Painless Compliance, and a Thousand Audits a Day

Germán /hɜːmən/

Automating Governance, Risk and Compliance

Germán Fuentes Capella

german@trigosec.com

The cloud operations audit

How audits are done today

Me alone with the auditor

Just a difference of focus

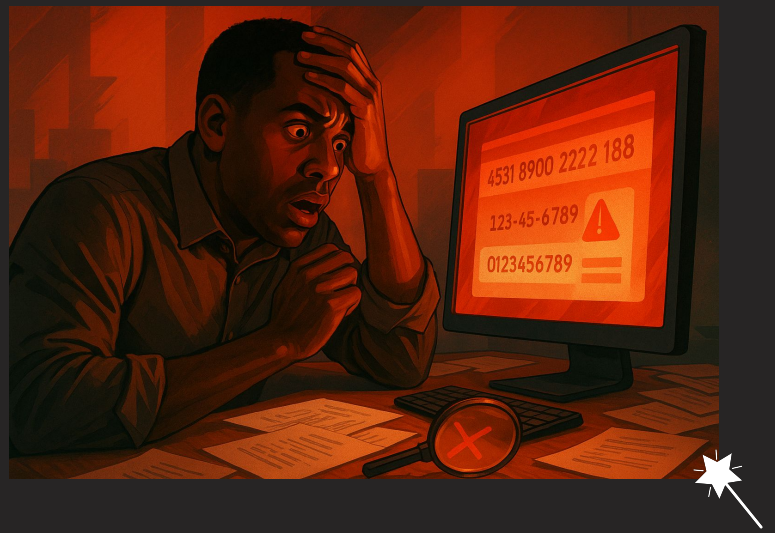
Traditionally: verification

Mine: better ways of working

Sounds familiar?

Sounds familiar?

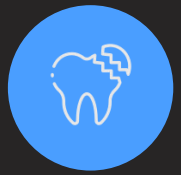
Sounds familiar?



Challenges in manual compliance

Out of cycle

Late discovery



Reactive & disruptive

Knowledge silos

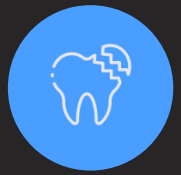
Fear & Uncertainty


Back to 1999
Home
About
About

Challenges in manual ~~compliance~~ testing

Out of cycle

Late discovery



Reactive & disruptive

Knowledge silos

Fear & Uncertainty

An audit is just a **test plan** we run **once a year**, **manually**, involving **dozens of people**

Compliance as a Product Feature

> As an **[auditor, security officer, ...]**,
> I want **[a list of all databases]**,
> so that **[I can verify encryption and prevent data breaches by copying files]**.

Compliance as a Product Feature

As an **[auditor, security officer, ...]**,

I want **[a list of all databases]**,

so that **[I can verify encryption and prevent data breaches by copying files]**.

Compliance as a Product Feature

As an **[auditor, security officer, ...]**,

I want **[a list of all databases]**,

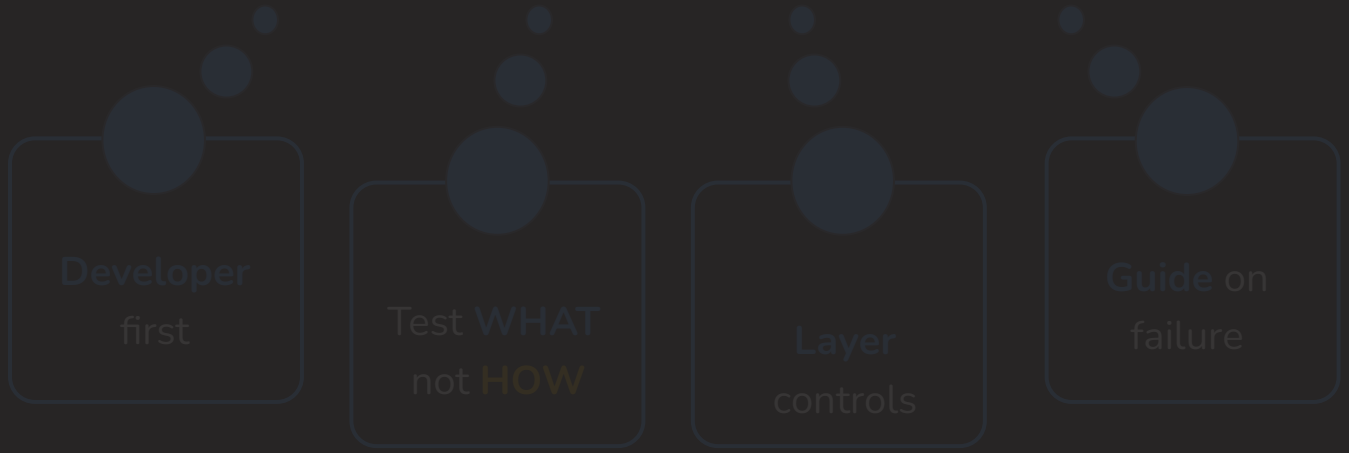
so that **[I can verify encryption and prevent data breaches by copying files]**.

