INFOSTRUCTURE

PROTECTING DIGITAL HEALTHCARE

A Cybersecurity Guide for the Healthcare Sector

IDB

AUTHORS: Pablo Alzuri, Florencia Cabral, Santiago Paz, Ariel Nowersztern y Pablo Libedinsky.
DESIGN: www.souvenirme.com

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Inter-American Development Bank, its Board of Directors, or the countries they represent.

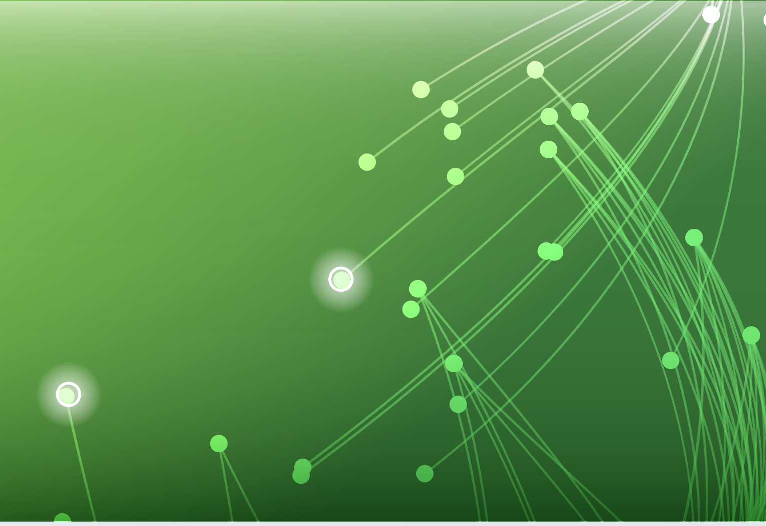
INFOSTRUCTURE

IDB

PROTECTING DIGITAL HEALTHCARE

A Cybersecurity Guide for the Healthcare Sector

Table of Contents



Foreword

The COVID-19 pandemic has accelerated the digitalization of our societies, and cybersecurity has moved to the forefront of the world's concerns. **Digitalization is key to accelerating economic and social recovery, which is why it is one of the five strategic pillars of Vision 2025, the IDB Group's plan to drive inclusive and sustainable post-pandemic growth**. The need to protect this growing digital space explains the importance of understanding cybersecurity's role in digital transformation.

Cybersecurity is particularly relevant in the healthcare sector due to the sensitivity of the information it manages. The technologies that support electronic health records, telemedicine, and other advanced medical devices are critical systems, and they have unfortunately been targeted by multiple attacks in recent years. Protected Health Information (PHI) is the highest-priced data on the black market, with values tens of times higher than that of other data like credit card numbers[a].

In 2020, **healthcare data leaks in the United States rose 55 percent**, according to the Department of Health and Human Services. Of these leaks, 67 percent were due to cybersecurity incidents[b].

According to a study published by the Inter-American Development Bank (IDB) and the Organization of American States in 2020, the Latin America and the Caribbean region continues to face significant challenges. Many countries in this region still have ad-hoc cybersecurity activities and initiatives that lack a strategic vision. **Only 13 countries have a national cybersecurity strategy and only 9 have a critical infrastructure protection plan**. According to ITU's Global Cybersecurity Index, only 1 out of 55 countries in the world that stand out for their commitment to cybersecurity is located in this region (Uruguay).

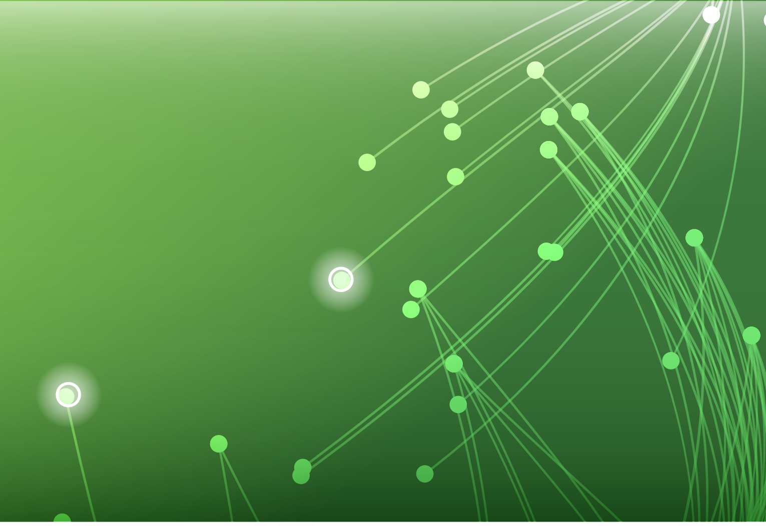
At the IDB, we are very aware of these challenges, which is why we developed this guide that aims to facilitate access to knowledge and support tools to assess and improve the state of cybersecurity at health organizations and protect the citizens of our region.

Miguel Porrúa
Data and Digital Government
Cluster Coordinator,
Innovation to Serve the Citizen (ICS),
Institutions for Development (IFD)

Luis Tejerina
Lead Specialist
Social Protection and Health (SPH),
Social Sector (SCL)

[a] https://www.securelink.com/blog/healthcare-data-new-prize-hackers/
[b] https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY21Q1HealthcareBreachReport2021.pdf

Executive Summary



The healthcare sector was among those most targeted by hackers in 2019.[1] It is also the industry that has suffered the most damaging attacks in recent years. The average cost per cyberattack in the healthcare sector in terms of lost business, prevention, detection, and recovery expenses is $7.13 million,[2] while the average cost of cyberattacks in all other industries is $3.86 million. In Brazil, for instance, the average cost of a cyberattack rose 10.5 percent from 2019 to 2020. Protected Health Information (PHI) fetches the highest price of all types of data on the black market, with values tens of times higher than other data like credit card numbers.[3]

Furthermore, **80 percent of the information compromised by these cyberattacks is personal data**, and the healthcare sector takes longer than any other sector to detect a possible information breach: worldwide, an average of 329 days elapses from a successful attack until the institution realizes its data has been breached. Our region has one of the longest attack detection times in the world.

For these reasons, healthcare organizations must be equipped with tools to face this reality and to enhance their information security by implementing frameworks, controls, and guidelines. Working frameworks provide a context that allows organizations to perform different types of information security or cybersecurity activities in a systematized and controlled manner, as well as to define and put in place technical and managerial security controls or measures, supported by guidelines that define practical tools and address specific problems. In line with this reality, different governments and international organizations have created regulatory frameworks like the European Community's General Data Protection Regulation (GDPR) and the United States' Health Insurance Portability and Accountability Act (HIPAA). Both frameworks regulate how personal data is handled and protected by the different stakeholders involved, according to the context. The HIPAA in particular focuses on personal health data.

This paper compiles and classifies the current global knowledge on norms, frameworks, standards, best practice, and cybersecurity implementation guidelines in order to orient readers on how to use them. It also proposes a seven-step strategy for implementing or enhancing cybersecurity at healthcare organizations.

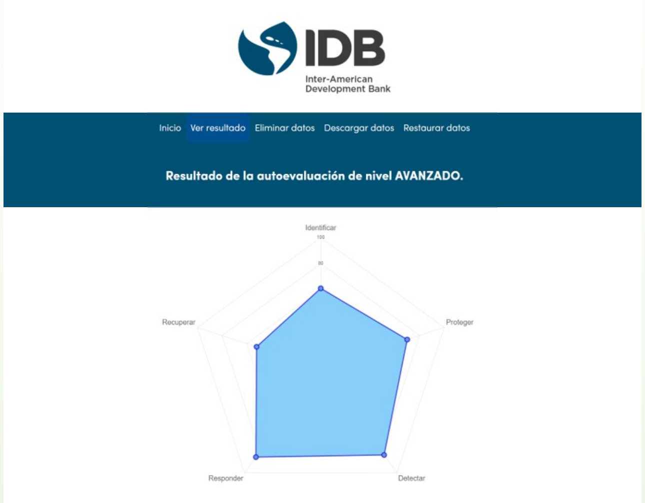
[1] Verizon, 2020.
[2] IBM, 2020.
[3] Neveux, Ellen, 2021.

THE SEVEN STEPS FOR IMPLEMENTING CYBERSECURITY ARE:

1. Make cybersecurity a priority for the organization’s strategic management.
2. Define the organization’s cybersecurity structure.
3. Set cybersecurity objectives and goals.
4. Assess the organization’s current state using a GAP analysis.
5. Develop a cybersecurity master plan.
6. Implement the master plan.
7. Evaluate the results and remaining risk.

The self-assessment tool developed by the IDB (described in detail in this paper’s annexes) should be used to assess an organization’s current state through a GAP analysis, as indicated in step 4. This self-assessment tool includes a set of multiple choice questions to assess how well an organization aligns with industry best practice based on the NIST cybersecurity framework.[4] **This tool helps identify gaps and provides recommendations as the basis of a master plan.**

A cybersecurity master plan is a management tool that is implemented to meet cybersecurity objectives and goals. It is simply a program with a fixed duration, scope, and budget that groups all cybersecurity projects that need to be carried out to meet a set of goals and objectives and reduce the existing gap.



Resultado de la autoevaluación de nivel AVANZADO.

