satec_

RFC 2350

CSIRT-SATEC

Proyecto: CSIRT-SATEC
Nivel de seguridad: N0 - Público
Fecha: 11/02/2022, **Versión**: 1.0

REGISTRO DE CAMBIOS

VERSIÓN	FECHA	REVISOR	RESUMEN DE LOS CAMBIOS PRODUCIDOS
1.0	11/02/2022	SATEC	**Primera versión**

ÍNDICE

1_ DIFUSIÓN

1.1. Destinatarios del documento

Los destinatarios del presente documento son los clientes del CSIRT-SATEC, 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.

1.2. Introducción

El presente documento contiene toda la información que el CSIRT-SATEC considera relevante para los potenciales destinatarios del documento descritos en el apartado anterior. El documento está organizado conforme al modelo recomendado por la RFC 2350 de IETF, disponible en **https://tools.ietf.org/html/rfc2350**.

1.3. Fecha de la última actualización

La fecha de última actualización, junto con la evolución de versiones del documento y los cambios introducidos en cada una de ellas, se reflejan en el apartado **Registro de Cambios** del propio documento.

1.4. Localizaciones en las que se puede acceder al documento

El documento es accesible públicamente a través del sitio web de Satec, en concreto en la sección correspondiente al CSIRT-SATEC:

https://www.satec.es/csirt/

1.5. Autenticación del documento

Este documento ha sido firmado con la clave PGP de la cuenta **incidentes.ciberseguridad@satec.es** del CSIRT-SATEC. Tanto la clave pública como la firma se encuentran disponibles en la página web del CSIRT-SATEC:

https://www.satec.es/csirt/

1.6. Lista de distribución para notificaciones

No existe una lista de distribución para notificar cambios en este documento. Las nuevas versiones, cuando se generen, sustituirán a la anterior en **https://www.satec.es/csirt/.**

2_ Información de contacto

2.1. Nombre del equipo

CSIRT-SATEC.

2.2. Dirección

Avda. de Europa, 34 A

28023 Aravaca (Madrid)

España

2.3. Zona horaria

Europa Central (CET/CEST)

2.4. Teléfono de contacto

+34 901 116 529

2.5. Número de fax

No se dispone de número de fax.

2.6. Direcciones de correo electrónico

Reporte y gestión de incidentes: **incidentes.ciberseguridad@satec.es**
Consultas: **consultas.ciberseguridad@satec.es**

2.7. Otros medios de comunicación

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

2.8. Claves públicas y cifrado

CSIRT-SATEC emplea para las comunicaciones relacionadas con respuesta a incidentes la dirección incidentes.ciberseguridad@satec.es con la siguiente clave PGP:

Fingerprint: 81FA CBD8 1F93 8C24 D060 04E1 8373 BA36 4A43 9163

Esta clave se encuentra disponible en la dirección web anteriormente mencionada en este documento. El cifrado PGP debe ser empleado en todas las comunicaciones por correo electrónico que, dado su nivel de confidencialidad, así lo requieran.

Para comunicaciones administrativas o consultas se emplea la dirección consultas.ciberseguridad@satec.es asociada a la siguiente clave PGP:

Fingerprint: 70B3 B733 A74E 0C8C FA55 D59B 6089 5C0E 7C75 04D6

2.9. Componentes del equipo

El equipo se encuentra constituido por personal desempeñando los siguientes perfiles:

- CSIRT Security Analyst (nivel N1)
- CSIRT Security Analyst (nivel N2)
- CSIRT Security Analyst (nivel N3)
- CSIRT Security Trainer
- CSIRT Administrator
- CSIRT N1 Technical Manager
- CSIRT Technical Manager
- CSIRT Architect
- CSIRT Process Consultant
- Satec Group Legal Consultant
- Satec Group IT & Multicustomer Services Director
- Satec Group Executive Technical Director
- Satec Group Finance Director

Por razones de privacidad el listado de personal perteneciente al equipo no se publica en este documento.

2.10. Horas de funcionamiento

El CSIRT-SATEC funciona en horario 24x7.

2.11. Información adicional

Para encontrar información adicional relacionada con el CSIRT-SATEC puede consultarse el sitio web de Satec, y más en concreto la sección del CSIRT: **https://www.satec.es/csirt/**

2.12. Puntos de contacto

El canal principal de contacto con el CSIRT-SATEC para la comunicación y gestión de incidentes de seguridad es el correo electrónico, a través de la dirección: **incidentes.ciberseguridad@satec.es**

Se habilita también el teléfono como medio alternativo, siendo el número el indicado con anterioridad:

+34 901 116 529

Para otro tipo de comunicaciones se puede utilizar la siguiente dirección: **consultas.ciberseguridad@satec.es**

3_ Objetivos

3.1. Misión

Las organizaciones cuentan con entornos cada vez más complejos, ligados a unos exigentes requisitos de flexibilidad y disponibilidad respecto a los modelos de consumo de las aplicaciones y servicios por parte de sus usuarios, donde el perímetro clásico desaparece y la superficie de ataque se incrementa, requiriéndose una adaptación específica de los procesos de seguridad.

