contratistas

- ✓ Tomar conciencia de su responsabilidad de reportar eventos y debilidades.
- ✓ Recibir las capacitaciones y participar en las campañas de sensibilización que se realicen al interior de la entidad.
- ✓ Reportar oportunamente los incidentes o eventos de seguridad de la información y cualquier comportamiento anormal que se presente en la empresa o en sus activos de información.



# Roles que participan en el proceso

## Gerencia Administrativa y Financiera

- ✓ Hacer la valoración económica del activo de información involucrado en un evento/incidente de Seguridad de la Información.

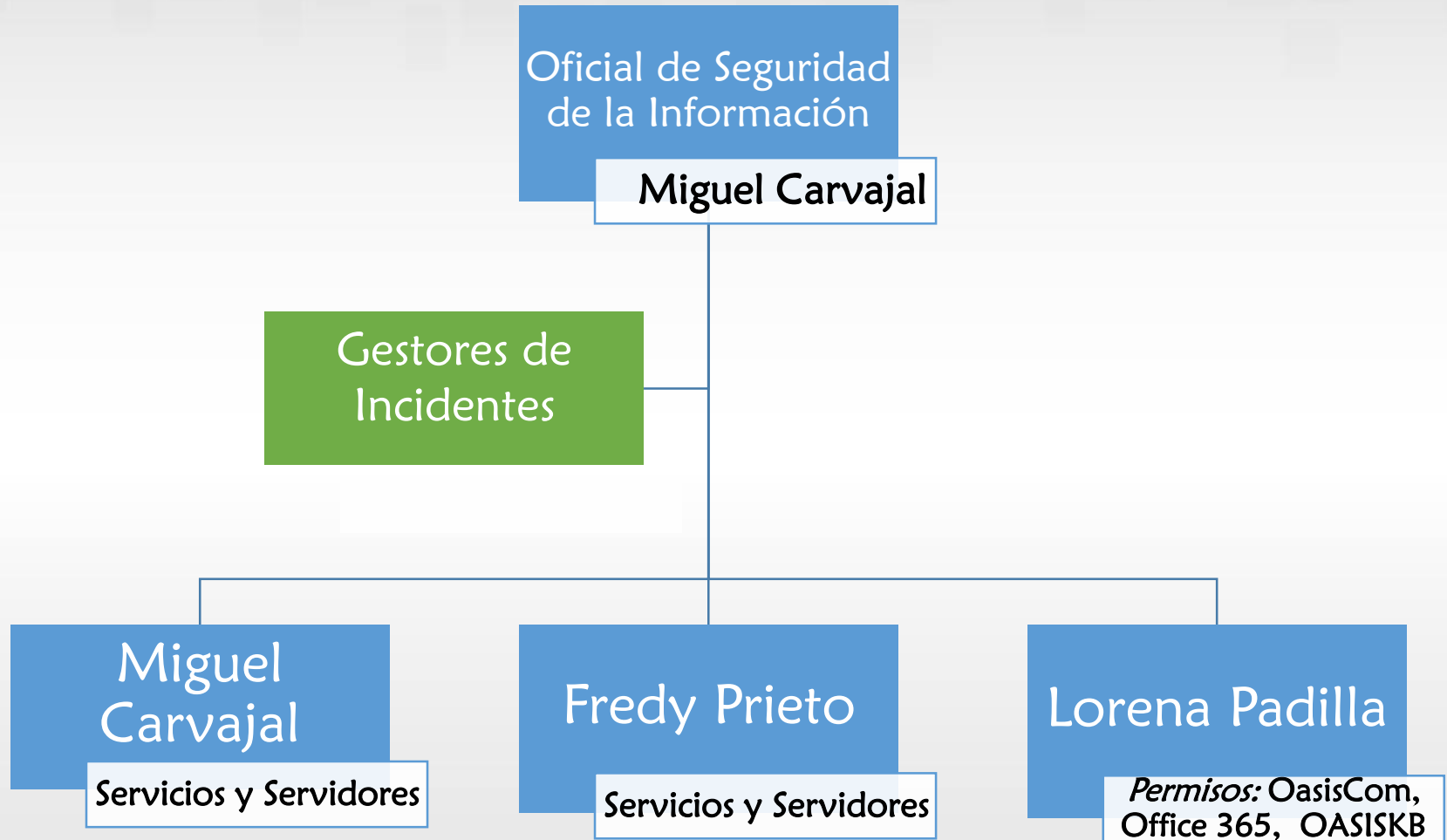


## Analista de Procesos

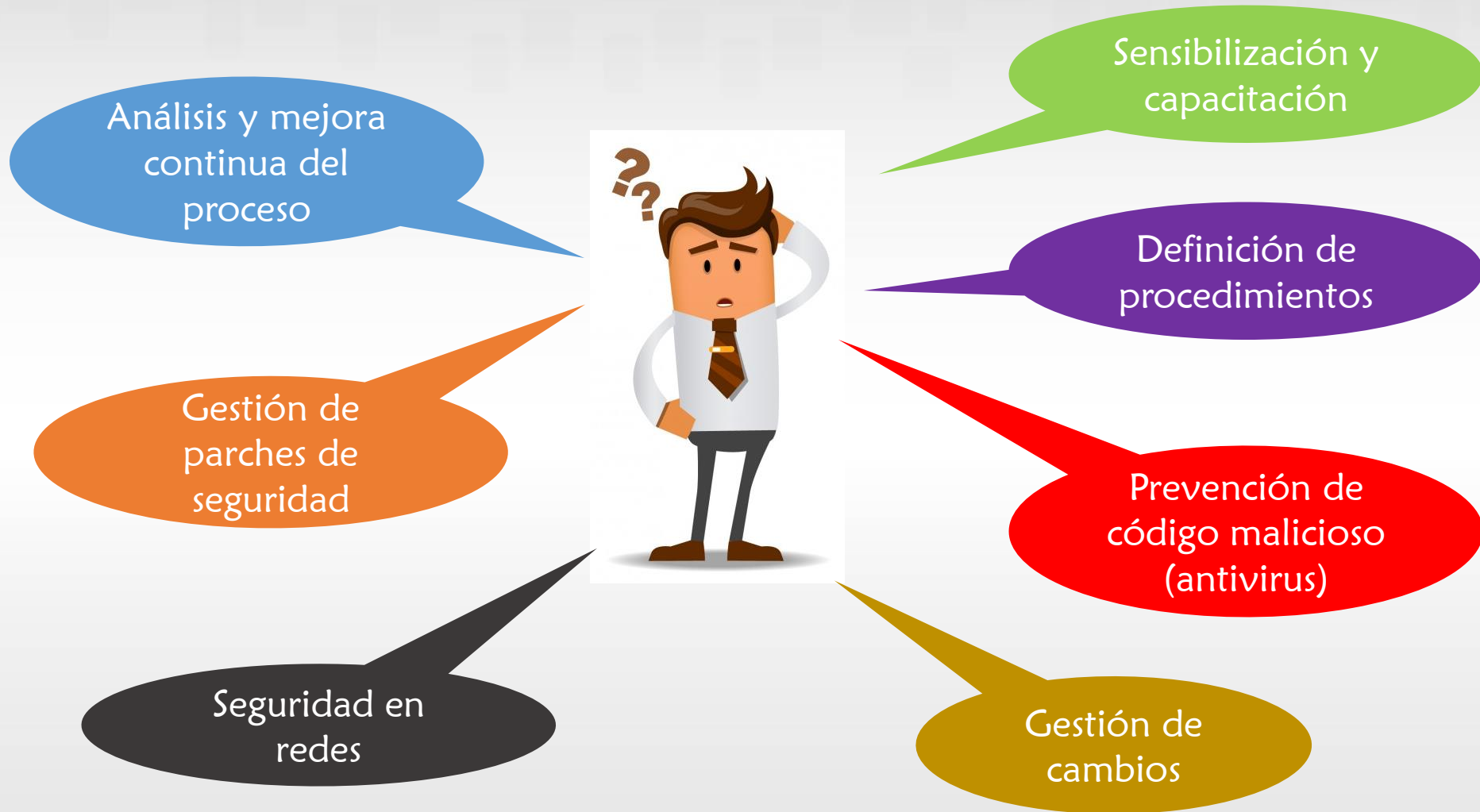
- ✓ Mantener constante capacitación y sensibilización en cuanto al reporte de incidentes de Seguridad de la Información.