Visit the tool: www.iadb.org/cybereval

[4] National Institute of Technical Standards (NIST), 2018 (a).

Introduction

Although cybersecurity has been taking shape for several decades, it still is not commonly implemented in the healthcare sector. Numerous papers have been published online and in academic media on related topics like frameworks, definitions of controls, guidelines, and best practice. Best practice in this field is wide and varied. This poses a major challenge for organizations assessing which path to take. They need an overview of the topic and a straightforward understanding of the aspects and considerations relevant to their choice.

The health emergency forced the healthcare industry to adopt information and communication technologies at a faster pace. The quality of the healthcare services offered to citizens in many countries of Latin America and the Caribbean (LAC) has improved, and strides have been made in digital health services through teleconsultation or telemedicine and in giving citizens access to electronic medical records, among other areas.

With the increased use of ICTs in LAC, especially in the healthcare industry, the sector faces growing risks of cybersecurity incidents. The healthcare sector was among the most targeted by hackers in 2019,[5] and it is also the industry that has suffered the most damaging attacks in recent years. Furthermore, the data the sector processes is confidential and highly sensitive, so the so the non-monetary impact of these attacks can also be extremely serious. Cybersecurity incidents are on the rise: the Healthcare Information and Management System Society (HIMSS)[6] survey found that 75.7 percent of the North American organizations surveyed in 2018 reported at least one significant cybersecurity incident in the previous 12 months; only 21.2 percent reported no significant security incidents in the past 12 months; and 3.2 percent stated that they did not know.

Cyberattacks are also trending upward in Latin America and the Caribbean. The average cost of a cyberattack in Brazil rose by 10.5 percent from 2019 to 2020.[7] 80 percent of the information compromised is personal data, and the healthcare sector takes the longest to detect an information breach—worldwide, an average of 329 days from a successful attack until the institution realizes its data has been breached. In fact, our region has one of the longest attack detection times in the world. In recent years there have been multiple incidents in the region, including exposures of sensitive data in Mexico,[8] Chile,[9] and Argentina.[10]

To understand how important and urgent it is to act on this issue in the healthcare sector, we analyze the 2017 WannaCry incident in the United Kingdom.[11] This incident disrupted services at third of hospitals and around 8 percent of

[5] See Verizon, 2020.
[6] See Healthcare Information and Management System Society, HIMSS North America, 2018.
[7] See IBM, 2020.
[8] See DataBreaches.net. The Office of Inadequate Security, 2018.
[9] See Carvajal, Víctor and Jara, Matías, 2016.
[10] See Clarín Tecnología, 2018.
[11] Ver UK Department of Health & Social Care, 2018.

general practice clinics in the UK, resulting in around 19,000 cancelled appointments. While it is difficult to estimate information technology costs, this incident is estimated to have cost £19 million (US$ 26 million) in cancelled appointments, and £73 million (US$100 million) had to be spent on support or consultants to restore affected data and systems in the months following the attack.

Additionally, the sector has begun to use much more new technology, especially the Internet of medical things (IoMT). This poses new challenges for the sector and new risks that could impact patient safety. IoMT's current low penetration rate in LAC is expected to change in the next few years, so the sector must be prepared to face new challenges.

Given the growing computerization of ICTs in LAC's healthcare sector and the risks this computerization entails, this paper aims to serve as a practical guide to help relevant stakeholders define their information security strategy based on the legislation in force, industry best practice, and applicable standards.

This paper also addresses low cybersecurity implementation and provides a guide to with seven specific and strategic steps to support cybersecurity implementation at healthcare institutions.

Additionally, **it compiles and classifies the existing global knowledge on norms, frameworks, standards, best practice, and implementation guidelines** to orient the reader on how to implement the proposed seven-step strategy. Step 4 of this strategy involves performing a GAP analysis to assess the current situation using the self-assessment tool for the healthcare sector detailed in the annexes to this paper.

This document **is intended for people with cybersecurity responsibilities or for information technology authorities in the healthcare sector**. It aims to demystify cybersecurity so it is no longer considered the exclusive domain of the IT sector, and it confirms the relevance of the commitment and responsibility of all healthcare staff.

Those seeking a strategic overview of the topic should at least read the sections "***Seven Steps for Implementing Cybersecurity***" and "***Recommendations and Final Thoughts***" Those who want more technical details should read the whole document.

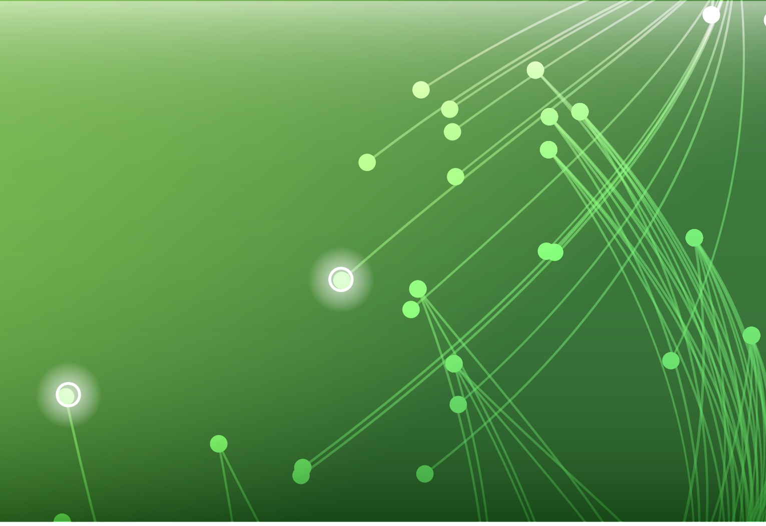
WANNACRY

WannaCry is a ransomware for Microsoft Windows that appeared in May 2017 and affected around 230,000 computers in more than 150 countries. It impacted critical healthcare services, telephone service providers, banks, transportation systems, universities, private companies, and others. The attack encrypted victims' files, held them, and demanded payment of a ransom in Bitcoin on the promise of releasing them. It exploited known vulnerabilities in Microsoft Windows (EternalBlue and DoublePulsar), which had released a patch to address the issue almost two months earlier, meaning the incident could have been avoided if the operating systems had been updated with the patch. It had a KillSwitch that queried a website and stopped propagation if the website was available. For this reason, the usual practices for containing an incident (isolating the affected computers and networks) had a negative effect and increased spread.
It is never recommended to give in to this type of extortion and make a payment to the cybercriminals. In this particular case, it is uncertain whether it would have been possible to recover the data even by paying, due to a flaw in the malware itself. WannaCry was the starting point for other types of ransomware and strategies used by cybercriminals.

REFERENCES:

- latam.kaspersky.com/resource-center/threats/ransomware-wannacry
- assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf
- www.welivesecurity.com/la-es/2017/05/12/wannacry-ransomware-nivel-global/
- www.bbc.com/mundo/noticias-39929920
- blog.segu-info.com.ar/2017/05/wannacrypt-al-menos-15-paises-afectados.html
- www.welivesecurity.com/la-es/2021/05/12/wannacry-como-evoluciono-escena-ransomware/

What is cybersecurity?



Company information and the systems that store and process it are among organizations' key assets. The healthcare sector in particular uses very sensitive personal information that is highly coveted by cybercriminals due to its high value on the black market.[12] The issue of cybersecurity should thus involve the entire organization, from the board of directors to entry-level employees.

Cybersecurity, or IT security, implements measures to protect IT assets like systems, networks, computers, or digital documents from possible attacks that affect their completeness, confidentiality, and/or availability. These attacks can impact continuity of care for healthcare system users or the image of organizations.

Cyber-attacks can be quite varied and dynamic, generating new strategies or honing existing ones, so it is essential to have the people, technology, and processes needed to effectively mitigate or eliminate an attack. If any of these three elements is overlooked, it might not be possible to quickly respond to an incident or cyber-attack.

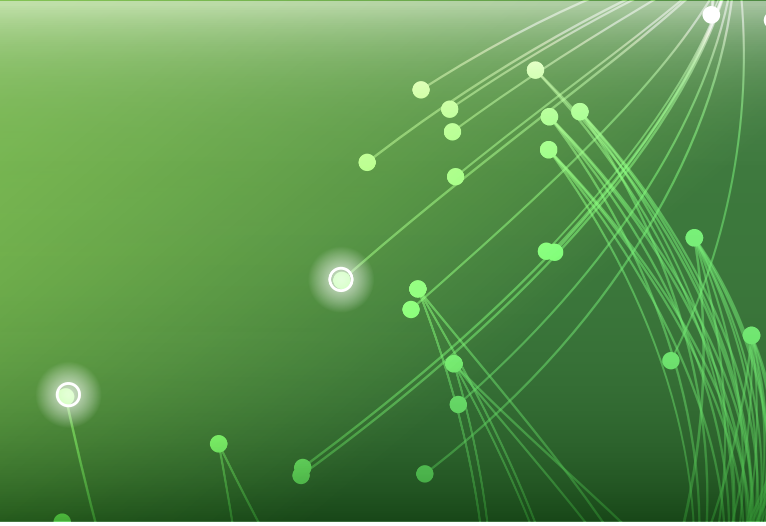
Organizations tend to invest in isolated protection technologies, like antivirus software or firewalls, on the understanding that these types of tools enhance security levels. Although these technologies improve the situation, they usually fall short of their objective. To better understand this point, consider the example of antivirus software: at the IT team manager's request, an organization acquires a corporate antivirus solution to protect its devices like PCs, laptops, or cell phones. **This measure in itself does not guarantee that devices are protected**. It simply means the company has the tool, but if the institution lacks people to configure and deploy it, the initiative will be insufficient and some devices may remain unprotected, making them vulnerable points of entry to the organization. Furthermore, if the technical team does not have processes and procedures for updating and maintaining the solution days or weeks after installation, they will not be able to detect new signatures or viruses, leaving the devices unprotected.

