# Analysis of New Technologies in Information Security to Mitigate Data Risks in a Public Organization

## 4.Discusión

El sector público tiene muchas caras a las que hacer frente en el presente mundo cibernetizado. En especial el área de información de la seguridad. Entre las potenciales consecuencias dañinas, si es descuidada la seguridad pública, se puede nombrar:

* Filtrado de información sensible.
* Pérdida de información sensible.
* Desprestigio de la entidad pública.
* Daño temporal o permanente a los activos de la entidad.
* Perjuicio de las contrataciones.
* entre muchos otros potenciales daños.

El artículo muestra el proceso y resultados de un estudio de artículos afines para la aplicación de nuevas tecnologías a las empresas pública ecuatorianas y así minimizar los riesgos de vulnerabilidad de datos en estas. Para esto propone un modelo conceptual, un proceso algorítmico y unos casos de uso.

Se analiza y propone modelos para la mejora de los protocolos de seguridad informática en el sector público.

Se consideran principalmente las siguientes tecnologías:

* Blockchain
* Hyperledger
* Smart contracts

**Blockchain** aparece al rededor del 2008 como la respuesta de la emergente moneda digital Bitcoin al problema de la seguridad transaccional sin necesidad de una autoridad central. Entre las muchas ventajas de las cadenas de bloques se encuentra su incapacidad de ser alterada sin consenso. Es considerado como seguro por diseño y no tardó mucho tiempo para que frameworks de blockcahains aparezcan a la luz.

**Hyperledger** es una inicitava de código abierto orientada a la creación de frameworks, herramientas y librerías para blockchains.

**Smart contracts** es un protocolo para llegar a cabo transacciones seguras sin importar las parte implicadas; desligándose de la necesidad de una autoridad central. El protocolo de Bitcoin es en sí considerado una forma de Smart Contract.

Estas tecnologías son usadas para la propuesta a las empresas públicas de un mejor conjunto de prácticas e idiosincrasia informativa.

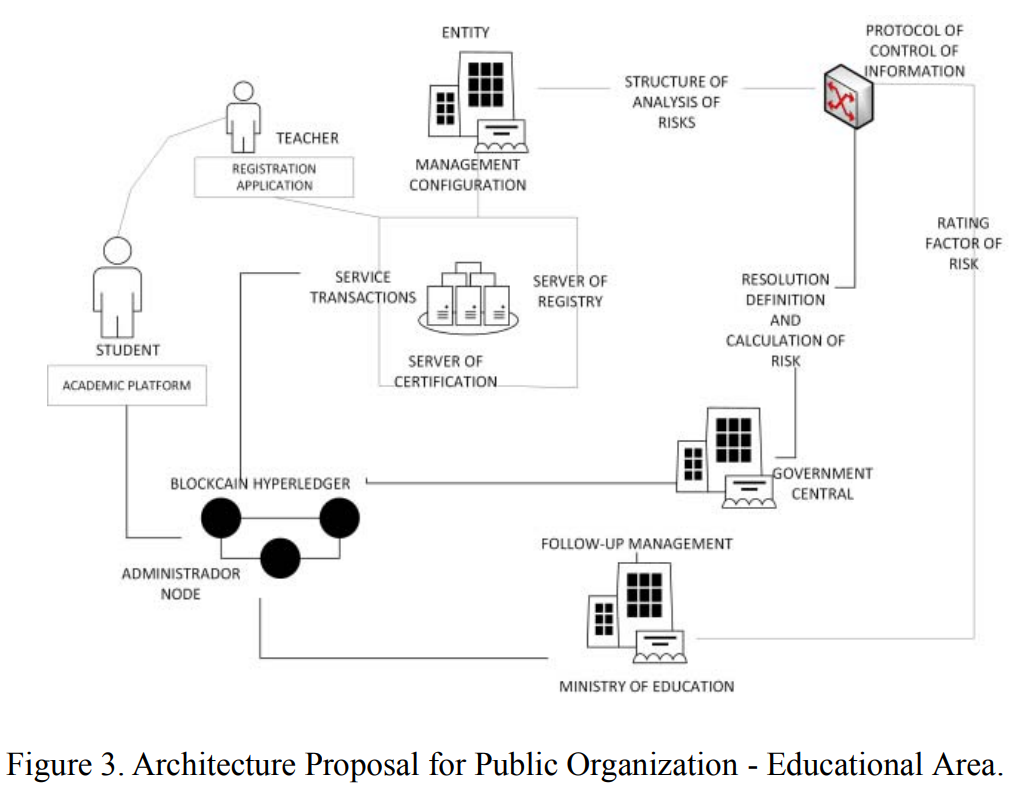
Como agentes intervenidos en el cambio de tecnologías se propone:

* El gobierno central
* Entidades académicas
* Ministro de educación
* Administradores

Estos serían los actores que dan consenso para la actualización de la información en los bloques de información.