# Equipo de Seguridad de la Información



# Prevención de incidentes



# Política de comunicación

OasisCom comunica internamente los incidentes presentados que pueden afectar la operación de la empresa.



OasisCom comunica en su página web y redes sociales los incidentes que puedan afectar a las demás empresas del sector.

# Proceso para contacto con autoridades



Los incidentes categorizados como **críticos**, (Intento o robo de información), según análisis del Oficial de Seguridad de la Información y las Gerencias de OasisCom serán reportados a las instancias correspondientes.

- ❖ Policía Nacional de Colombia
- ❖ Fiscalía General de la Nación
- ❖ MinTIC

# Reporte y registro de eventos

Canal principal  
para reportar



**AMEJ - MEJORAS**



**Fecha y hora:** reporte, descubrimiento del incidente, inicio y fin de la investigación.

**Nombre completo:** de quien reporta, quien registra, quien investiga.

**Descripción del evento o incidente.**

**Elementos involucrados en el evento:** hardware, software, datos, procesos.

**Resultados de la investigación.**

Canal alternativo  
para reportar



**seguridadinformacion@oasiscom.com**

✓ Colaboradores de OasisCom

✓ Contratistas

✓ Clientes de OasisCom



La respuesta al reporte se realizará por correo electrónico





## Categorización de eventos, debilidades e incidentes

EVENTOS	DEBILIDADES	INCIDENTES
✓ Acceso a los sistemas de información.	✓ Fallas de monitoreo.	✓ Ataques: dirigidos, no dirigidos, internos, externos.
✓ Denegación de servicios.	✓ Falta de conocimiento.	✓ Código dañino.
✓ Acceso no autorizado.	✓ Ausencia de controles.	✓ Daños físicos.
✓ Información no actualizada.	✓ Configuración deficiente.	✓ Abuso de privilegios y usos inadecuados.
✓ Alarmas de sistemas de monitorización		✓ Fuga de información.
✓ Mala gestión del conocimiento.		✓ Corrupción de la información.
✓ Diligenciamiento errado de la información.		✓ Ingreso no autorizado.

# Niveles de criticidad



## Crítico/alto

- ✓ Representa una seria amenaza.
- ✓ Afecta de forma inmediata uno o más activos de la información.
- ✓ Pone en peligro información sensible.



## Moderado/medio

Es un evento que puede ser una amenaza potencial, pero que no se identifica como una amenaza seria y/o inmediata.



## Insignificante/bajo

Es un evento que podría ser una amenaza menor o es el resultado de una actividad no autorizada, pero que no compromete recursos críticos o información sensible.

