# Redguard Security Survey 2026 – Les entreprises suisses appliquent-elles les bases de la Cybersécurité ?

Auteur : Luca Mutti

Découvrez l'évolution du niveau de cybersécurité des organisations et entreprises suisses au cours des huit dernières années. Les résultats s'alignent sur la norme minimale pour les TIC et couvrent des éléments clés essentiels tels que la gestion des risques, la gestion des fournisseurs, la sensibilisation et la formation, la surveillance et la gestion des logs, la sauvegarde, la gestion des incidents, la gestion de la continuité d'activité (*Business Continuity Management* - BCM) ainsi que la communication de crise. Les entreprises participantes ont évalué leur niveau de sécurité actuel à l'aide de notre *Quick-Test*. Apprenez quelles mesures nous recommandons tout particulièrement sur la base des résultats de l'enquête.

## La norme minimale pour les TIC devient obligatoire pour de plus en plus de secteurs

Avec la publication de la norme minimale pour les TIC par la Confédération, la Suisse dispose depuis 2018 d'une directive uniforme et transsectorielle visant à se protéger contre les risques cyber. Le respect de cette norme devient de plus en plus obligatoire pour les **opérateurs d'infrastructures critiques**. Ainsi, des valeurs de maturité spécifiques sont obligatoires pour le secteur de l'électricité depuis le 1er juillet 2024 et pour le secteur du gaz depuis le 1er juillet 2025. Il est probable que **des exigences comparables suivent pour d'autres secteurs**.

Mais qu'en est-il du niveau de sécurité actuel des entreprises suisses ? Pour la huitième fois déjà, Redguard SA publie les résultats de son enquête sur la norme minimale pour les TIC.

## La cybersécurité prend de l'importance

Il est généralement admis que le thème de la cybersécurité a considérablement gagné en importance au cours des dernières années et qu'il est également **pris au sérieux par les directions d'entreprise**. Selon l'enquête de cette année, 85 % des entreprises (contre 77 % l'année précédente) déclarent que le sujet de la cybersécurité bénéficie du soutien total de la direction. Cette **professionnalisation** se manifeste au niveau du personnel. Dans 75 % des organisations interrogées, la **responsabilité de la cybersécurité** est définie et pourvue en personnel. En ce qui concerne les ressources financières, la situation est relativement stable : 70 % des entreprises (contre 71 % l'année précédente) déclarent disposer d'un **budget de sécurité suffisant**.

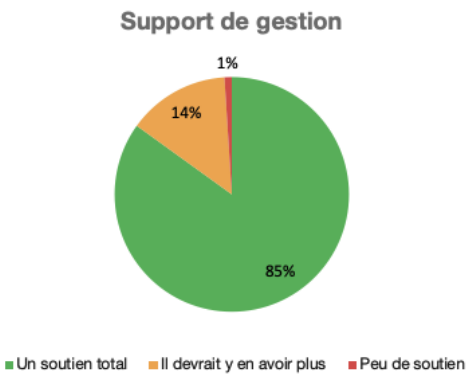


*Figure 1 : Le soutien de la direction est-il présent ?*

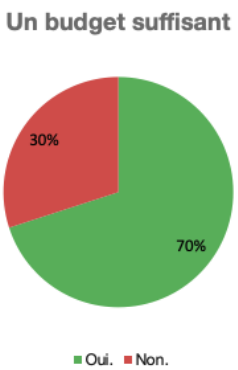


*Figure 2 : Le budget de sécurité disponible est-il suffisant ?*

## Comment fonctionne l'évaluation *Quick-Test* de Redguard ?

Le Quick-Test de Redguard sur la norme minimale TIC se compose cette année de 18 questions ciblant les éléments clés de cette norme. Les organisations et entreprises participantes répondent aux questions sur la base d'une auto-évaluation. L'analyse leur permet d'évaluer rapidement leur niveau de sécurité et de définir des mesures complémentaires.