Therefore, **cybersecurity needs to have a strong and consistent strategy, involve the whole organization, and be managed in a structured way**. This paper examines a number of internationally proven techniques that will help leaders in the field meet these conditions.

The reality and context of organizations and their services have changed over the years. During the current health emergency, healthcare institutions must offer readily available and accessible services to a large number of stakeholders. This situation exposes organizations and opens a large number of gaps to potential attackers, jeopardizing assets and people's security.

[12] Neveux, Ellen, 2021.

The state of the art



In recent decades, work has been done globally on the issue of information security and cybersecurity. Although this work involves a strong technical component, it has been accompanied by international and national regulations and standards governing the matter.

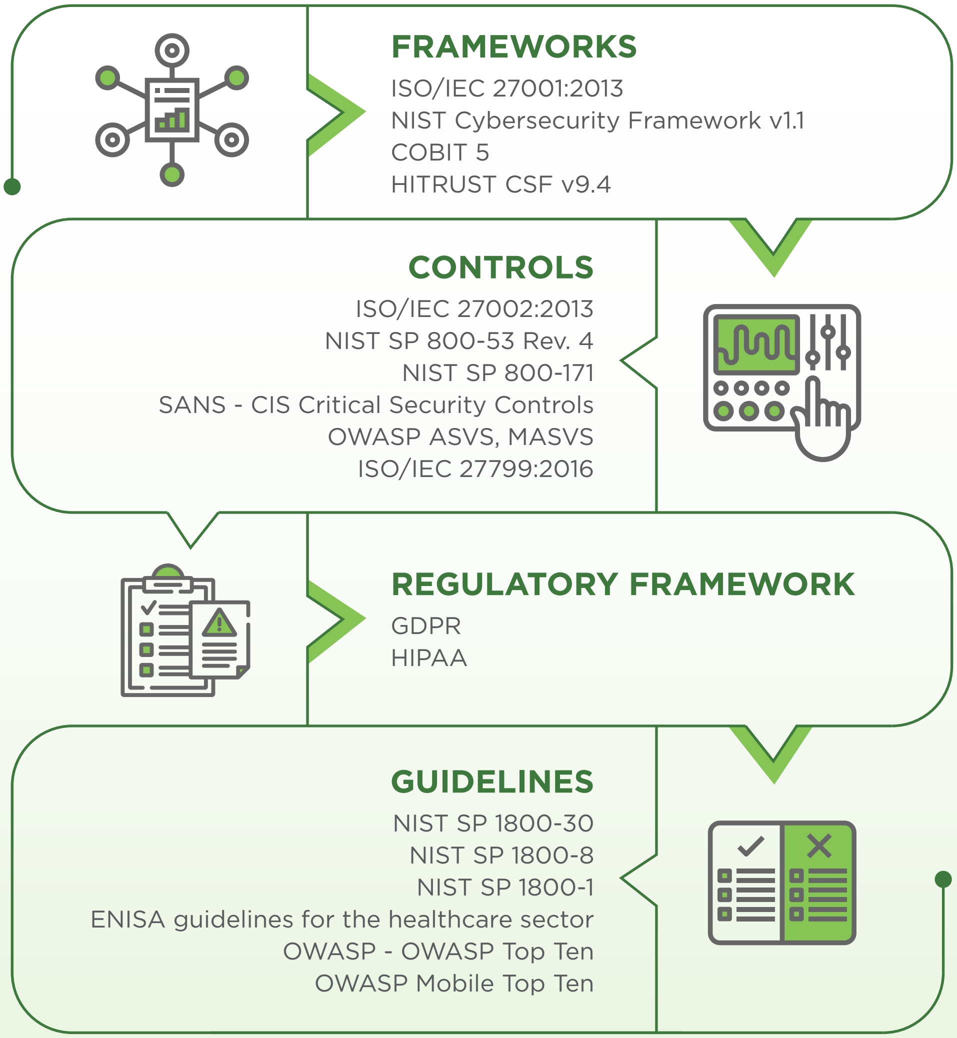
Different types of common and proven tools are available to the various players in the ecosystem, which include regulators, operators, and service providers. These tools can be sorted into four groups: frameworks, controls, guidelines, and regulatory frameworks. Using these tools in conjunction with each other makes the whole system consistent, from regulation, implementation, execution, to control and monitoring.

Frameworks give organizations **tools to implement different information security activities in a systematized and controlled way**. These frameworks use different approaches, but they generally provide mechanisms to define organizations' security objectives and maturity profiles or levels. They apply a risk analysis that defines the controls to be implemented and allows organizations to make technical, managerial, or resource decisions to achieve these objectives.

Controls are technical or management security measures **intended to achieve specific information security objectives**. For example, NIST SP 800-53 (a publication from NIST defining control standards) defines activities to ensure organizations use account management as an access control measure.

Lastly, guidelines are practical tools that address specific issues. For instance, NIST SP 1800-8 details how to manage assets, protect against threats, and mitigate vulnerabilities in wireless infusion pumps. They also offer useful concepts related to the IoMT.

FIGURE 1 • Summarizes the main frameworks, controls, guidelines, and applicable regulations



FRAMEWORKS

ISO/IEC 27001:2013
NIST Cybersecurity Framework v1.1
COBIT 5
HITRUST CSF v9.4

CONTROLS

ISO/IEC 27002:2013
NIST SP 800-53 Rev. 4
NIST SP 800-171
SANS - CIS Critical Security Controls
OWASP ASVS, MASVS
ISO/IEC 27799:2016

REGULATORY FRAMEWORK

GDPR
HIPAA

GUIDELINES

NIST SP 1800-30
NIST SP 1800-8
NIST SP 1800-1
ENISA guidelines for the healthcare sector
OWASP - OWASP Top Ten
OWASP Mobile Top Ten

Given the wide variety of methods, standards, and best practices available, one of the main challenges is to choose which standards, frameworks, controls, and guidelines to adopt.

>> Framework

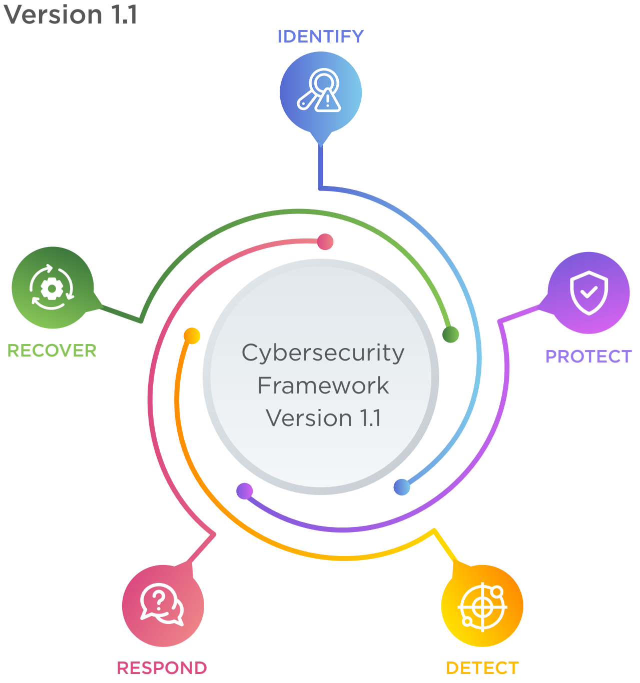
This paper focuses on the four most widely adopted frameworks worldwide.[13] Three are for organizations in general and one is specifically designed for the healthcare industry.

- **NIST-CSF[14]**

  The National Institute of Standards and Technology (NIST) has defined a framework of measures and controls for organizations that provide critical services in the United States. The aim of the framework is to identify, assess, and manage cybersecurity risks.

  To this end, the framework defines five functions: identification, detection, protection, response, and recovery, which provide a comprehensive approach to cybersecurity risk management. It also draws comparisons with industry standards and best practice.

FIGURE 2 • Cybersecurtiy Framework Version 1.1



Source: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

The framework has different levels of implementation, which range from Level 1 (Partial), Level 2 (Risk Informed), Level 3 (Repeatable) and Level 4 (Adaptive). which reflect the management of its cybersecurity risks based on the organization's risk management policies.

Finally, the framework defines profiles for both the organization's current state (Current Profile) and its target state, as well as specifying the organization's goal, in line with the accepted risks.

- **HITRUST CSF[15]**

  HITRUST is an alliance created in 2007 between global corporations such as Google, AT&T, Amazon, and others. HITRUST CSF is a privacy and security framework for healthcare organizations. Its approach is based on information security risk management, and it provides a clear overview of compliance with applicable regulations through mapping, though most of the mapped standards are not applicable in LAC. The HITRUST CSF CORE is based on ISO/IEC 27001 and 27002. It defines controls and groups them into categories, leveraging the main categories of the 27000 family. It also adds specific categories to assess an information security risk management (ISRM) program.

