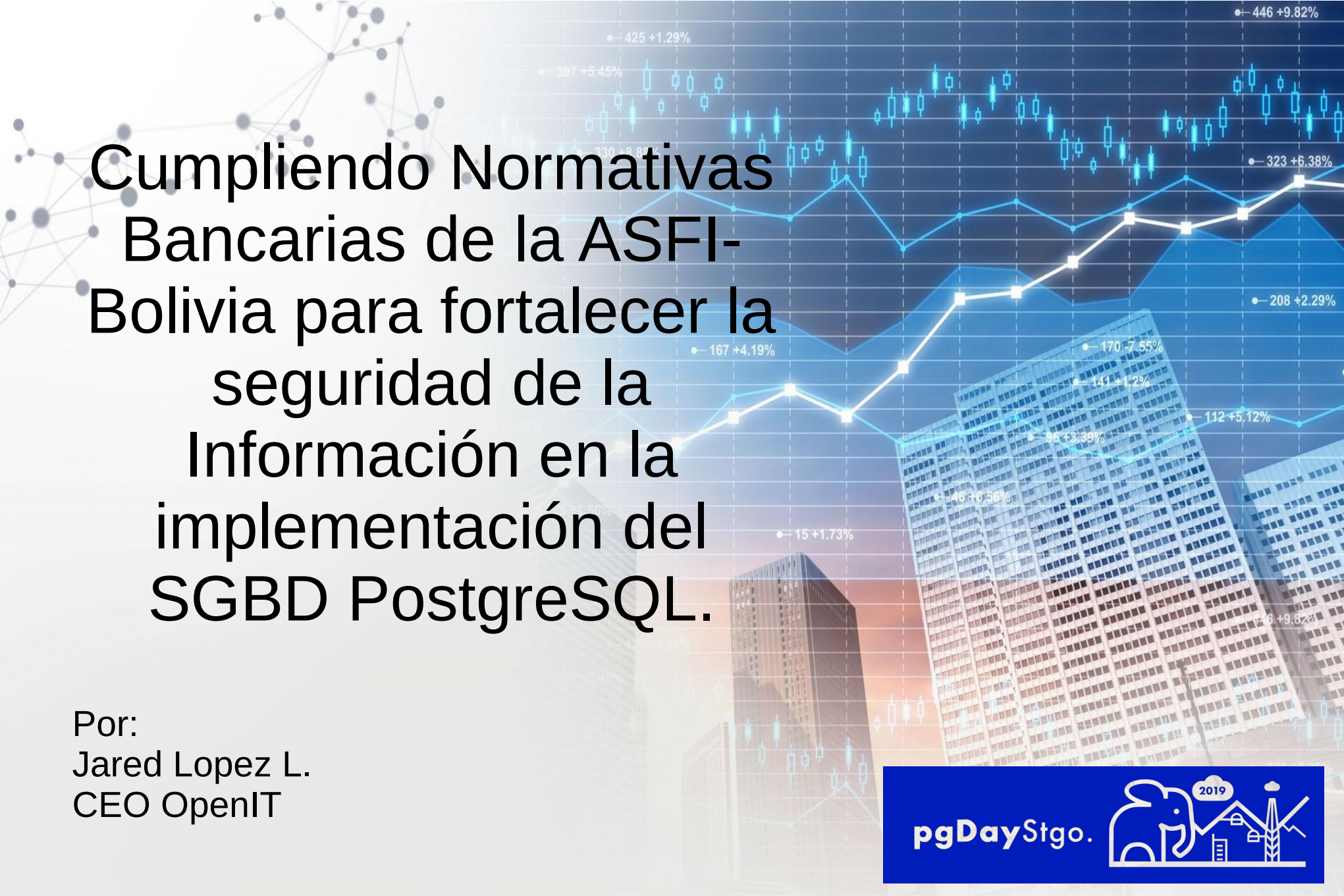
Cumpliendo Normativas Bancarias de la ASFI-Bolivia para fortalecer la seguridad de la Información en la implementación del SGBD PostgreSQL.