# Tiempos de respuesta



**Alto**

Máximo 8 horas hábiles

**Medio**

Máximo 24 horas hábiles

**Bajo**

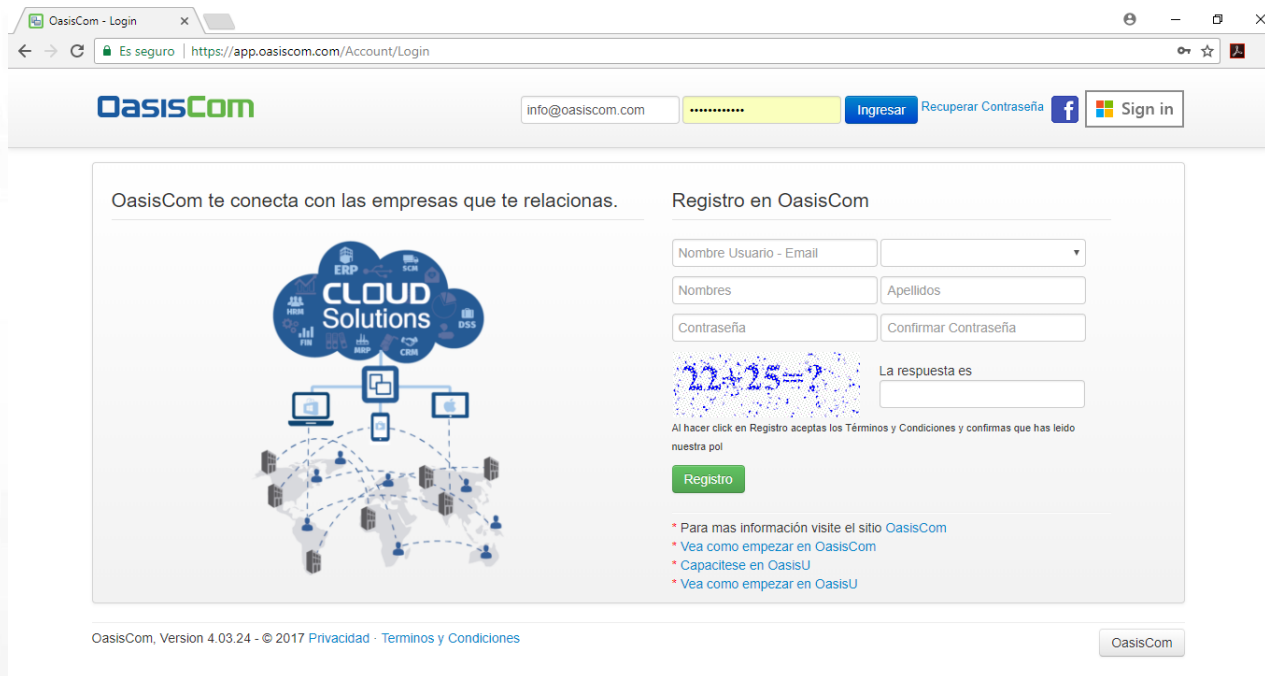
Máximo 48 horas hábiles

# Procedimiento Gestión de Incidentes



# Reporte de Eventos de Seguridad de la Información en AMEJ

Ingresa este link: <http://www.app.oasiscom.com/>



The screenshot shows a web browser window with the address bar displaying "https://app.oasiscom.com/Account/Login". The page features the OasisCom logo and a navigation bar with a search bar, a login button, and a "Recuperar Contraseña" link. Below the navigation bar, there is a section titled "OasisCom te conecta con las empresas que te relacionas." which includes a diagram of a cloud network. To the right of this section is a "Registro en OasisCom" form. The form contains fields for "Nombre Usuario - Email", "Nombres", "Apellidos", "Contraseña", and "Confirmar Contraseña". There is also a CAPTCHA image showing the equation "22+25=?" and a text input field for the answer. A green "Registro" button is located below the CAPTCHA. At the bottom of the page, there is a footer with the text "OasisCom, Version 4.03.24 - © 2017 Privacidad · Terminos y Condiciones" and a small "OasisCom" logo.

OasisCom - Login x

Es seguro | <https://app.oasiscom.com/Account/Login>

OasisCom

info@oasiscom.com

Ingresar

Recuperar Contraseña

f Sign in

OasisCom te conecta con las empresas que te relacionas.

Registro en OasisCom

Nombre Usuario - Email

Nombres

Apellidos

Contraseña

Confirmar Contraseña

22+25=?

