PERFIL DE CBRT- CERT SE HA ESTABLECIDO EN CUMPLIMIENTO DE RFC-2350.

1. Información del Documento

1.1. Fecha de la última actualización

Esta es la versión 1.0 del 1 de diciembre de 2022.

1.2. Lista de distribución para notificaciones

Los cambios a este documento no se distribuyen por una lista de correo. Cualquier pregunta o comentario específico, por favor diríjase a la dirección de correo **contacto@cbrt.com.do**

2. Información de Contacto

2.1. Nombre del equipo

CERT-CBRT

2.2. Zona horaria

UTC / GMT -4 horas

2.3. Otras telecomunicaciones

Ninguna

2.4. Correo electrónico

Informe de incidentes: *incidentes@cbrt.com.do*
Información de carácter general: info@cbrt.com.do

2.5. Miembros del equipo

Una lista completa de los miembros del equipo CERT-CBRT no está disponible públicamente. Los miembros del equipo se identificarán ante la parte informante con su nombre completo en una comunicación oficial sobre un incidente.

2.6. Otra información

La información general de los servicios proporcionados por el CERT-CBRT y sobre el propio organismo se encuentran publicadas en el portal web **cbrt.com.do**

2.7. Puntos de contacto con el cliente

En cualquier caso, utilice la dirección de correo *info@cbrt.com.do* Nuestro horario de respuesta es 24*7*365 es todos los días de la semana el Oficial de turno está disponible para incidentes y se puede contactar correo incidentes@cbrt.com.do

3. Carta

3.1. Misión

CBRT es una empresa que lleva seguridad como servicio, que considera la información y los datos como un elemento fundamental para la estrategia comercial de sus clientes por tanto es imprescindible responder de una manera eficaz y rápida al momento de detectar alguna violación de seguridad. Por tanto, el CERT-CBRT tiene la misión de proveer el soporte necesario para la respuesta a incidentes en todas sus fases. Realizando sus labores de manera remota o presencial para mantener una gestión centralizada de la seguridad de sus clientes.

3.2. Comunidad Atendida

Los incidentes atendidos por el CERT-CBRT serán aquellos que afecten a sistemas de los clientes internos y externos, así como cualquier otro sistema en el que se procese información clasificada.

3.3. Patrocinio y / o Afiliación

CERT-CBRT está patrocinado por **Cybersecurity Blue & Red Team SRL.** CERT-CBRT busca estar afiliado a instituciones alrededor del mundo con la finalidad de colaborar, compartir información y brindar soporte en la respuesta de incidentes cibernéticos. Está formado por un equipo multidisciplinario y con basta experticia**;**

- Gerente de Operaciones especialista en Ciberseguridad
- Coordinador del Centro de Operaciones(SOC)
- Analistas y especialistas en gestión de incidentes cibernéticos

3.4. Autoridad

El objetivo principal es la coordinación de la respuesta a incidentes y el manejo adecuado que deben tener los clientes como tal asesoramos.

4. Políticas

4.1. Tipos de incidentes y nivel de soporte

CERT-CBRT maneja diferentes tipos de incidentes y sus criterios de determinación de peligrosidad, el nivel de apoyo dependerá de ambos factores y de la gravedad que determine el personal del CERT-CBRT.

4.2. Cooperación, interacción y divulgación de información

CERT-CBRT maneja de manera confidencial toda la información sin importar su prioridad. Aquella información de naturaleza muy sensible solo se comunica y almacena en un entorno seguro y en caso de ser necesario utilizando tecnologías de cifrado. Toda la información suministrada al CERT-CBRT será utilizada para ayudar a resolver incidentes de seguridad. La información solo se distribuirá a otros equipos y miembros según la necesidad de saber y preferiblemente de forma anónima. El CERT-CBRT utiliza el TLP para el intercambio de información.

4.3. Comunicación y autenticación

El método preferido de comunicación es por correo electrónico. incidentes@cbrt.com.do

5. Servicios

5.1 Servicios Reactivos

Estos servicios se activan para el manejo de un incidente, La respuesta a incidentes proporciona disponibilidad 24/7 para coordinar la recuperación de todo tipo de incidentes relacionados con las TIC y

consiste en experiencia, herramientas y otras capacidades para actuar, analizar y comunicarse con las partes interesadas y los medios de comunicación.

- Respuesta a incidentes cibernéticos
- Clasificación del Incidente
- Coordinación del Incidente
- Resolución del Incidente

5.2 Servicios Proactivos

Estos servicios tienen como objetivo provee información oportuna para ayudar a proteger la infraestructura de la comunidad, anticipándose a los ataques cibernéticos. Por tanto, la implementación de estos servicios reducirá el número de incidentes futuros.

- Evaluaciones de ciberseguridad
- Gestión de Riesgos basado en Marcos de Referencia
- Análisis de Vulnerabilidades
- Educación y cultura
- Auditorias y pruebas de penetración holística de 360°
- Protección 360
- Inteligencias de amenazas
- Monitorio en tiempo real 24x7x365 (SOC como Servicio)

6. Formularios De Notificación De Incidentes

Para informar incidente enviar comunicación: *incidentes@cbrt.com.do*

7. Descargos de Responsabilidad

CERT-CBRT toma todas las precauciones en la preparación de información, notificaciones, alertas e informes, pero no asume ninguna responsabilidad por errores u omisiones, ni por danos resultantes del uso de la información suministrada.