

# Taller de capacitación y concientización: Ciberseguridad documental de los sistemas contables legales.

Elsa Beatriz Suarez Kimura y Diego Sebastian Escobar.

Cita:

Elsa Beatriz Suarez Kimura y Diego Sebastian Escobar (2017). *Taller de capacitación y concientización: Ciberseguridad documental de los sistemas contables legales. Conferencia Interamericana de Contabilidad 2017. Asociación Interamericana de Contabilidad, Lima.*

Dirección estable: <https://www.aacademica.org/escobards/23>

ARK: <https://n2t.net/ark:/13683/ptuD/5kR>



Esta obra está bajo una licencia de Creative Commons.  
Para ver una copia de esta licencia, visite  
<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es>.

*Acta Académica es un proyecto académico sin fines de lucro enmarcado en la iniciativa de acceso abierto. Acta Académica fue creado para facilitar a investigadores de todo el mundo el compartir su producción académica. Para crear un perfil gratuitamente o acceder a otros trabajos visite: <https://www.aacademica.org>.*

**Taller de capacitación y concientización:**  
**Ciberseguridad documental de  
los sistemas contables legales**

Disertantes:

Dra. Elsa Beatriz Suarez Kimura

Mg. Diego Sebastián Escobar



# INTRODUCCIÓN



# **SISTEMA DE REGISTROS CONTABLES**

Definiciones

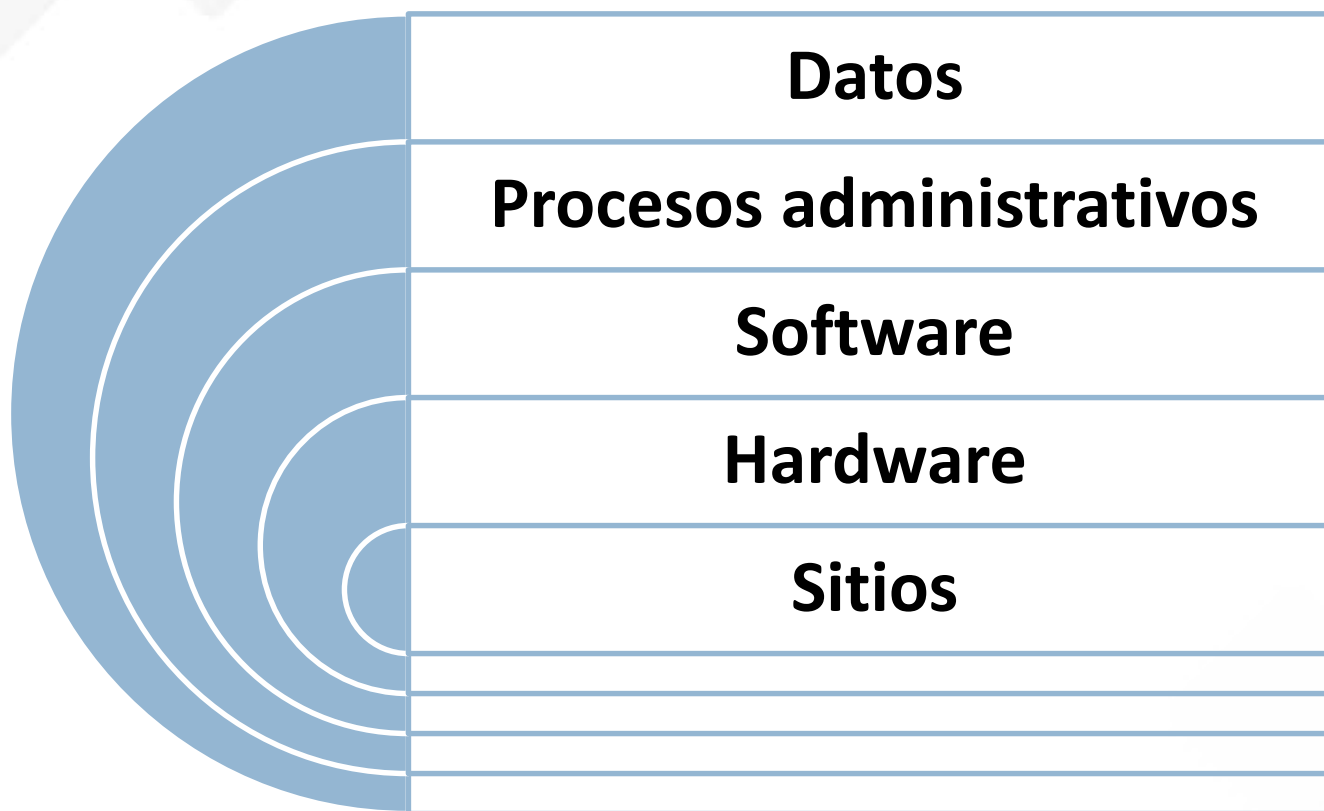


# Definición de sistema de registros

Se entiende como sistema de registro contable al conjunto de elementos interrelacionados, destinados al registro de las operaciones y hechos económicos-financieros. El mismo comprende los elementos de organización, control, guarda o conservación, exposición y análisis.



