



# Guía: Seguridad Informática

Contenido suministrado por  **KALKI**  
CONSULTING

# A quien le afecta?

Compañías que tienen, usan o hacen soporte técnico de ordenadores, teléfonos inteligentes, correo electrónico, paginas web, medios sociales, o servicios de computación en la nube



Compañías que crean, recogen o guardan los siguientes tipos de información:

Propiedad Intelectual	Información privada sobre su compañía	Nombres y registros de clientes	Información confidencial. Por ejemplo adquisiciones y fusiones
Información sobre pagos. Por ejemplo tarjetas de crédito	Acceso a la pagina web de una compañía	Historial Clínico de pacientes	Información personal identificable

- **En la Compañía:**
  - Tecnología (Puede ser subcontratado)
  - Recursos Humanos
  - Grupo legal y de cumplimiento (Interno/Externo)
  - Finanzas
  - Relaciones Publicas
  - Auditoria Interna
  - Oficial de seguridad de información (Para compañías de tamaño medio y grandes)
- **Externo a la compañía:**
  - Autoridades federales y estatales
  - Grupos de Industria

***En definitiva, la responsabilidad siempre recaerá en el propietario de la empresa y el riesgo se reducirá a los inversores, accionistas, empleados y clientes.***

# Mi negocio es pequeño, Quien quiere mi información?

Hoy en día, el delito cibernético está motivado por razones financieras. Los criminales son muy organizados. Sus herramientas son sofisticadas. Los criminales cibernéticos, como los matones, se aprovechan de los blancos más fáciles con la seguridad más débil, como las pequeñas empresas.

## Que Tengo

Propiedad Intelectual
Nombre de clientes y informacion de pagos
Ordenadores, telefonos inteligentes, correo electronico, etc
Informacion Medica
Detalles sobre cuentas (nombre de usuarios/palabras claves/datos sobre media social)

## Quien lo quiere?

Criminales organizados/Hackers
Empleados descontentos
Empleados oportunistas
Competidores
Ladrones

## Por que?

Extorsion y ganancias financieras
Robo de identidad
Fraude
Fraude de Seguro Medico
Propagacion de Malware

**Y  
ahora  
que?**

# Impacto de robo de datos

El impacto de los incidentes cibernéticos son los más costosos para los individuos, empresarios, empresas y la economía. Solo en el 2012, resulto en un coste para las empresas de un total de 1 billón de dólares.

## Cual es el impacto?

Reputacion y problemas de imagen para la marca

Acciones legales y costos asociados

Violación de las normas de la industria e.g. PCI-DSS

Violación de las normas federales e.g., HIPAA

Perdida de investigación y desarrollo, tiempo y dinero

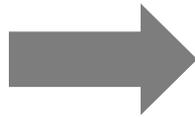
Y?

## El Costo de seguridad cibernética



# Como se produce el delito cibernetico?

Pequeños negocios depende de la tecnología



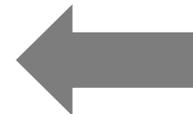
Vulnerabilidades se descubren en todos los sistemas



Tecnologías sin protección son explotadas



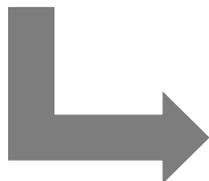
Hackers crean código malicioso (malware) para explotar tecnologías que no están protegidas



Los sistemas vulnerables son "secuestrados" por el malware



Malware compromisa cuentas de correo electrónico y de redes sociales con contraseñas débiles para propagarse



