RFC 2350: CONTEXTO DEL EQUIPO CSIRT GT

Área de Cumplimiento Normativo

Tipo de documento		**POLÍTICA**	
Versión	**Estado**	**Fecha**	**Autor**
V.0.0	Borrador	12/05/2020	Área de GRC
V.1.0	Derogado	17/11/2020	Área de GRC
V.2.0	Derogado	30/04/2021	Área de Cumplimiento Normativo
V.3.0	Vigente	21/02/2022	Área de Cumplimiento Normativo

USO PÚBLICO

Control de Cambios			
Versión	**Fecha**	**Autor**	**Cambio**
V.1.0	17/11/2020	ALR	*DOC. inicial*
V.2.0	30/04/2021	Cumplimiento Normativo	*Cambio Nomenclatura, actualización del contexto.*
V.3.0	21/02/2022	Cumplimiento Normativo	*Cambio en estructura organizativa*

Índice de contenido

1 OBJETO Y CAMPO DE APLICACIÓN

El presente documento tiene como objeto identificar y describir el contexto en el que el Equipo de Respuesta a Incidentes de Seguridad Informática de Global Technology, en adelante CSIRT Global Technology o CSIRT GT, lleva a cabo sus funciones, a través de la identificación de las siguientes cuestiones:

- Estructura de la organización, establecimiento y marco organizativo del equipo CSIRT GT.
- Identificación del equipo, composición, misión y servicios prestados.
- Ámbito de actuación y posibles receptores del servicio.

2 DOCUMENTACIÓN

2.1 Estándares y regulaciones externas

Para la redacción de este procedimiento se ha tomado como base de referencia la RFC 2350 del CCN-CERT.

2.2 Principal legislación

- N/A

2.3 Documentación de referencia

- ***Fichas de perfil de puestos.***

3 TÉRMINOS Y DEFINICIONES

- **CSIRT,** o equipo de respuesta a incidentes de seguridad informática: Este es un nombre genérico para describir un equipo de respuesta a incidentes. Su función es idéntica a una CERT o Equipo de Respuesta a Emergencias Informáticas, pero, "CERT" es una marca registrada mundial del Centro de Coordinación CERT (CERT/CC), que pertenece al Software Engineering Institute (SEI) de la Universidad Carnegie Mellon (CMU) en los EE.UU.
- **SOC,** Centro de Operaciones de Seguridad, es Un área física o sala en un edificio donde se lleva a cabo la monitorización en tiempo real, el control de la seguridad y el envío y coordinación de incidentes de las redes y el flujo de Internet.
- **Áreas de servicios:** las áreas de servicio agrupan los servicios relacionados con un aspecto común.
- **Servicio:** es un conjunto de funciones reconocibles y coherentes orientadas hacia un resultado específico.
- **Función**: es una actividad o conjunto de actividades destinadas a cumplir el propósito de un servicio en particular. Cualquier función puede ser compartida y utilizada en el contexto de varios servicios.

4 DESCRIPCIÓN

Desde sus inicios en 2009 el Equipo de Seguridad Gestionada SOC de Global Technology viene desempeñando servicios especializados de ciberseguridad. El CSIRT Global Technology como equipo especializado nace de la evolución y restructuración de los servicios prestados en materia de ciberseguridad y seguridad de la información bajo un marco único de gestión, con el objetivo de prestar a sus clientes, de manera más eficaz y coordinada, un servicio que abarque de íntegramente la gestión de incidentes de ciberseguridad.

Desde sus inicios hasta la actualidad Global Technology aboga por la mejora continua y el desarrollo de su equipo profesional, potenciando la formación y aprendiendo de las experiencias en el desempeño de sus funciones. Esta dedicación ha derivado en un equipo plenamente integrado y coordinado, de carácter multidisciplinar que aborda la ciberseguridad y la gestión de incidentes de manera holística e integral bajo los máximos estándares de seguridad nacional e internacionalmente reconocidos. prueba de ello, son las diferentes certificaciones de reconocido prestigio con los que cuenta la organización, como lo son:

- ISO/IEC 27001
- ISO/IEC 27701
- ISO 9001
- ISO 14001
- ENS NIVEL MEDIO

4.1 Identificación del Equipo

4.1.1 Datos de identificación

- ***Nombre del Equipo:*** *GLOBAL TECHNOLOGY CSIRT (CSIRT-GT)*
- ***Dirección:***
  - C/ Libreros, 48, 2º izq.
  - 28801 - Alcalá de Henares (Madrid)
- ***Zona Horaria:*** *CET UTM +0100 / CEST UTM +0200*

4.1.2 Datos de Contacto

- ***Teléfono de información:*** *900 809 401*
- ***Direcciones de Correo Electrónico:***
  - Consultas de carácter general: administracion@globalt4e.com
  - Otras direcciones de correo electrónico para contactar: se les proporciona a las partes interesadas en función de las características de la prestación de servicios pactada.
- ***Otras Comunicaciones:*** Una vez establecida la relación de servicios Global Technology habilita para sus clientes todas aquellas comunicaciones necesarias para la prestación de los mismos, como teléfono de emergencias, repositorios de información, herramientas de videoconferencia, conexiones de red seguras, uso de SMS u otras en función de las necesidades específicas del cliente y/o servicio.