Por:
Jared Lopez L.
CEO OpenIT



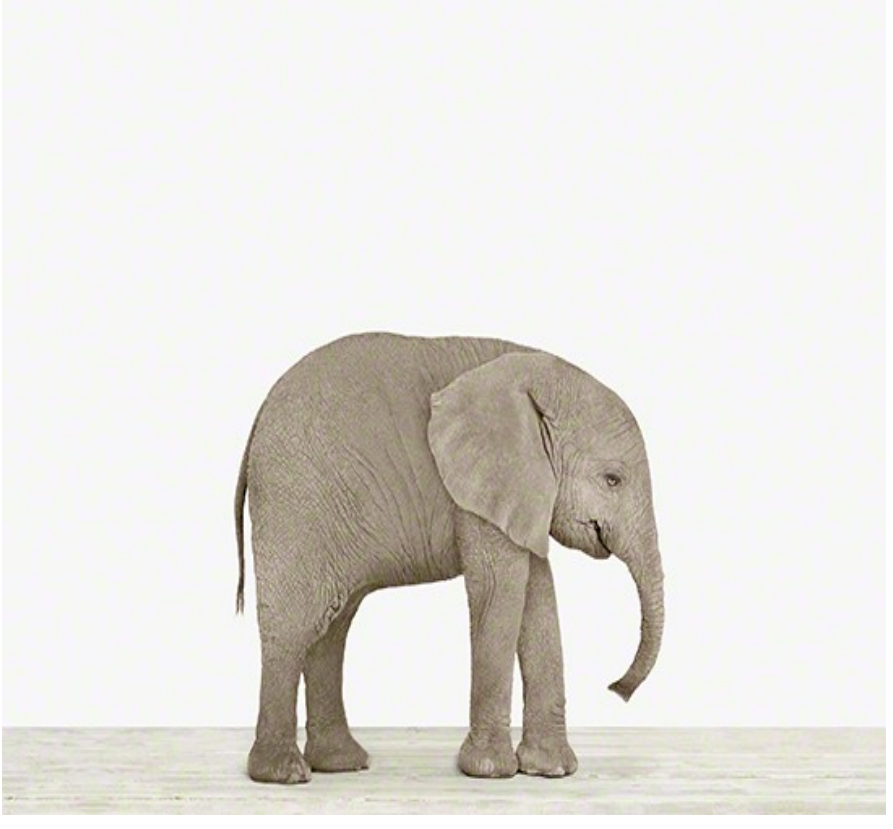
pgDayStgo. 2019

INTRODUCCIÓN

- PostgreSQL ha demostrado ser un SGBD **óptimo** para cualquier situación y circunstancia, mejorando cada vez en las nuevas versiones, en las cuales incorpora nuevas opciones y servicios que facilitan el trabajo de quien lo usa y colocándose entre los cuatro SGBD más utilizados por todo tipo de usuarios incluyendo empresas

POSTGRESQL POR DEFECTO.

- El SGBD PostgreSQL por defecto solo tiene niveles de seguridad **básicos** dentro del control de acceso, esto implica: autenticación de Usuarios y el como y donde puede conectarse un cliente.



Como pasar de un
PostgreSQL
bebe a un elefante
maduro y fuerte!

NORMATIVA ASFI- BOLIVIA

En Bolivia las entidades financieras son el único sector que cuenta con **reglamento** de seguridad de información de **cumplimiento obligatorio** por la ASFI (autoridad de supervisión del sistema financiero), en esta charla veremos como PostgreSQL cumple con estas normativas.

