CERT WHC - RFC 2350

1. INFORMACIÓN DEL DOCUMENTO

1.1. Historial de Actualizaciones y Autorizaciones

AUTORIZACIONES			
Validación del documento: CERT WHC - RFC 2350			
Función	**Nombre**	**Rol**	**Firma**
Elaboró	Ismael Guerrero	Responsable de Monitoreo de Seguridad	-
Revisó	Diana Posada	Director de Operaciones	-
Autorizó	Sergio López	Director General	-

VERSIONES		
Versión	**Descripción**	**Fecha**
01	Emisión inicial del documento.	13 de enero de 2025

1.2. Lista de Distribución

1.3. Ubicación en donde se puede localizar este documento

Este documento se encuentra actualizado en la página de internet en la página www.whitehatconsultores.com/cert-whc

Las notificaciones de actualización se realizan vía correo electrónico a los clientes activos de Servicios Administrados de WHC.

Si se tiene alguna duda sobre la actualización de este documento, diríjase al correo electrónico cert.whc@whitehatconsultores.com.

Ubicación del documento

Español: www.whitehatconsultores.com/cert-whc

Inglés: www.whitehatconsultores.com/cert-whc

Tabla de contenido

2. Información de Contacto

2.1. Nombre del Equipo

CERT-WHC

2.2. Dirección

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

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

2.3. Zona Horaria

Ciudad de México, Zona Centro UTC- 6.

2.4. Número de Teléfono

Teléfono Principal (Celular): 5543880876

Teléfono Fijo (Teams): 5556016632

2.5. Número de Fax

No se cuenta con este medio de comunicación

2.6. Otros Medios de Comunicación

Ninguno

2.7. Dirección de Correo Electrónico

cert.whc@whitehatconsultores.com

monitoreo@whitehatconsultores.com

2.8. Miembros del Equipo

A continuación, se muestra un esquema sobre la estructura de los miembros del CERT-WHC

Nota: Información adicional como nombres, números telefónicos y otros datos no se muestran ya que se trata de información de datos personales y son confidenciales.

2.9. Más Información

Ninguna

2.10. Horarios de Atención

El Equipo de Respuesta a Incidentes está disponible 7x24 los 365 días del año.

2.11. Puntos de Contacto del Cliente

Los métodos de comunicación con el Equipo de Respuesta a Incidentes es el correo electrónico establecido en el punto 2.7, vía telefónica en el punto 2.4 y a través de la página de internet www.whitehatconsultores.com/cert-whc

3. Constitución

3.1. Misión

White Hat Consultores es un equipo de especialistas enfocados en seguridad de la información y servicios de TI con un alto nivel de certificación y experiencia.

Su *misión* es proveer a las organizaciones y a las personas de soluciones de administración de riesgo y servicios de TI para brindar libertad en un entorno de riesgo digital, así como la optimización y eficiencia en la operación.

Su *visión* es ser la empresa especialista líder en servicios de seguridad de la información y servicios de TI, integrando las mejores prácticas a nivel internacional entregando soluciones de valor al negocio de nuestros clientes.

3.2. Circunscripción

Los servicios que ofrece el CERT-WHC están enfocados a empresas en México, Estados Unidos y Latinoamérica, agregando valor independientemente de su tamaño o industria, enfocándose al monitoreo avanzado de identidades que es el nuevo perímetro de seguridad que las empresas deberían proteger ya que es lo que se ataca

3.3. Patrocinio/Afiliación

WHC forma parte de un grupo especializado de seguridad de Microsoft a través de los programas MCI, CSI , FAST Track Ready y MISA principalmente, que apoyan a su circunscripción a detectar y responder a eventos de seguridad que pudieran comprometer la seguridad de los activos de información en su infraestructura mediante el monitoreo, análisis y correlación de eventos de seguridad, incluyendo las posibles amenazas en el ambiente OnPremise y Cloud.

Además, WHC cuenta con diversas fuentes de consulta complementarias para mantenerse al día sobre las amenazas más recientes como UNAM CERT, Guardia Nacional CERT-MX, Microsoft Defender Threat Intelligence, Centro Criptológico Nacional (CCN) de España, entre otros.

3.4. Autoridad

El CERT-WHC es un área interna de White Hat Consultores bajo la autoridad de la Dirección de Operaciones de Seguridad que proporciona servicios de seguridad a diversos clientes externos, el CERT-WHC no dispone de autoridad sobre sus clientes, por lo cual ante un evento o incidente de seguridad proporciona recomendaciones de mitigación y en algunos casos, cuando se encuentre en el alcance contractual y tecnológico, se proporciona atención y respuesta.