4.1.3 Claves *Públicas* y cifrado de información

Global Technology hace uso de diferentes tecnologías y herramientas para el cifrado de las comunicaciones, entre las que se encuentran las herramientas de cifrado usadas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia (CCN-CERT) y el Instituto Nacional de Ciberseguridad de España (INCIBE-CERT). Las herramientas de cifrado, los correos de contacto y claves PGP asociadas se facilitan a los clientes y partners una vez establecida las relaciones contractuales y a otras partes interesadas previa solicitud y acuerdo de las partes.

4.1.4 *Horario de Atención:*

El equipo de respuesta a incidentes está disponible en función de los servicios contratados, en los siguientes horarios:

- ***Consultas sobre servicios:*** horario de oficina (9.00h-18.30h)
- ***Incidentes catalogados con peligrosidad baja o media:*** Servicio 12x5 (8.00h-20.00h)
- ***Incidentes catalogados con peligrosidad alta o crítica***: Servicio de guardia de 24x7x365.

4.1.5 *Puntos de contacto para la comunidad:*

La comunicación entre el Equipo del CSIRT GT y los organismos a los que da soporte se realiza principalmente a través de:

- Herramienta de Ticketing.
- *Buzón de correo electrónico de soporte.*
- Teléfono de contacto directo.
- Teléfono de emergencias.

Además, Global Technology cuenta con un *Buzón de recepción de informes de vulnerabilidades a disposición del público en general para todo aquel que desee informar sobre una vulnerabilidad que pueda afectar a sus sistemas o los de sus clientes:* infovulnerabilidades@globalt4e.com

4.1.6 *Más Información:*

La información general sobre los servicios proporcionados se encuentra detallado en el *Marco de Servicios* publicado en la web corporativa. https://www.globalt4e.com/

4.2 Marco del CSIRT GT y Ámbito de actuación

4.2.1 *La Misión*

El objetivo principal del CSIRT GT es brindar a sus clientes una amplia gama de servicios orientados a la seguridad de la información y la ciberseguridad, con una visión holística e integral. Contribuyendo de manera proactiva a la mejora continua de su ciberseguridad, y aportando los instrumentos necesarios para dar una respuesta rápida y eficiente frente a las ciberamenazas.

4.2.2 Ámbito de actuación y Sectores de actividad

El CSIRT GT es un equipo de carácter comercial, que presta sus servicios dentro del territorio nacional, y ocasionalmente en proyectos internacionales, en una gran variedad de sectores de actividad entre los que se encuentran, sin limitarse a ellos, los siguientes:

- Administraciones públicas.
- Empresas del sector TIC.
- Transportes.
- Finanzas.
- Alimentación.
- Empresas aseguradoras.
- Educación.

De entre los que destacan sus servicios a Infraestructuras Críticas de algunos de los sectores anteriormente mencionados.

4.2.3 Autoridad

El CSIRT GT ofrece asesoramiento constante a sus clientes en materia de seguridad de la información y ciberseguridad, llevando a cabo aquellas acciones que requieran sus clientes a nivel operativo, técnico y administrativo. Teniendo siempre dicho cliente la potestad principal y ultima de decisión sobre las acciones a realizar.

4.2.4 Responsabilidad

El equipo contribuye a la mejora de la seguridad de la información de sus clientes y ciberseguridad. Además de proporcionar recomendaciones y avisos técnicos y operativos, sensibilización, formación y consultoría en la materia, tanto a sus clientes como a su entorno operativo, contribuyendo y promoviendo la cultura de ciberseguridad.

4.3 Estructura organizativa

4.3.1 Situación orgánica

Las instalaciones del CSIRT GT se sitúan en las oficinas principales de Global Technology ubicadas en Calle Libreros 48, Alcalá de Henares (Madrid) y en las instalaciones de polígono Malpica, calle F, oeste, #73 (Zaragoza). en ambas sedes se cuenta con Centro de Operaciones de Ciberseguridad “SOC”. El SOC se coordina con el resto de las áreas de la organización para la prestación de servicios. De manera que, el CSIRT presta servicio de forma mixta, tanto a la propia entidad a nivel interno, atendiendo las necesidades del resto de

departamentos y áreas; como al entorno externo, atendiendo a las necesidades de todos los clientes de Global Technology.