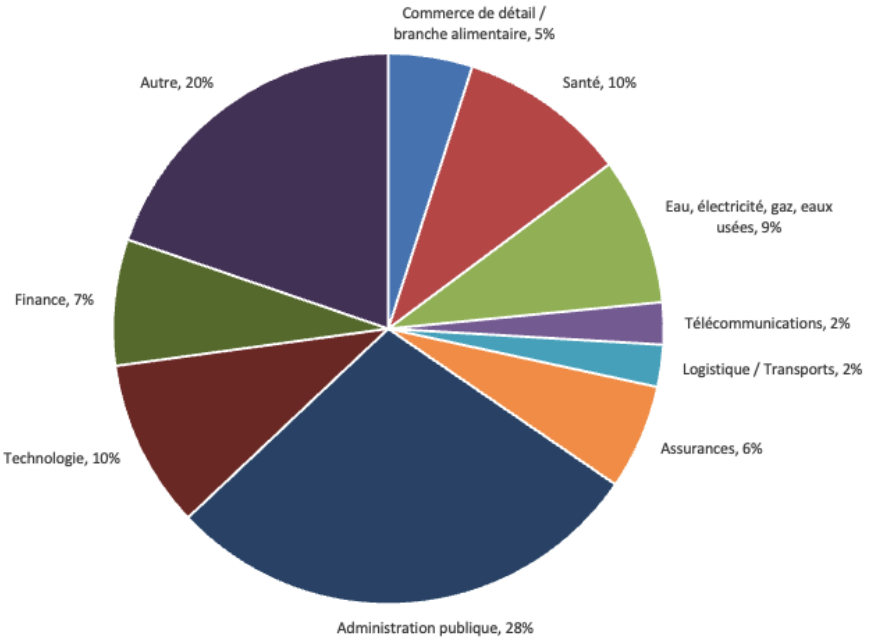


*Figure 3 : Entreprises interrogées par secteur d'activité (%)*

## Près de 100 organisations suisses ont participé

Cette année encore, Redguard a invité de nombreuses organisations suisses à évaluer leur niveau de sécurité. Près de 100 organisations issues de divers secteurs se sont intéressées à la norme et ont soumis leur auto-évaluation.

La Figure 3 montre que les résultats du *Security Survey* reposent une fois de plus sur une large base. Les entreprises et organisations participantes sont issues des secteurs les plus variés, avec une répartition très équilibrée. L'Administration publique arrive en tête avec 28 %, suivie de la Technologie (10 %) et de la Santé (10 %). En même temps, des entreprises de tailles très diverses ont contribué au « Redguard Security Survey », comme le montre la Figure 4. Selon les participants, 28 % sont de grandes entreprises comptant plus de 500 collaborateurs. **Les PME constituent à nouveau la part la plus importante** avec 37 % de petites entreprises (1-50 employés) et 25 % d'entreprises de taille moyenne (51-200 employés).

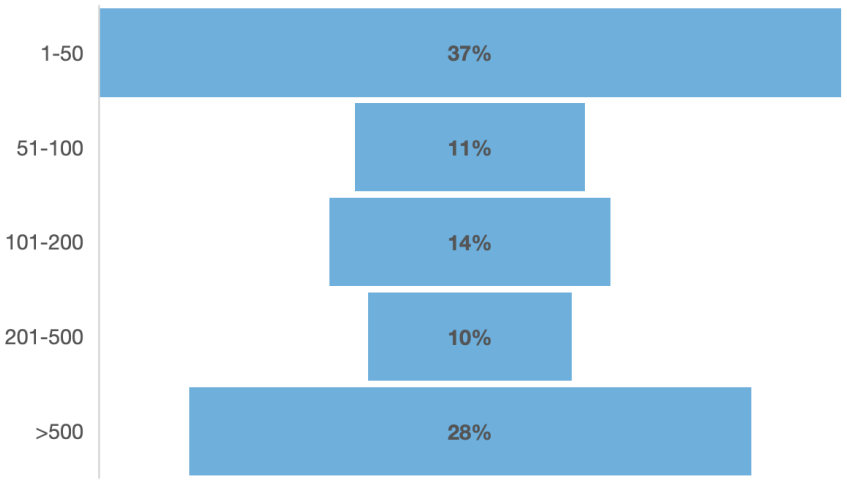


*Figure 4 : Entreprises interrogées par nombre de collaborateurs*

## Niveau de maturité accru pour presque toutes les fonctions – néanmoins juste en dessous de la valeur minimale

Dans le cadre de l'enquête de cette année, les participants ont évalué leur niveau de maturité pour quatre fonctions sur cinq comme étant nettement supérieur à celui de l'année précédente. Bien que le score global de toutes les entreprises (2,5) reste inférieur à la valeur minimale « non officielle » de 2,6, une nette augmentation de la maturité a été constatée par rapport à l'année précédente (score = 2,3). Il convient toutefois de souligner que les secteurs actuellement réglementés (électricité / gaz) devraient viser une valeur cible de 3 (et donc « mise en œuvre »).