Como una de las principales ventajas del método propuesto, usando las tecnologías y protocolos antes mencionados, es la ausencia de necesidad de terceras partes para la consecución de transacciones. Proponiendo inclusive que las organizaciones públicas podrían bien ser completamente organizadas por Smart Contracts.

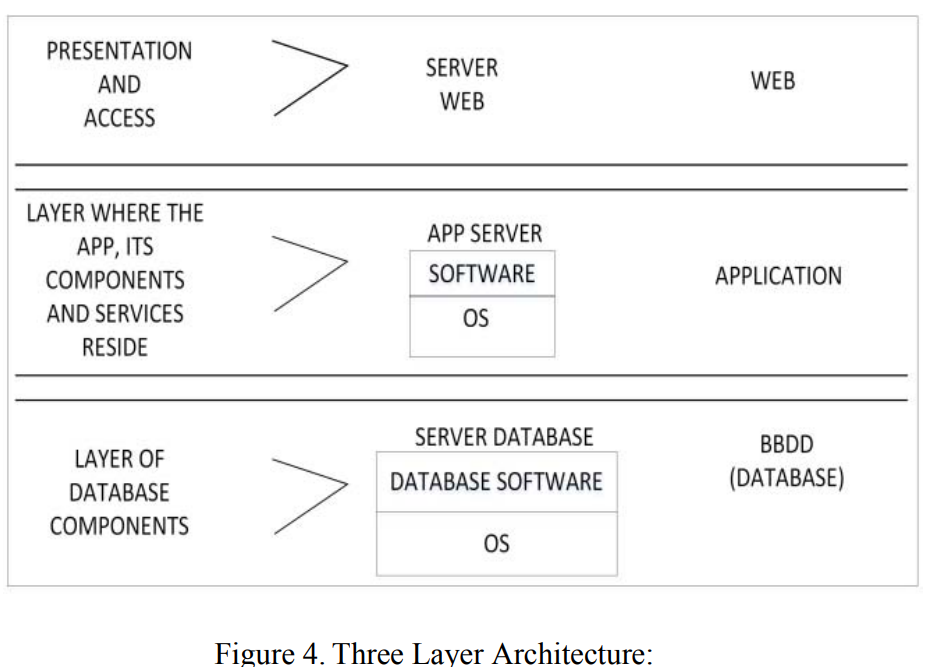
Se propone un esquema que propone la mejora de la transferencia de información entre dispositivos con recursos limitados.



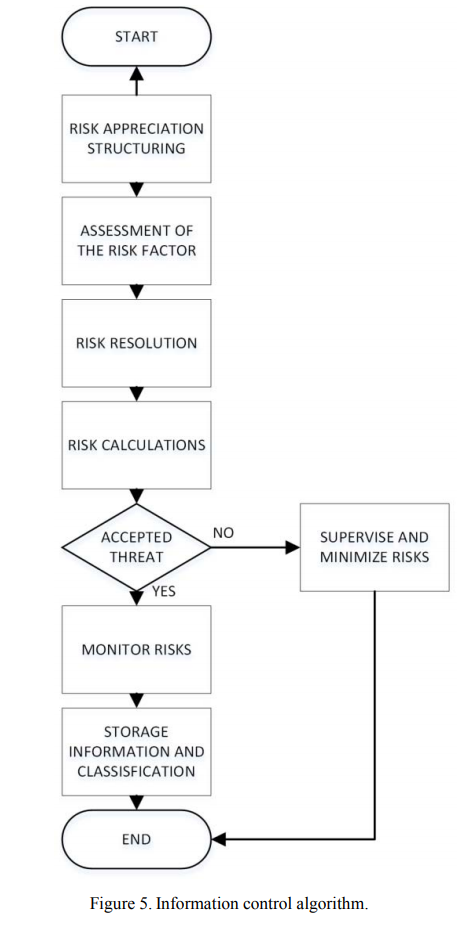
Finalmente, el artículo propone un framework de administración de riesgos adaptativo. Con enfoque en la defensa de la infraestructura en riesgo.

Se propone una arquitectura multicapa con división de responsabilidades:

1. Capa web
2. Capa de aplicación
3. Capa de datos



Finalmente se propone el siguiente algoritmo como la vía para el control de la información:



## 5.Conclusión

Se propone como eje de la solución dos propuestas:

1. Adopción de Blockchains para un mayor nivel de seguridad y consistencia a la información generada, administrar la información y evitar acciones maliciosas.
2. Adopción de la metodología de control de la información de la referencia “*An Improved Information Security Risk Assessments Method for CyberPhysical- Social Computing and Networking*”, para recolectar datos históricos y mitigar riesgos futuros gracias a los protocolos establecidos.

Se considera en la conclusión a la tecnología de Blockchain como una opción fundamental para el control, fiabilidad, disponibilidad, inmutabilidad y robustez contra las fallas y ataques maliciosos.