  HITRUST CSF allows organizations to be certified by an external agent to validate the implementation and execution of their information security management system.

- **ISO/IEC 27001[16]**

  The ISO 27000 family, created by the International Organization for Standardization, is a global standard for information security that specifies the requirements for implementing, maintaining, and improving an information security risk management system. The latest version available at the

[13] Ver Healthcare Information and Management System Society, HIMSS North America, 2018.
[14] National Institute of Technical Standards (NIST), 2018 (a).
[15] HITRUST, 2019.
[16] International Standards Organization (ISO), 2013 (a).

time of writing this paper is the 2013 version, amended in 2015, which details 130 requirements.

This family of standards allows organizations to be certified by an external agent to validate the implementation and execution of their information security management systems.

- **COBIT[17]**

LThe Information Systems Audit and Control Association (ISACA) is a non-profit organization with a membership of over 450,000 professionals from more than 188 countries, who play a wide variety of roles in the field of information technology. One of its main products is COBIT (Control Objectives for Information and related Technology). COBIT 5, issued in 2012, and COBIT 2019, issued in 2018, are currently in force.

COBIT is a framework for ensuring effective IT governance. Although this framework is not specific to information security, the 2019 version is aligned with different information security frameworks, controls, and guidelines, particularly the ISO/IEC 27000 family, NIST Cybersecurity Framework v1.1, and version 9 of the HITRUST® Common Security Framework, dated September 2017.

[17] Information System Audit and Control Association (ISACA), 2019.

>> Controls

This paper focuses on the six most widely adopted groups of controls at a global level, of which five are intended for organizations in general and one has been specifically designed for the healthcare sector.

- ISO/IEC

  These standards provide specific guidance to organizations that want to implement an information security management system.

  Organizations should select these controls based on their level of risk acceptance and applicable regulations.

- ISO/IEC 27002[18]

  This standard was first published in 2005. It was updated several times until 2013, and it was amended in 2015. Countries decide if they adapt to the update or not. It aims to provide best practice guidelines for improving an organization's information security management system in the main security categories (35) and specific controls (114), which are grouped into 14 control clauses, as shown in Table 1.

  Each clause contains one or more control categories and sets out the objective and controls needed to achieve each category, guidelines for implementing those controls, and other relevant information.

TABLE 1 • Control clauses of ISO / IEC 27002

Information Security Policy	Operational Security
Information Security Organization	Communications security
Security related to human resources	System procurement, development and maintenance
Asset management	Relations with suppliers
Access control	Information security incident management
Cryptography	Information security aspects of business continuity management
Physical and environmental security	Compliance

[18] International Standards Organization (ISO), 2013 (b).

- ISO/IEC 27799[19]

  This standard was published in 2008 and updated in 2016. Unlike the other standards, which are generic, ISO/IEC 27799 provides specific guidance on implementing 14 control clauses in ISO/IEC 27002 (shown in Table1) at organizations in the healthcare sector or with custody of patient data.

  Personal data is important, and its confidentiality, integrity, and availability must be safeguarded, but patient data, in particular, must have additional safeguards, since it could jeopardize people's physical safety if compromised. For this reason, most countries classify this type of data as sensitive information that must comply with specific regulatory standards. Also relevant is this information's ready availability, which is essential for efficient medical care and during disasters or emergencies. This standard thus applies greater restrictions to the controls and provides more precise information on the best way to use them.

  ISO/IEC 27799 includes 3 annexes. The first addresses threats to health information security. The second contains a practical action plan for using the standard to implement ISO/IEC 27002 at healthcare organizations. The third annex is a checklist organizations can use to assess their own compliance, in support of achieving the compliance clause.

  To more clearly illustrate how ISO/IEC 27799 builds on ISO/IEC 27002, consider the following example. In the **Asset Responsibility** category of the **Asset Management** clause, both standards have the identical objective of **identifying the organization's assets and defining suitable protection responsibilities**. One of the associated controls is the **Asset Inventory**, which, under ISO/IEC 27799, must comply with the controls defined in ISO/IEC 27002:2013 8.1.1, but it also includes the following controls:

  - Accounting for health information assets.

  - Designating a custodian for those health information assets.

  - Having rules for acceptable use of these assets that are identified, documented, and implemented.

- NIST

  NIST issues and updates special publications defining the catalogue of security and privacy controls to be performed by all U.S. federal and non-governmental organizations in their management of information security risks.

  There are two publications connected to the cybersecurity framework (NIST-CSF) mentioned earlier in this document: NIST SP 800-53 and NIST 800-171. They target companies and public institutions with a variety of characteristics and broadly share the main families of controls, but at different levels of depth.

[19] International Standards Organization (ISO), 2016.

- **NIST SP 800-53**[20]

  This publication was last updated in September 2020, resulting in the 5th revision of the document. It details the measures to be implemented by different types of federal systems and organizations to safeguard assets and people's privacy.

  The document is divided into three sections. The first introduces the subject matter, the second describes the fundamental concepts of the security and privacy controls, and the last delves into the catalog of controls. Table 2 lists its 20 families of controls.

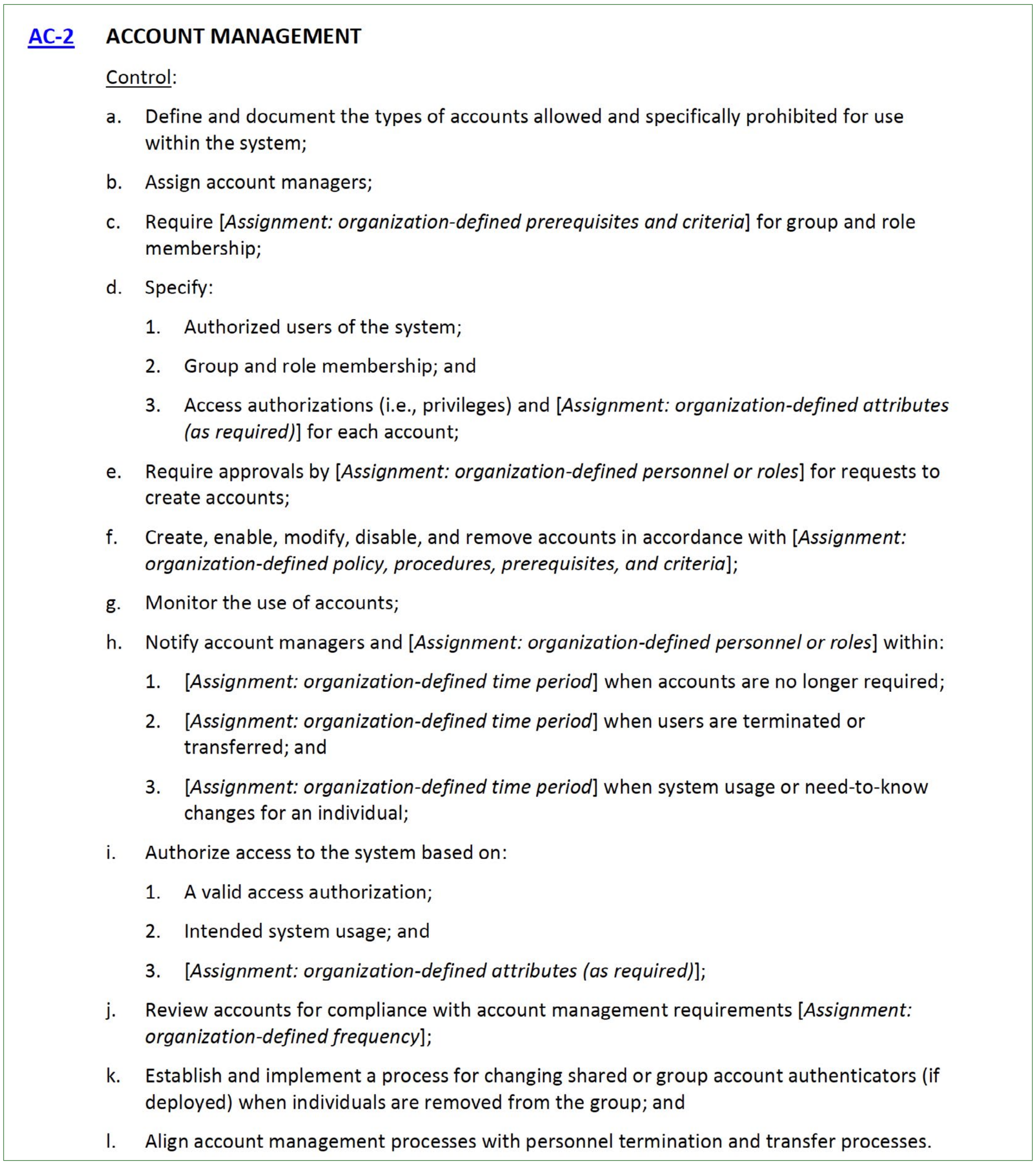
  Each control family is identified with a two-letter code; for example, access control is AC. Specific controls are listed within each family; for instance, AC-2 is account management. The publication provides an ordered list (a, b, c, etc.) of activities or tasks for each control. Figure 2 shows an example.

