ONECYBER

RFC 2350

HOJA DE CONTROL DE DOCUMENTO

TÍTULO	**RFC 2350**
CLASIFICACIÓN	**Pública**
AUTOR	**OneCyber**

REALIZADO POR	FECHA	VERSIÓN	MOTIVO
OneCyberSec	15/05/2024	1.0	
REVISADO POR	**FECHA**	**VERSIÓN**	**MOTIVO**
APROBADO POR	**FECHA**	**VERSIÓN**	**MOTIVO**
Dirección			

CONTROL DE VERSIONES

VERSIÓN	FECHA	REVISOR	RESUMEN DE CAMBIO PRODUCIDOS
1.0	15/05/2024	OneCyber	Primera versión

Contenido

1. INFORMACIÓN DEL DOCUMENTO

Este documento contiene información sobre CSIRT-OneCyber y su estructura se basa en la RFC 2350. La información compartida en este documento describe las responsabilidades, los servicios y otra información relevante sobre CSIRT-OneCyber.

2. INFORMACIÓN DE CONTACTO

2.1. NOMBRE DEL EQUIPO

CSIRT-OneCyber

2.2. DIRECCIÓN

Camino San Lázaro, 174 - Los Rodeos - Edificio Binter 1

38206 San Cristóbal de La Laguna - Santa Cruz de Tenerife

2.3. ZONA HORARIA

UTC +0 / Western European Time (WET)

2.4. TELÉFONO DE CONTACTO

+34 922 985082

2.5. NÚMERO DE FAX

No se dispone de número de fax.

2.6. DIRECCIONES DE CONTACTO

- Reporte y gestión de incidentes: csirt@onecyber.es
- Consultas: info@onecyber.es
- Otros: https://onecyber.es/contacto/

2.7. OTROS MEDIOS DE COMUNICACION

No se dispone de otros medios de comunicación adicionales a los indicados

2.8. CLAVES PÚBLICAS Y CIFRADO

CSIRT-OneCyber emplea para las comunicaciones relacionadas con respuesta a incidentes la dirección csirt@onecyber.es con la siguiente clave PGP:

- Fingerprint: 901B B323 FBCD F272 6D41 6896 74B8 06D5 B600 9029

Esta clave se encuentra disponible en la dirección web https://onecyber.es/csirt

2.9. COMPONENTES DEL EQUIPO

Los nombres y la información de los miembros que forman el CSIRT-OneCyber no se difunden públicamente. En el caso de que se haga un informe, el personal será identificado con su nombre completo a través de una comunicación formal.

2.10. PUNTOS DE CONTACTO

El canal principal de contacto con el CSIRT-OneCyber para la comunicación y gestión de incidentes de seguridad es el correo electrónico, a través de la dirección: csirt@onecyber.es.

Se habilita también el teléfono como medio alternativo, siendo el número el indicado con anterioridad: +34 922 985082

Para otro tipo de comunicaciones se puede utilizar la siguiente dirección: info@onecyber.es

3. OBJETIVOS

3.1. MISIÓN

La misión de CSIRT-OneCyber es posicionarse como un punto neutral de referencia para la respuesta sistemática a los incidentes cibernéticos, con el objetivo de apoyar el desarrollo y la mejora de la seguridad cibernética. OneCyber también fortalecerá la comunicación entre las partes interesadas en ciberseguridad y otros equipos de CSIRT en la región.

CSIRT-OneCyber prestará asistencia a cualquier parte que informe de un incidente con el máximo esfuerzo y llevará a cabo continuamente actividades que aumenten las capacidades de ciberseguridad.

3.2. CIRCUNSCRIPCIÓN

Los servicios ofrecidos por CSIRT-OneCyber están destinados a todas las empresas y/u organizaciones, tanto públicas como privadas, que se suscriban a ellos.

3.3. AFILIACIÓN

El CSIRT-OneCyber está ubicado dentro de la Dirección de Operaciones en el organigrama del OneCyberSec.

3.4. AUTORIDAD

CSIRT-OneCyber actuará voluntariamente para brindar asistencia a cualquier parte que requiera ayuda con cuestiones relacionadas con la ciberseguridad.