SECCIONES DONDE INTERVIENE LA BD POSTGRESQL

- De las **13 secciones,** 7 interviene directamente el cumplimiento de BD PostgreSQL.
  - SECCIÓN 3:ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACÍON
  - SECCIÓN 4:ADMINISTRACIÓN DELCONTROL DE ACCESOS
  - SECCIÓN 5:DESARROLLO,MANTENIMIENTO E IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN
  - SECCIÓN 6:GESTIÓN DE OPERACIONES DE TECNOLOGÍA DE INFORMACIÓN
  - SECCIÓN 7:GESTIÓN DE SEGURIDAD EN REDES Y TE L E COMUNICACIONES
  - SECCIÓN 10:CONTINUIDAD DEL NEGOCIO
  - SECCIÓN 11:ADMINISTRACIÓN DE SERVICIOS Y CONTRATOS CON TERCEROS RELACIONADOS CON TECNOLOGÍA DE LA INFORMACIÓN

SECCIÓN 3:ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACÍON

- Artículo 3°(Licencias de software)Todo software utilizado por la entidad supervisada debe **contar con las licencias respectivas**.La entidad supervisada, debe definir los procedimientos necesarios para la instalación, mantenimiento y administración de software, así como la custodia de licencias

SECCIÓN 3:ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACÍON

- En Bolivia se tiene una **Ley Nº 164**, de 8 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación para el Sector de Telecomunicaciones. Para el uso de Software Libre y estándares abiertos, por el cual se puede establecer la base legal para el uso de licencias como **"PostgreSQL License"** y no se vea un hueco legal para no utilizarlo.

SECCIÓN 4:ADMINISTRACIÓN DEL CONTROL DE ACCESOS

- Artículo 3°(**Administración de contraseñas de usuarios**) La entidad supervisada debe definir políticas de administración de contraseñas que respondan a su análisis y evaluación de riesgos en seguridad de la información, así como a la clasificación de la información.

SECCIÓN 4:ADMINISTRACIÓN DEL CONTROL DE ACCESOS

- Esta se puede configurar de forma local abilitando el modulo “passwordcheck” o por medio del archivo pg_hba.conf ligando para que LDAP/AD lo gestione esas politicas.

SECCIÓN 4:ADMINISTRACIÓN DEL CONTROL DE ACCESOS

- Artículo 5°(Registros de seguridad y pistas de auditoría)Con el objeto de minimizar los riesgos internos y externos relacionados con accesos no autorizados, pérdidas y daños de la información, la entidad supervisada, con base en el análisis y evaluación de riesgos en seguridad dela información, debe **implementar pistas de auditoría** que contengan los datos de los accesos y actividades de los usuarios, excepciones y registros de los incidentes de seguridad de la información.

SECCIÓN 4:ADMINISTRACIÓN DEL CONTROL DE ACCESOS

- Los registros de logs se pueden configurar a diferentes niveles (postgresql.conf), dando un registro tan detallado como se necesite. Claro esta que esto puede causar incremento en el almacenamiento.
- Ej:
  - log_statement = 'all'
  - log_destination = 'stderr'
  - logging_collector = on
  - log_min_duration_statement = 0

SECCIÓN 5:DESARROLLO,MANTENIMIENTO E IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN

- Artículo 6° -(Controles criptográficos)En el desarrollo de los sistemas de información, la entidad supervisada debe implementar métodos de **cifrado** estándar que garanticen la **confidencialidad** e **integridad** de la información.

SECCIÓN 5:DESARROLLO,MANTENIMIENTO E IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN

- Utilizando "pgcrypto" funciones de sha128 o sha512 o mas simples como MD5
- Ej: (md5)
  - INSERT INTO tbl_Password VALUES (CRYPT('NuevaClave', GEN_SALT('md5')));
  - INSERT INTO tbl_TestPassword VALUES (CRYPT('NuevaClave2', GEN_SALT('md5')));
- Ej: (sha256)
  - INSERT INTO tbl_TestPassword VALUES (ENCODE(DIGEST('AnveshPassword','sha256'),'hex'));

SECCIÓN 5:DESARROLLO,MANTENIMIENTO E IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN

- Artículo 10° -(**Datos de prueba en ambientes de desarrollo**)Para utilizar información de producción en los ambientes de desarrollo y pruebas, se debe aplicar un procedimiento de **enmascaramiento** de datos a efectos de preservar la confidencialidad de dicha información.