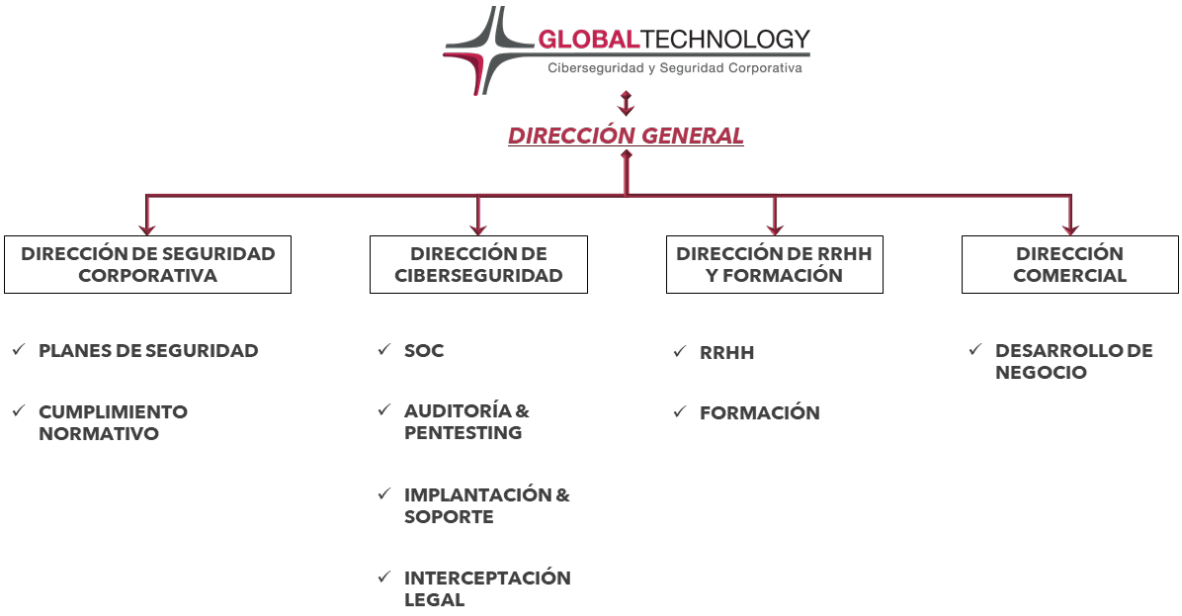

Gráfico 1: *Organigrama general.*

4.3.2 Estructura del CSIRT y Composición del equipo

El Equipo está compuesto por personal especializado de las diferentes áreas en materia de seguridad de la información y ciberseguridad, que trabajan de manera coordinada en función de las circunstancias particulares y las demandas de la actividad / servicio en particular, se nutre de la colaboración con otras áreas de la organización para el desempeño de los servicios, a través de equipos de trabajo multidisciplinares y especializados en función de las características del proyecto.

Esta metodología proporciona un elemento clave para la prestación de servicios totalmente a medida, en función de sus necesidades del cliente, aportando una visión de carácter integral de las necesidades y las posibles soluciones, obteniendo un resultado eficaz y de calidad de una forma más eficiente.

4.3.2.1 Liderazgo del Equipo CSIRT

El liderazgo del equipo CSIRT GT recae sobre el Director General como representante de la organización, a nivel operativo el Responsable SOC es el encargado de dirigir y coordinar las acciones operativas de los diferentes equipos que conforman el CSIRT, así como de solicitar el apoyo de las otras áreas cuando sea pertinente. En conexión directa con la Dirección de Ciberseguridad.

4.3.2.2 Equipos que lo conforman

A grandes rasgos el CSIRT Global Technology se estructura en diferentes equipos funcionales tal y como muestra el *gráfico 2, a continuación:*