La fonction « Protéger » enregistre la valeur la plus élevée, comme les années précédentes, avec 2,9 (contre 2,7 l'année précédente). **Le thème « Sauvegardes », nouvellement intégré**, a immédiatement atteint une valeur étonnante de 3,3, contribuant de manière significative à cette augmentation. La mise en œuvre de mesures de sécurité techniques semble ainsi beaucoup plus facile pour les répondants que les sujets fortement liés aux processus et à l'organisation, tels que la gestion de la continuité d'activité (*BCM*) ou la gestion des risques.

L'évaluation montre que les participants se sont améliorés dans presque toutes les fonctions. La seule exception est la fonction « Détecter », dont la valeur est restée identique à celle de la dernière évaluation. Cela pourrait s'expliquer par le fait que 37 % des entreprises participantes sont de petites entreprises (< 50 employés), qui ont tendance à être moins bien positionnées dans le domaine « Détecter », et en particulier dans celui de la gestion des logs, que les entreprises moyennes et grandes.

Les deux fonctions « Réagir » et « Récupérer » constituent depuis des années le bas du classement de l'évaluation. On ne peut que spéculer sur les raisons possibles. Nos expériences montrent toutefois que certaines entreprises ont tendance à ne pas s'attaquer au *BCM* pendant longtemps en raison de sa complexité. Une autre raison pourrait être que les entreprises pensent toujours qu'elles ne seront pas la cible d'une cyberattaque – et se soucient donc moins de la réaction aux incidents ou du rétablissement après une telle attaque. À ce sujet, nous ne pouvons que répéter que tout le monde peut être touché, y compris – et parfois surtout – les PME.

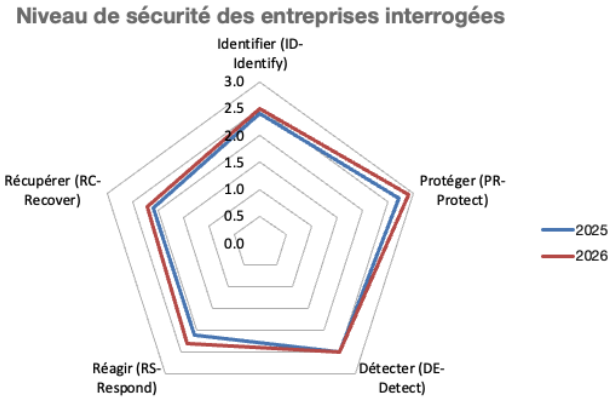


*Figure 5 : Résultats du « Redguard Security Survey 2026 »*

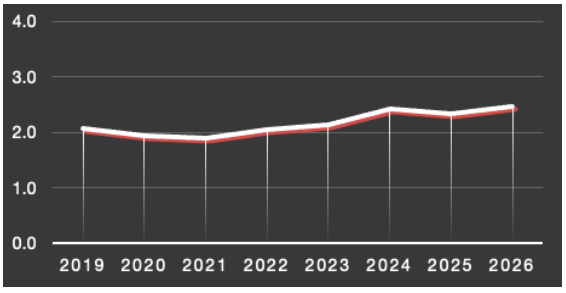


*Figure 6 : Évolution du niveau de maturité et comparaison avec l'année précédente*

| Fonction | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 |
|---|---|---|---|---|---|---|---|---|
| Identifier (ID-Identify) | 2.0 | 2.0 | 2.0 | 2.1 | 2.2 | 2.4 | 2.4 | 2.5 |
| Protéger (PR-Protect) | 2.3 | 2.3 | 2.1 | 2.1 | 2.3 | 2.8 | 2.7 | 2.9 |
| Détecter (DE-Detect) | 2.2 | 1.9 | 1.9 | 2.1 | 2.1 | 2.5 | 2.5 | 2.5 |
| Réagir (RS-Respond) | 2.2 | 1.8 | 1.7 | 1.9 | 2.1 | 2.3 | 2.1 | 2.3 |
| Récupérer (RC-Recover) | 1.7 | 1.7 | 1.8 | 2.0 | 2.0 | 2.1 | 2.1 | 2.2 |
| **Niveau de maturité** | **2.1** | **1.9** | **1.9** | **2.0** | **2.1** | **2.4** | **2.3** | **2.5** |

*Tableau 1 : Résultats chiffrés en comparaison annuelle*

## Vers un renforcement législatif de la protection des infrastructures critiques

Les efforts des entreprises suisses reflètent une évolution également fortement encouragée au niveau national et politique. Le 18 février 2026, le Conseil fédéral a décidé de renforcer la protection des infrastructures critiques, essentielles pour la population et l'économie. La mise en œuvre de deux motions vise à créer des bases légales contemporaines afin de développer de manière proactive la résilience générale.