4. POLÍTICAS

4.1. Tipos de incidentes gestionados y nivel de soporte proporcionado

El CSIRT-OneCyber ofrece servicios de detección, análisis y respuesta a incidentes de seguridad que afecten la integridad, disponibilidad y/o confidencialidad de la información manejada por los sistemas y procesos de sus clientes. La clasificación de incidentes se basa en las directrices del Centro Criptológico Nacional de España (CCN-CERT) según la Guía de Seguridad de las TIC CCN-STIC 817 del Esquema Nacional de Seguridad (ENS). Estos incidentes se categorizan y priorizan según su tipología y criticidad, estableciendo tiempos de respuesta acordes con esta clasificación. El nivel de soporte proporcionado depende de los acuerdos contractuales con cada cliente. La interacción durante la gestión de incidentes, los canales de comunicación utilizados y el intercambio de información con otros actores, como CSIRTs, se define contractualmente, respetando las regulaciones legales y normativas vigentes.

4.2. Cooperación, interacción y distribución de información

El CSIRT-OneCyber interactúa diariamente con diversos actores, intercambiando información según el papel que desempeñan en su red de relaciones. Estos actores incluyen otros CSIRTs, autoridades legales, fuentes de información e inteligencia, clientes, proveedores, fabricantes y dentro de cada uno de estos grupos, se comunica con una variedad de roles como ingenieros y analistas de seguridad, administradores de sistemas, expertos legales, responsables de seguridad, responsables de recursos humanos y usuarios finales.

Por su relevancia en el ámbito nacional se identifican los siguiente:

- **CCN-CERT** (https://ccn-cert.cni.es): Se le comunican los incidentes relevantes de seguridad de la información y sistemas que afectan a organismos y empresas públicas.
- **INCIBE-CERT** (https://incibe-cert.es): Se le comunican los incidentes relevantes de seguridad de la información y sistemas que afectan a los ciudadanos, organismos y empresas del sector privado.
- **AEPD** (Agencia Española de Protección de Datos - https://www.aepd.es/es): Se le comunican los incidentes en caso de que éste haya puesto en riesgo o provocado la filtración de datos de carácter personal protegidos por el Reglamento.
- **ESPDEF-CERT** (https://emad.defensa.gob.es/unidades/mcce/): Se le comunican los incidentes relevantes de seguridad que pudieran afectar al ámbito de la defensa nacional.

4.3. Comunicación y autenticación

Como se ha establecido con anterioridad en este documento, los canales de comunicación entre el CSIRT-OneCyber y sus clientes son fundamentalmente 2, el correo electrónico y el teléfono,

siendo el primero el utilizado como canal principal y para el intercambio de información con un cierto grado de confidencialidad.

En el caso del correo electrónico, se utilizarán claves PGP para la firma de correos y para el cifrado de la información que por su grado de confidencialidad deba ser protegida.

El teléfono se utilizará sin cifrar, para comunicaciones en las que la información intercambiada tenga un grado bajo de confidencialidad y por tanto no requiera de protección especial. Este tipo de información también podrá ser intercambiada por correo electrónico sin hacer uso del cifrado mediante claves PGP.

5. SERVICIOS PROPORCIONADOS

5.1. Análisis y gestión de vulnerabilidades

Gestión del ciclo de vida de las vulnerabilidades mediante el análisis continuo de la configuración de la infraestructura de nuestros clientes en relación con las amenazas y vulnerabilidades conocidas.

5.2. Detección y análisis de eventos

Alerta temprana a través de la supervisión en tiempo real, correlación de eventos, análisis y notificación ante incidentes de seguridad.

5.3. Concienciación y formación

Simulación de campañas de phishing personalizadas y análisis de las respuestas de los usuarios para evaluar su nivel de concienciación sobre estos ataques. El servicio se complementa con material educativo para los usuarios, con el fin de mejorar su capacidad de detectar y reaccionar ante este tipo de amenazas.

5.4. Auditorías de hacking ético

Análisis profundo de las vulnerabilidades de los sistemas del cliente, donde un experto en ciberseguridad intenta acceder a los sistemas aprovechando las vulnerabilidades existentes y emite un informe detallado.

5.5. Gestión de EDR

OneCyber se especializa en la gestión de múltiples EDR (Endpoint Detection and Response) de diversos fabricantes. Nos encargamos de supervisar, administrar y optimizar estas soluciones de seguridad para proteger los endpoints de nuestros clientes contra amenazas avanzadas. Al gestionar una variedad de EDR, podemos ofrecer una protección integral y personalizada, adaptándonos a las necesidades específicas de cada cliente y garantizando una respuesta rápida y efectiva ante cualquier incidente de seguridad.