Malware recopila información confidencial y se la manda a los criminales



Los criminales usan la información para conseguir ganancias financieras

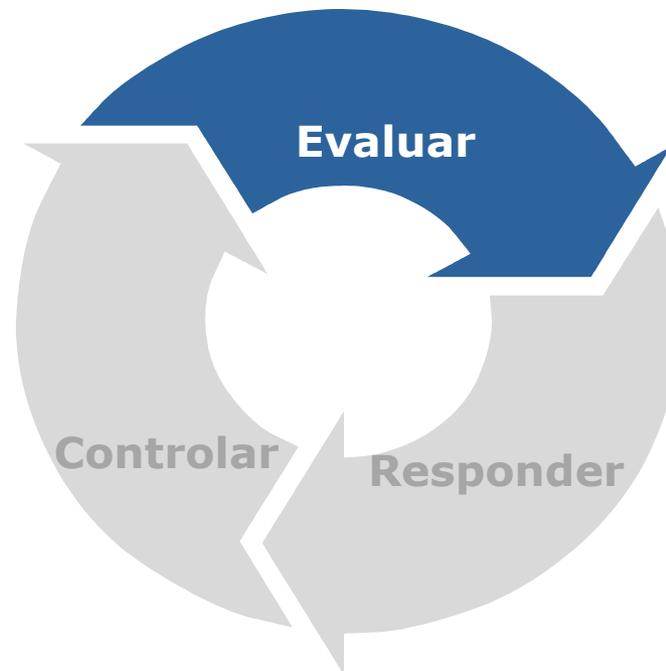


## Hay 3 sencillos pasos para reducir el riesgo de la delincuencia cibernetica e incidentes.

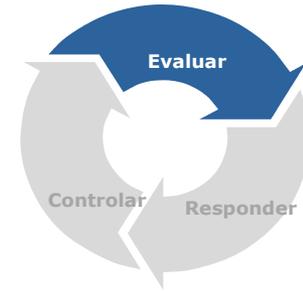
### Primer paso:

Llevar a cabo una auto evaluacion. Este incluye:

- Documentar sus activos de informacion
- Identifique si tiene obligaciones reglamentarias de contrato
- Identifique su habilidad de responder a un caso de ataque
- Valide contramedidas esenciales

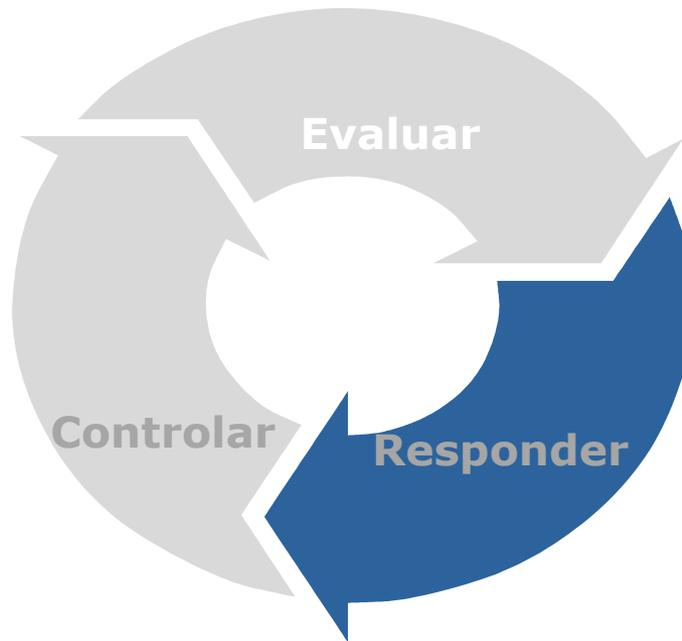


- Que datos recopila, almacena, procesa y transfiere?
- Quien tiene acceso a los datos?
- Que dispositivos pueden usarse para almacenar los datos?
- Que haría si los pierde?
- Si lo pierde, a quien debe notificar?
- Que pasa si un empleado deja la compañía?
- Como responde si información privada es compartida a través de un correo electrónico o una página de media social por equivocación?
- Como puede asistir a las autoridades en el caso de un ataque cibernético?