# Elementos del sistema contable



# Requisitos exigidos en los Sistemas

- Un sistema contable legalmente constituido para tutelar a los terceros en los conflictos individuales y universales, debe satisfacer fundamentalmente dos garantías:

**Asegurar que los registros sean inalterables**

**Asegurar que las registraciones sean verificables**

# Riesgos identificados de llevar los registros contables en soportes tecnológicos

1. Fraude por alteración del registro.
2. Fraude por sustitución del soporte.
3. Virus informático.
4. Perención del soporte.



# **CONSIDERACIONES DE LOS REGISTROS CONTABLES EN LAS SOCIEDADES COMERCIALES**

Requerimientos



# Marco legal de las Sociedades Comerciales

**Código Civil y  
Comercial (2015)**

**Ley General de  
Sociedades  
(2015)**

**Disposición Nro.  
7/2015 de la IGJ  
(Inspección  
General de  
Justicia).**

# Definiciones del código civil y comercial

## ARTICULO N° 329

Sustitución de soporte del sistema de información contable.

La petición que se formule al Registro Público debe contener una adecuada descripción del sistema, **con dictamen técnico de Contador Público** e indicación de los antecedentes de su utilización. Una vez aprobado, el pedido de autorización y la respectiva resolución del organismo de contralor, deben transcribirse en el libro de Inventarios y Balances. (...)

(...) La autorización sólo se debe otorgar si los medios alternativos son equivalentes, en cuanto a **inviolabilidad, verosimilitud y completitud**, a los sistemas cuyo reemplazo se solicita.

# **¿QUÉ CONDICIONES DEBEN CUMPLIR LOS SISTEMAS DE REGISTRACIÓN CONTABLE RESGUARDADOS EN MEDIOS TECNOLÓGICOS?**



# Requisitos de la Seguridad de la Información en el Sistema Contable

Número	Descripción
1	Descripción del proceso administrativo - contable
2	Plataforma de hardware
3	Plataforma de software de base y aplicaciones
4	Política de gestión de seguridad de la información
5	Control de accesos lógicos y físicos
6	Back-up / Archivo de la documentación respaldatoria
7	Pautas de confiabilidad
8	Integridad de los registros contables
9	Resguardo y documentación de los soportes



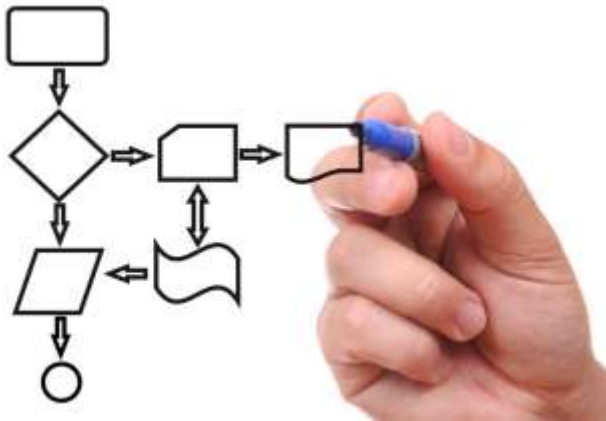
# 1

## ANÁLISIS DEL PROCESO ADMINISTRATIVO-CONTABLE

# Flujograma

- **Confección y análisis del circuito administrativo - contable completo:**

Deben surgir claramente los datos que ingresan a partir de la documentación contable (facturas de compras, ventas, ingresos, egresos, etc.), su procesamiento y la salida que genera, la cual será coincidente con todos los registros contables de la sociedad.





2

## PLATAFORMA DE HARDWARE UTILIZADA



# Descripción del tipo de plataforma de hardware



**Sistemas de micro computadoras**



**Sistemas de Rango Medio**



**Sistema de Computadoras Centrales (Mainframe)**



**Sistemas de computación en la nube**

# Modalidades de Servicio

**SOFTWARE  
COMO  
SERVICIO**

**INFRAESTRUC-  
TURA COMO  
SERVICIO**

**PLATAFORMA  
COMO  
SERVICIO**



# Software como servicio

Estamos en presencia de un modelo de Software como servicio (o SaaS), cuando el usuario encuentra en la nube las herramientas finales con las que puede implementar directamente los procesos de su empresa: una aplicación de contabilidad, de correo electrónico, un workflow, un programa para la gestión documental de su empresa, etc.



# Plataforma como servicio

Entre estas dos aproximaciones se pueden encontrar otras intermedias llamadas PaaS (Plataforma como Servicio), en las que se proporcionan utilidades para construir aplicaciones, como bases de datos o entornos de programación sobre las que el usuario puede desarrollar sus propias soluciones.



# Infraestructura como servicio

En el caso de Nube de infraestructura (IaaS), el proveedor proporciona capacidades de almacenamiento y proceso en bruto, sobre las que el usuario ha de construir las aplicaciones que necesita su empresa prácticamente desde cero. Tal vez se pueda decir que éste es el modelo más primitivo de nube, que se inició con los sitios de Internet que proporcionaban capacidad de almacenamiento masivo a través de la red y los servidores de alojamiento web.



# Plataforma de Hardware utilizada

## Preguntas orientativas:

¿El Hardware utilizado se corresponde con el nivel de transacciones de la operatoria de la empresa?

¿Cuáles son los soportes de los registros contables?