SECCIÓN 5:DESARROLLO,MANTENIMIENTO E IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN

- No se tiene herramientas internas de postgres, por lo que se pueden sugerir:
  - Contrib https://gitlab.com/dalibo/postgresql_anonymizer
  - Herramientas comerciales https://www.datasunrise.com/masking/postgresql/

SECCIÓN 6:GESTIÓN DE OPERACIONES DE TECNOLOGÍA DE INFORMACIÓN

- Artículo 2° -(**Administración de las bases de datos**)La entidad supervisada debe realizar la administración de bases de datos, en función a procedimientos formalmente establecidos para este propósito, los cuales consideren mínimamente lo siguiente: a. **Instalación**, administración, migración y mantenimiento de las bases de datos;b. Definición de la **arquitectura** de información para organizar y aprovechar de la mejorforma los sistemas de información;c. Establecimiento de mecanismos de **control** de acceso a las bases de datos;d.**Documentación** que respalde las actividades de administración de las bases de datos;e. Realización de estudios de capacidad y desempeño de las bases de datos que permitandeterminar las necesidades de expansión de capacidades y/o la afinación en formaoportuna.

SECCIÓN 6:GESTIÓN DE OPERACIONES DE TECNOLOGÍA DE INFORMACIÓN

- Diferentes fuentes de Instalación
  - Paquetes de repositorio por distribución.(Ubuntu, CentOS, etc.)
  - Instaladores realizados por empresas(2ndQuadrant, EDB, etc.)
    - https://www.2ndquadrant.com/en/blog/pginstaller-install-postgresql/
    - https://www.enterprisedb.com/downloads/postgres-postgresql-downloads
  - Código fuente.
- Dentro de lo que es la administración el punto que se debe tomar mucha importancia es al monitoreo para tener claro si los recursos que se tiene son los necesario y poder tener proyecciones a futuro.

https://pgcluu.darold.net/

SECCIÓN 6:GESTIÓN DE OPERACIONES DE TECNOLOGÍA DE INFORMACIÓN

- Artículo 3° -(Respaldo o copia de seguridad)La entidad supervisada debe efectuar **copias de seguridad** de todos los datos e información que considere necesarios para el continuo funcionamiento de la misma..

SECCIÓN 6:GESTIÓN DE OPERACIONES DE TECNOLOGÍA DE INFORMACIÓN

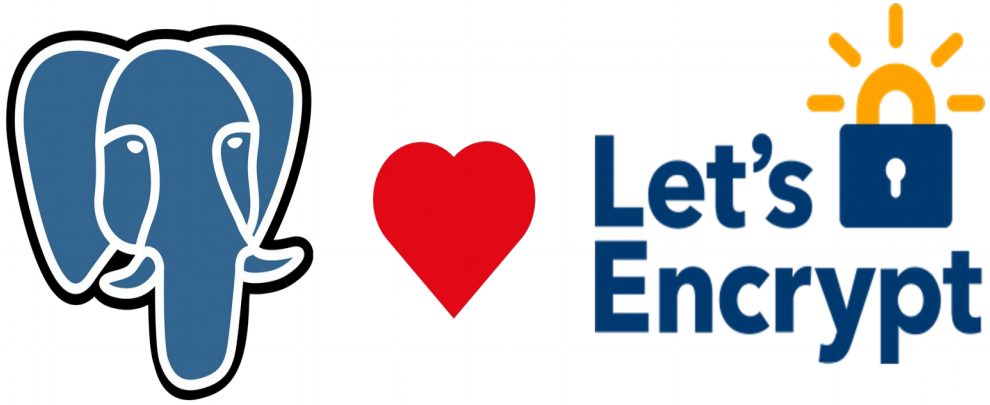
- Se pueden generar backups:
  - Programados, completos/incrementales.
    - pg_dump y pg_dumpall
  - Por herramienta Bartman para colocar un sistema de backups.
    - https://www.pgbarman.org/

