ACD-TRC

DOCUMENTO DE CONSTITUCION

Pasión por la tecnología

DATOS DE CONTROL

CLIENTE	TRC
REFERENCIA	
TIPO DE TRABAJO	DOCUMENTACIÓN INTERNA
FECHA	02/01/2024

REALIZADO POR	SUPERVISADO POR	AUTORIZADO POR	REVISADO POR
EMILIO RICO			

REGISTRO DE EDICIONES

EDICIÓN	FECHA	PARTES QUE CAMBIAN	DESCRIPCIÓN DE CAMBIOS
V1	02/01/2024	n.a.	n.a.

ÍNDICE DE CONTENIDO

1. INTRODUCCION.

El presente documento tiene como objetivo establecer y definir las políticas, responsabilidades, procedimientos y recursos necesarios para la operación efectiva del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) de la empresa TRC.
El documento está organizado conforme al modelo recomendado por la RFC 2350 de IETF, disponible en:

- https://tools.ietf.org/html/rfc2350.

1.1 Alcance.

Este documento se aplica a todo el personal, recursos y sistemas de información de la empresa TRC que estén involucrados en la detección, respuesta y mitigación de incidentes de seguridad informática.

1.2 Destinatarios.

Los destinatarios del presente documento son los clientes del ACD-TRC, además de cualquier otro CSIRT constituido u organización con un interés legítimo en los servicios provistos, y el público en general. En consecuencia, el documento puede ser distribuido libremente, estando sujeto exclusivamente a controles de copyright.

1.3 Localizaciones de este documento.

El documento es accesible públicamente a través del sitio web de TRC, en concreto en la sección correspondiente al ACD-TRC: https://www.grupoTRC.com/csirt

1.4 Autenticación del documento.

Este documento ha sido firmado con la clave PGP de la cuenta **csirt@grupotrc.com** del ACD-TRC. Tanto la clave pública como la firma se encuentran disponibles en la página web del ACD-TRC: https://www.grupoTRC.com/csirt

2. INFORMACION DE CONTACTO.

2.1 Nombre del equipo

- ACD-TRC

2.2 Dirección del equipo

Calle Albasanz 25, 28037 Madrid. España

2.3 Zona horaria

Madrid, España (UTC+1)

2.4 Teléfono de contacto

Se habilita el siguiente número de teléfono como medio alternativo:

- +34 912 670 105

2.5 Direcciones de correo electrónico.

Gestión de incidentes: **csirt@grupotrc.com**

2.6 Claves públicas.

ACD-TRC emplea la siguiente dirección de correo para las comunicaciones relacionadas con la respuesta a incidentes:

- csirt@grupotrc.com
- clave PGP: 399BE493235E667BF458C56047514C227B278F0F

Para comunicaciones administrativas o consultas se emplea la dirección:

- sat@grupotrc.com asociada
- clave PGP: 6B23B2435EA762A96B81C515C169CB4A3035100D

Estas claves públicas se encuentran disponibles en página web del CSIRT.

2.7 Miembros del equipo.

No se facilitará ninguna información acerca de los miembros del equipo que constituye el CSIRT

3. MISION.

3.1 Propósito

El ACD-TRC es un CSIRT privado que se crea por mandato de la Dirección del Grupo TRC, con el objetivo de prestar servicio tanto interno (CSIRT interno) como externo a otros organismos y empresas, ya sean éstas públicas o privadas (CSIRT comercial). El ACD-TRC tiene como misión dar respuesta a los retos de ciberseguridad, poniendo a disposición de todo el Grupo TRC y de sus clientes externos los servicios de seguridad necesarios para proteger sus sistemas de información ante incidentes de seguridad que pudiesen llegar a afectar la integridad, confidencialidad o disponibilidad de la información y/o dañar las operaciones o reputación de los afectados.

El propósito que los servicios del ACD-TRC pretende proporcionar a sus clientes consisten en:

- Mejorar la visibilidad en tiempo real de su situación de ciberseguridad.
- Anticiparse a posibles amenazas y reducir la superficie de ataque.
- Detectar de forma temprana los incidentes y contenerlos rápidamente.
- Responder eficazmente ante incidentes de seguridad y limitar el impacto.
- Recuperar la actividad en el menor tiempo posible.

3.2 Funciones

3.2.1 Respuesta a Incidentes de Ciberseguridad

- Detección y análisis de incidentes de seguridad cibernética.
- Coordinación y ejecución de la respuesta a incidentes cibernéticos.
- Mitigación y recuperación de sistemas afectados.
- Evaluación post-incidente y lecciones aprendidas.