¿Si se cambiaran los soportes, se pueden consultar los registros anteriores en cualquier momento si así fuera requerido?

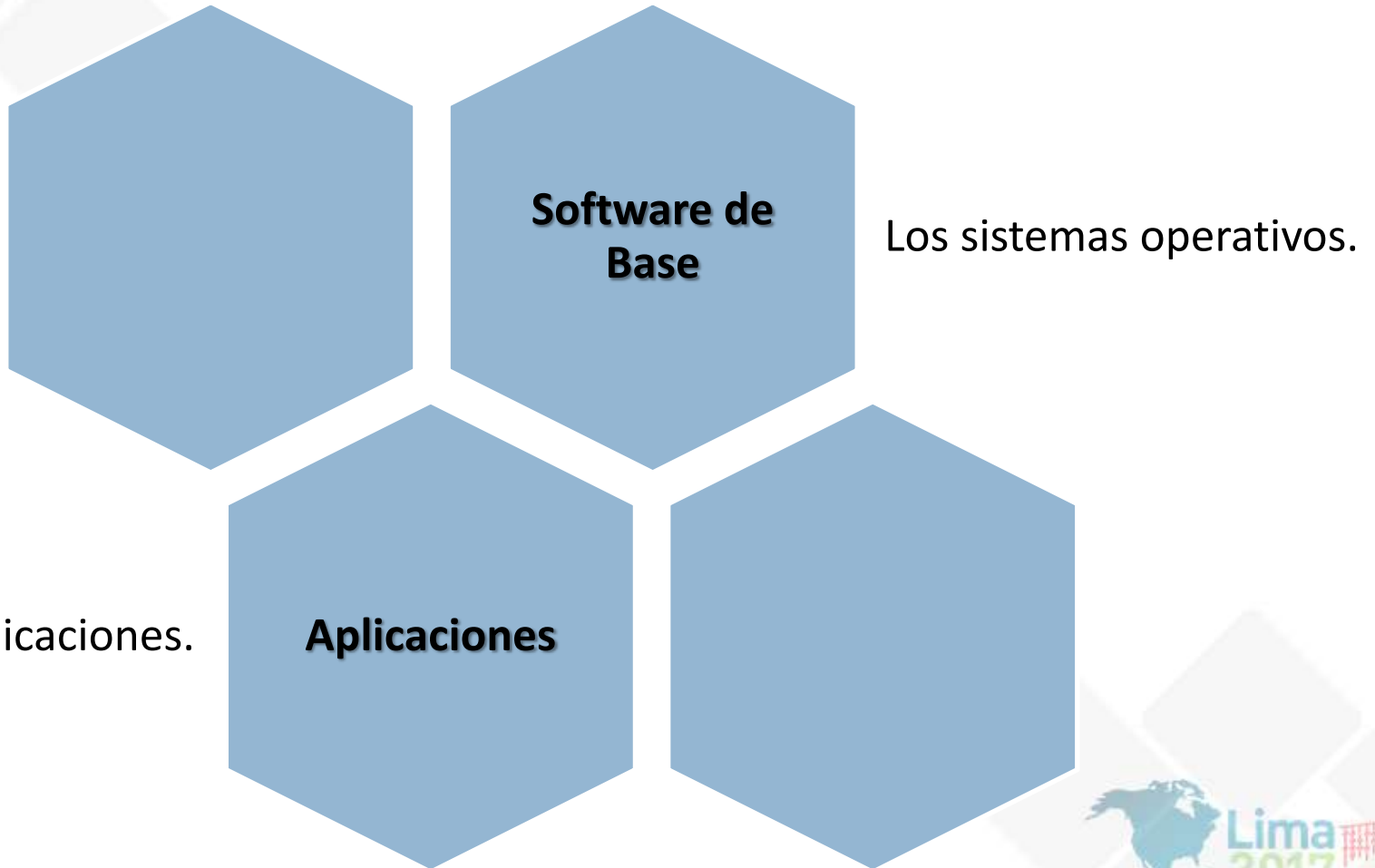




# 3

## **ANÁLISIS DEL SOFTWARE DE BASE Y APLICACIONES UTILIZADAS**

# Plataforma de Software de Base y aplicaciones utilizadas

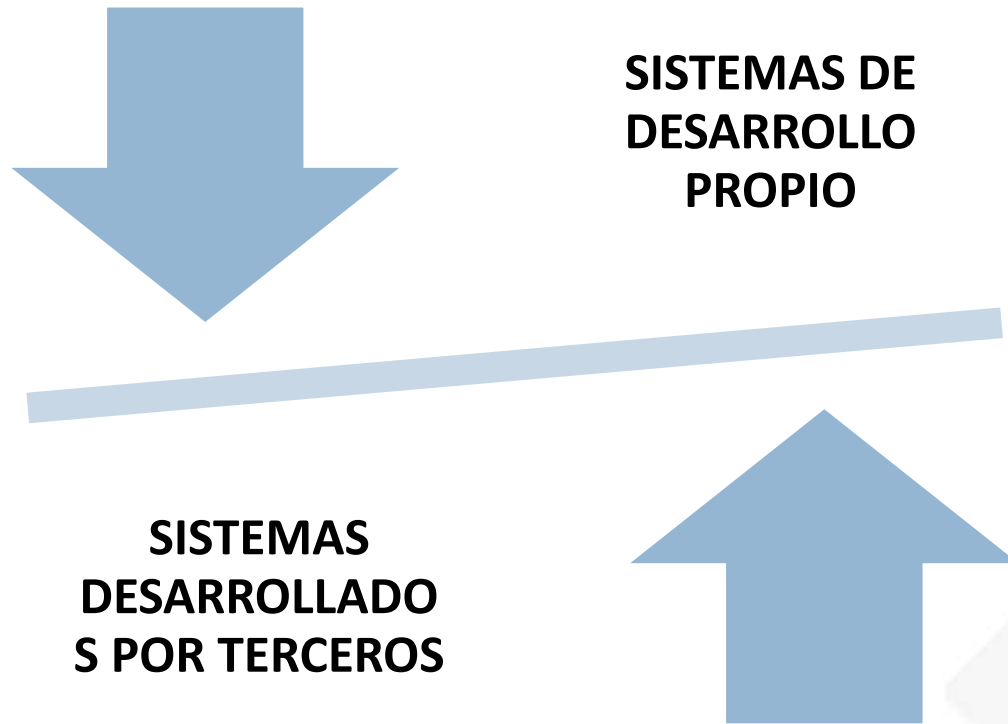


La correcta instalación y actualización del Software utilizado, con herramientas debidamente instaladas.





# Clasificación de los Sistemas de información



# Buenas Prácticas de Seguridad de la Información

## LA DOCUMENTACIÓN DE LOS SISTEMAS DE DESARROLLO PROPIO

- Verificar la documentación del: procesamiento que realiza, los casos de uso, la arquitectura del sistema, los controles para evitar la carga de datos incorrectos,
- Verificar existencia de módulos de auditoría

## LA DOCUMENTACIÓN DE LOS SISTEMAS DESARROLLADOS POR TERCEROS

- Verificar la documentación de los controles para evitar la carga de datos incorrectos.
- Verificar existencia de módulos de auditoría



4

# **POLÍTICA DE GESTIÓN DE SEGURIDAD INFORMÁTICA**



# Política de Gestión de Seguridad de la información

La **política de seguridad** es un documento de alto nivel que se establece el compromiso de la organización con la seguridad de la información.

Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad.

<b>3.</b>	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN .....</b>	<b>11</b>
3.1.	Aspectos Generales.....	13
3.2.	Sanciones Previstas por Incumplimiento.....	14
<b>4.</b>	<b>ORGANIZACIÓN DE LA SEGURIDAD .....</b>	<b>15</b>
4.1.	Infraestructura de la Seguridad de la Información .....	16
4.1.1.	Comité de Seguridad de la Información .....	16
4.1.2.	Asignación de Responsabilidades en Materia de Seguridad de la Información ...	17
4.1.3.	Proceso de Autorización para Instalaciones de Procesamiento de Información ..	18
4.1.4.	Asesoramiento Especializado en Materia de Seguridad de la Información .....	18
4.1.5.	Cooperación entre Organismos.....	18
4.1.6.	Revisión Independiente de la Seguridad de la Información .....	19
4.2.	Seguridad Frente al Acceso por Parte de Terceros .....	19
4.2.1.	Identificación de Riesgos del Acceso de Terceras Partes .....	19
4.2.2.	Requerimientos de Seguridad en Contratos o Acuerdos con Terceros.....	19
4.3.	Tercerización .....	20
4.3.1.	Requerimientos de Seguridad en Contratos de Tercerización .....	20





