CERT WHC - RFC 2350

1. DOCUMENT INFORMATION

1.1. Updates and Authorisations History

AUTHORISATIONS			
Document validation: CERT WHC - RFC 2350			
Function	**Name**	**Rôle**	**Signature**
Prepared by	Ismael Guerrero	Security Monitoring Manager	-
Revised by	Diana Posada	Director of Operations	-
Authorised by	Sergio López	General Director	-

VERSIONS		
Version	**Description**	**Date**
01	Initial emission of the document.	January 13th, 2025

1.2. Distribution List

1.3. Where to find this document

The updated version of this document can be found at www.whitehatconsultores.com/cert-whc

Update notifications are sent via email to all WHC Administered Services active clients.

Any questions about the updates of this document should be sent to cert.whc@whitehatconsultores.com.

Document Location

Español (Spanish): www.whitehatconsultores.com/cert-whc

English: www.whitehatconsultores.com/cert-whc

Table of contents

2. Contact Information

2.1. Team Name

CERT-WHC

2.2. Address

Av. Insurgentes Sur 1106, Piso 10 Col. Tlacoquemécatl del Valle

Alcaldía Benito Juárez C.P. 03200, México, CDMX

2.3. Time Zone

Ciudad de México, Zona Centro UTC- 6.

2.4. Telephone number

Main Telephone Number (Mobile): 5543880876

Fixed Line (Teams): 5556016632

2.5. Fax Number

Not available

2.6. Other Means of Communication

None

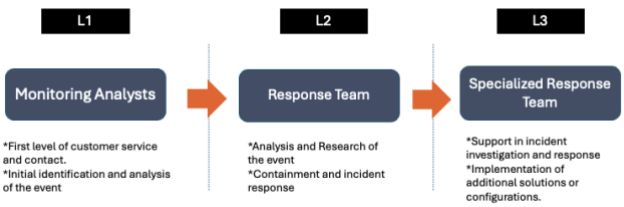
2.7. Email Addresses

cert.whc@whitehatconsultores.com

monitoreo@whitehatconsultores.com

2.8. Team members

The following chart illustrates the structure of the CERT-WHC team.



Note: Additional information such as names, telephone numbers and other data are not shown because they are personally identifiable data and hence confidential.

2.9. More information

None

2.10. Working Hours

The response team is available 24/7, 365 days a year.

2.11. Client Contact Points

To contact the Incident Response Team via email see point 2.7, via telephone see point 2.4. Alternatively use can be made of the following website www.whitehatconsultores.com/cert-whc

3. Constitution

3.1. Mission

White Hat Consultores is a team of specialists focused on information security and IT services with a high level of certification and experience.

Its *mission* is to provide organisations and people with risk administration solutions and IT services in order to bring freedom in a digital risk environment, as well as to optimise their operations.

Its *vision* is to be the leading specialist enterprise in relation to information security and IT services integrating the best practices in the international arena and delivering solutions of true value to the business of our customers.

3.2. Jurisdiction

The services offered by the WHC-CERT are targeted at enterprises in México, the USA, and Latin America irrespective of their size or industry. As mentioned, its objective is to add value to these businesses by focusing on advanced monitoring of identities which is the new security boundary which enterprises should be protecting given its susceptibility to attacks.

3.3. Sponsorship/Affiliation

WHC is part of a specialised Microsoft security group through the programmes MCI, CSI, FAST Track Ready y MISA among others. These support their jurisdiction to detect and respond to security events which might compromise the security of the information assets in their infrastructure. This is done through the monitoring, analysis and correlation of security events, including the posible threats to the Cloud and On-premises environments

Furthermore, WHC features diverse complementary reference sources to keep us updated on the most recent threats. Examples of these sources are: UNAM CERT, Guardia Nacional CERT-MX, Microsoft Defender Threat Intelligence, Centro Criptológico Nacional (CCN) de España, but we may use others as well.

3.4. Authority

The WHC-CERT is an internal area of White Hat Consultores under the authority of the Security Operations Directorate. Its aim is to provide security services to our external clients. The CERT does not have authority over its clients, consequently, in a security event or incident its role is to give mitigation recommendations, and, in some cases, depending on the contractual and technological circumstances, it may furnish attention and incident response.

4. Policies

4.1. Incident types and support levels

The WHC-CERT offers support for any type of event or security incident to its internal and external jurisdictions. The attention times will vary depending on the level of severity of the incidents, and on the contractually established levels of service.

4.2. Cooperation, interaction, and information disclosure

The WHC-CERT may carry out cooperation activities with different security partners. These operative contributions allow us to improve our response activities and attention times.

4.3. Communication and authentication

Information is communicated with the use of Microsoft Purview's labels. This allows us to classify the data according to its level of sensitivity. Once applied, the labels include protection settings such as encryption and content marks (headers, footnotes, water seals) to make sure that only the authorised users have access to the information in question.

5. Services

5.1. Security Events Monitoring

This is the continuous security monitoring performed for a client to detect and respond to cyberthreats in real time. It utilises advanced analyses to correlate security events and respond in a timely fashion. The data is gathered from several suppliers, such as network devices, servers, and apps; it is then presented in a unified interface which allows for complete visibility and a quick response to the incidents. Additionally, it helps to comply with security regulations and to reduce the detection and response time. The automatization and analysis by a specialised combined team ensures an efficient and precise threat management.

5.2. Security Incidents Response

A security incident management service focuses on identifying, prioritising, and containing cyber-attacks in an efficient manner. It uses tested procedures based on security frameworks and best practices which help to minimise the impact and to reduce the recovery times of an operation. The response includes analysis, investigation, containment, and in some instances the restoring of affected systems or the accompaniment to carry through the said recuperation actions.

5.3. Vulnerability Analysis

A vulnerability analysis service evaluates an IT infrastructure to identify and correct security flaws. It uses advanced tools to scan networks, apps, and systems in search of known vulnerabilities. The results are presented in detailed reports which prioritise the threats according to their severity. This service helps to prevent cyber-attacks by identifying weaknesses before they can be exploited. The combination of automated analyses and manual reviews ensures that a comprehensive and accurate assessment is conducted.

5.4. Security Threat Intelligence

A threat intelligence service gathers data from multiple information sources, both public and private to identify patterns and tendencies of attacks which might affect our clients according to their own infrastructure, the sector they belong to, and other factors. This information allows the security teams to take informed decisions and be proactive when mitigating risks.

6. Incident Notification Form

There is no incident notification form that is publicly available. All communication should take place in a secure manner via the emails cert.whc@whitehatconsultores.com or monitoreo@whitehatconsultores.com in accordance with the previously established agreements between the clients and ourselves.

7. Disclaimer

This document is provided solely for general informative purposes. We do not assume any liability for errors or omissions in its contents.

All the measures in our power will be taken to make sure all information is correct and appropriately managed. However, the WHC-CERT cannot assume any liability for any losses or damages ensuing from the use of the information in this document including, but not limited to indirect losses, or any consequences of any type or form, whether loss or damage that may ensue through the use of the information herein.

The information or materials in this site are to be used under your own risk, we cannot, and do not assume any responsibility for its use. It is your own responsibility to make sure that any product, service, or information available through this site meets your own security standards.

We make no guarantees or representations regarding the accuracy, completeness, or reliability of the content provided. By using the information herein, you acknowledge that we are not liable for any damages, losses, or consequences resulting from its use. Please consult a professional or perform independent research before taking decisions based on the content of this document.

Thank you.

END OF DOCUMENT