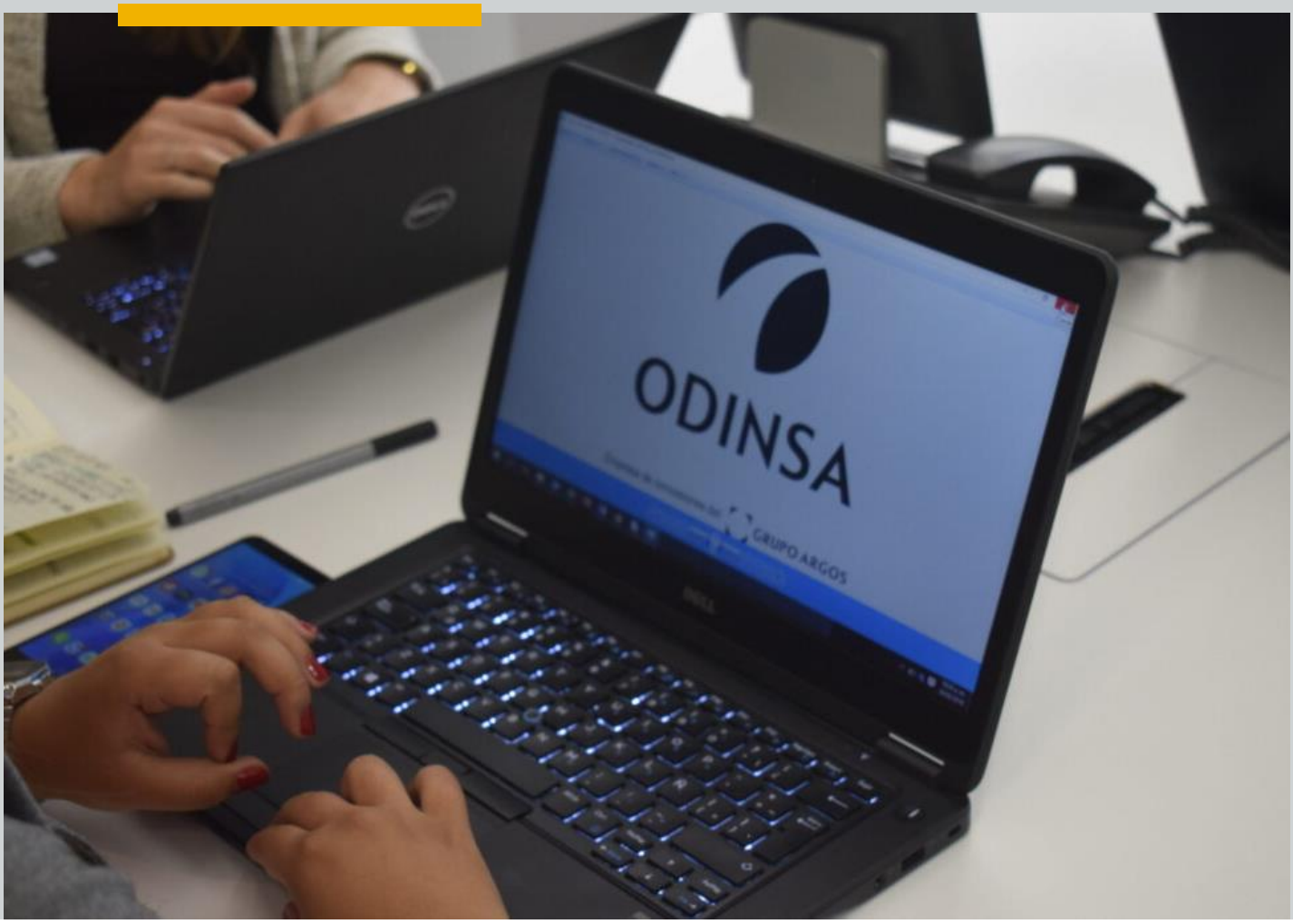

Guide to the Secure Use of IT Resources

OD-TI-003

ODINSA

Content

AUDIENCE

This guide applies to all personnel employed by ODINSA and its affiliated companies, hereinafter the Companies, as well as contractors and third parties who have access to the Companies' technological resources.

1. OBJECTIVE

To establish the rules for safe and honest use that the recipients of this regulation must comply with regarding the various IT and telecommunication resources provided by the Companies for the development of their business activity, or the personal resources of employees in which information of the Companies is managed or delivered to them for custody.

2. SCOPE OF APPLICATION

The regulations contained in this document are mandatory for employees of the Companies, as well as for those persons contractually or statutorily linked to them.

In the case that other entities, public or private, make use of any of the Companies' IT resources pursuant to a legal provision or an order from a competent authority, or access information circulating through such media, it is an obligation to notify in writing the officials who represent them and/or any other third party of the existence of this regulation so that the information security measures contained herein are adopted by such entities in order to prevent damage to the information.