# 5

## **CONTROL DE ACCESOS LÓGICOS Y FÍSICOS**

# Control de Accesos Lógicos

**Sistema Operativo**

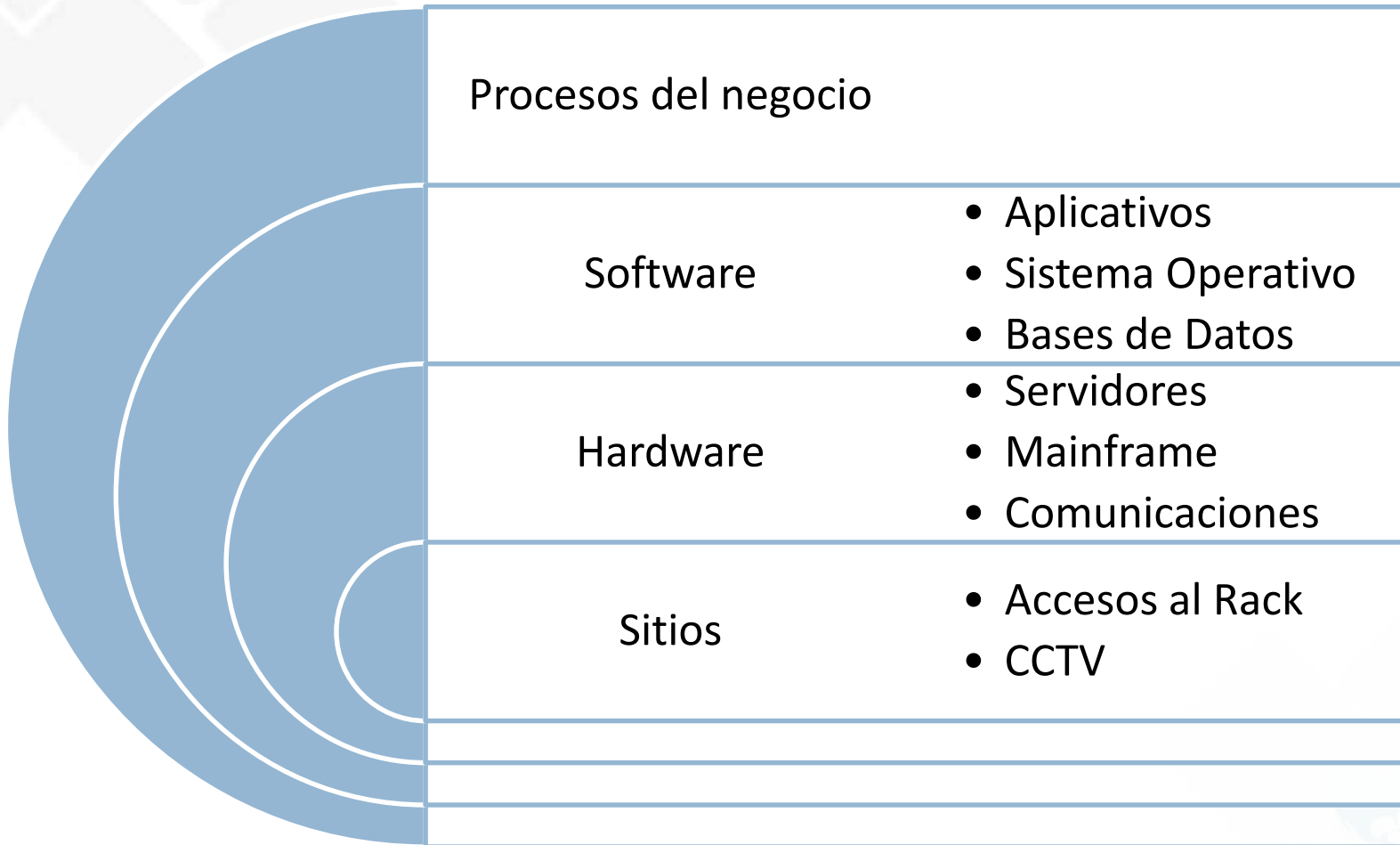
**Bases de datos**

**Aplicaciones**

**LOS  
CONTROLES DE  
ACCESOS  
LÓGICOS**

- Verificar mediante los módulos de auditoría de los sistemas: derechos de acceso y el tratamiento dado a los incidentes de seguridad en el acceso

# Control de Accesos Físicos





6

**BACK-UP / ARCHIVO DE LA  
DOCUMENTACIÓN RESPALDATORIA /  
PLAN DE CONTINGENCIA**





# Copias de resguardo

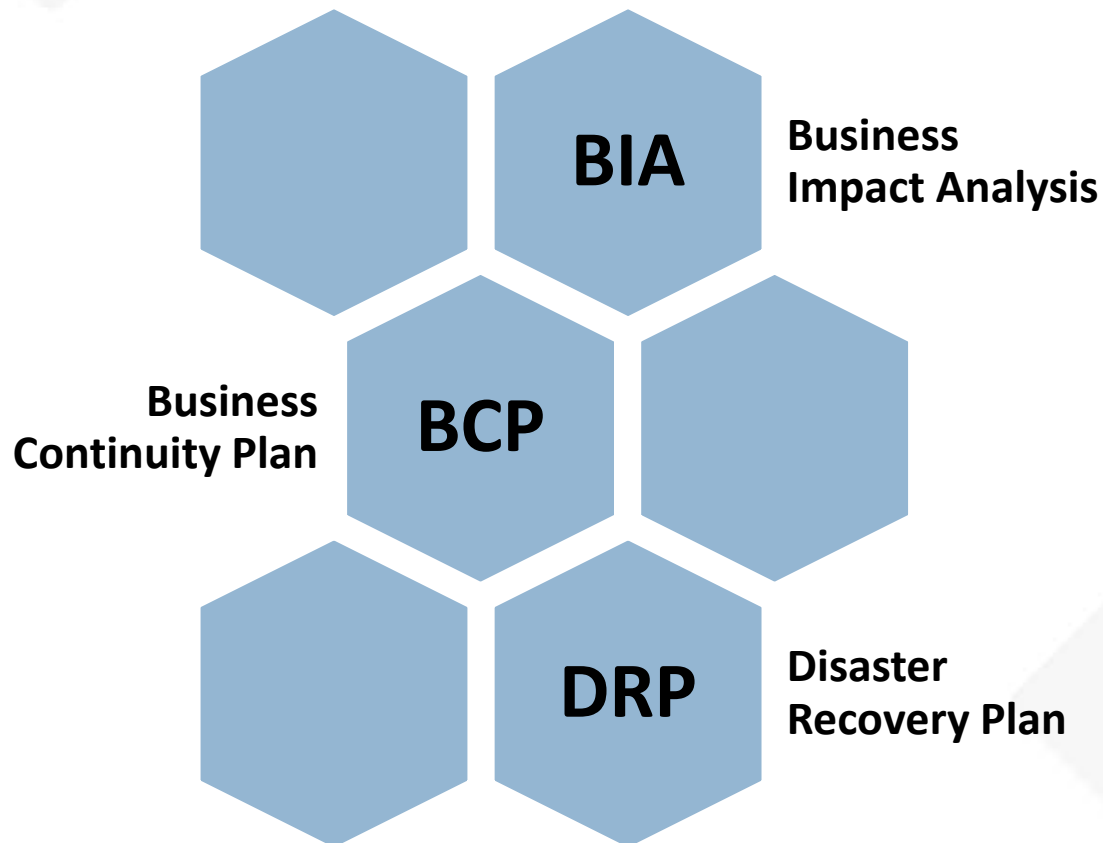
- ¿Cómo se define la continuidad del negocio?

