 [Translated from Portuguese to English - www.onlinedoctranslator.com](https://www.onlinedoctranslator.com/en/?utm_source=onlinedoctranslator&utm_medium=docx&utm_campaign=attribution)

**Incident Communication and Reporting**

Employer: Cyber ​​SecurityUP

Name: Joas A Santos

|  |  |
| --- | --- |
| **INCIDENT IDENTIFICATION INFORMATION** | |
| Date and Time of Notification | |
| Incident name: | |
| Analyst Name: | Date and Time of Detection |
| Function: | Location: |
| Email/Cell Phone: | System or Application: Linux, Windows, Website |
| **INCIDENT SUMMARY** | |
| **Incident Type:**  ☐ Denial of Service ☐ Malware ☐ Dump of Data  ☐ Unauthorized Access ☐ Phishing ☐ Other | |
| **Incident Description:** | |
| **Name and contact details of the people involved:** | |
| **Incident Severity**  ☐ Critical ☐ Average  ☐ High ☐ Low | |
| **Affected Systems:**  ☐ On-premises ☐ IoT/ICS  ☐ Cloud ☐ Physical | |
| **ACTIONS** | |
| **Identification Measures (Incident Verified, Evaluated, Options Evaluated):** | |
| **Containment Measures:** | |
| **Collected Evidence (System Logs, IoCs, etc.):** | |
| **Eradication Measures:** | |
| **Recovery Measures (Optional)** | |
| **Other mitigation methods:** | |

Form developed for internal use -Joas Antonio dos Santos / Cyber ​​Security UP

|  |
| --- |
| **IMPACT OF THE INCIDENT** |
| **IMPACT OF THE INCIDENT:**  ☐ Users ☐ Others  ☐ Intellectual Property ☐ Financial |
| **Affected users:** |
| **COMMUNICATION** |
| **Reviewed by:**  ☐ Security Officer ☐ Department/Team  ☐ Tech Leader ☐ Other |
| **Recommended actions taken:** |
| **Initial report completed by:** |
| **Follow-up completed by:** |

|  |
| --- |
| **Lessons Learned** |
| **How well did workforce members respond?** |
| **Have documented procedures been followed? Were they adequate?** |
| **What information was needed before?** |
| **Have any measures or actions been taken that may have inhibited recovery?** |
| **What can workforce members do differently the next time an incident occurs?** |
| **What corrective actions can prevent similar incidents in the future?** |
| **What additional resources are needed to detect, analyze and mitigate future incidents?** |
| **Other conclusions or recommendations:** |
| **additional remarks** |
|  |
| Commitment Indicators |
|  |
| **additional remarks** |

**Improved Journal of AHIMAA Developed Form**

**Subscriptions**

**SOC Analyst INCIDENT RESPONSER LEADER SOC Manager**

**\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_**