3.2.2 Inteligencia de Ciberamenazas

- Recopilación y análisis de inteligencia de ciberamenazas.
- Evaluación de la exposición a amenazas emergentes.
- Colaboración con fuentes externas para obtener inteligencia relevante.
- Implementación de medidas proactivas basadas en inteligencia.

3.2.3 Educación y Concientización en Ciberseguridad

- Desarrollo y entrega de programas de concientización en ciberseguridad.
- Capacitación continua para empleados sobre las últimas amenazas y buenas prácticas.

3.3 Actividad desarrollada

Para conseguir su misión, el ACD-TRC

- Cuenta con personal altamente cualificado y con experiencia en materia de seguridad de la información, con capacidad para la prestación de los servicios ofertados, así como de analizar y responder adecuadamente ante cualquier incidente de seguridad.
- Dispone de un conjunto de procedimientos y herramientas necesarios y adecuados para la prestación de los servicios ofertados y alineados con el cumplimiento de la normativa legal.

- Realiza una monitorización continua, reduciendo los tiempos de detección de posibles incidentes, identificando qué amenazas requieren de intervención inmediata, y discriminando los falsos positivos.
- Realiza tareas proactivas y preventivas para la mejora de la seguridad de sus clientes.
- Intercambia información técnica sobre incidentes con otros CERT / CSIRTs para así mejorar la respuesta conjunta ante los mismos.
- Ejecuta periódicamente procesos de auditoría de Calidad y Seguridad sobre los servicios suministrados, tomando como base los estándares y normativas comúnmente reconocidos en el sector.
- Aplica las mejores prácticas comúnmente reconocidas en el sector

Todos los servicios de seguridad gestionados que se ofrecen desde el SACD-TRC a los clientes y/o sus sistemas de información, tienen el ENS de nivel medio.

4. Circunscripción.

Los servicios proporcionados por ACD-TRC están dirigidos a todos los departamentos, unidades y servicios de las empresas pertenecientes al Grupo TRC, así como a las empresas y/u organismos externos, ya sean públicos o privados, que se suscriban a los mismos.

4.1 Autoridad

El ACD-TRC está ubicado dentro de la Dirección de Ciberseguridad del Grupo TRC. El ACD-TRC opera, dentro del Grupo TRC, bajo la autoridad del Responsable de la Seguridad de la Información Corporativo y de la Dirección de Ciberseguridad.

5. Políticas.

5.1 Tipos de incidentes gestionados y nivel de soporte proporcionado.

El ACD-TRC está autorizado para atender todo tipo de incidencias de seguridad informática que se produzcan en su circunscripción.

La tipología de los incidentes de seguridad gestionados se corresponde con lo establecido por el Centro Criptológico Nacional de España, CCN-CERT, tomando como referencia la Guía de Seguridad de las TIC CCN STIC 817 de Gestión de Ciberincidentes en el ámbito del Esquema Nacional de Seguridad (ENS), disponible en la dirección:

- https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

El nivel de soporte prestado en cada caso dependerá de lo establecido contractualmente con cada cliente del ACD-TRC.

Los recursos se asignarán de acuerdo con las siguientes prioridades:

- Amenazas a la seguridad física de los seres humanos.
- Ataques a nivel de raíz o de sistema a cualquier sistema de información de gestión o cualquier parte de la infraestructura de la red troncal.
- Ataques a nivel de raíz o de sistema en cualquier máquina de servicio público grande, ya sea multiusuario o de propósito dedicado.
- Compromiso de cuentas de servicios confidenciales restringidas o instalaciones de software, en particular aquellas utilizadas para aplicaciones MIS que contienen datos confidenciales, o aquellas utilizadas para la administración del sistema.
- Ataques de denegación de servicio sobre cualquiera de los tres elementos anteriores. Cualquiera de los anteriores en otros sitios, con origen en la circunscripción de ACD-TRC .
- Ataques a gran escala de cualquier tipo.

- Amenazas, acoso y otros delitos penales que involucren cuentas de usuarios individuales.
- Compromiso de cuentas de usuarios individuales en sistemas multiusuario.
- Compromiso de los sistemas de escritorio.
- Falsificación y tergiversación, y otras violaciones de las normas y regulaciones locales relacionadas con la seguridad.
- Denegación de servicio en cuentas de usuarios individuales.

Los tipos de incidentes distintos de los mencionados anteriormente se priorizarán según su aparente gravedad y extensión.