Es un conjunto de acciones de las organizaciones con el objetivo de recuperar y /o restaurar sus funciones críticas parcialmente o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.



# Back-up / Archivo de la documentación respaldatoria / Plan de contingencia

► Documentos Básicos:





7

## PAUTAS DE CONFIABILIDAD

# Pautas de confiabilidad

- Firmar convenios y contratos de confiabilidad con:
  - Empleados
  - Proveedores

**CONFIDENCIAL**



8

## **INTEGRIDAD DE LOS REGISTROS CONTABLES**



# Problemática de la documentación digital

PROBLEMAS

- Cómo determinar al autor
- Fácilmente alterable
- Puede ser objeto de repudio
- No permite reemplazar al papel en todas sus formas.

*Herramientas de  
la Seguridad  
Informática*

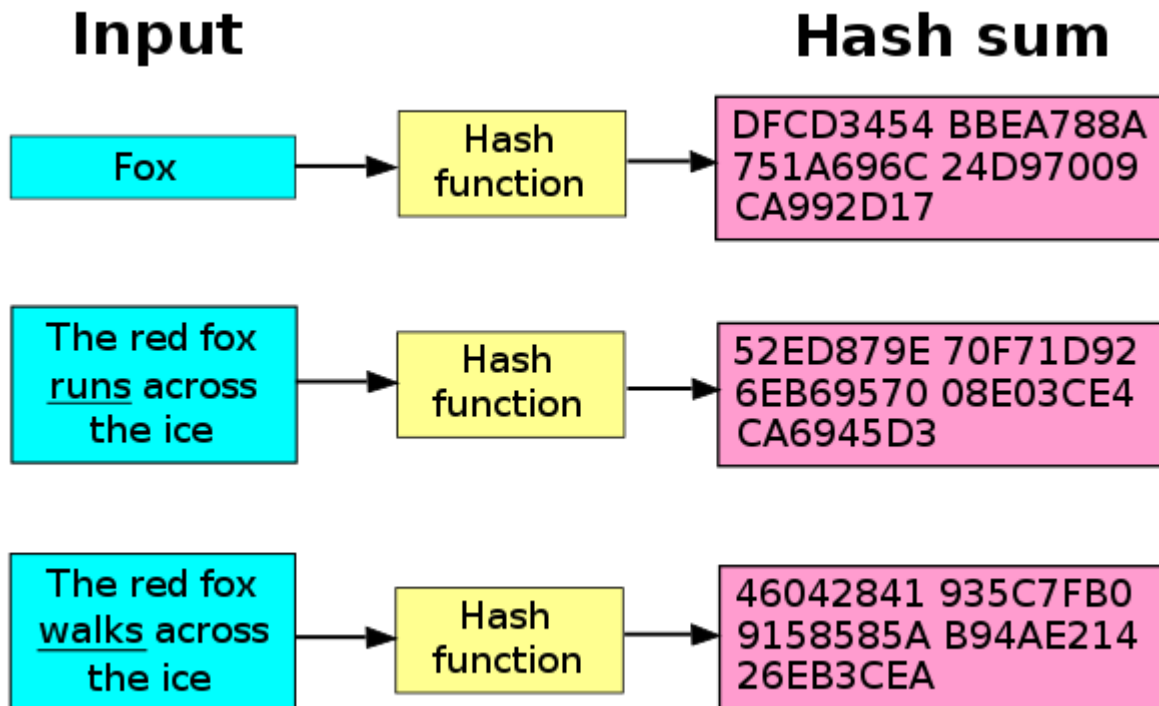
**Función de HASH**

**Firma digital  
/ electrónica**



# Función de HASH

¿Qué es una función de hash?



# ¿En qué documentos y archivos digitales lo podría utilizar?

Datos (Documentos, Planillas,  
PDFs, etc.)



Multimedia

Bases de Datos

Páginas Web

CD DVD

Disco Rígido





# Firma electrónica / Firma Digital

¿Cómo funciona?

- Papeles de trabajo (Auditoría)
- Correos Electrónicos
  - Contratos



- Certificado Privados



- Se firma el Documento



# ¿La Firma Digital es segura?

Clave Privada



Clave Pública



Cumpliendo con los estándares para establecer  
calcular las claves...

¿En cuánto tiempo se puede calcular la otra clave?