A esta nueva realidad de las organizaciones se suma que los ataques y métodos empleados son cada vez más sofisticados y diversos, enfrentándonos a una “profesionalización" de los atacantes y estando todos cada vez más expuestos al cibercrimen. Del mismo modo, también los dispositivos y las soluciones de seguridad disponibles son cada vez más sofisticados y diversos.

Existen además una serie de obligaciones legales que, según el sector, deben tenerse en consideración, yendo desde la mera notificación de incidentes hasta la necesidad de disponer de un CSIRT.

En este contexto, el CSIRT-SATEC es un CSIRT privado que se crea por mandato de la Dirección del Grupo Satec, 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 CSIRT-SATEC tiene como misión dar respuesta a los retos de ciberseguridad arriba mencionados, poniendo a disposición de todo el Grupo Satec 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.

De esta manera, los beneficios que el CSIRT-SATEC 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.

Para conseguir su misión, el CSIRT-SATEC:

- Ofrece una serie de servicios, descritos en el **apartado 5** de este documento, que pueden ser contratados individualmente o por bloques, según las necesidades específicas de cada cliente potencial.
- 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 del conjunto de procedimientos y herramientas necesarios y adecuados para la prestación de los servicios ofertados.
- Realiza una monitorización continua, centralizando la visibilidad de actividad y potenciales amenazas de todos los elementos o herramientas de una organización, a través de un SIEM, reduciendo de manera

notable los tiempos de detección de posibles incidentes, identificando qué amenazas requieren de intervención inmediata, y cuáles son falsos positivos.

- Realiza tareas proactivas y preventivas para la mejora de la seguridad de sus clientes.
- Intercambia información técnica sobre incidentes con otros CSIRTs para así mejorar la respuesta conjunta ante los mismos.

De cara a mantener los máximos estándares de calidad y cumplimiento en el desarrollo de su misión, el CSIRT-SATEC:

- Cuenta con las políticas y procedimientos necesarios para asegurar el cumplimiento de la normativa legal aplicable a los servicios suministrados.
- Ejecuta periódicamente procesos de auditoria de Calidad y Seguridad sobre los servicios suministrados, tomando como base para las mismas estándares y normativas comúnmente reconocidos en el sector, como es el caso del Esquema Nacional de Seguridad.
- Aplica las mejores prácticas comúnmente reconocidas en el sector, tomando como referencia para su constitución y operativa las indicaciones de la RFC2350 (Expectations for Computer Security Incident Response), disponible en **https://datatracker.ietf.org/doc/html/rfc2350**, y solicitando su adhesión a la organización FIRST (Forum of Incident Response and Security Teams), **https://www.first.org/.**
- Establece estrictos requisitos de comportamiento ético y confidencialidad para todo el personal perteneciente al servicio.

3.2. Circunscripción

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

3.3. Afiliación

El CSIRT-SATEC está ubicado dentro de la Dirección de Operaciones en el organigrama del Grupo Satec.

3.4. Autoridad

El CSIRT-SATEC opera, dentro del Grupo Satec, bajo la autoridad del Responsable de la Seguridad de la Información corporativo y de la Dirección de Operaciones.

4_ Políticas

4.1. Tipos de incidentes gestionados y nivel de soporte proporcionado

El CSIRT-SATEC presta servicios de detección, análisis y respuesta a incidentes de seguridad que puedan afectar a la integridad, disponibilidad y/o confidencialidad de la información gestionada por los sistemas y procesos de sus clientes.

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) (**https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html**). Siguiendo estas recomendaciones, los incidentes de seguridad se clasifican según su tipología y criticidad, estableciéndose los tiempos de respuesta a los mismos en base a esta clasificación.

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

El nivel de interlocución durante la gestión del incidente, los canales a utilizar, la información que puede o no ser intercambiada con otros actores, como pueden ser otros CSIRTs, y el nivel de protección al que debe ser sometida se definirán con cada cliente a nivel contractual, o incluso si fuera necesario en el momento de la detección del incidente, siempre respetando el marco legal y las normativas que regulen esas comunicaciones.

4.2. Cooperación, interacción y distribución de información

El CSIRT-SATEC interactúa en su operativa diaria con un número importante de actores, con los que intercambia diversa información en función del papel que juega cada uno de ellos en su ecosistema de relaciones.

Estos actores pueden ser otros CSIRTs, autoridades legales, fuentes de información e inteligencia, organizaciones clientes, proveedores, fabricantes, prensa, y dentro de cada uno de ellos, puede establecerse comunicación con personal que juega roles muy diferentes, como ingenieros y analistas de seguridad, administradores de sistemas, expertos legales, responsables de seguridad, responsables de RRHH, usuarios finales, o periodistas.

De entre todos estos actores, existen 3 que por su especial relevancia en el ámbito nacional español se identifican en este documento:

- 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.
- Agencia Española de Protección de Datos, AEPD (**https://www.aepd.es/es**), en caso de 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.

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 FIRST (Forum of Incident Response and Security Teams), **https://www.first.org/.**

En este escenario, es crítico establecer un procedimiento claro de qué información puede ser intercambiada en cada situación con cada tipo de actor.