La respuesta es

Al hacer click en Registro aceptas los Términos y Condiciones y confirmas que has leído nuestra pol

Registro

\* Para mas información visite el sitio [OasisCom](#)

\* [Vea como empezar en OasisCom](#)

\* [Capacitese en OasisU](#)

\* [Vea como empezar en OasisU](#)

OasisCom, Version 4.03.24 - © 2017 Privacidad · Terminos y Condiciones

OasisCom

## Reporte de Eventos de Seguridad de la Información en AMEJ

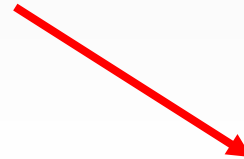
Ingresa con tu usuario y contraseña



<input type="text" value="info@oasiscom.com"/>	<input type="password" value="....."/>	<input type="button" value="Ingresar"/>	<a href="#">Recuperar Contraseña</a>		 <input type="button" value="Sign in"/>
--	--	---	--------------------------------------	---	--

## Reporte de Eventos de Seguridad de la Información en AMEJ

Ingresa a la aplicación AMEJ (Oportunidades de Mejoras)



Home Oportunidades De Mejora - [amej] x


AMEJ

amej - Oportunidades De Mejora

Documento	Número	Ubicación	Fecha	Hora	Ubicación1	Concepto	Proyecto	Prioridad	Tercero	Nombre Tercero	Estado	Empleado	Nombre Empleado
-----------	--------	-----------	-------	------	------------	----------	----------	-----------	---------	----------------	--------	----------	-----------------

## Reporte de Eventos de Seguridad de la Información en AMEJ

Crea un nuevo reporte dando click en el símbolo +



The screenshot shows the OasisCom S.A.S. interface. The top header is blue with the OasisCom logo and 'OASISCOM S.A.S.'. Below the header, there's a navigation bar with 'Home' and 'Oportunidades De Mejora -[amej]'. A red arrow points to the '+' icon in the toolbar. The toolbar contains various icons for document management. Below the toolbar is a table with the following columns: Documento, Número, Ubicación, Fecha, Hora, Ubicación1, and Concepto. The table has one empty row for data entry. The bottom right corner shows 'Página 1'.

	Documento	Número	Ubicación	Fecha	Hora	Ubicación1	Concepto
<input type="checkbox"/>							



# Reporte de Eventos de Seguridad de la Información en AMEJ

Documento **IS**

Ingreso automático

Ubicación **0**

Estos campos se diligencian automáticamente

Home Oportunidades\_De\_Mejora [-amej] x

Agregar registro

Documento	<b>IS</b>	Número		Ubicación	<b>0</b>	Fecha	19/02/2019	Hora	18:06
Ubicación1	<b>100</b>	Concepto	<b>IS</b>	Proyecto	<b>10100</b>	Prioridad		Tercero	830003840
Nombre Tercero	OASISCOM S.A.S.	Estado		Empleado	1033779173	Nombre Empleado	PADILLA AMORTEGUI	Descripcion	
Tipo de Medio		Nombre de tipo de medios		Tema		Nombre Tema		Observacion	
Periodo	2	Año	2019						

Área o gerencia en donde se presenta el evento

Concepto **IS**

Proyecto **10100**

Campo diligenciado por el Gestor de Incidentes

Guardar Cancelar

# Reporte de Eventos de Seguridad de la Información en AMEJ

Nit. de OasisCom  
830003840

Home Oportunidades\_De\_Mejora -[amej] x

Agregar registro

Documento	IS	Número		Ubicación	0	Fecha	19/02/2019	Hora	18:06
Ubicación1	100	Concepto	IS	Proyecto	10100	Prioridad		Tercero	830003840
Nombre Tercero	OASISCOM S.A.S.	Estado		Empleado	1033779273	Nombre Empleado	PADILLA AMORTEGUI M	Descripcion	
Tipo de Medio		Nombre de tipo de medios		Tema		Nombre Tema		Observacion	
Periodo	2	Año	2019						