3. RIGHTS OF THE COMPANIES

The Companies inform the recipients of this regulation that, with regard to the IT resources indicated below, they legally exercise rights of ownership, intellectual property rights, and rights of access to public and/or private networks and services, by virtue of contractual relationships with third parties.

The Companies adopt the necessary security measures and controls to ensure the respect and protection of such IT resources.

4. HONEST USE OF IT RESOURCES

All employees and third parties must know and comply with the **Cybersecurity Policy**, which is mandatory.

All information stored, created, or transmitted using the Company's resources is related to the functions of the user's position, is for exclusive use, and is used for business purposes. The Company authorizes the exceptions expressed in the subsequent sections of this document.

Employees may access only the information related to the functions of their position. Third parties who require access to information systems may access only the information necessary for the purpose of their contract.

Customer privacy is respected, and reasonable measures are taken to ensure the security of personal data that is collected, stored, processed, and disclosed.

The use, operation, and handling of information systems comply with the requirements of applicable national and international laws regarding software licensing, copyright, information privacy, retention of information records, and all current legal provisions.

Violations of the Cybersecurity Policy or its guidelines by employees will trigger security incident handling measures and will be subject to disciplinary action by Human Resources.

4.1. HARDWARE

4.1.1. Use of Hardware

Computers, servers, and peripheral devices provided and/or delivered by the Companies to the recipients of this regulations for the execution of the corporate purpose are intended solely and exclusively for business activities.

Hardware provided and/or delivered by the Companies must be treated under the best conditions of use, maintenance, and hygiene by the employee responsible for it.

4.1.2. Prohibitions regarding Hardware

Due to the multiple risks to information as an intangible asset and to the Companies' IT resources that store it, arising from malware (malicious software designed to cause harmful actions in an information system) that may be freely available or free of charge, such software must be subject to a security analysis and a licensing review; once these analyses have been approved by the Technology team it may be used, otherwise its installation will be denied.

It is also strictly prohibited to install software or computer programs offered under a paid license regime whose license has not been obtained through the Companies.

Company laptops assigned to an employee may not be lent to third parties under any circumstances, due to the Companies' information contained therein.

Recipients of this regulations may not change the configuration of hardware delivered by the Companies, since such activity may create a security breach, and they will be responsible for any damages.

The installation of encryption software on equipment without the Companies' authorization will be treated as a disciplinary matter in accordance with the provisions determined for

this purpose.

The creation and connection of personal wifi networks or hotspots is prohibited, since these may compromise the security of the organization's platforms and information. In view of the above, the Companies' visitor wifi may be used.

4.1.3. Exceptions to business use of Hardware

On an exceptional and limited basis, recipients of this regulations may store on hardware assigned for the performance of their duties or services, text files related to academic activities, information concerning their immediate family, and personal information concerning their assets. All such information is personal to the user of the hardware, therefore the Company is not responsible for its loss.

The Companies authorize employees, regardless of their type of engagement with the Company, to use their own hardware, including mobile devices, cell phones, tablets, among others. If these devices handle Company information, users must accept and comply with the regulations and adopt the IT security recommendations determined by the Technology team.

4.2. SMARTPHONES

The Companies may assign to employees, when required by their activities, a smartphone and/or a voice and data plan, and use must comply with the Mobile Phone Business Rules document published by the Company.

4.2.1. Prohibitions regarding smartphones and/or voice or data services provided by the Companies

It is prohibited to alter the security configuration of a smartphone assigned by the Companies, as well as network security controls, since such actions pose a risk to the security of the Companies' information assets.

4.3. SOFTWARE

4.3.1. Use of software

Only software duly licensed by the Companies may be installed on computer equipment delivered by them.

The Companies will inform and notify the recipients of this regulation, when assigning IT resources for the performance of their functions, of the inventory of programs installed on their equipment, which will be the only ones authorized for use.

During the term of the contractual relationship, the Companies' Technology team will monitor and verify compliance with this provision in order to prevent violations of intellectual property regulations and/or attacks on their information assets from malware (malicious software designed to cause harmful actions in an information system) installed

on the hardware.

Recipients of this regulation are obligated to use the software assigned and/or acquired for the performance of their duties in accordance with the specifications in the user and/or technical manuals, as applicable. Any errors in the software's functionality must be reported to the Technology team or the Service Desk.

Free software required by the organization in the development of its business activities, or acquired independently by employees, must be approved and authorized by the Technology team.

4.3.2. Prohibitions regarding software

It is prohibited to copy or reproduce software delivered by the Companies to the recipients of this regulation or acquired directly by employees, since such conduct violates intellectual property laws.

Developing derivative works without the authorization of the owner of the original work is contrary to intellectual property regulations.

