1. Información del Documento

1.1. **Fecha de la última actualización:** 03 de Octubre de 2019.
1.2. **Listas de Distribución:** No disponible.
1.3. **Ubicación del Documento:** La versión actual de este documento se encuentra disponible en el sitio web del Centro de Ciberseguridad IQsec CERT https://cert.iqsec.com.mx/
1.4. **Autenticación del Documento:** Este documento es firmado por la llave PGP del Centro de Ciberseguridad.

2. Información de Contacto

2.1. **Nombre del Equipo:** Centro de Ciberseguridad IQSec CERT.
2.2. **Dirección:** Patriotismo 399 Col. San Pedro de los Pinos, Alcaldía Benito Juárez, C.P. 03800, CDMX.
2.3. **Zona Horaria:** UTC-GMT -6.
2.4. **Número de Teléfono:** + 52 (55) 4163 1750
2.5. **Número de Fax:** No disponible.
2.6. **Otras Comunicaciones:** No disponible.
2.7. **Dirección de Correo Electrónico:** cert@iqsec.com.mx.
2.8. **Llaves Públicas y encriptación de información:** Las comunicaciones cifradas con el Centro de Ciberseguridad IQSec CERT deberán utilizar esta llave:

Nombre: Centro de Ciberseguridad IQSec CERT.
E-mail: cert@iqsec.com.mx.
Public PGP key ID: 4AFE5930
Fingerprint: 96D2 D878 4EA9 3B93 4F63 2854 CB57 B0A4 4AFE 5930

2.9. **Miembros del Equipo:**

El director del Centro de Ciberseguridad IQsec CERT, es el Ing. Alejandro Núñez Sandoval, cuenta con una plantilla de 23 especialistas en ciberseguridad y el lider del equipo de respuesta a incidentes es el Ing. Jesus Noya.

2.10. **Más Información**

La información general sobre el Centro de Ciberseguridad IQSec CERT, sus servicios, boletines y recomendaciones de seguridad, puede consultarse en el sitio https://cert.iqsec.com.mx.

El Centro de Ciberseguridad CERT IQSec, cuenta con un horario de atención de lunes a domingo las 24 horas los 365 días del año.

2.11. **Puntos de Contacto**

La comunicación con el equipo del Centro de Ciberseguridad IQSec CERT, para el reporte de incidentes se realiza mediante los siguientes mecanismos:

1. Correo electrónico.
    a. cert@iqsec.com.mx.
2. Vía telefónica.
    a. Ext. + 52 (55) 4163 1750
3. Vía sistema de tickets.
    a. https://soporte.iqsec.com.mx/sp

3. Carta

3.1. Misión

Anticipar y responder a incidentes de ciberseguridad con experiencia y objetividad para cubrir las necesidades de la operación de tecnologías de seguridad, cumplimientos regulatorios y protección de activos de las grandes empresas en México con el compromiso de innovar, investigar y generar conocimiento.

3.2. Contitución

El Centro de Ciberseguridad IQsec CERT, fue creado en la Ciudad de México el día 29 de junio del 2016.

3.3. Patrocinio / Afiliación

El Centro de Ciberseguridad IQsec CERT, es una unidad de negocio de la empresa IQSec S.A. de C.V.

3.4. Autoridad

El Centro de Ciberseguridad IQsec CERT, fue constituido por instrucción de la Dirección General de la empresa IQSEC S.A de C.V., para responder a incidentes de ciberseguridad, con el compromiso de innovar, investigar y generar conocimiento.

4. Políticas

4.1. Tipo de Incidentes y nivel de Soporte

Se definira la prioridad de un incidente, con base en la críticidad del activo y la sensibilidad de la información del cliente, clasificando en alta media y baja, a menos que sea etiquetada explicitamente como prioridad alta.

4.2. Cooperación, Interacción y divulgación de la Información

El Centro de Ciberseguridad IQsec CERT, valora la importancia de la cooperación e intercambio de información con otras organizaciones, que pueden contribuir o hacer uso de sus servicios, para el intercambio de información de incidentes, IQsec se adhiere al protocolo TLP (Traffic Ligth Protocol).

4.3. Comunicación y Autenticación

El Centro de Ciberseguridad IQSec CERT, hace uso de correo electrónico cifrado/firmado mediante llaves PGP para el intercambio de información confidencial con otros equipos CSIRT.

5. Servicios

5.1. Respuesta a incidentes

Acciones coordinadas ante ataques de seguridad con el objetivo de minimizar el impacto en la organización, limitando los daños y reduciendo el tiempo de recuperación de los servicios.

5.2. Servicios administrados Servicios Administrados

Administración de soluciones de seguridad con el mejor costo-beneficio.

5.3. Supervisión continua

Recolección de bitácoras y análisis de eventos mediante las tecnologías que mejor se adapten a los requisitos y necesidades de la organización. Monitoreo de las aplicaciones, red y dispositivos, para detección de amenazas avanzadas.

5.4. Detección de actividad anómala

Diseño e implementación de controles que permitan identificar irregularidades en el comportamiento de los usuarios o en las transacciones aplicativas, relacionadas con actividades maliciosas o fraudes.

5.5. Protección de datos en procesos de negocio

Implementación de controles disuasivos, detectivos, y correctivos en los procesos de negocio críticos de la organización para proteger sus datos sensibles.

6. Formas de notificación de incidentes

La comunicación con el equipo del Centro de Ciberseguridad IQSec CERT, para el reporte de incidentes se realiza mediante los siguientes mecanismos:

1. Correo electrónico.
    a. cert@iqsec.com.mx.

El correo debe incluir la siguiente información:

- ***Datos de contacto e información de la organización:***
- ***Nombre de la persona y nombre de la organización y dirección, dirección de correo electrónico, número de teléfono:***
- ***Breve resumen del incidente / emergencia / crisis; Tipo de evento:***
- ***Fuente de indicación (es decir, el sistema produjo una alerta, etc.):***
- ***Sistema afectado (es decir, activo de red, etc.):***
- ***Impacto estimado (es decir, pérdida de comunicaciones, etc.):***
- ***Otras particularidades:***

2. Vía telefónica.
    a. Ext. + 52 (55) 4163 1750
3. Vía sistema de tickets.
    a. https://soporte.iqsec.com.mx/sp

7. Descargo de responsabilidad

Se tomarán todas las precauciones y se aplicarán todos los controles necesarios para la preparación y notificación de alertas de seguridad, el equipo Centro de Ciberseguridad IQSec CERT no se responsabiliza por el mal uso o daño resultante del uso de la información contenida.