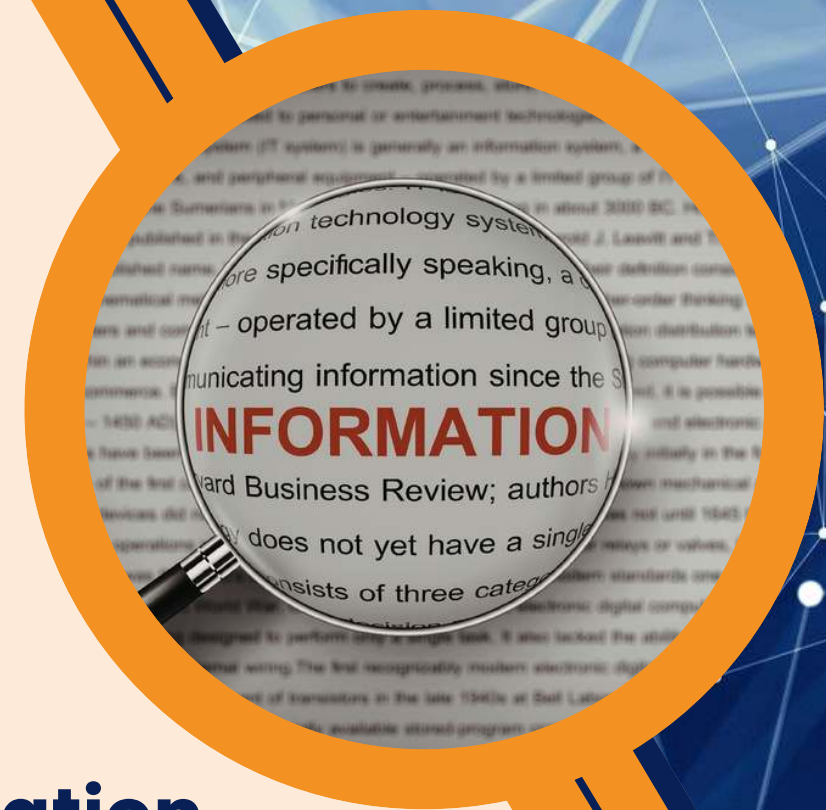




**CYBERFERO**

# Data classification (netwrix data classification)



- ✓ Automatic content discovery and classification
- ✓ Highlighting of high-risk areas (overexposure)
- ✓ Reduction of "rot" (useless/old/duplicate data)
- ✓ Clear reporting and remediation plan

[www.cyberfero.com](http://www.cyberfero.com)

# WHY IS THIS ACTIVITY STRATEGIC?

In companies, risk doesn't just arise from attacks: it arises from information chaos.

It often happens that:

- 01 Folders and repositories grow for years without governance
- 02 Documents with personal data end up in "convenient" positions, therefore too accessible
- 03 Permissions and sharing remain open even when roles and people change
- 04 Historical archives and duplicates increase the risk surface and management costs

The result is simple: exposure increases, control decreases, and in the event of an incident or audit, it becomes difficult to demonstrate that data is being managed appropriately.





# WHAT DOES DATA CLASSIFICATION REALLY DO?

Data classification means identifying and cataloging content based on what it contains (personal data, confidential data, critical documents), so that it can be protected, archived properly, or removed when no longer needed.

It is not a "documentary" exercise: it is an operational work that leads to clear decisions on:

- Where should sensitive files be kept
- Who should be able to see them
- What should be kept, archived or deleted

# WHAT DO WE ANALYZE AND WHAT DO WE FIND?

The service identifies content typically found in any organization, for example:

- ✓ HR documents (CVs, contracts, personnel administrative documentation)
- ✓ Customer and supplier documents (contracts, offers, records, correspondence)
- ✓ Administrative and legal documentation
- ✓ Projects, price lists, agreements, confidential materials
- ✓ Historical archives, duplicates and "forgotten" folders

**In parallel, we highlight where content is overexposed (accessible to more people than necessary), one of the most frequent causes of incidents and data leaks.**



# HOW DO WE WORK?



## 1) Assessment and scope

Together, we define the repositories to be analyzed and the objective (compliance, risk reduction, rationalization, audit support). We set criteria and priorities, without blocking operations.



## 2) Discovery and classification

We activate scanning and classification with consolidated rules and, when necessary, with customized criteria. The result is a readable map: where the data is located, what type it is, and where it is concentrated.



## 3) Risk analysis and rot

We produce evidence on:

- ✓ Areas with sensitive data in inappropriate locations
- ✓ Permissions excessive with respect to the principle of "minimum access"
- ✓ Rot: Redundant, obsolete, or useless data that only increases risk and costs



## 4) guided remediation and control over time

We deliver a prioritized action plan (rapid interventions + structural interventions). Upon request, we conduct periodic audits to maintain order and governance.

# SENSITIVE DATA

(repository, areas, content types)

**Evidence of overexposure**

(where access is too wide)



**Remediation plan**

what to do, where, with what urgency and impact

**Root analysis**

with cleaning/archiving priority



**Report per audit e**

**governance**

(readable by management, compliance and IT)

# WHO NEEDS IT?

This service is suitable for:

- 01 Companies with file servers, shared folders, or cloud repositories that have grown over time
- 02 Organizations that handle a lot of customer and employee data and want to reduce real-world exposure
- 03 Realities that have frequent changes of roles and people (accesses that are difficult to maintain consistent)
- 04 Companies that want to seriously prepare for audits, inspections or formal requests without rushing to the last minute



# WHY CYBERFERO?



Cyberfero brings a security service provider approach:

**TECHNOLOGY + METHOD +  
OPERATIONAL RESPONSIBILITIES.**

We don't just deliver a photograph:

**WE LEAD TO CONCRETE CHOICES, WITH PRIORITIES  
AND A MEASURABLE IMPROVEMENT PATH.**



# CYBERFERO

**For over 10 years a leader in the Cybersecurity and Security sector**

Cyberfero is a Managed Security Service Provider (MSSP) specializing in providing comprehensive security solutions for businesses of all sizes. As a trusted partner, we offer a broad range of security services designed to protect your organization from cyber threats, data breaches and other security risks.

[Website](#)

## Contacts



**+39 0522 1685330**



**<https://www.cyberfero.com>**



**[info@cyberfero.com](mailto:info@cyberfero.com)**



**Via Statuto 3, 42123 - Reggio nell'Emilia (RE)**