SECCIÓN 7:GESTIÓN DE SEGURIDAD EN REDES Y TE L E COMUNICACIONES

- 1° - (Políticas y procedimientos)
- b.Garantizar la protección de los **datos** que se **transmiten** a través de la red de telecomunicaciones, mediante técnicas de **cifrado** estándar a través de equipos o aplicaciones definidas para tal fin;

SECCIÓN 7:GESTIÓN DE SEGURIDAD EN REDES Y TE L E COMUNICACIONES

- Se puede implementar conexiones seguras por medio de SSL para tener cifrado las comunicaciones.
  - https://medium.com/@pavelevstigneev/postgresql-ssl-with-letsencrypt-b53051eacc22



SECCIÓN 10:CONTINUIDAD DEL NEGOCIO

- Artículo 1°- (**Plan** de Contingencias Tecnológicas)
- Artículo 2°- (Plan de **Continuidad** del Negocio)
- Artículo 4°- (**Pruebas** de los planes de contingencias tecnológicas y continuidad del negocio)

SECCIÓN 10:CONTINUIDAD DEL NEGOCIO

- Aunque este apartado se puede tener algo mucho mas extenso, dentro de la arquitectura base de postgres se tiene:
  - Replicación y procesos de failover (Hot Standby y Streaming replication).
- Herramientas de empresas.
  - EDB Replication Server.
  - Postgres-BDR - 2ndQuadrant .
- Todas ayudan al plan de contingencia tecnológica.

SECCIÓN 11:ADMINISTRACIÓN DE SERVICIOS Y CONTRATOS CON TERCEROS RELACIONADOS CON TECNOLOGÍA DE LA INFORMACIÓ

- Artículo 9° -(**Acuerdo de nivel de servicio**) La entidad supervisada de forma previa a la contratación de un proveedor externo de tecnología de información, debe establecer un Acuerdo de Nivel de Servicio (**SLA**), en el contrato respectivo, de acuerdo a su análisis de riesgo tecnológico y de acuerdo a la criticidad de sus operaciones. Los parámetros del Acuerdo de Nivel de Servicio, deben referirse al tipo de servicio, soporte y asistencia a clientes, previsiones para seguridad y datos, garantías del sistema y tiempos de respuesta, disponibilidad del sistema, conectividad, multas por caídas del sistema y/o líneas alternas para el servicio.

SECCIÓN 11:ADMINISTRACIÓN DE SERVICIOS Y CONTRATOS CON TERCEROS RELACIONADOS CON TECNOLOGÍA DE LA INFORMACIÓ

- El modelo de negocio de las **empresas** que dan servicios sobre **FOOS**, son los que **mejores** prestaciones dan a los clientes sobre los SLA que necesitan.
- Cubriendo tiempos cortos y servicios de 24x7.
  - Español: https://www.2ndquadrant.com/es/soporte/
  - Ingles: https://www.enterprisedb.com/services-support/support
  - Ingles: https://www.postgresql.fastware.com/postgresql-support-compare-plans

CONCLUSIONES

- PostgreSQL con los componentes nativos cumple con la mayor parte de la normativa de seguridad de la ASFI.
- Varios de los procesos, se deberían automatizar para no tener errores humanos, algo parecido a “mysql_secure_installation”.
- Se debe inculcar una cultura de seguridad en las implementaciones y desarrollo de PostgreSQL.

BASADO EN

- REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – ASFI.
  - http://servdmzw.asfi.gob.bo/CircularValores/Textos/L11T01.pdf

PREGUNTAS?