TABLA 2 • NIST SP 800-53 Control Families

Access control	Physical and environmental security
Training and awareness	Planning
Audit	Program management
Evaluation, authorization and follow-up	Personnel security
Configuration management	Processing and transparency of personally identifiable information (PII)
Contingency plan	Risk assessment
Identification and authentication	Procurement of systems and services
Incident response	Systems and communications protection
Maintenance	Systems and information integrity
Media protection	Supply chain risk management

[20] National Institute of Technical Standards (NIST), 2020 (b).

FIGURE 3 • User account management



AC-2 **ACCOUNT MANAGEMENT**

Control:

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require [*Assignment: organization-defined prerequisites and criteria*] for group and role membership;

d. Specify:

   1. Authorized users of the system;
   2. Group and role membership; and
   3. Access authorizations (i.e., privileges) and [*Assignment: organization-defined attributes (as required)*] for each account;

e. Require approvals by [*Assignment: organization-defined personnel or roles*] for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with [*Assignment: organization-defined policy, procedures, prerequisites, and criteria*];

g. Monitor the use of accounts;

h. Notify account managers and [*Assignment: organization-defined personnel or roles*] within:

   1. [*Assignment: organization-defined time period*] when accounts are no longer required;
   2. [*Assignment: organization-defined time period*] when users are terminated or transferred; and
   3. [*Assignment: organization-defined time period*] when system usage or need-to-know changes for an individual;

i. Authorize access to the system based on:

   1. A valid access authorization;
   2. Intended system usage; and
   3. [*Assignment: organization-defined attributes (as required)*];

j. Review accounts for compliance with account management requirements [*Assignment: organization-defined frequency*];

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

Each control is divided into different sections, such as:

- An explanation of the control (discussion).
- Related controls.
- A section on control enhancements.

- **NIST SP 800-171**[21]

This publication was released in February 2020 as revision document number 2, which was then updated in January 2021. It details measures for safeguarding Controlled Unclassified Information (CUI) in different types of non-federal systems and organizations. In the case of healthcare, all clinical documents fall under this classification.

[21] National Institute of Technical Standards (NIST), 2020 (c).

The document has three chapters. The first introduces the subject matter, the second describes the fundamental concepts of the 14 families of security and privacy controls, and the last delves into the catalog of controls. Table 3 details the 14 families of proposed controls.

For each control family, the document defines sub-controls, which are grouped according to basic requirements under FIPS Publication 200 and a second set of derived requirements under NIST 800-53. For example, in the access control family (Figure 3), limiting system access to authorized users is a basic requirement, while applying the principle of least privilege in activities performed on that system or application based on the organization's responsibility to ensure its business activity is considered a derived requirement.

Among the main differences between the NIST SP 800-53 and NIST SP 800-171 publications is their level of depth in addressing certain topics of utmost importance to organizations. More specifically, NIST SP 800-171 does not define families of controls for contingency planning, personal data management (PII), or supply chain risk management, among others.

NIST SP 800-171 has several annexes. Annex D, shown in Figure 4, maps each control using NIST 800-53 and ISO/IEC 27001.

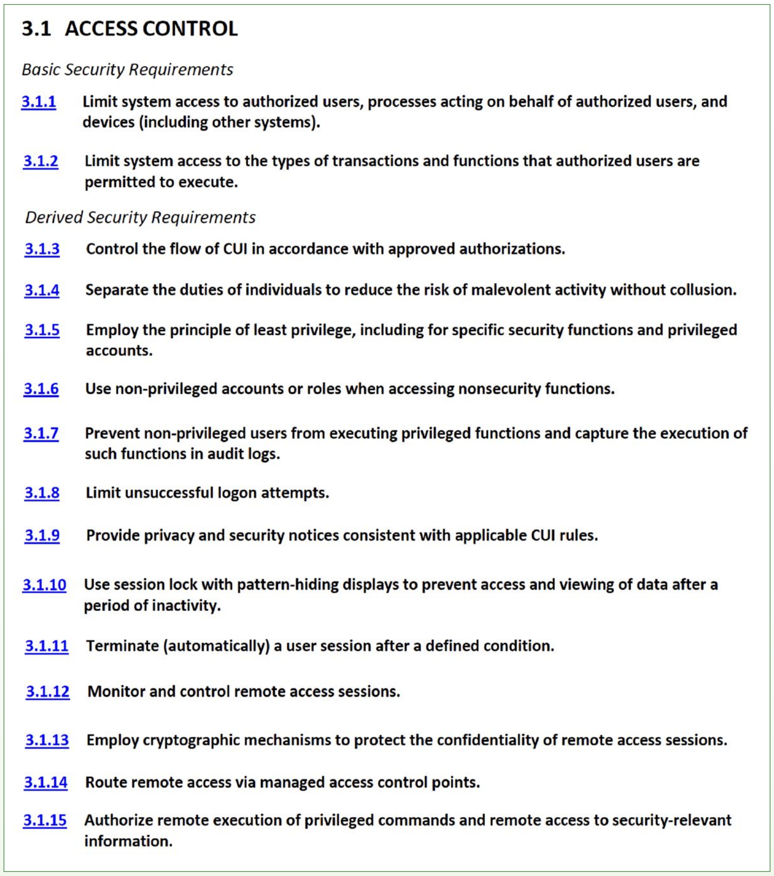
Annex E specifies which NIST SP 800-53 controls must be implemented to meet the basic requirements of NIST SP 800-171.

TABLE 3 • NIST SP 800-171 Control Families

Access control	Media protection
Training and awareness	Personnel security
Audit	Physical protection
Configuration management	Risk assessment
Identification and authentication	Security assessment
Incident response	Systems and communications protection
Maintenance	Systems and information integrity

[22] National Institute of Technical Standards (NIST), 2006.

FIGURE 4 • Access control



3.1 ACCESS CONTROL

Basic Security Requirements

3.1.1 **Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).**

3.1.2 **Limit system access to the types of transactions and functions that authorized users are permitted to execute.**

Derived Security Requirements

3.1.3 **Control the flow of CUI in accordance with approved authorizations.**

3.1.4 **Separate the duties of individuals to reduce the risk of malevolent activity without collusion.**

3.1.5 **Employ the principle of least privilege, including for specific security functions and privileged accounts.**

3.1.6 **Use non-privileged accounts or roles when accessing nonsecurity functions.**

3.1.7 **Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.**

3.1.8 **Limit unsuccessful logon attempts.**

3.1.9 **Provide privacy and security notices consistent with applicable CUI rules.**

3.1.10 **Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.**

3.1.11 **Terminate (automatically) a user session after a defined condition.**

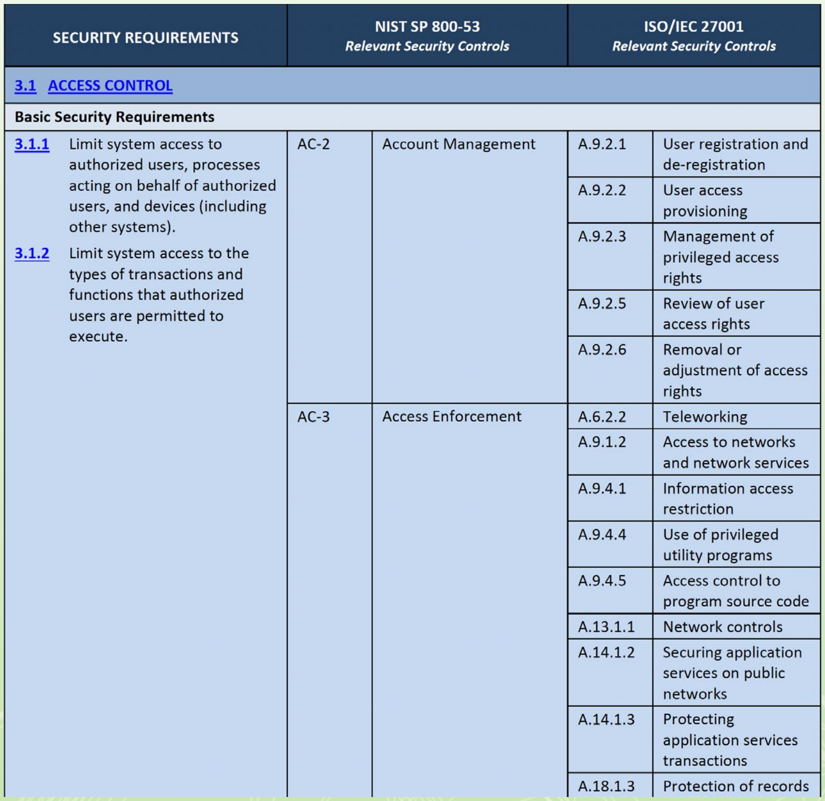
3.1.12 **Monitor and control remote access sessions.**

3.1.13 **Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.**

3.1.14 **Route remote access via managed access control points.**

3.1.15 **Authorize remote execution of privileged commands and remote access to security-relevant information.**

FIGURE 5 • Controls mapping - NIST 800-53 and ISO / IEC 27001



SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1 ACCESS CONTROL				
Basic Security Requirements				
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). 3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2	Account Management	A.9.2.1	User registration and de-registration
			A.9.2.2	User access provisioning
			A.9.2.3	Management of privileged access rights
			A.9.2.5	Review of user access rights
			A.9.2.6	Removal or adjustment of access rights
	AC-3	Access Enforcement	A.6.2.2	Teleworking
			A.9.1.2	Access to networks and network services
			A.9.4.1	Information access restriction
			A.9.4.4	Use of privileged utility programs
			A.9.4.5	Access control to program source code
			A.13.1.1	Network controls
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
			A.18.1.3	Protection of records

- **SANS CIS Critical Security Controls**[23]

  The Center for Internet Security (CIS) is an independent organization made up of IT experts from different business areas. Its goal is to internationally promote best practice in cybersecurity.