La première motion acceptée porte le titre « **Bases légales modernes pour la protection des infrastructures critiques** ». Elle exige une adaptation des dispositions légales existantes afin que la Confédération puisse à l'avenir édicter des exigences contraignantes en matière de sécurité de fonctionnement et de rétablissement des perturbations. Cela doit garantir que les systèmes d'approvisionnement critiques deviennent plus robustes et puissent mieux maintenir leurs services pour la société en cas d'événements tels que des attaques ciblées ou des catastrophes naturelles.

La deuxième motion, intitulée « **Pour une meilleure sécurité des données numériques essentielles de la Suisse** », demande la création d'une base légale pour une meilleure protection des informations pertinentes pour la sécurité. Cela permettra d'adresser des exigences claires et contraignantes à la Confédération, aux cantons ainsi qu'aux exploitants d'infrastructures critiques.

D'ici la fin de 2026, le Département fédéral de la défense, de la protection de la population et des sports (DDPS) élaborera, en étroite collaboration avec d'autres services, les principes directeurs pour les **projets de loi correspondants**. Cela souligne à nouveau très clairement l'importance réglementaire croissante de la cybersécurité.

## Nous vous aidons à satisfaire à la norme minimale pour les TIC

La norme minimale pour les TIC est conçue de manière à pouvoir être mise en œuvre par toutes les entreprises, indépendamment de leur secteur d'activité et de leur taille. Malgré le guide et l'outil d'évaluation de l'Office fédéral pour l'approvisionnement économique du pays, des connaissances spécialisées approfondies ainsi qu'une approche pragmatique sont essentielles pour la réussite de la mise en œuvre de la norme minimale pour les TIC. Redguard accompagne les entreprises dans l'application de la norme minimale pour les TIC.

**Identifier – Connaissez vos risques et abordez la sécurité de l'information de manière stratégique**

Redguard vous aide à identifier et à recenser systématiquement les cyber-risques de votre organisation. Sur la base de vos risques, nous élaborons avec vous une stratégie de sécurité de l'information afin de les traiter et de les contrôler.

Vérifiez dans quelle mesure vos données sont traitées en dehors de votre infrastructure et édictez des directives correspondantes concernant le traitement de vos données d'entreprise par des tiers. Redguard vous apporte son aide à cet égard.

**Protéger – Protégez vos systèmes et formez vos collaborateurs**

Élaborez des directives pour la protection de vos systèmes et mettez-les en œuvre. Redguard vous aide à définir les mesures adéquates, par exemple dans les domaines de la gestion des accès, du *firewalling*, de la segmentation du réseau ainsi que de la protection contre les *malwares*.

Les mesures techniques ne suffisent pas à elles seules : formez vos collaborateurs et montrez-leur la contribution qu'ils peuvent apporter à la sécurité de l'information. Redguard vous soutient avec des modules d'e-learning, des offres de formation classiques, des démonstrations de *Live-Hackings* et des campagnes de *phishing*, ou un *Managed Service* complet dans le domaine de la sensibilisation.

**Détecter – Connaissez vos vulnérabilités et testez vos défenses**

Configurez vos systèmes et processus de manière à pouvoir détecter d'éventuels incidents de sécurité et anomalies.

Collectez toutes les données de log pertinentes dans un emplacement centralisé afin d'accroître la traçabilité complète et de faciliter le travail des Incident Responders (répondeurs aux incidents) et des experts en forensique informatique en cas d'attaque.

Mettez vos systèmes et la sécurité de l'information à l'épreuve à l'aide de tests d'intrusion ou d'une simulation d'attaque. Les spécialistes de Redguard effectuent des tests et des attaques ciblés pour votre compte et vous indiquent ainsi des pistes d'amélioration.

**Réagir – Planifiez et exercez votre réaction aux incidents de cybersécurité**

Les plans de réaction vous aident à réagir correctement en cas d'urgence et à gagner du temps. Grâce à un plan de réaction, vous avez déjà répondu à de nombreuses questions au préalable : Qui est responsable dans votre organisation en cas d'incident de cybersécurité ? Comment informez-vous vos collaborateurs et clients ? Arrêtez-vous complètement les systèmes ou maintenez-vous un mode de fonctionnement dégradé ?

Avec Redguard, vous pouvez vous entraîner à l'urgence au moyen d'un exercice de simulation sur table (*Tabletop Exercise* - TTX). Parcourez étape par étape un scénario adapté à votre organisation et déduisez-en des possibilités d'amélioration et des mesures.