Tenga en cuenta que no se brindará soporte directo a los usuarios finales; se espera que se comuniquen con su administrador del sistema, administrador de red o jefe de departamento para obtener ayuda. En la mayoría de los casos, el CSIRT del Grupo TRC proporcionará indicaciones sobre la información necesaria para implementar las medidas adecuadas.

ACD-TRC se compromete a mantener a la comunidad informada sobre posibles vulnerabilidades y, cuando sea posible, informará a esta comunidad de dichas vulnerabilidades antes de que sean explotadas activamente.

5.2 Cooperación, interacción y distribución de información.

El ACD-TRC interactúa en su operativa diaria con otros CSIRTs, autoridades legales, fuentes de información e inteligencia, organizaciones clientes, proveedores, fabricantes, etc. Pero especialmente con los tres (3) CERT nacionales de referencia:

- CCN-CERT (**https://ccn-cert.cni.es),** al que se comunican los incidentes relevantes de seguridad de la información y sistemas que afectan a organismos y empresas públicas.
- INCIBE-CERT (**https://incibe-cert.es**), al que se comunican los incidentes relevantes de seguridad de la información y sistemas que afectan a los ciudadanos, organismos y empresas del sector privado.
- ESPDEF-CERT (**https://emad.defensa.gob.es/unidades/mcce/**), al que se comunican los incidentes relevantes de seguridad que pudieran afectar al ámbito de la defensa nacional.

Adicionalmente, para aquellos casos en que el incidente haya puesto en riesgo o provocado la filtración de datos de carácter personal protegidos por el Reglamento General de Protección de Datos (RGPD) europeo y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) que regula el tratamiento de datos de carácter personal en España, se efectuaran las diligencias necesarias con la Agencia Española de Protección de Datos, AEPD (**https://www.aepd.es/es**),

Además, se considera fundamental establecer relaciones formales de cooperación con otros CSIRTs, por lo que en el momento de redacción de este documento se está iniciando el proceso para formar parte de la comunidad Trusted Introducer (https://www.trusted-introducer.org) a nivel europeo y CSIRT.es (https://csirt.es/) a nivel nacional.

Para facilitar la cooperación, distribución e intercambio de información con clientes, organismos u otros CSIRTs, se hará uso del protocolo FIRST TLP (https://www.first.org/tlp), para el etiquetado de la información

El ACD-TRC se compromete a no compartir información con otras partes sin un acuerdo y autorización previos del propietario de la misma, salvo en los supuestos en los que exista una obligación legal o normativa superior que obligue a compartir dicha información.

Como medidas adicionales, además de lo anterior, el ACD-TRC se compromete a:

- Aplicar en todo momento las medidas técnicas y legales adecuadas para la protección de la información.
- Anonimizar dentro de lo posible la información compartida y dentro de la misma seleccionar exclusivamente datos relevantes para la resolución de los incidentes.
- Proteger la privacidad de la información personal y siempre dentro de los supuestos recogidos en las normativas europea y española de protección de datos personales.
- Detener la distribución de información en el momento en que el propietario de la misma notifique la denegación del permiso para ello (salvo en los supuestos en los que exista una obligación legal o normativa superior que obligue a compartir dicha información).

5.3 Comunicación y Autenticación

Teniendo en cuenta el tipo de información que probablemente tratará el CSIRT del Grupo TRC, los teléfonos se considerarán suficientemente seguros para su uso, aunque no estén cifrados. El correo electrónico no cifrado no se considerará particularmente seguro, pero será suficiente para la transmisión de datos de baja sensibilidad. Si es necesario enviar datos altamente sensibles por correo electrónico, se utilizará PGP. Las transferencias de archivos por red se considerarán similares al correo electrónico a estos efectos: los datos confidenciales deben cifrarse para su transmisión.

Cuando sea necesario establecer cierto grado de confianza, y siempre antes de revelar información confidencial, se verificará la identidad de la otra parte. Dentro de la comunidad y con sitios vecinos conocidos, las referencias de personas conocidas y de confianza serán suficientes para identificar a alguien. De lo contrario, se utilizarán métodos apropiados, como una búsqueda de miembros de FIRST, el uso de WHOIS y otra información de registro de Internet, etc., junto con llamadas telefónicas o correos electrónicos para garantizar que la otra parte no sea un/a impostor/a. Los correos electrónicos entrantes cuyos datos deben ser confiables se verifican personalmente con el remitente o mediante firmas digitales (en particular, se admite PGP).