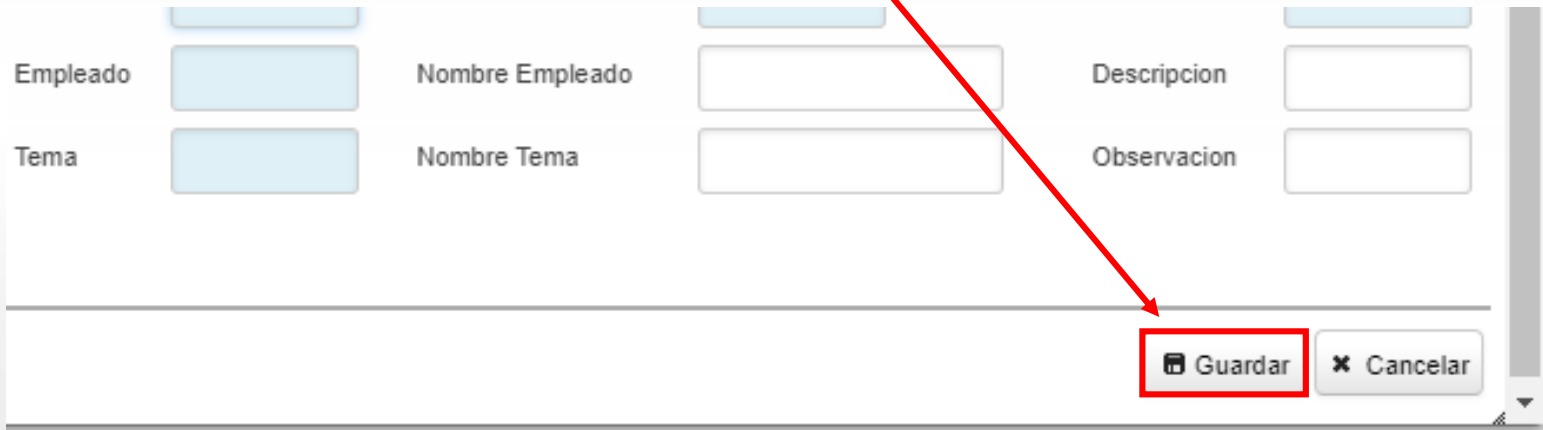
Guardar Cancelar

Cédula de la persona  
que reporta el evento

Describa detalladamente el  
evento que se le presentó  
o identificó

# AMEJ

## Guardar el registro



The screenshot shows a web form for 'AMEJ' with the following fields:

Empleado	<input type="text"/>	Nombre Empleado	<input type="text"/>	Descripcion	<input type="text"/>
Tema	<input type="text"/>	Nombre Tema	<input type="text"/>	Observacion	<input type="text"/>

At the bottom right, there are two buttons: 'Guardar' (highlighted with a red box and a red arrow pointing to it) and 'Cancelar'.

# iGRACIAS!

## ¡FUGA DE INFORMACIÓN!

### Escenario:

- ✓ Formáis parte de un negocio de ingeniería que tiene una oficina con algunos ordenadores, una red con wifi y conexión a internet. Proporcionáis acceso remoto a los sistemas de la empresa a vuestros colaboradores, que trabajan a distancia.
- ✓ Para vuestra actividad tenéis contratados: la conexión a internet, el alojamiento web para la tienda online, los servicios de una gestoría y el soporte informático.
- ✓ Vais a lanzar el diseño de un nuevo producto, en el que lleváis trabajando los últimos seis meses.
- ✓ En el último año ha habido muchos cambios de colaboradores externos, unos se han ido y otros son nuevos.
- ✓ Una empresa de nueva creación acaba de sacar al mercado un diseño exactamente igual al que estas a punto de lanzar. Sospechas que alguno de los colaboradores de esa empresa trabajaron en el pasado en tu empresa.

## ¿Qué ha pasado?

✓ Dudáis si revocasteis el acceso remoto a los sistemas de la empresa a los ex empleados que dejaron la empresa. Lo comprobáis, no se lo revocasteis. Se lo pusisteis en bandeja.

✓ No han podido tener acceso porque habías cifrado la información confidencial ¿o no? El procedimiento existe pero, en este caso no lo estabais aplicando.

