RDOWEB

Aspects of SECURITY



1- Contents

This document describes good practices adopted in the development and maintenance of the RDOWEB software, which aim to mitigate security risks and conveniently protect the information stored in its database.
This document may contain confidential or privileged information. If you are not the addressee or authorized person, you must not use, copy or disclose the information contained herein or take any action based on this information.

01

INDEX
Summary and legal notice.

02

ABOUT RDOWEB
Concepts that define the tool from a safety point of view.

03

PILLARS OF SECURITY
The main points that guide security actions in RDOWEB.

04

CONTROLLING THE RISKS
Risks managed by the application.

05

ABOUT WEBDUTOS
Get to know a little about us.

06

CONTACT



The RDOWEB was created for information management, control, and issuance of Construction Site Journals, in compliance with resolution 1094 CONFEA. It uses a high performance SQL database in a WEB environment.

It has a configurable workflow to control access to information and resources for consolidation of each journal issued.



Pillars of Security

To minimize risks, increase the reliability and quality of RDOWEB 3 fundamental aspects have been considered still in its development.

1 CONFIDENTIALITY

Technical measures capable of keeping information secret have been adopted. Examples practiced at RDOWEB:

encrypted passwords,

2-step authentication and workflow with different permission levels.

2 INTEGRITY

Because it is a web system, much attention is paid to ensure trust in the source of the information. For example, only authenticated users can access RDOWEB, and communication is done over the HTTPS protocol.

3 AVAILABILITY

Ensuring that information is available to authorized users when needed.

Some measures adopted: use of state-of-the-art infrastructure and Amazon AWS datacenter in Brazil, daily backups and constant monitoring.

Risk Control

Application Managed Risks

Data Validation

The use of browsers makes it possible for users to make arbitrary entries. To prevent this from compromising the application or the security of your data, all information is also checked on the server side before being written to the database.

Authenticated users

To gain access to RDOWEB, each user must enter his password and his identity is verified for all the operations he performs on system.

Password Policy

Besides imposing a minimum quality standard for passwords, the RDOWEB also saves them encrypted. To authenticate a user, you must re- encrypt the password and compare the result with the hash saved in the database.



Risk Control

Application Managed Risks: Continued



Two-factor authentication

After the software administrator has created the password, the user is required to enter his new definitive password. The mechanism is two-step, with the generation of a token sent to the user's email address. In this way, not even the enterprise administrator will know the user's definitive password.



Predefined Response Fields

The pre-defined response fields do not allow the user to type data, but to choose from a list of options saved by the site administrator. For example, the list of subcontractors, equipment, positions, among others. This improves the quality of the information and prevents arbitrary data entry.



Workflow with different permission levels

Each user has a configurable access level, which indicates to the software their permissions to access the information. Before being processed, each piece of information is checked against the authenticated user's permission matrix.

Risk Control

Cloud Application Security

Communication Protocol: *https*



The HTTPS protocol is used to prevent information transmitted between the client and the server from being viewed by third parties. All communication performed by RDOWEB uses the HTTPS protocol. This ensures that there will be no data interception.

Server side data validation



To prevent unwanted data from being recorded, all information is checked on the server as well, ensuring consistency at both ends of the connection. Data typed in go through consistency of format, type, size, access permission, and edit permission.

Firewall



Protection against intrusions by IP identification. The application does not communicate directly with the server in the datacenter, but goes through an additional layer of security "Cloud security".

Risk Control

Cloud Application Security

State-of-the-art infrastructure

Use of state-of-the-art infrastructure (Amazon AWS) geolocated in Brazil to minimize latency, enable high availability and elastic capacity.

Daily Backups

Backup copies are performed daily and automatically for files, application, and database.

Data Audit/Log

Every operation performed by the users is replicated in a separate database, generating a log that contains information such as the original data, date, time of change, and the name of the user who made the change.

About Webdutos

We are committed to delivering not only the best programs, but also the best service



Webdutos is a company specialized in software for engineering companies, with solutions used to support the management of works in various segments such as pipeline construction, infrastructure, industrial assembly and civil construction.

Our software works in a modular way, working in an integrated or separate way, and is operated through a simple web browser, reducing costs for the enterprise IT and providing management-level access for managers who need to make quick decisions.

Robust, simple, elegant programs accompanied by the best service. We have been doing this for 16 years in large, medium, and small enterprises.

Know more at webdutos.com.br

CONTACT

Access for more details

www.rdoweb.com.br

Or send email to

contato@rdoweb.com.br

Office:

254 Monsenhor Silva Barros Square - center - Taubaté/SP

Tel. +55 12 3413 6082 | +55 12 9 97570306 | +55 12 9 98114 6861