  CIS Critical Security Controls version 7.1 defines a set of 20 controls, including best practice and defenses to mitigate the most frequent attacks on systems and networks. These controls are categorized into three implementation groups based on the sensitivity of the assets to be protected, the size and maturity of the organization, and other factors.

  The first part of each control explains its importance and implications. The publication then describes a set of sub-controls, detailing the best practice associated with that specific control and the implementation group it should be included in. Finally, the document includes a section for each case with a diagram showing how system entities, procedures, and tools interact to help implement the different activities.

  Table 4 shows how controls and sub-controls are presented in CIS version 7.1.

  For example, the control "Inventory and Control of Enterprise Assets" has eight sub-controls: five for the Identify function, one for Respond, and two for Protect. Sub-control 1.1 requires use of an active discovery tool, provides a detailed description of the sub-control, and indicates that it should be included in implementation groups 2 and 3. An active discovery tool uses scans or similar techniques to proactively identify equipment connected to the organization's network and update the inventory of assets.

TABLA 4 • CIS Control 1: Inventario y control de activos *hardware*

CIS Control 1: Inventory and control of hardware assets.							
Sub-control	Type of Asset	Security Function	Control	Description	Implementation groups		
1.1	Equipment	Identification	Using an active discovery tool	Use an active discovery tool to identify computers connected to the organization's network and update the hardware asset inventory.		●	●
1.2	Equipment	Identification	Using a Passive Discovery tool of assets	Use a passive discovery tool to identify devices connected to the organization's network and automatically update the asset inventory.			●

[23] Center for Internet Security (CIS), 2019.

- **OWASP ASVS**[24] and **MASVS**[25]

  The Open Web Application Security Project (OWASP) is a non-profit foundation working to improve web application security. It has hundreds of local chapters around the world and tens of thousands of members. OWASP generates multiple open source projects, including the Application Security Verification Standard (ASVS) and the Mobile Application Security Verification Standard (MASVS). These projects for web or mobile device applications, respectively, provide a basis for testing technical security controls as well as a list of secure development requirements.

They can potentially be used:

- As metrics, using the controls and tests on the controls as evaluation criteria.
- As guidelines, using the controls as a guide for secure development.
- In procurement, using the controls as requirements to evaluate software or including them in the contracts.

[24] Open Web Aplication Security Project (OWASP), 2020 (a).
[25] Open Web Aplication Security Project (OWASP), 2020 (b).

>> Guidelines

The following section contains a table with the main security guidelines applicable to the healthcare sector. This table is not exhaustive and is intended to be a starting point for experts wishing to delve deeper into the subject.

TABLE 5 • Main guidelines

Name of the guide	Description
NIST SP 1800-30[26]	Practical guide for a telemedicine and remote patient monitoring (RPM) solution.
NIST SP 1800-24[27]	Guidance on how to protect the imaging ecosystem, focusing on picture archiving and communication systems (PACS) in healthcare delivery organizations (HDOs).
NIST SP 1800-8[28]	Detailed guidelines on how to manage assets, protect against threats, and mitigate vulnerabilities in wireless infusion pumps. This publication uses a risk assessment approach and looks at currently available cybersecurity standards and HIPAA. It is based on principles such as defense in depth. While it initially appears to be focused on wireless infusion pumps, its concepts can be applied to areas of the IoMT.
NIST SP 1800-1[29]	Guidelines for protecting medical records on mobile devices. This publication shows how to use commercially available or open source tools and technologies that meet cybersecurity standards to help organizations using mobile devices share electronic medical records more securely.
ENISA - Procurement Guidelines for Cybersecurity in Hospitals[30]	Guidelines to improve the procurement cycle and help hospitals meets cybersecurity objectives.
ENISA - Security and Resilience in eHealth Infrastructures and Services[31]	This document describes the state of the art and studies the approach and means used to protect critical health systems in each member country.
ENISA - Cyber security and resilience for Smart Hospitals[32]	This publication presents research and makes recommendations on smart hospitals and relevant issues. It defines assets and classifies threats to them, presenting attack scenarios and analyzing their effects, recovery, and best practice.
ENISA - ICT security certification opportunities in the healthcare sector[33]	European Union Agency for Cybersecurity (ENISA), 2019. This publication explores guidelines and regulations in healthcare information technology and IoMT.
OWASP Top Ten[34]	OWASP ranking of the 10 most critical security concerns for web application security.
OWASP Mobile Top Ten[35]	OWASP ranking of the 10 most critical security concerns for mobile application security.

[26] National Institute of Technical Standards (NIST), 2021.
[27] National Institute of Technical Standards (NIST), 2020 (a).
[28] National Institute of Technical Standards (NIST), 2018 (c).
[29] National Institute of Technical Standards (NIST), 2018 (b).
[30] European Union Agency for Cybersecurity (ENISA), 2020.
[31] European Union Agency for Cybersecurity (ENISA), 2015.
[32] European Union Agency for Cybersecurity (ENISA), 2016.
[33] European Union Agency for Cybersecurity (ENISA), 2019.
[34] Open Web Aplication Security Project (OWASP), 2017.
[35] Open Web Aplication Security Project (OWASP), 2016.

>> Regulatory framework

There are optional or mandatory regulations that govern behavior and define how organizations should act. For information security or cybersecurity in the healthcare sector in particular, the applicable regulations depend on the country and even the city or state in which the organization is located.

Nevertheless, two regulatory frameworks have gained prominence at the global level and have inspired many countries in recent years. Both regulate the use of personal data, define how data must be processed, and specify responsibilities in the event of an information breach and fines for non-compliance, among other points. These frameworks are the European Union's General Data Protection Regulation (GDPR)[36] and the United States' Health Insurance Portability and Accountability Act (HIPAA).[37]

The European GDPR covers the processing of natural persons' data by organizations such as companies or corporations that:

- are established in the European Union (EU), regardless of whether or not the data is processed there;
- offer goods or services to individuals based in the EU.

This regulation emphasizes that organizations must accurately analyze and assess the risks of data processed throughout its entire life cycle, from when it is captured to when it is erased.

Under the GDPR, organizations are responsible instituting technical and organizational measures to guarantee people's rights and freedoms in relation to their data. Among several definitions, it states that individuals must be kept informed about the use of their data to obtain their consent and notify them of any possible breach of their data security.

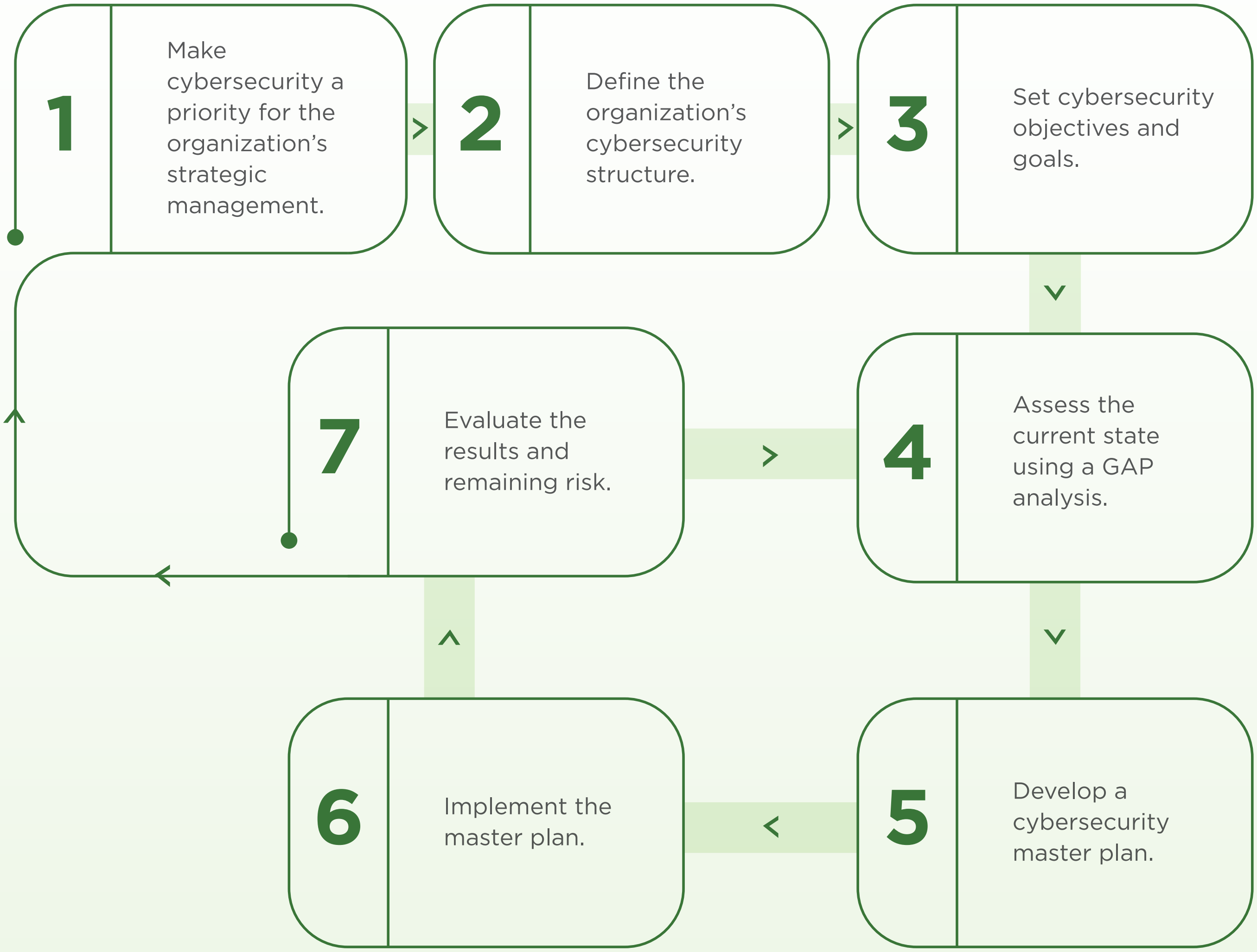
Data processing in the healthcare sector is considered high risk, so organizations must take specific steps like keeping records of processing activity or defining specific roles like data protection officer (DPO). Some general activities must be ongoing, like policy definition, training and awareness plans for organizations, and others.