Compliance as a Product Feature

As an **[auditor, security officer, ...]**,
I want **[a list of all databases]**,
so that **[I can verify encryption and prevent data breaches by copying files]**.

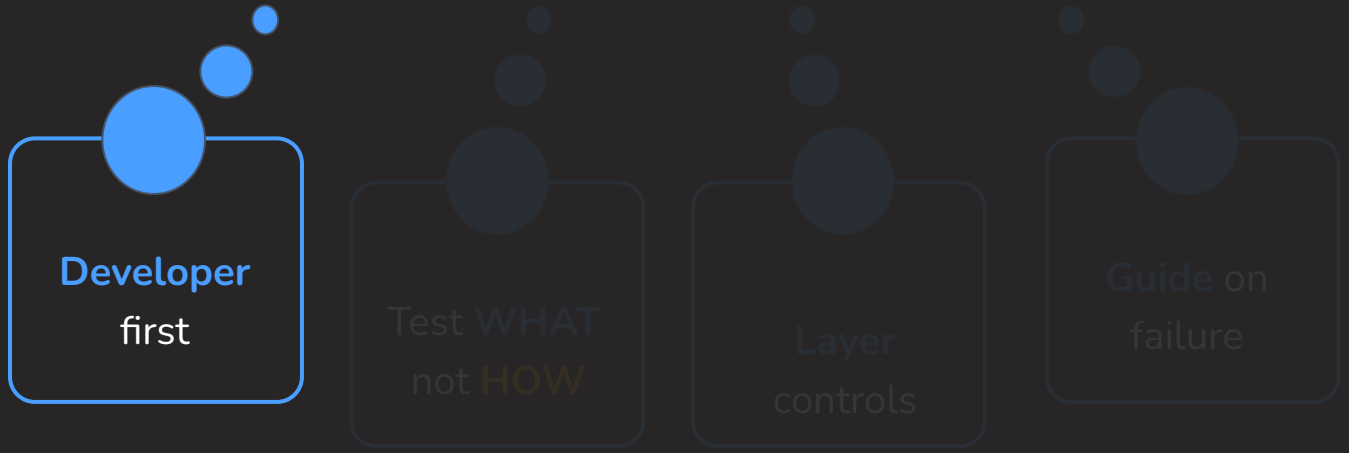
Automated compliance checks

Compliance ❤️ TDD

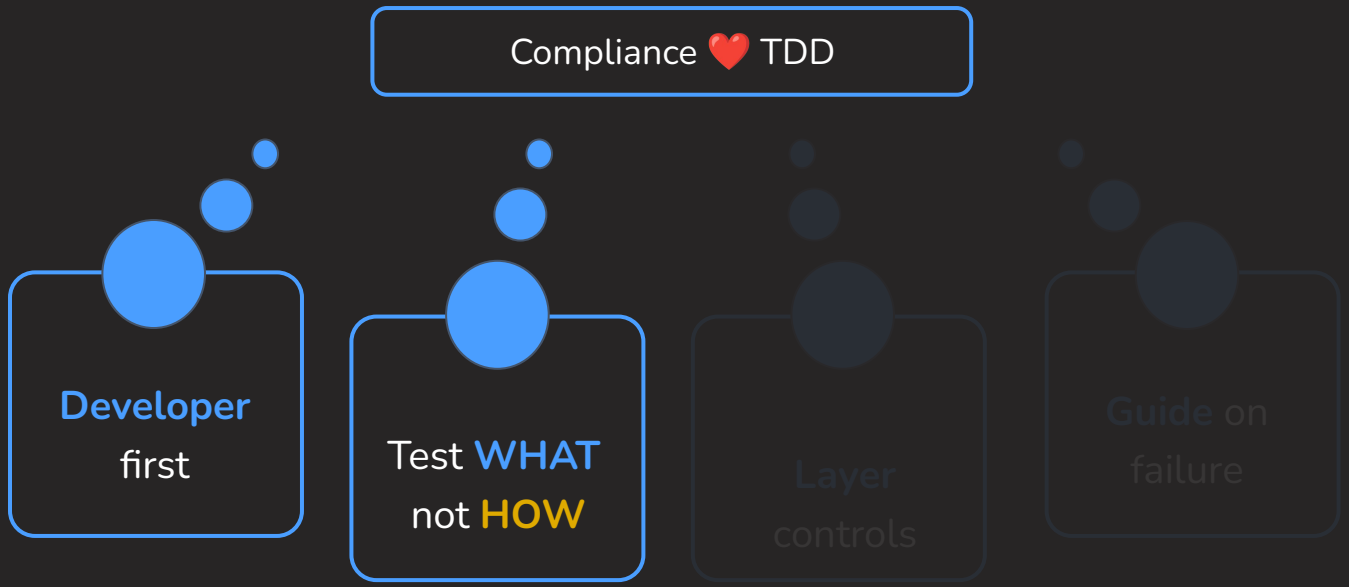


Automated compliance checks