6. Servicios proporcionados.

6.1 Respuesta a incidentes.

ACD-TRC ayudará a los administradores de sistemas en la gestión de los aspectos técnicos y organizativos de las incidencias. En particular, prestará asistencia o asesoramiento respecto de los siguientes aspectos de la gestión de incidentes:

6.1.1 Clasificación de incidentes

Las actividades de clasificación de incidentes incluyen:

- Evaluación de informes: interpretación de los informes de incidentes entrantes, su priorización y relación con los incidentes y tendencias en curso.
- Verificación - Apoyo en la determinación de si realmente ha ocurrido un incidente y su alcance.

6.1.2 Coordinación de incidentes

Las actividades de coordinación de incidentes incluyen:

- Categorización de la información: Categorización de la información relacionada con incidentes (archivos de registro, información de contacto, etc.) con respecto a la política de divulgación de información.
- Coordinación - Notificación a las partes involucradas según sea necesario, según la política de divulgación de información.

6.1.3 Resolución de Incidentes

Las actividades de resolución de incidentes incluyen:

- Asistencia técnica: esto puede incluir análisis de sistemas comprometidos.
- Erradicación - Eliminación de la causa de un incidente de seguridad y sus efectos.

Además, ACD-TRC recopilará estadísticas sobre incidentes que ocurran dentro o involucren a la comunidad, y notificará a la comunidad según sea necesario para ayudarla a protegerse contra ataques conocidos.

6.2 Actividades proactivas.

ACD-TRC participará en servicios proactivos con el objetivo de reducir el número de incidencias reales proporcionando información adecuada y adecuada sobre posibles incidencias a la ciudadanía. ACD-TRC realizará actividades proactivas para mejorar el rendimiento y las capacidades, tales como:

- Servicios de información.
- Actividades de formación y simulación.
- Análisis forense y de malware.
- Coordinación y contextualización de Ciber Inteligencia.
- Caza de amenazas.

7. Comunicación de Incidentes.

Cuando un cliente detecta un evento o incidente de seguridad, se lo reportará al ACD-TRC a través del correo **csirt@grupotrc.com**, como se ha indicado anteriormente.

Las medidas de confidencialidad serán las establecidas con cada cliente al inicio de la prestación del servicio y deberán incluir la máxima información disponible con arreglo a lo siguiente:

NOTIFICAR	DESCRIPCIÓN
Asunto	Descripción general el incidente.
Descripción	Descripción detallada de lo sucedido
Fecha y Hora del Incidente	Indicar con la mayor precisión posible cuándo ha ocurrido el incidente
Fecha y hora de detección	Indicar con la mayor precisión posible cuándo se ha detectado el incidente
Clasificación de taxonomía del incidente	Posible clasificación del incidente en función de la taxonomía descrita. Esta clasificación se determina en el Procedimiento de Gestión de Incidentes de Seguridad del ACD-TRC, y será entregada a cada cliente por la vía estipulada con cada uno de ellos al inicio de la prestación del servicio.
Categorización de impacto del incidente	Impacto estimado en la entidad, en función del nivel de afectación del incidente. Esta categorización se determina en el Procedimiento de Gestión de Incidentes de Seguridad del ACD-TRC, y será entregada a cada cliente por la vía estipulada con cada uno de ellos al inicio de la prestación del servicio.
Recursos afectados	Indicar la información técnica sobre el número y tipo de activos afectados por el incidente, incluyendo toda la información posible entre la siguiente: ▪ Número de ordenadores, servidores o dispositivos afectados ▪ Nombre del equipo e IP ▪ Función del equipo ▪ Zona horaria ▪ Hardware ▪ Sistema operativo ▪ Software afectado ▪ Ficheros afectados ▪ Configuración de seguridad ▪ Protocolo/puerto
Origen del incidente	Indicar la causa del incidente si se conoce, por ejemplo, apertura de un fichero sospechoso, conexión de un dispositivo USB, acceso a una página web maliciosa, etc.
Adjuntos	Incluir documentos adjuntos que puedan aportar información que ayude a conocer la causa del problema o a su resolución (capturas de pantalla, ficheros de registro de información, correos electrónicos, etc.).

Madrid, a 5 de enero de 2024

Fdo: ALFREDO ESTIRADO BRONCHALO
CONSEJERO DELEGADO GRUPO TRC

Grupo TRC.
c/ Albasanz 25. 28037. Madrid
www.grupotrc.com
CONTACTO:
Mail: grupotrc@grupotrc.com
Tlf: 91 267 00 00