This document provides an introduction to the topic rather than a complete analysis of the applicable regulations. Although the regulations described are not applicable in LAC, an overview of them is important because they have served as a guide for laws in countries in the region and it is desirable for organizations in countries that do not have them, to use them as a reference. For a more in-depth analysis, the dashboard (https://socialdigital.iadb.org/en/sph/dashboard) developed by the IDB contains information on the national regulatory frameworks for implementing electronic health records (EHR) in 26 countries in the region.

[36] This regulation can be found in European Union, 2016, and information on personal data protection rules in and outside the EU can be found in European Commission (n.d.).
[37] Information regarding the "Health Insurance Portability and Accountability Act" can be found on the HHS website: https://www.hhs.gov/hipaa/index.html.

A seven-step approach to implementing cybersecurity

FIGURE 6 • 7 steps to implementing cybersecurity



1 Make cybersecurity a priority for the organization's strategic management.

2 Define the organization's cybersecurity structure.

3 Set cybersecurity objectives and goals.

4 Assess the current state using a GAP analysis.

5 Develop a cybersecurity master plan.

6 Implement the master plan.

7 Evaluate the results and remaining risk.

After gaining familiarity with the different tools available for cybersecurity in the sector, the next order of business is the implementation process, which must be systematic, structured, and continuous, since change will not happen overnight.

Although there are different approaches to incorporating information security into an organization, we propose a simple method as a strategic guide for organizations' management teams.

We propose a seven-step continuous improvement cycle, shown in Figure 6.

Below is a brief description of each step and a discussion of its implications and benefits for the organization:

1 MAKE CYBERSECURITY A PRIORITY FOR THE ORGANIZATION'S STRATEGIC MANAGEMENT

The aim of healthcare organizations is to save lives. To achieve this goal, they seek to ensure patient safety, which among many other things involves focusing on proper information security management and cybersecurity. For this reason, organizations' strategic management should include objectives, goals, and milestones that place cybersecurity on organizations' agenda. An example is adding ISO/IEC 27001 certification to an organization's aims and critical processes.

2 DEFINE THE ORGANIZATION'S CYBERSECURITY STRUCTURE

To meet the objectives, goals and milestones established in step 1 and to promote information security management, it is important to have a suitable organizational structure. This structure should include an information security manager for the organization and an information security committee, at minimum.

The information security committee's main objectives should be to:

- Set strategic guidelines, together with their corresponding objectives, goals and annual milestones.
- Define general responsibilities.
- Design, approve, and follow up on information security policies.
- Support and follow up on the projects defined in the Master Plan. It is the committee's responsibility to obtain the resources needed for these projects to succeed.
- Speak for the organization and facilitate interactions on information security matters with agents outside the organization.

The entire information security structure should be established by the committee at this stage. An example is incident response management, which can be approached in different ways: through an incident response team; a centralized incident response center; or a decentralized incident response center, among others. For each security function, the structure that best suits the organization needs to be defined, as does the chain of authority, responsibilities, and the composition of the team, with the associated profiles.

3 SET CYBERSECURITY OBJECTIVES AND GOALS

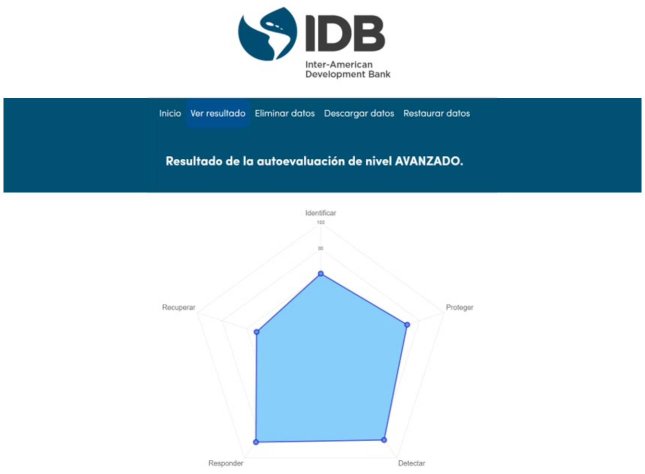
Organizations need to set clear information security and cybersecurity objectives and goals. These objectives and goals should take into account organizational objectives, like compliance requirements, applicable national and international regulations, industry best practice, and organizational risk profile. The organizational risk profile can be defined by several factors, including an organization's size and resources, the sensitivity of the assets it manages, its current maturity level, and the acceptable risk thresholds established. It is also essential to define the metrics and indicators to be used to assess these objectives and goals.

4 ASSESS THE ORGANIZATION'S CURRENT STATE USING A GAP ANALYSIS

Once the information security objectives and goals have been set, the current state of affairs at the organization needs to be identified. This analysis should examine the differences between the current situation and the target situation (usually known as a GAP analysis).

Different tools can be used to perform this analysis for different objectives. If an organization decides to adopt a framework, this framework should be used to perform the GAP analysis, through specialized consultancies or assessment tools (most frameworks have assessment or self-assessment tools).

When an organization decides initially not to adopt a framework, the IDB has developed different tools to facilitate assessment of the current situation. One is a **self-assessment tool for the health sector** (described in detail in the annexes to this paper), based on industry best practice and the NIST cybersecurity framework.[38] This tool uses a simple questionnaire that helps calculate gaps and provides recommendations that can be used to develop the master plan.



Resultado de la autoevaluación de nivel AVANZADO.

Visit the tool: www.iadb.org/cybereval

It is important to include an information security risk analysis in the assessment of the organization's current state to prioritize the gaps detected and the suggested controls, and to evaluate the risk that remains after implementing these controls.

5 DEVELOP A CYBERSECURITY MASTER PLAN

The information security manager should draw up a master plan, with support and advice from the security committee. This plan should include information security objectives, specific goals, and a portfolio of projects and/or services. It should clearly reflect the contribution of each project and/or service to the previously defined goals, and the different milestones on the path to achieving the outcome. It should also contain management indicators for the projects and services for monitoring strategic variables.

To ensure the plan's feasibility, it should include the estimated costs of the projects and/or services, as well as the funding method. Finally, it is recommended that the plan include risk management for the projects and/or services.

[38] National Institute of Technical Standards (NIST), 2018 (a).

6 IMPLEMENT THE MASTER PLAN

At this stage, the aim is to monitor the master plan comprehensively to ensure its success. The information security manager must track the plan's implementation, analyzing the management indicators and associated risks. He or she should also inform the committee of any major deviations to establish corrective measures and the corresponding resources.

7 EVALUATE THE RESULTS AND REMAINING RISK

The outcome of the plan's implementation should be assessed periodically by analyzing its impact on the organization. This evaluation should analyze the organization's current status, taking into consideration the remaining risks. For unfavorable outcomes, the continuous improvement cycle should be relaunched, starting at step 4. Organizations should review their strategic vision at more frequent intervals and in the event of changes in their reality, and they should start the continuous improvement cycle again from step 1.

Recommendations and final considerations

In recent decades, healthcare organizations have experienced numerous attacks that have affected the availability of their services and the confidentiality of patients' personal and clinical data. This has led organizations to recognize the need to prioritize and address cybersecurity issues. This paper recommends that organizations start by applying a comprehensive strategic approach, as suggested in the "Seven-step approach to implementing cybersecurity" section.

While the seven steps provide a comprehensive approach, **organizations would be well advised to review the proposed methodology based on their maturity level**. Each organization should have a strategy that measures the maturity at each step and allows for the creation of a continuous improvement plan to reach the level the organization desires in the long term.