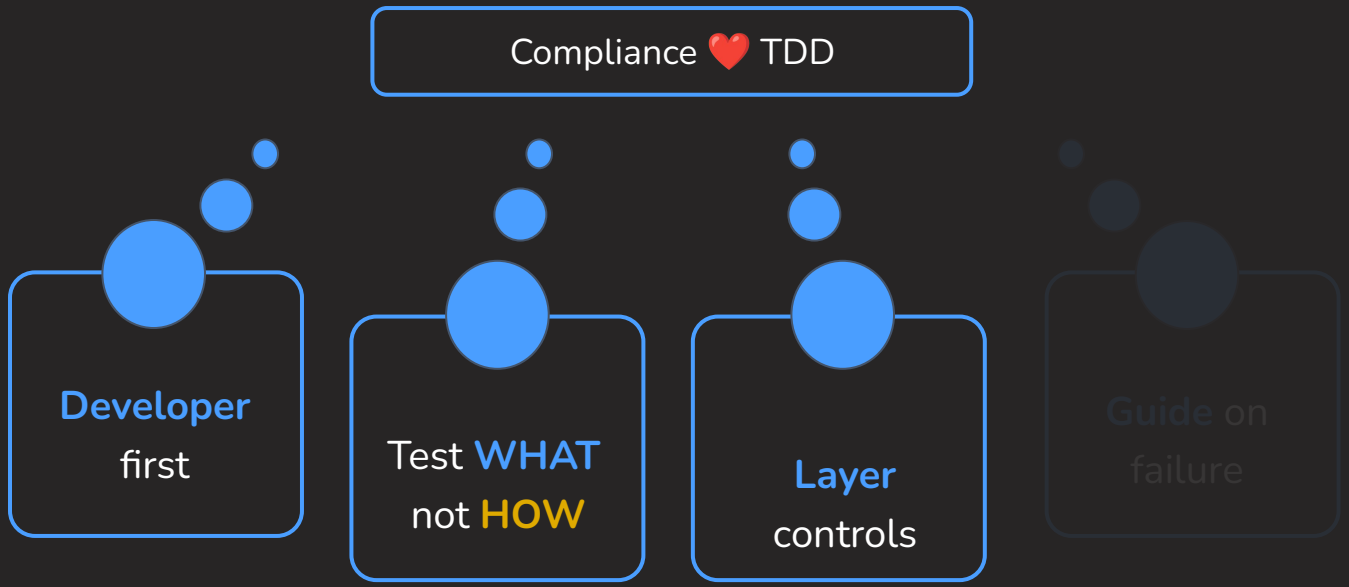
Compliance ❤️ TDD



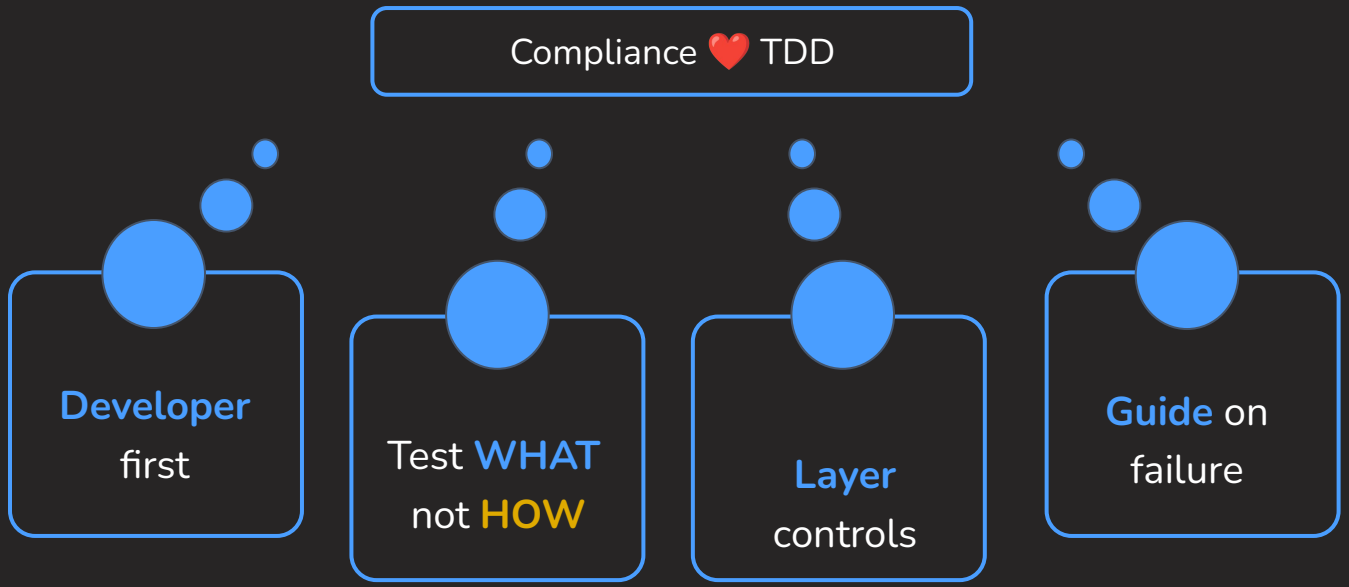
Automated compliance checks



Automated compliance checks

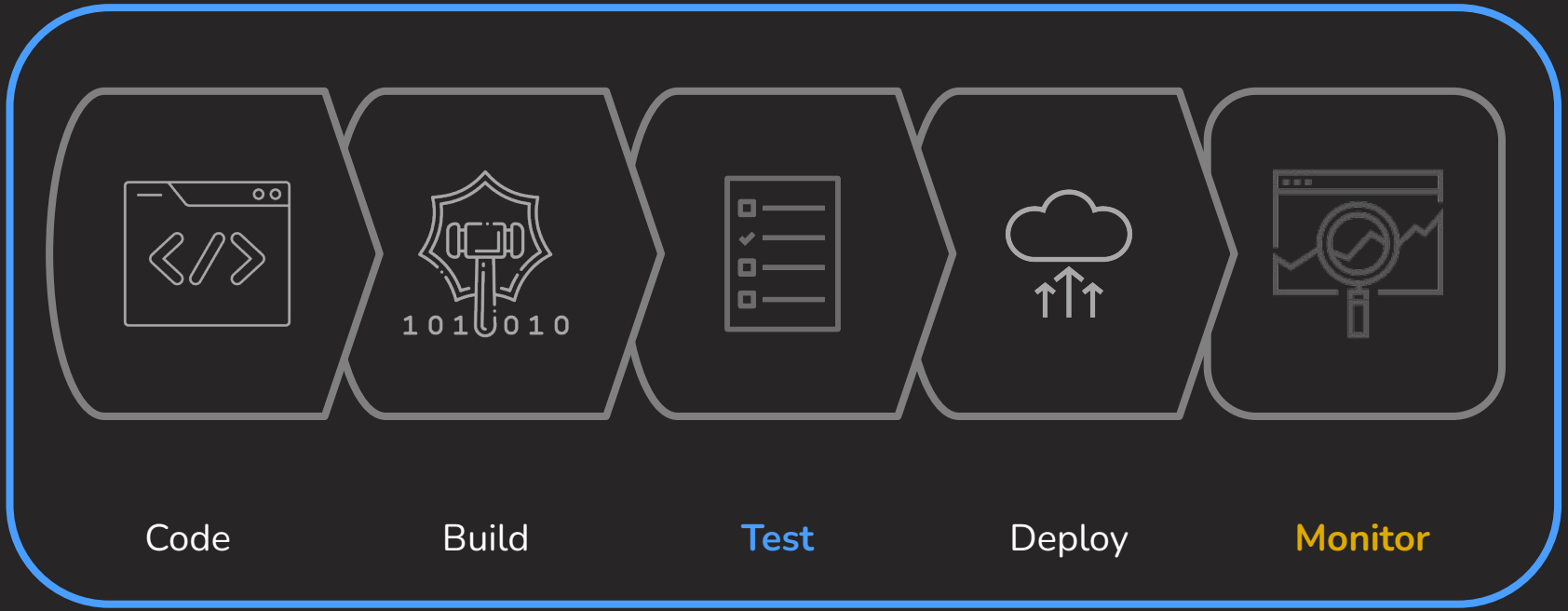


Automated compliance checks



Built right in your CI/CD

1000 times/day



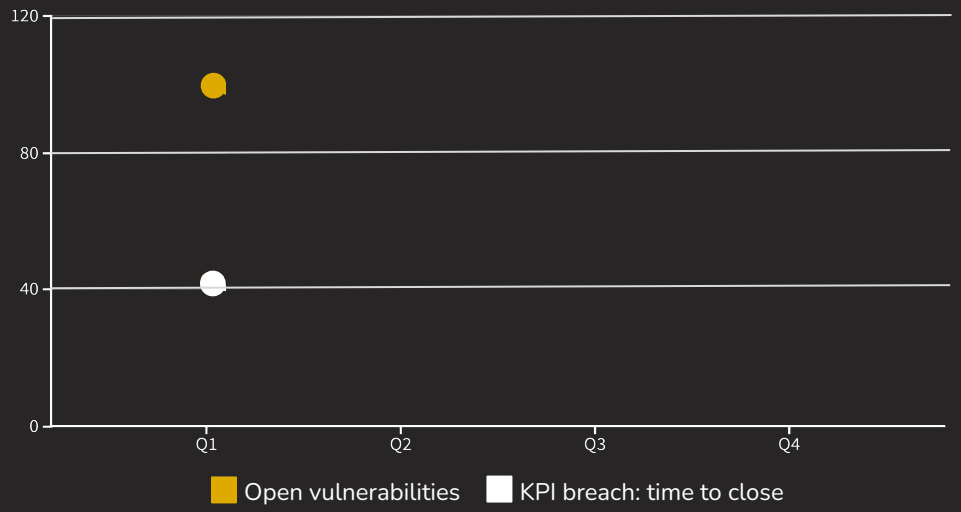
Built right in your CI/CD

Code Build **Test** Deploy **Monitor**