Recipients of this regulation may not change the configuration of authorized software, since such activity may create a security breach in the software and in the IT security architecture, and they will be responsible for any resulting damages.

Software installed and used by an employee generates traces or logs, which may be subject to audit procedures.

4.3.3. Exceptions to business use of software

Office software, such as word processors, among others, may exceptionally be used for academic activities and basic personal activities. All such information is personal to the user, therefore the Company is not responsible for its loss.

4.4. INTERNET

4.4.1. Internet use

Recipients of this regulation must use the Internet responsibly and follow the security measures established by the Technology team in order to avoid security breaches in information.

The same provisions for honest use established for the Internet apply to the use of the Companies' Corporate Intranet.

4.4.2. Prohibitions regarding the Internet

Recipients of this regulation are prohibited from using the Internet while providing services to the Companies, whether on personal or Company devices, to access sites that may contain malware or malicious software, such as pornography, gaming, betting, auction, entertainment, or software download or exchange sites, among others.

As a security measure, the transfer and/or receipt of files exchanged through free and/or public programs that are not authorized by the Technology team is prohibited.

4.4.3. Exceptions regarding business use of the Internet

Recipients of this regulation may use the Internet for academic activities, activities concerning their immediate family, and financial activities during their free time. Likewise, it is noted that this activity may be subject to monitoring.

4.5. EMAIL

Email is a form of correspondence which, like physical correspondence, must be organized, administered, and preserved by the Companies in compliance with the obligations established in commercial law regarding trade books.

Correspondence that may be generated through corporate email is part of the Companies' trade books and therefore constitutes confidential information under the Commercial Code.

4.5.1. Evidential effects

The information contained in corporate email may be correspondence and therefore constitutes full proof of the Companies' business dealings, and will be managed in compliance with commercial regulations on correspondence. It also has full validity and probative value under Law 527 of 1999, provided that it complies with the attributes of integrity, authenticity, and confidentiality.

Corporate email and the information contained therein may constitute evidence in cybersecurity incidents that have legal and/or judicial repercussions.

4.5.2. Technological measures

All information sent through corporate email assigned to the recipients of this regulation is the property of the Companies. The Companies will adopt technological measures aimed at managing emails that pose a risk to the organization.

With regard to sensitive personal information that may be identified in the content of corporate emails through the Companies' Technology team and/or any designee, the holder of the corporate email account will be notified so that the information can be removed and handled appropriately.

4.5.3. Purpose of corporate email

Corporate email is assigned by the Companies to the recipients of this regulation for the sole purpose of serving as a mechanism for internal and external communication related to the performance of activities that comprise the ordinary course of business.

4.5.4. Privacy risks associated with the use of email

The use of email for the personal purposes determined herein must in all cases be under the responsibility of the recipient of this regulation .

Recipients of this regulation are advised not to disclose personal information or privacy through corporate email; the voluntary exposure of such information constitutes an individual decision, and the recipient assumes the implications of that action.

4.5.5. Prohibitions

Information transmitted through corporate email may not violate human rights or contain data contrary to morality and good customs.

Corporate email is a tool for individual use that may not be transferred to other persons, and the person who allows its use will be responsible for any damage it may cause.

4.5.6. Access by third parties and authorities

Officials of the judicial and executive branches of public power may only access corporate email in the cases established in Articles 63 and following of the Commercial Code.

Prior to access by authorities to the correspondence contained in corporate email, or by any other third party entitled to such access, the Companies' Legal Management of Corporate Affairs will verify that the public official and/or the third party has the authority to access such information. If such authority exists, the authority or third party will be notified of the information security and access requirements that must be observed in order to prevent risks to the information.

4.6. MONITORING, MAINTENANCE, AND SUPPORT

The Technology team will perform monitoring, maintenance, and support tasks that allow access to all information stored on hardware or transmitted through the network, as well as to establish the activities performed by the employee based on the traceability of logs and records generated during the use of IT resources. In carrying out this activity, the Companies will act in compliance with the Information Use Policy and other related regulations, rules, and procedures that develop the Cybersecurity Policy.

The Technology team will identify and remove from hardware any computer programs or software installed without authorization, due to the risks of attacks on information and any risks to intellectual property that may exist.

4.7. AUDITING

In compliance with the duty to protect information assets and in accordance with good cybersecurity practices, it is necessary to carry out periodic audits of Company hardware, software, email, services, and networks in order to prevent attacks against information, adopting the decisions considered appropriate to protect information owned by the Company or delivered for custody.

The Companies inform recipients of this regulation that activities carried out through such IT resources leave marks or traces (logs) that make it possible to establish with precision the actions performed in terms of time, manner, and place.

Based on the results of the audit, the Company will determine compliance with the obligations contained herein and will define the legal repercussions of any noncompliance; in such case, it may exercise the legal actions it considers appropriate where applicable.