El CSIRT-SATEC, siguiendo las políticas de seguridad de la información del Grupo Satec, establece los siguientes niveles de clasificación de la información:

- CONFIDENCIAL: Información que se maneja dentro del organismo u organización propietario de la misma, a la que sólo puede acceder un número reducido de personas.
- RESTRINGIDA: Información manejada dentro del organismo u organización propietaria de la misma, a la que pueden acceder miembros del personal interno, subcontratados, y de terceras partes interesadas. Los destinatarios pueden ser grupos genéricos de personas, por ejemplo, pertenecientes a un departamento concreto.
- INTERNA: Distribución interna libre, pero necesita autorización expresa para su distribución externa.
- PÚBLICA: Información de uso público, cuya distribución no afecta negativamente a intereses u operaciones del organismo u organización propietaria.

De cara a facilitar la cooperación, distribución e intercambio de información con clientes, organismos u otros CSIRTs, se establece la equivalencia entre esta clasificación y el protocolo FIRST TLP, que será el utilizado por el CSIRT-SATEC para el etiquetado y subsiguientes medidas de protección de la información en base a dicho etiquetado.

Clasificación información Grupo Satec	Correspondencia Protocolo FIRST TLP
CONFIDENCIAL	TLP:RED
RESTRINGIDA	TLP:AMBER
INTERNA	TLP:GREEN
PÚBLICA	TLP:WHITE

Los propietarios de la información serán los responsables de clasificarla, e indicar cómo y con quién se puede compartir la información en base a dicha clasificación. El CSIRT-SATEC 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 CSIRT-SATEC 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. Aunque de modo general nunca se compartirán datos personales, si fuese necesario hacerlo, y dentro de los supuestos recogidos en las normativas europea y española de protección de datos personales, se solicitara la autorización expresa al titular de los mismos.
- 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.

4.3. Comunicación y autenticación

Como se ha establecido con anterioridad en este documento, los canales de comunicación entre el CSIRT-SATEC 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.

Las cuentas utilizadas por parte del CSIRT-SATEC y las claves PGP asociadas son las siguientes:

incidentes.ciberseguridad@satec.es Fingerprint: 81FA CBD8 1F93 8C24 D060 04E1 8373 BA36 4A43 9163

consultas.ciberseguridad@satec.es Fingerprint: 70B3 B733 A74E 0C8C FA55 D59B 6089 5C0E 7C75 04D6

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, a través del análisis continuo de la configuración de la infraestructura de nuestros clientes respecto de las amenazas y vulnerabilidades conocidas.

5.2. Detección y análisis de eventos

Supervisión en tiempo real, correlación de eventos, análisis y notificación ante incidentes de seguridad.

5.3. Respuesta a incidentes

Añade al servicio de detección y análisis de eventos una capa de autonomía superior que permite minimizar los tiempos de reacción ante un ciberataque o un incidente de seguridad.

5.4. Concienciación y formación

Simulación de campañas de phishing personalizadas y análisis de la respuesta de los usuarios ante dichas campañas para evaluar el grado de concienciación de nuestros usuarios respecto a este tipo de ataques. El servicio se complementa con material de formación para los usuarios con el objeto de mejorar su capacidad de atención ante estos ataques.

5.5. 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.

5.6. Servicios gestionados

Nuestros equipos operativos expertos están disponibles en aquellos ámbitos tecnológicos (sistemas, OSS, aplicaciones…) en los que el cliente quiera delegar, parcial o totalmente, la gestión de su infraestructura. En cualquier de los ámbitos mencionados se aplica el principio de Seguridad por Diseño para el desarrollo de la solución.

6_ Formulario de comunicación de incidentes

Cuando un cliente detecta un evento o incidente de seguridad, se lo reportará al CSIRT-SATEC a través del correo **incidentes.ciberseguridad@satec.es**, como se ha indicado en apartados anteriores de este documento. En el intercambio de esta información se utilizarán las medidas de protección, mediante el uso de claves PGP, que se establecen en el Procedimiento de Gestión de la Información del CSIRT-SATEC. Estas medidas tendrán en cuenta tanto la clasificación de la información, como los acuerdos que se hayan establecido con cada cliente al inicio de la prestación del servicio.

En dicho correo deberá incluirse toda la información disponible de entre la que se lista en la siguiente tabla:

¿QUÉ NOTIFICAR?	DESCRIPCIÓN
Asunto	Frase que describe de forma general el incidente.
Descripción	Descripción detallada de lo sucedido.
Afectado	Indicar si se trata de un usuario o varios los afectados.
Fecha y Hora del Incidente	Indicar con la mayor precisión posible cuándo ha ocurrido el incidente.
Fecha y hora de detección del incidente	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 CSIRT-SATEC, 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 CSIRT-SATEC, 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.).

7_ Descarga de responsabilidad

Si bien se tomarán todas las precauciones en la elaboración de la información, notificaciones y alertas, CSIRT-SATEC no asume ninguna responsabilidad por errores u omisiones, ni por daños resultantes del uso de la información proporcionada durante la ejecución de sus servicios.