Built right in your CI/CD

Code Build **Test** Deploy **Monitor**

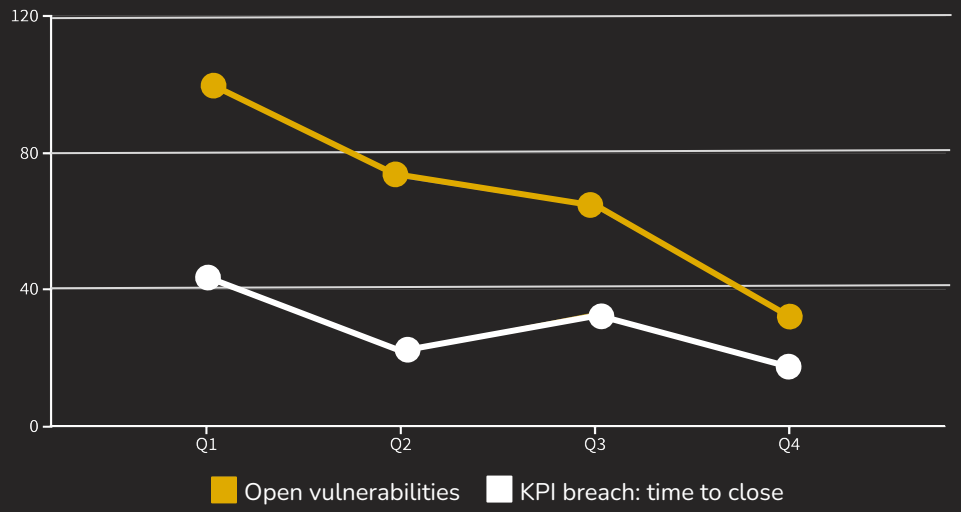
Add observability to your workflows



KPI breach: time to close

Team	Breaches
All	**43**
Team 1	**19**
Team 2	**24**

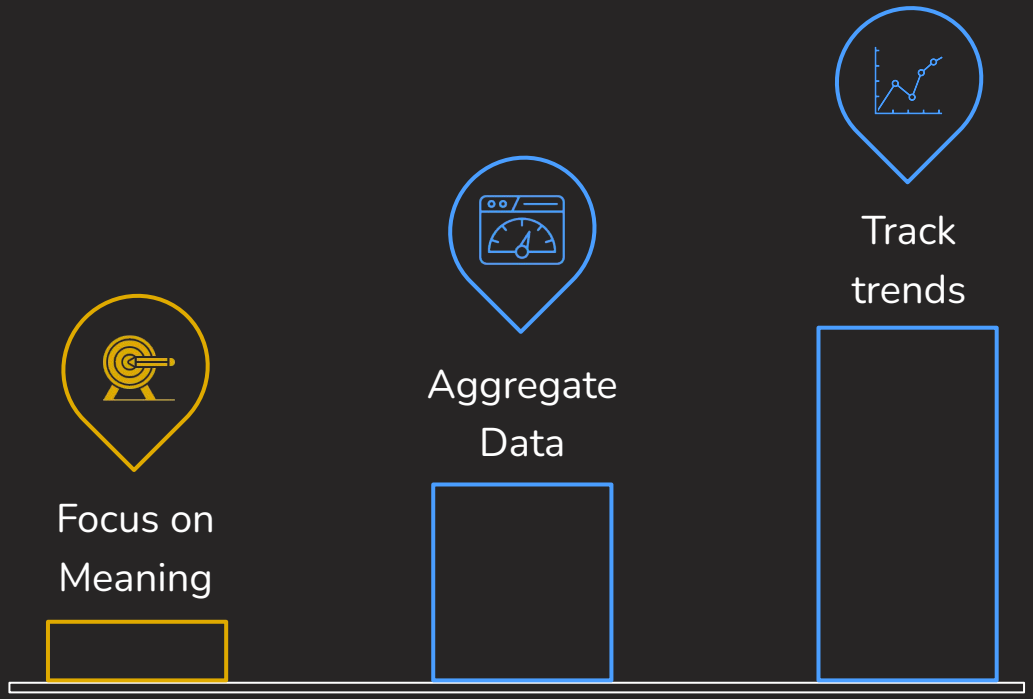
Add observability to your workflows



KPI breach: time to close

Team	Breaches
All	17
Team 1	9
Team 2	8

Risk-based alerting



Working with Auditors

First **supporter**

Must **understand** your approach

Involved **early**

Asset inventories as evidence

Driving Company Culture

Compliance as **differentiator**

Audit **ready**

Exciting

An **audit** is just a **test plan**, you can automate it

1. **Compliance** is part of your **product**
2. Build a **developer first** approach to **compliance**
3. Run your **compliance tests** in your **CI/CD**
4. **Process heavy** workflows shine with **dashboards** and **KPIs**
5. **Continuous compliance** requires **alerting based on risk changes**

Germán Fuentes Capella

german@trigosec.com

Back to the future

Thank you!

Germán /hɜːmən/

trigosec