# ¿La Firma Digital es segura?

Ejemplo \*\*\* CLAVE PRIVADA 2048 \*\*\*

c:

823427215415179540996660748057165507769220516579261219010182700597172417  
670894688448283849593286404387451417422439873537632752733928350383282961  
331428731652392657044591361450787096368126806133948396536032162839334957  
610749156560127927590793349351059161171930991318551977817134046321507469  
378640661481

n:

822232428759217044755591937028695012784697980446027582317024682945748203  
349756139476614171729812998304058996291264939329259846217662968832225753  
487463299329593910841608306970388847964283282954676759283119749712014562  
743246313867699797873968771576986320333088513858140133697707885848773466  
672683236076653537129170144766107629072147357132988233444051836584832849  
023240530313773434541536289631052609680300880614766571670825316119771189  
077518675473097090104524532032998817620416950071558878140970725392044657  
765516139092914121598155647242717934195403349840229962766497651041026754  
5088131687504361360947849966613183169592687



# ¿La Firma Digital es segura?

Ejemplo \* \* \* CLAVE PUBLICA 2048 \* \* \*

d:

121674304867513254788400189356966673644477991563617301694102937026620073336  
168723444345460647972750429644896770158141811785165888144138539945866926957  
160612646013772936060336036518892738912119807220892573993591507785188892907  
559811551748635935976959190646539331854793213643593593145882608742441634062  
683254560778878436933255287483573344468252496274873250126031302286464830114  
829230131444459831429486053631944973348018991149097850693179088764800588728  
189804475264925357778074520893784876040818150325888608449985643802745105224  
795226273593210371649643311053136498877441292912216206775319202278150085686  
8149620659341521641



# ¿La Firma Digital es segura?

Es prácticamente inquebrable si se implementa adecuadamente (aunque teóricamente no lo son) ya que se ...

**requieren 30.000.000 años...**

Deducir una clave a partir de la otra es computacionalmente irrealizable, aún disponiendo de recursos extremos (se presume que se requieren 30.000.000 de años de una computadora que opere a razón de (1MFlop = 1.000.000 de multiplicaciones y divisiones por segundo con números de 309 dígitos decimales) para deducir una sola clave privada RSA 1024-bits a partir de la pública, usando el algoritmo más eficiente conocido - SNFT)





# 9

## RESGUARDO DE LOS SOPORTES



# Resguardo de los soportes

- **Identificar la metodología de generación de CD o DVD y metodología de archivo de documentación respaldatoria y de los soportes.**
- **En el caso de microfilms, CD o DVD se requiere archivo ignífugo.**
- **El sistema y periodicidad en la numeración de los registros.**

# **CONSIDERACIONES DE LOS REGISTROS CONTABLES EN LAS SOCIEDADES POR ACCIONES SIMPLIFICADAS**

Requerimientos





# Marco legal de las SAS

**Ley Nro. 27.349  
de apoyo al capital  
emprendedor**

**Resolución  
General de la IGJ  
Nro. 6 y 8 del año  
2017 de Justicia).**

**Supletoriamente:  
Código Civil y  
Comercial (2015) y  
la Ley General de  
Sociedades (2015)**

# Los registros contables en la SAS

- La norma establece registros digitales.

Se individualizarán por medios electrónicos ante el Registro:

- ✓ Libro de actas
- ✓ Libro de registro acciones
- ✓ Libro diario
- ✓ Libro de Inventarios y Balances
- ✓ Otros

**Registros habilitados automáticamente** con la inscripción de la SAS

# SAS: Plataforma TAD para individualizar los registros

Plataforma

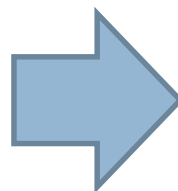


Sistema generador electrónico de documentos oficiales



# Registros digitales en las SAS

1 – Generar la documentación contable:



2 – Subir la documentación contable a la aplicación TAD:

## APLICACIÓN PLATAFORMA DEL MINISTERIO DE MODERNIZACIÓN

- Generar Criptograma
- Función cotejar criptograma con información registral



# Registros digitales en las SAS

## 3 – Descargar el criptograma:

### APLICACIÓN PLATAFORMA DEL MINISTERIO DE MODERNIZACIÓN

- Criptograma
- HASH para calcular la integridad.



## 4 – Registrar en el organismo el criptograma individualizado.



Registro de cada SAS

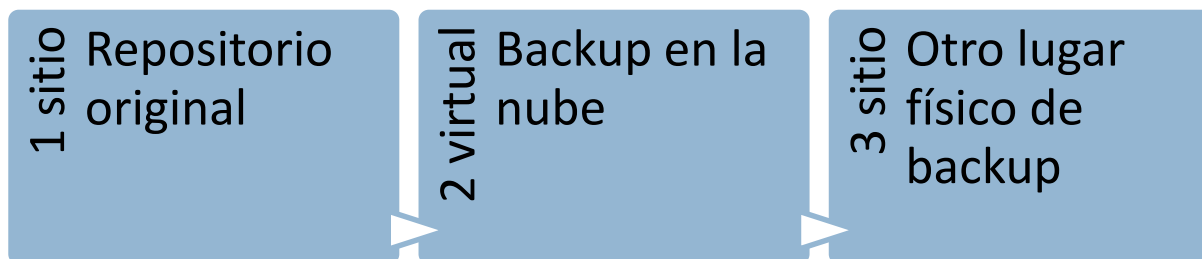


# Registros digitales en las SAS

## 5 – Documentar:

- ✓ Archivos digitales individualizados por los criptogramas (hash)
- ✓ Orden cronológico
- ✓ Carpetas por cada Registro digital