✓ No recordáis si habían firmado un acuerdo de confidencialidad pues eso lo lleva la gestoría que se ocupa de los RRHH. Lo comprobáis y sí los habían firmado. Podéis emprender acciones legales.

✓ Afortunadamente, los registros de acceso a los sistemas estaban activos y teníais copia de seguridad de los mismos. Así identificáis el momento y el usuario que se ha «llevado» el diseño. Ha sido un antiguo colaborador, hace unas semanas.

✓ Las pérdidas económicas serán importantes, pues os van a pisar el mercado y los inversores perderán su confianza en vosotros.

✓ En este caso, no afecta a información personal de clientes o proveedores, si hubiera sido así tendríais problemas con la AGPD (Agencia de Protección de datos) por incumplir la LOPD, que hubiera podido conllevar sanciones económicas.

# Actividad 1

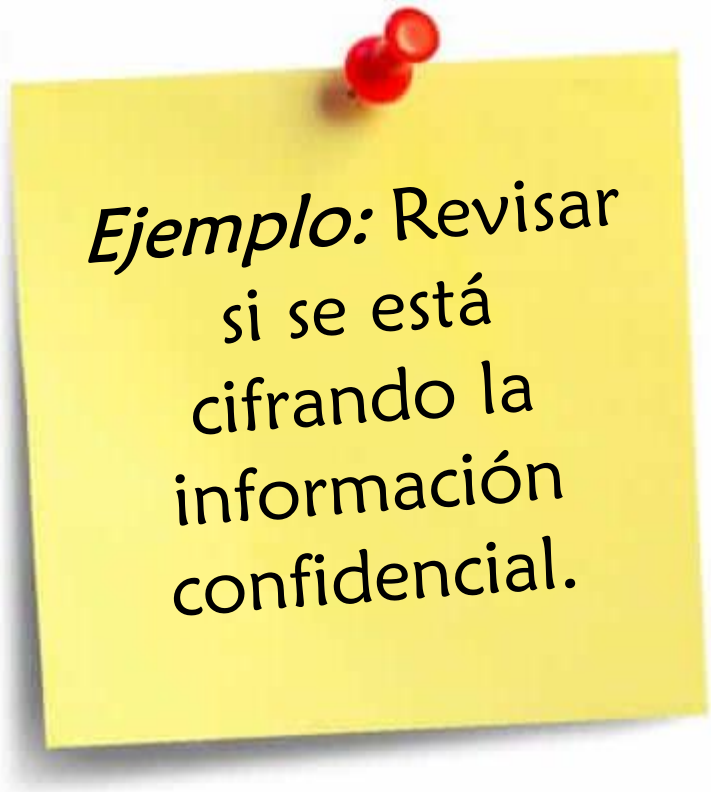
## Preguntas Guía

1. ¿Qué ha ocurrido?
2. ¿Dónde se ha originado?
3. ¿Qué dispositivos están afectados?
4. ¿Cuándo o desde cuándo ocurre?
5. ¿Quién ha podido hacerlo, por qué y cómo? Posibles causas.
6. ¿Cuáles son los daños materiales, personales y económicos? ¿Podemos valorarlos?
7. ¿Tendremos que avisar a nuestros clientes o usuarios?
8. ¿Tiene consecuencias sobre nuestra reputación?
9. ¿Tiene implicaciones legales?



**10 minutos**

# ¿Qué pueden hacer?



*Ejemplo:* Revisar  
si se está  
cifrando la  
información  
confidencial.



**5 minutos**



## Actividad 2

# ¿Qué pueden hacer?

Mantener la calma, evaluar la situación para valorar los daños y las causa, y así actuar en consecuencia.

Revisar si los colaboradores que ya no trabajan en la empresa habían firmado acuerdos de confidencialidad para emprender acciones legales por esta parte.

Ponerse en contacto con las autoridades correspondientes.

Identificar si ha habido una causa técnica, un error de procedimiento o una causa intencional (algún empleado interno) que haya permitido la fuga de información.