4.8. ROLES AND RESPONSIBILITIES

Assessments and decisions regarding noncompliance with the obligations derived from this regulation will be made by Human Resources Management, in accordance with the current disciplinary procedure.

4.9. EFFECTS OF NONCOMPLIANCE

Noncompliance with this regulation regarding the use of IT resources is considered serious due to the risks posed to the Companies' information assets, the personal data held by the organization as custodian, and creations protected by intellectual property, among others, and may therefore result in the disciplinary sanctions provided for such cases.

4.10. RESTRICTIONS ON THE USE OF THIS REGULATION

This personal data protection regulation is for the exclusive use of the Companies, therefore its copying, reproduction, distribution, transfer, publication, translation, and any other use by persons other than the Companies is prohibited, both out of respect for the intellectual property rights of its creators and for information security reasons.

4.11. ACCESS TO INFORMATION SYSTEMS

No employee may access a user account belonging to another employee, or attempt to read, change, or manipulate another employee's electronic communications, files, or software without that employee's authorization or that of authorized Company officials.

4.12. PUBLIC STATEMENTS

Employees must not make statements about the Company or its actual or supposed position on any matter through public forums, such as newsgroups, bulletin boards, web-logs, or chat areas, except for statements that have been previously reviewed and specifically authorized by the Company.

4.13. SOCIAL MEDIA

To ensure the protection of the Company's reputation and of information reproduced through social networks, it is important that all Company employees take the following into account:

- Employees must not use the Company's logo or other intellectual property unless authorized by the Company's Legal team. They must also not post videos, images, or any other written and/or audio reproduction of the Company's physical spaces, events,

offices, equipment, products, customers, suppliers, or visitors within the Company's facilities.

However, in accordance with strategy and taking into account the nature of social media, employees will have a presence in some spaces specifically designated for them, intended to reinforce the Company's positioning. In this case, employees may post photos or videos of Company events on their own personal social media accounts, provided that such content does not violate any confidentiality, privacy, or property obligations of the Company or third parties.

- Employees must not use Company email addresses to register for social media, blogs, or other online tools for personal use, unless previously authorized in writing by the Communications team.

- Without the Company's prior written authorization, employees are not authorized to speak on behalf of the Company or to state that such authorization has been granted.

4.13.1. Recommendations for employee interaction on social media

Employees may share and interact with content published on the Company's social media accounts, taking into account what is established in the Code of Business Conduct and following these guidelines:

- Internal matters must only be discussed within the Company, never in digital spaces.
- Interactions with content about the Company must be respectful, transparent, reliable, timely, and positive, avoiding offensive comments at all times.
- There will always be discussions on social media, nothing is personal, therefore employees should avoid getting involved in them.
- If a possible crisis scenario is identified on any social media platform, the employee should save evidence of the post and send it as soon as possible to members of the Odinsa Communications team, who will act in accordance with the defined strategy and protocol.
- The employee must wait for the brand to make an official statement and may replicate the brand's response, but at no time should make quotations or attach comments on a personal basis.

Employees who express their opinion on matters related to the Company's business must make it clear to readers in any communication that discusses or mentions the Company that the opinions expressed are those of the employee alone and do not represent the opinions of the Company.
Refrain from making defamatory statements and/or using malicious, derogatory, vulgar, obscene, threatening, and/or harassing language about the Company, its products and services, coworkers, Senior Management, partners, customers, suppliers, and competitors, among others.
Do not post personally identifiable information or confidential personal information about other employees, Senior Management, partners, customers, suppliers, competitors, and/or third parties without the prior written consent of that person.

Do not disclose any information about the Company, a specific customer, or a supplier unless the Legal team has granted written authorization or such information is publicly available.

Check privacy settings both for the profile and for the content shared.

Protect access to social network profiles with strong passwords, using two-factor authentication where feasible.

If you have any concerns or detect any suspicious activity in the emails you receive, in information systems, or in abnormal operation of your equipment, please contact the Technology team through Emma, SOS@odinsa.com, or extension 12345.

BIBLIOGRAPHY

Congreso de la República. (2014). *Ley 1581 de 2014. Por la cual se dictan disposiciones generales para la protección de datos personales.* Retrieved from http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Congreso de la República. (2014). *Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones*. Retrieved from http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

ISO International Organization for Standardization. (2013). *ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls.*

MinTIC. (2016). *Guía para la gestión y clasificación de activos de información.* Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

MinTIC. (2016). *Procedimientos de seguridad de la información.* Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

VERSION CONTROL

Number	Date	Description of change or modification
1	November 16, 2016	Initial issue

2	April 11, 2022	Adjustments for improvement opportunities in the Cybersecurity Process Audit
3	August 30, 2023	Approval body Strategic Cybersecurity Committee