One possible solution for this company would be to implement a role-based access control (RBAC) system. In a RBAC system, access to resources and functions within the system is determined by the roles that users have been assigned. For example, an office that is responsible for maintaining employee personal files could be assigned a "HR Manager" role, which would grant them access to the relevant files and functions within the system.

To ensure the security of the confidential documents, the system could use encryption to protect the documents while they are in transit between offices. Additionally, the system could implement a digital signature system, which would allow offices to securely sign and verify the authenticity of the documents.

To prevent unauthorized access to sensitive information, the system could implement a system of permissions and access levels. For example, an employee who is authorized to see and use certain information might be granted the "Employee" role, which would allow them to access only the information and functions that they are authorized to use. Another employee who is not authorized to see and use the same information might be assigned a different role, such as "Guest," which would limit their access to only the information and functions that are appropriate for their role.

Overall, a combination of RBAC, encryption, digital signatures, and access levels can provide a robust and secure solution for this company.