**Récupérer – Retour à la normale**

Créez un plan de rétablissement et fixez-vous des objectifs concrets de rétablissement : Combien de temps pouvez-vous au maximum vous passer de vos systèmes ? Quelle perte de données pouvez-vous accepter ?

Définissez votre stratégie de communication au préalable afin de pouvoir vous présenter avec assurance face à vos parties prenantes, même en situation de crise.

Redguard aide votre organisation à atteindre le niveau de sécurité minimal recommandé pour la fonction récupérer en élaborant avec vous des plans de rétablissement.

## Mesures recommandées: mise en œuvre globale du standard minimal TIC

Concentrez-vous sur votre cœur de métier pendant que nous élevons votre niveau en matière de sécurité de l'information. Avec une équipe d'environ **100 spécialistes en sécurité**, nous proposons des services complets auprès d'un seul et même fournisseur.

**État des lieux selon la norme minimale pour les TIC**

Faites évaluer en détail le niveau de maturité dans le domaine de la sécurité de l'information par un organisme indépendant. Nos spécialistes examinent vos systèmes, documents et processus. Les conclusions qui en résultent sont discutées plus en détail lors d'entretiens. Vous recevez un rapport contenant les vulnérabilités identifiées ainsi que des recommandations concrètes pour y remédier et améliorer ainsi la sécurité de l'information de votre entreprise.

**CISOaaS – Mise en œuvre et maintien de la norme minimale pour les TIC**

Avec le service « Security Officer as a Service », vous disposez d'un interlocuteur personnel qui se tient à votre disposition avec l'ensemble du savoir-faire de Redguard. Votre interlocuteur met en œuvre les recommandations d'action issues de l'évaluation de la situation en tant que consultant en sécurité et chef de projet au sein de votre organisation. Il veille également à ce que la norme minimale pour les TIC soit respectée et que le niveau de maturité soit amélioré en continu.

**Gestion de la continuité des activités (*Business Continuity Management* - BCM)**

Assurer la continuité de l'activité en cas d'urgence ou de crise est fondamental. De nombreuses étapes peuvent être planifiées et préparées au préalable en toute tranquillité afin d'être le mieux armé possible pour l'urgence. Nous vous aidons à analyser vos processus d'entreprise et actifs critiques sous la forme d'une analyse d'impact sur l'activité (*Business Impact Analysis* - BIA) et élaborons avec vous les plans d'urgence nécessaires. Les expériences pratiques de nos *Incident Responders* tirées de cas réels sont intégrées dans votre préparation aux situations d'urgence.

**Gestion des incidents**

**Prévention** : Outre les mesures préventives, nous vous aidons également à mettre en place une organisation appropriée de gestion des cyberincidents et à élaborer une planification des cyberincidents (Cyber-Incident-Planning).
**Pas seul en cas d'urgence** : Nous vous soutenons 24 heures sur 24 dans l'endiguement et l'analyse des cyberincidents et dans le rétablissement de vos activités commerciales. Notre équipe de réponse aux incidents (Incident Response Team)

couvre toutes les expertises nécessaires (technologie, exigences réglementaires, etc.) et est en contact permanent avec les autorités ainsi qu'avec d'autres équipes de réponse aux incidents. Nous assurons un déroulement structuré et des esprits froids.

**Darknet Monitoring**

Les attaquants sont de plus en plus sophistiqués et utilisent de plus en plus le Darknet pour vendre ou publier des informations volées aux entreprises. La protection des données d'entreprise sensibles contre la fuite et l'abus est donc plus importante que jamais. Notre service vous offre une solution proactive pour protéger votre entreprise contre de tels abus.

**SOC as a Service**

Confiez votre cybersécurité à des professionnels : Notre SOC basé sur le Cloud est géré par notre filiale FusionOne, où les experts de Redguard et de FusionOne travaillent main dans la main pour votre protection. L'offre de services est accessible à toutes les organisations et entreprises qui utilisent Microsoft 365. Le SOC a également été développé et testé avec des PME et répond à leurs besoins quotidiens et à leur budget.

**L'OT-Security en point de mire**

La norme minimale pour les TIC s'adresse aussi bien à l'infrastructure IT qu'à l'infrastructure OT. Les deux domaines fusionnent de plus en plus. En conséquence, une approche globale est nécessaire pour sécuriser les composants OT. Nos experts en sécurité combinent les perspectives des deux mondes et vous aident à mettre en place un dispositif de sécurité global pour les deux domaines.

Vous souhaitez savoir la sécurité de votre organisation entre de bonnes mains ? Appelez-nous – Nous vous conseillons sans engagement.