- ***El equipo de Gestión de Crisis:*** integrado por los responsables/coordinadores de los diferentes equipos, el apoyo de las otras áreas y la participación del director de operaciones en contacto directo con la dirección general conforma un comité de gestión especializada y respuesta inmediata ante una posible crisis.
- ***Equipo de Gestión de Incidentes:*** es el equipo principal del CSIRT GT y el núcleo de prestación de los servicios ofertados, en él se integra el equipo SOC formados por Técnicos de sistemas de nivel 1 y 2, los cuales realizan las funciones de Gestión de Eventos y Vulnerabilidades, con el apoyo y en interacción continua con los profesionales más especializados de la organización en materia de gestión de incidentes, que conforman el nivel 3 de dicho servicio.
- ***Equipo de Auditoria y Pentesting:*** dicho equipo está compuesto por profesionales especializados en Auditoría de sistemas de información, Hacking Ético y análisis forense.
- ***Equipo de implantación y Soporte:*** realiza diferentes funciones destinadas a la implantación de soluciones de seguridad y al soporte técnico proactivo y reactivo tanto de las soluciones implementadas como de los servicios.
- **Apoyo interno:** cuenta con personal integrado en otras áreas de la organización como lo son el equipo de Cumplimiento Normativo, el de Seguridad Corporativa y el de Formación, que trabajan conjuntamente con el CSIRT para aunar esfuerzos, aportando diferentes puntos de vista, para prestar un servicio aún más especializado principalmente en las áreas de Conciencia situacional y Transferencia de conocimientos.

4.3.2.3 Roles y responsabilidades

Los roles y responsabilidades de cada uno de los integrantes del equipo se encuentran detallados en las *fichas de perfil de puestos* desarrolladas por la organización, estás se encuentra a disposición de las partes interesadas bajo solicitud en función de sus necesidades, previa autorización.

4.3.2.4 Competencias personales

A grandes rasgos, el espíritu de Global Technology promueve un equipo flexible, creativo, con fuertes habilidades analíticas, con un afincado sentido de la profesionalidad y la confidencialidad; y grandes capacidades de adaptación para explicar asuntos de dificultad técnica de manera ágil y sencilla a todo tipo de públicos.

4.3.3 Modelo de financiación establecido

Al ser un equipo comercial, el CSIRT Global Technology se autofinancia a través de los servicios que presta a sus clientes, así como siendo beneficiario

de la partida presupuestaria que la organización destina anualmente al proyecto y su mejora continua.

4.4 Políticas

Desde el año 2016, Global Technology cuenta con la certificación ISO/IEC 27001 de su Sistema de Gestión de Seguridad de la Información implementado para su servicio de seguridad gestionada, este sistema se estructura en múltiples políticas y procedimientos operativos que tienen como objetivo definir e implementar las mejores prácticas en la materia tomando la norma como referencia. Entre ellas destacan La política de:

- Clasificación, Tratamiento y Etiquetado de la Información.
- Uso Aceptable y Responsable de los Activos de información.
- Gestión de Acceso Lógico a sistemas y aplicaciones.
- Seguridad Física y Áreas Seguras
- Gestión de Incidentes.
- Gestión de Vulnerabilidades.
- Gestión de Parches.
- Copias de Seguridad.
- Plan de Continuidad del Negocio.

4.4.1 Tipo de Incidentes y nivel de soporte:

Los servicios prestados por el equipo CSIRT GT proporcionan asesoramiento y resolución para todo tipo de incidentes en materia de seguridad de la información y ciberseguridad. Categorizando los mismos en función de sus características haciendo uso de la taxonomía de Referencia empleada por el Incibe-Cert (Enlace) para la Clasificación de Incidentes de Seguridad.

Dependiendo de los servicios contratados por el cliente, las acciones llevadas a cabo, por parte del equipo, abarcan parte o todo el ciclo de vida de la gestión de incidentes.

4.5 Cooperación con otros equipos

El CSIRT GT colabora con otros equipos especializados en la mejora de la seguridad, para ello puede compartir la naturaleza de los incidentes detectados en el ejercicio de sus funciones y los métodos de actuación llevados a cabo para su resolución. no obstante, se considera información confidencial cualquier dato que pueda comprometer los sistemas de información o identificar a nuestros clientes no compartiendo ningún tipo de información relevante a los mismos, salvo consentimiento previo. Tal y como establece la política de divulgación de vulnerabilidades de la organización ***GT-CSIRT-PL08-Política de informe y divulgación de vulnerabilidades.***

4.6 Marco de Servicios

Los servicios proporcionados por Global Technology *se encuentran identificados en la web corporativa de la organización.*

5 ROLES Y RESPONSABILIDADES

La Dirección de Global Technology: prestar al CSIRT GT el apoyo necesario para el desempeño de sus funciones y la mejora continua.

Todos los Equipos: prestar los servicios bajo los mayores estándares de calidad y seguridad de la información, llevando a cabo la misión del CSIRT GT de la mejor manera posible.

6 REGISTROS

El cumplimiento con lo establecido en este documento queda registrado a través de todas las políticas y procedimientos establecidos en la organización, que forman parte de los sistemas de gestión.

7 ANEXOS

- N/A.