The seven steps are based on the cybersecurity team's experience in applying industry best practice and are aligned with international frameworks. To effectively, efficiently, and sustainably implement cybersecurity at an organization, the organization must adopt a framework and have an organizational structure to support it. As stated in step 2, organizations must define key roles, like the CISO and information security committee, and establish cybersecurity responsibilities for all staff. In this context, one of the main challenges organizations face is choosing which information security methods, standards, and practices to follow.

In defining its information security and cybersecurity objectives and goals, organizations have to decide whether they need or want to pursue certification; this will guide them in choosing the most appropriate framework.

In our view, the NIST-CSF is a very good option. Its approach is based on improving cybersecurity measures and controls, so it can be implemented quickly and produce measurable short-term results. It is designed to strike a good balance between costs and outcomes.

For organizations that need certification, we recommend the ISO/IEC 27000 or HITRUST CSF family of standards. Both serve as a guide to adopting an information security management system. The advantage of adopting the ISO/IEC 27000 family of standards is that, as a general-purpose standard (not specific to the healthcare sector), it has a high level of penetration in organizations, so it is easier to find the human resources needed to adopt it. In contrast, the HITRUST CSF standard has been adapted for the health sector, which is advantageous because organizations do not have to adapt a general standard to their specific sector.

Organizations need to establish the controls to be implemented based on the framework selected. All controls should be weighed according to the organization's information security requirements and objectives.

For organizations that use the NIST-CSF, we recommend they adopt the minimum controls recommended for healthcare organizations, as specified in special publication NIST SP 800-171 r2.

We recommend that institutions that decide to align with the ISO/IEC 27000 family of standards adopt the controls specified for the healthcare sector in ISO/IEC 27799. For those following HITRUST CSF, we recommend using the controls it sets out.

Regardless of which standard it chooses, each organization must make its own decisions based on aspects like the complexity of adopting the standards at the organization. If the organizational situation precludes implementing the recommended measures, while working to prepare the necessary conditions, we suggest it look for another approach and adopt technical measures based on practical standards and guidelines like the CIS Critical Security Controls.

Finally, organizations should consider using other types of specific controls for particular cases: for example, OWASP ASVS and MASVS for application security requirements or specific guidelines from international organizations like ENISA or NIST for areas like the IoMT.

In LAC, great strides are being made in the field of cybersecurity awareness. This progress is driving policy and regulatory changes. Although each country is creating its own regulations, most are based on previous experiences, particularly HIPAA and GDPR. It is therefore important to define measures and controls that are compatible with HIPAA and GDPR, as this helps ensure compliance with current and future local and international regulations.

We believe that more and more good information security practices will be adopted over the next decade at the organization and government level in different critical sectors, with great benefits for the LAC health sector in particular.

Acknowledgement

Cristina Pombo, Jennifer Nelson, and Pablo Orefice.

References

- **Carvajal, Víctor and Jara, Matías, 2016:** "Grave falla en la red del Minsal dejó expuesta información confidencial de pacientes," CIPER, 5 March, 2016, retrieved from: https://www.ciperchile.cl/2016/03/05/grave-falla-en-la-red-del-minsal-dejo-expuesta-informacion-confidencial-de-pacientes/.

- **Center for Internet Security (CIS), 2019:** "CIS Critical Security Controls. Versión 7.1," retrieved from https://www.sans.org/critical-security-controls.

- **Clarín Tecnología, 2018:** "Ciberdelito. Pagan miles de dólares en criptomonedas para recuperar historias clínicas robadas," at Clarin.com, January 27, 2018, retrieved from https://www.clarin.com/tecnologia/pagan-miles-dolares-criptomonedas-recuperar-historias-clinicas-robadas_0_ByjjB7qSM.html.

- **Comisión Europea, n.d.:** "Protección de datos. Normas sobre protección de datos personales dentro y fuera de la UE," retrieved from https://ec.europa.eu/info/law/law-topic/data-protection_es.

- **DataBreaches.net. The Office of Inadequate Security, 2018:** "Telemedicine company exposed data of more than 2 millions patients in Mexico," August 8, 2018, retrieved from https://www.databreaches.net/telemedicine-company-exposed-data-of-more-than-2-millions-patients-in-mexico/.

- **European Union Agency for Cybersecurity (ENISA), 2015:** "Security and Resilience in eHealth Infrastructures and Services," retrieved from https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services.

- **European Union Agency for Cybersecurity (ENISA), 2016:** "Cyber security and resilience for Smart Hospitals," retrieved from https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals.

- **European Union Agency for Cybersecurity (ENISA), 2019:** "ICT security certification opportunities in the healthcare sector," retrieved from https://www.enisa.europa.eu/publications/healthcare-certification.

- **European Union Agency for Cybersecurity (ENISA), 2020:** "Procurement Guidelines for Cybersecurity in Hospitals," retrieved from https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

- **Healthcare Information and Management System Society (HIMSS), HIMSS North America, 2018:** "2018 HIMSS Cybersecurity Survey," retrieved from https://www.himss.org/sites/hde/files/d7/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf.

- **HITRUST, 2019:** "HITRUST Cybersecurity Framework," retrieved from https://hitrustalliance.net/product-tool/hitrust-csf/.

- **IBM, 2020:** "Cost of a Data Breach Report 2020," retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.

- **Information System Audit and Control Association (ISACA), 2019:** "COBIT 2019," retrieved from https://www.isaca.org/resources/cobit.

- **Information System Audit and Control Association (ISACA), 2019 (b):** "COBIT 5 Implementation," retrieved from https://www.isaca.org/resources/cobit.

- **International Standards Organization (ISO), 2013 (a):** "ISO/IEC 27001. Information Security Management," technical standard, retrieved from https://www.iso.org/isoiec-27001-information-security.html.

- **International Standards Organization (ISO), 2013 (b):** "ISO/IEC 27002. Code of Practice for Information Security Controls," technical standard, retrieved from https://iso.org/standard/54533.html.

- **International Standards Organization (ISO), 2016:** "ISO/IEC 27799 Health informatics. Information security management in health using ISO/IEC 27002," technical standard, retrieved from https://www.iso.org/standard/62777.html.

- **National Institute of Technical Standards (NIST), 2006:** "FIPS-200. Minimum Security Requirements for Federal Information and Information Systems," retrieved from https://csrc.nist.gov/publications/detail/fips/200/final.

- **National Institute of Technical Standards (NIST), 2018 (a):** "Framework for improving Critical Infrastructure Cybersecurity. Version 1.1," retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

- **National Institute of Technical Standards (NIST), 2018 (b):** "SP1800-1. Securing Electronic Health Records on Mobile Devices," retrieved from https://csrc.nist.gov/publications/detail/sp/1800-1/final.

- **National Institute of Technical Standards (NIST), 2018 (c):** "SP1800-8. Securing Wireless Infusion Pumps in Healthcare Delivery Organizations," retrieved from https://csrc.nist.gov/publications/detail/sp/1800-8/final.

- **National Institute of Technical Standards (NIST), 2020 (a):** "SP1800-24. Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector," retrieved from https://csrc.nist.gov/publications/detail/sp/1800-24/final.

- **National Institute of Technical Standards (NIST), 2020 (b):** "NIST Special Publications 800-53, revision 5. Security and Privacy Controls for Information Systems and Organizations," retrieved from https://nvd.nist.gov/800-53.

- **National Institute of Technical Standards (NIST), 2020 (c):** "NIST Special Publications SP 800-171, revision 2. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations", retrieved from https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

- **National Institute of Technical Standards (NIST), 2021:** "SP1800-30. Securing Telehealth Remote Patient Monitoring Ecosystem (2nd Draft)," retrieved from https://csrc.nist.gov/publications/detail/sp/1800-30/draft.

- **Neveux, Ellen, 2021:** "Hackers, breaches, and the value of healthcare data," retrieved from https://www.securelink.com/blog/healthcare-data-new-prize-hackers/.

- **Open Web Application Security Project (OWASP), 2016:** "Top 10 Mobile Application Security Risks," retrieved from https://owasp.org/www-project-mobile-top-10/.

- **Open Web Application Security Project (OWASP), 2017:** “Top 10 Web Application Security Risks,” retrieved from https://owasp.org/www-project-top-ten/.

- **Open Web Application Security Project (OWASP), 2020 (a):** “OWASP Application Security Verification Standard (ASVS) version 4.0.2,” retrieved from https://owasp.org/www-project-application-security-verification-standard/.

- **Open Web Application Security Project (OWASP), 2020 (b):** “OWASP Mobile Application Security Verification Standard (MASVS) version 1.3,” retrieved from https://github.com/OWASP/owasp-masvs.

- **UK Department of Health & Social Care, 2018:** “Securing cyber resilience in health and care. Progress update, October 2018,” retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf.

- **European Union, 2016:** “Reglamento General de Protección de Datos. Y listado de empresas de protección de datos,” retrieved from https://rgpd.es/.

- **U.S. Department of Health & Human Services, n.d.:** “Health Information Privacy,” retrieved from https://www.hhs.gov/hipaa/index.html.

- **Verizon, 2020:** “Verizon 2020 Data Breach Investigations Report,” retrieved from https://enterprise.verizon.com/en-gb/resources/reports/dbir/2020/data-breach-statistics-by-industry/.

IDB