## 6 – Realizar 2 copias una en un servicio de la nube y otro en un lugar físico.

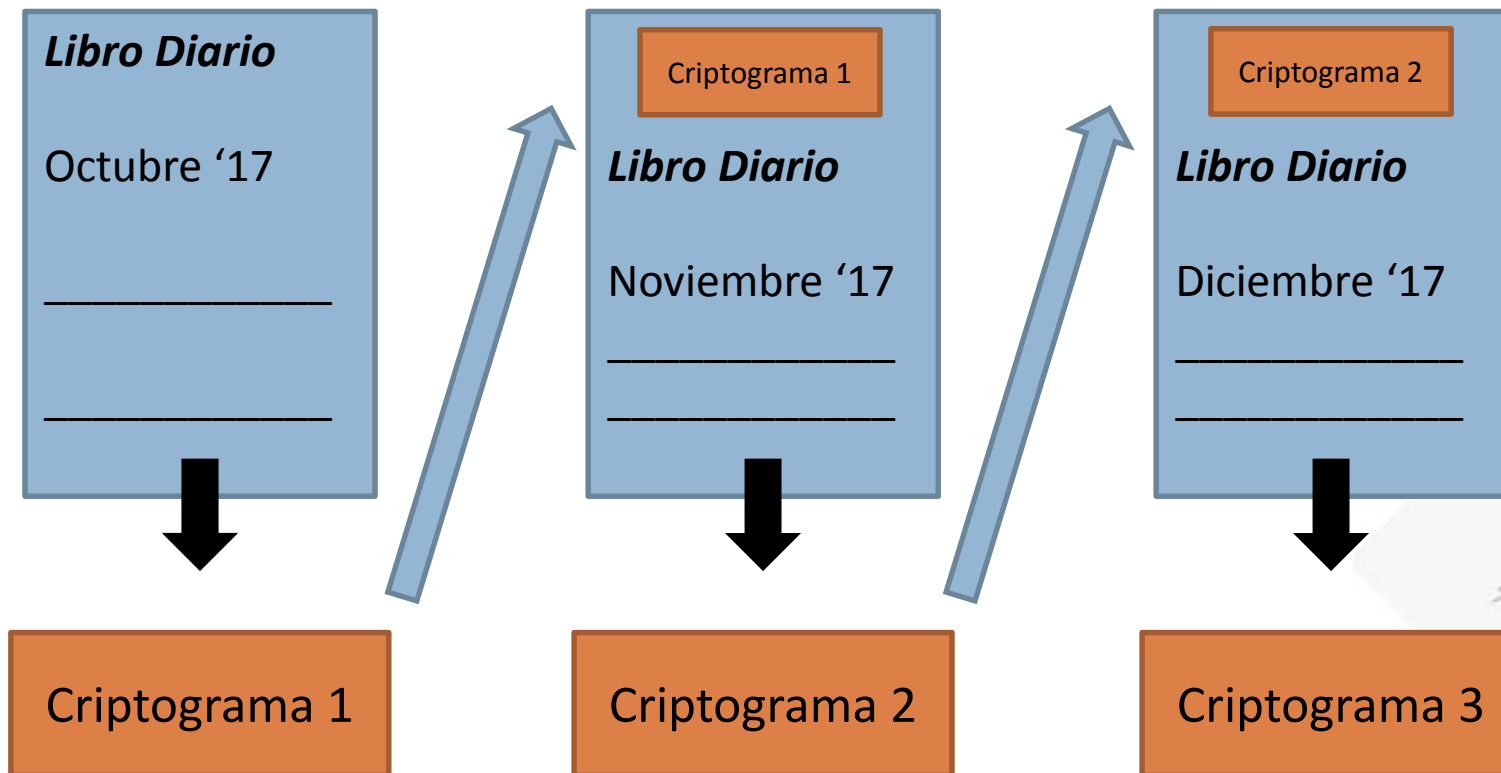


# Principales cambios registrales

- ✓ Archivos digitales son individualizados por los criptogramas (hash)
- ✓ Tienen un orden cronológico
- ✓ Cada carpeta se considerado cada registro digital
- ✓ Cada documento tiene un recibo de encriptamiento del organismo y luego se registra el mismo
  
- ✓ Plazo para individualizar y asentar:
  - Libro Diario: 90 días de la operación.
  - Libro de actas: 10 días de celebrada la reunión.
  - Libro de inventario y balance: Dentro de los 4 meses.

# ¿Cómo se asegura la correlatividad y secuencia de los registros?

Cada documento se encabeza con el criptograma (con el hash) del documento anterior.





# REFLEXIONES FINALES





## Contacto:

**Dra. Elsa Beatriz Suarez Kimura**

[esuarezkimura1@yahoo.com](mailto:esuarezkimura1@yahoo.com)

**Mg. Diego Sebastián Escobar**

[@escobards](mailto:escobards@gmail.com)