# Que pasa después de la evaluación?

Una vez que determine el riesgo, necesita poder responder

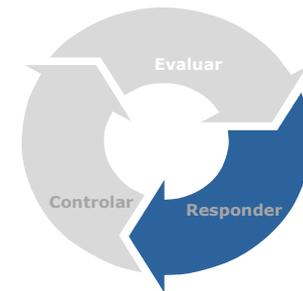


## Segundo paso:

Respuesta a la evaluación cibernética:

- Identifique quien necesita acceso y cuanto
- Desarrollar una política de seguridad y privacidad que proteja a su empresa en caso de un incidente
- Educar a todos en su negocio para saber qué hacer en caso de un incidente
- Asegúrese de que su entorno tecnológico tiene las medidas básicas en el lugar para responder a un incidente

- ¿Ha desarrollado una política de seguridad?
- ¿Se ha comunicado la política a todos los empleados?
- Haga que sus empleados confirmen por escrito que entienden la política de seguridad.
- ¿Tiene políticas de privacidad que informan a sus clientes cómo proteger sus datos?
- ¿Han sido capacitados sus empleados para responder a un incidente, como la pérdida o robo de un USB o portátil o un hack?
- ¿Se ha asegurado de que su entorno de tecnología tiene las medidas básicas para responder a un incidente, como el antivirus en todos los equipos (incluidos los Apple MACs), encriptación, y actualizaciones de automáticas de software y copias?



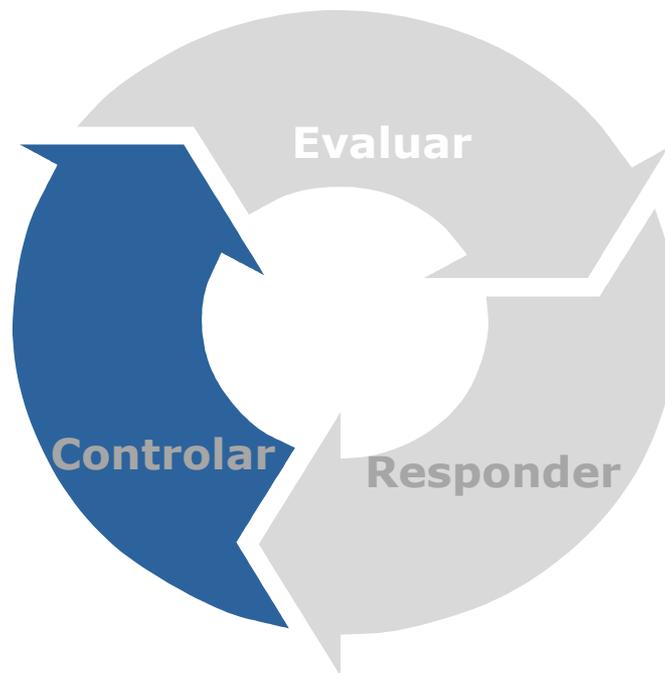
# ¿Cómo monitorea los incidentes cibernéticos?

Después de evaluar y responder, como controla los incidentes cibernéticos.

## Tercer Paso:

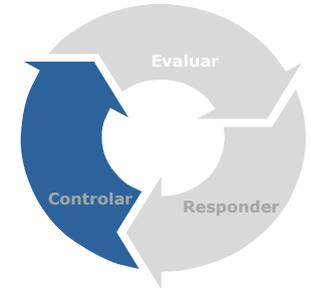
Una vez que entienda dónde están los riesgos, usted debe considerar las políticas y procedimientos para detectar:

- Actividad maliciosa externa
- Empleado con acceso no autorizado
- Problemas con la tecnología



Con la supervisión de la seguridad cibernética debe ser capaz de:

- Esté atento a los intentos de acceso externo a su red
- Determinar si los riesgos cibernéticos han cambiado
- Observar los empleados o contratistas para asegurarse de que están utilizando las tecnologías y los datos apropiados
- Determinar si hay problemas o vulnerabilidades con su tecnología antes de que ocurra un incidente



Tecnología se centra normalmente en las operaciones, pero la seguridad cibernética es una disciplina que se centra en el riesgo. La seguridad no es siempre la prioridad del personal técnico.