4. Políticas

4.1. Tipos de incidentes y nivel de soporte

El CERT-WHC proporciona soporte a cualquier evento o incidente de seguridad a sus circunscripción interna y externa, los tiempos de atención dependerán de su nivel de criticidad y, de acuerdo con, los niveles de servicio establecidos de manera contractual con cada uno de estos.

4.2. Cooperación, interacción y divulgación de información

El CERT-WHC puede realizar actividades de cooperación con diversos partners de seguridad para la contribución operativa con el fin de mejorar las actividades de respuesta y los tiempos de atención a los eventos o incidentes de seguridad de su circunscripción.

4.3. Comunicación y autenticación

La información es divulgada a través de etiquetas de seguridad con Microsoft Purview que permite clasificar los datos según su nivel de sensibilidad, una vez aplicadas, estas etiquetas incluyen configuraciones de protección como cifrado y marcas de contenido (encabezados, pies de página y marcas de agua), asegurando que solo los usuarios autorizados tengan acceso a la información sensible, solo en caso de ser necesario.

5. Servicios

5.1. Monitoreo de Eventos de Seguridad

Es el monitoreo continuo de seguridad de un cliente para detectar y responder a amenazas cibernéticas en tiempo real. Utiliza análisis avanzados para correlacionar eventos de seguridad y responder de manera oportuna un posibles incidentes de seguridad. Los datos se recopilan de múltiples fuentes, como dispositivos de red, servidores y aplicaciones, y se presentan en una interfaz unificada, lo que permite una visibilidad completa y una respuesta rápida a incidentes. Además, ayuda a cumplir con normativas de seguridad y a reducir el tiempo de detección y respuesta. La automatización y el análisis por parte de un equipo especializado combinado aseguran una gestión eficiente y precisa de las amenazas.

5.2. Respuesta a Incidentes de Seguridad

Un servicio de Gestión de Incidentes de Seguridad se enfoca en identificar, priorizar y contener ciberataques de manera eficiente. Utiliza procedimientos probados basados en marcos de seguridad y mejores prácticas que apoyen a minimizar el impacto y a reducir los tiempos de recuperación. La respuesta incluye el análisis, investigación, contención, respuesta y en algunos de los casos restauración de sistemas afectados o en su defecto, el acompañamiento para realizar las acciones de recuperación.

5.3. Análisis de Vulnerabilidades

Un servicio de análisis de vulnerabilidades de seguridad evalúa la infraestructura de TI para identificar y corregir fallos de seguridad. Utiliza herramientas avanzadas para escanear redes, aplicaciones y sistemas en busca de vulnerabilidades conocidas. Los resultados se presentan en informes detallados que priorizan las amenazas según su severidad. Este servicio ayuda a prevenir ciberataques al identificar puntos débiles antes de que sean explotados. La combinación de análisis automatizados y revisiones manuales asegura una evaluación exhaustiva y precisa.

5.4. Inteligencia de Amenazas de Seguridad

Un servicio de inteligencia de amenazas recopila datos de múltiples fuentes de información públicas y privadas para identificar patrones y tendencias de ataques que pudieran afectar a los clientes de acuerdo con la infraestructura que maneja, el sector al que pertenece, entre otros aspectos. Esta información permite a los equipos de seguridad tomar decisiones informadas y proactivas para mitigar riesgos.

6. Formulario de Notificación de Incidente

No se cuenta con un formulario público disponible para el reporte de un evento o incidente, toda comunicación debe ser a través del correo electrónico establecido de manera segura cert.whc@whitehatconsultores.com o monitoreo@whitehatconsultores.com por los medios establecidos previamente con cada uno de los clientes externos.

7. Disclaimer

La información proporcionada en este documento es solo para fines informativos generales. No asumimos ninguna responsabilidad por errores u omisiones en el contenido.

Si bien se tomarán todas las medidas necesarias para el manejo de la información, el CERT-WHC no se hace responsable por cualquier pérdida o daño, incluyendo sin limitación, pérdidas indirectas o consecuentes, o cualquier pérdida o daño que pueda surgir.

El uso de cualquier información o material en este sitio es bajo su propio riesgo, por lo cual no seremos responsables. Es su responsabilidad asegurarse de que cualquier producto, servicio o información disponible a través de este sitio cumpla con sus requisitos específicos.

Gracias

FIN DEL DOCUMENTO