Firmar acuerdos de confidencialidad con cada empleado y colaborador donde acepten, por escrito, las políticas internas de confidencialidad y seguridad, y las sanciones a las que se exponen en caso de incumplirse.

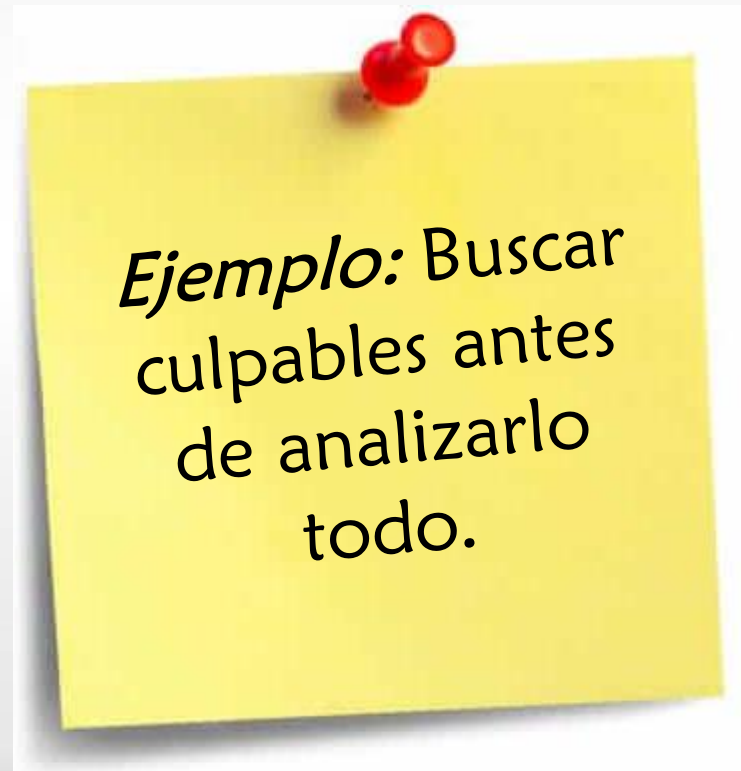
Revisar los permisos de los antiguos empleados. Revocar los permisos de los colaboradores que ya no trabajan en la empresa.

Incorporar medidas técnicas que detecten e impidan la fuga de información confidencial.

# ¿Qué no deben hacer?



**5 minutos**



## Actividad 3

# ¿Qué no deben hacer?

Ocultar información que pueda estar relacionada con el problema.

No establecer control de acceso a los documentos confidenciales.

Intentar resolverlo tú sólo, sin buscar ayuda.

No cifrar la información confidencial, no destruirla convenientemente o no aplicar los procedimientos sistemáticamente.

No tener control sobre las cuentas de acceso a los colaboradores..

No guardar registro de los accesos a los sistemas.

Dar permisos a los servicios críticos de la empresa o de acceso a directorios con información confidencial de manera indiscriminada, a todos los usuarios.

# ¿Cómo podrías evitarlo? Lecciones aprendidas

*Ejemplo: Tener a mano la lista de contactos de apoyo y de denuncia para estos casos.*



**5 minutos**

## ¿ Cómo podrías evitarlo?

Es importante realizar una clasificación para tener identificada la información confidencial. Así la podremos proteger adecuadamente

Tenemos que analizar nuestros riesgos, pues está claro que esto puede ocurrir pero no debe volver a pasar, tenemos que tomar medidas

Tener presente el procedimiento de Gestión de Incidentes para aplicarlo.

Siempre firmaremos acuerdos de confidencialidad con los empleados y colaboradores que hayan de manejar información confidencial. Estos acuerdos se extenderán más allá del contrato laboral.

Tenemos que tener a mano la lista de contactos de apoyo y de denuncia para estos casos.

# Reportar incidente en AMEJ - OasisCom

Como actividad, responde las preguntas e ingresa a AMEJ de OasisCom y registra el incidente (FUGA DE INFORMACIÓN)

En el campo “Observación” indicar que es “Actividad de Capacitación Gestión de Incidentes”