Seguridad cibernética esta basada en 3 principios:

**1. Confidencialidad**

- información limitada a los que necesitan saberlo

**2. Integridad**

- Cambios a la información deben ser autorizado

**3. Disponibilidad**

- La información necesita estar disponible cuando se necesita cibernética

*Profesionales de la seguridad cibernética creen en la "defensa en profundidad", lo que significa que no dependen de una sola persona o un sistema para proteger el negocio.*

### Confidencialidad:

Información compartida solo con los que necesitan saber:

#### **Si:**

- Asegúrese que los empleados tienen acceso a lo único que necesitan saber
- Asegúrese de que todo el personal tiene su propia cuenta y contraseña
- Mantenga las palabras claves fuertes y únicas

Y

#### **No hacer:**

- No anote su palabra clave y no la comparta
- Comparta información sobre la compañía con gente externa
- No tome por seguro que los correos y las paginas de web son seguras

### **Integridad:**

Asegurarse con los cambios a la información son autorizados significa:

### **Hacer:**

- Actualización regular de parches de antivirus y software de sistema
- Enumerar los dispositivos que almacenan datos de su empresa
- Contar con un proceso para el cambio de los datos importantes

Y

### **No hacer:**

- Descargar automáticamente el software porque es gratis
- Utilizar las redes “peer-to-peer” para compartir archivos o de música libre
- Asumir cualquier dispositivo de tecnología es inmune contra el malware

### Disponibilidad:

Asegurarse que los datos e información necesaria para su negocio significa que:

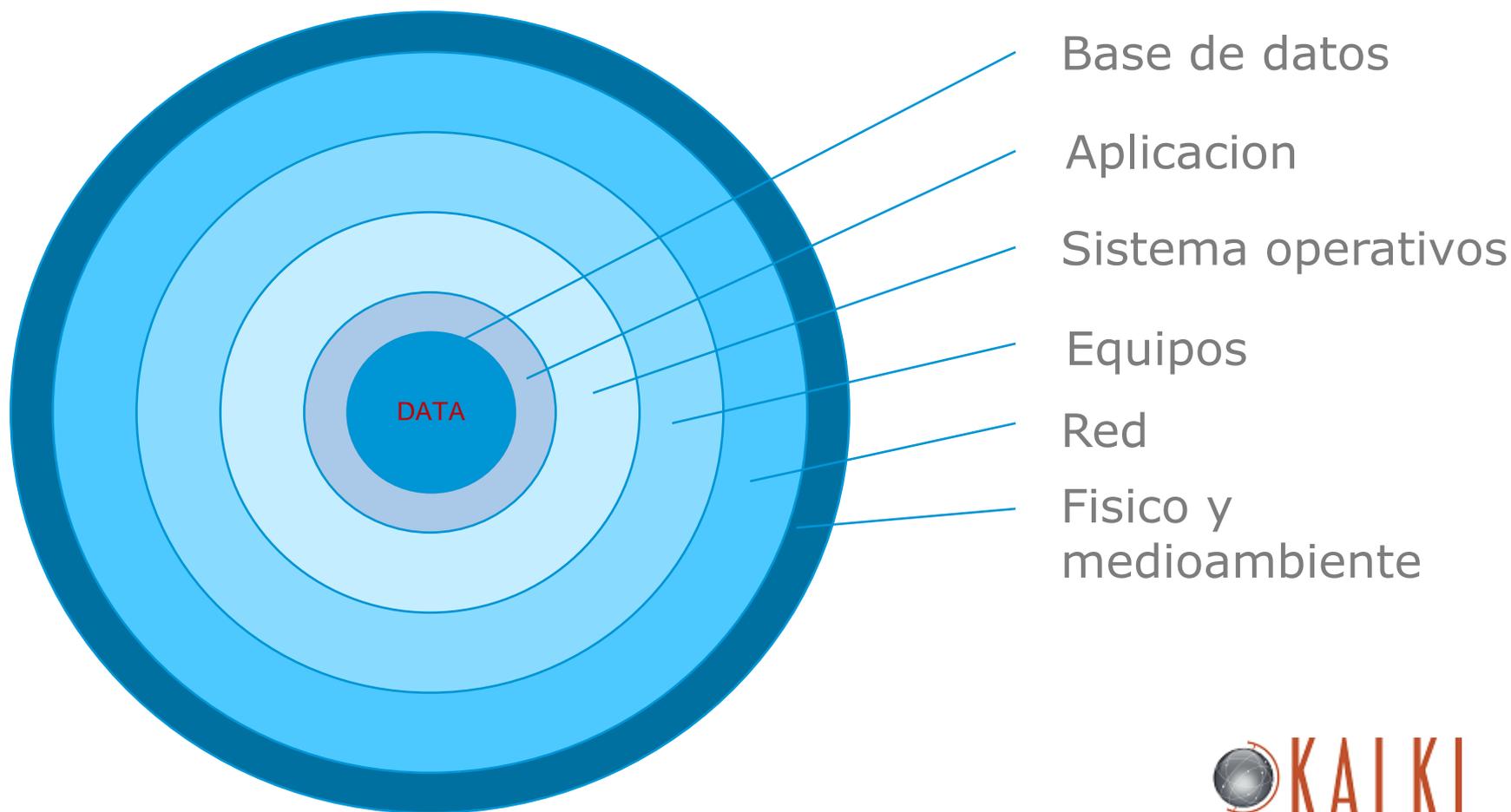
#### **Hacer:**

- Tener copias de seguridad periódicas de los datos y mantenerlos fuera de las instalaciones
- Considere la posibilidad de bloqueos de ordenador, incluso en una oficina compartida
- Planea para un desastre natural o un incidente técnico y...

#### **No hacer:**

- Asumir que las copias de seguridad automáticas trabajan, al menos que se hagan pruebas con regularidad
- Suponer que los datos se han eliminado una vez que el dispositivo sea removido
- Suponer que su proveedor de correo electrónico lo protege

Hay múltiples capas que componen la tecnología que utilizamos. Defensa en profundidad requiere tener en cuenta seguridad en cada capa



El dueño de la empresa se preocupa...?	Perdidas monetarias	Problemas de reputacion	Acciones legales	Reglas de la industria	Violaciones de leyes federales
	Si / No	Si / No	Si / No	Si/ No	Si / No
Tiene el negocio...?	Informacion bancaria y de pagos	Propiedad Intelectual	Nombres de clientes y registros	Expedientes medicos	Informacion privada y sensible
	Si / No	Si / No	Si / No	Si/ No	Si / No
Se protéje con...?	Politica de Seguridad	Capacitacion de los empleados	Respuesta a incidentes	Seguridad cibernetica	Seguridad fisica
	Si / No	Si / No	Si/ No	Si / No	Si / No

**Si su respuesta es si a cualquiera de las preguntas previas es si, usted debe:**

- Trabajar con un profesional calificado de Seguridad Cibernetica para evaluar el riesgo
- Disponer de un conjunto de documentos que le protegerá si es parte de una auditoria
- Implementar políticas y procedimientos que le permiten detectar y responder a incidentes
- No depender de una tecnología o software para protegerse!



Fundada y basada en Nueva York, Kalki Consulting LLC provee servicios de seguridad cibernética a las empresas pequeñas, medianas y empresas con ofertas de evaluación, respuesta y seguimiento cibernéticos independientes.

Kalki se compromete a ayudar a sus clientes a entender y gestionar el cumplimiento normativo y la exposición cibernética a un incidente de seguridad.

Para mas información:

Pagina Web: <http://www.kalkiconsulting.com>

Twitter: [@kalkiconsulting](https://twitter.com/kalkiconsulting)

Facebook: <https://www.facebook.com/KalkiConsulting>

Teléfono: 1-855-GO-KALKI (1-855-465-2554)

