NUNSYS-CERT RFC 2350

Clasificación de información:

Tipo de documento	Documento general
Nombre del archivo	Nunsys-CERT_RFC_2350_v2.4_ES.docx
Clasificación	PUBLICO
Ámbito de distribución	Público
Responsable	Gerente de NUNSYS-CERT

VERSION CONTROL		
Description	**Version**	**Date**
Luis Bernal: Preliminary version.	1.0	01/04/2018
Luis Bernal: Preliminary version.	1.1	16/04/2018
Rafael Vidal: Modified 3.2 and 3.4	1.2	17/04/2018
Luis Bernal: Team member deleted	1.3	11/05/2018
Luis Bernal: Team member added	1.4	05/09/2018
Luis Bernal: Team members modified	1.5	19/12/2018
Miguel Roca: General review and adaptation	2.0	11/06/2020
Miguel Roca: Team member added	2.1	10/07/2020
Miguel Roca: Team members modified	2.2	06/10/2020
Miguel Roca: Team members modified	2.3	14/01/2021
Oscar Atienza: Modified 2.6 and 2.7	2.4	04/03/2021

INDICE

1 INFORMACIÓN DEL DOCUMENTO

1.1 Fecha de la última actualización

La versión actual de este documento es la 2.4 y fue publicada el 4 de marzo de 2021.

1.2 Lista de distribución

Actualmente Nunsys no utiliza ninguna lista de distribución como medio de notificación de cambios en el documento.

1.3 Ubicación donde puede encontrarse este documento

La versión actual de este documento puede encontrarse en la página web de Nunsys:

https://www.nunsys.com/rfc2350/

1.4 Autenticación de este documento

Este documento ha sido firmado digitalmente con la clave PGP de NUNSYS -CERT (ver sección 2.6).

2 INFORMACIÓN DE CONTACTO

2.1 Nombre del equipo

NUNSYS-CERT
Nunsys S.L. – Computer Emergency Response Team

2.2 Dirección

Nunsys S.L.
Calle Gustave Eiffel, 3
46980 Paterna, Valencia
España

2.3 Zona horaria

Central europea: CET (UTC/GMT +1), CEST (UTC/GMT +2)

2.4 Número de teléfono

+34 902 88 16 26

2.5 Dirección de correo electrónico

sat@nunsys.com

2.6 Claves públicas e información de cifrado

sat@nunsys.com
ID de la clave: 9ABFFCC4
Fingerprint 631B 7475 E00B 00D9 52F5 AC03 9648 B393 9ABF FCC4

La clave PGP pública está disponible en la página web de Nunsys:

https://www.nunsys.com/nunsys-cert/pgp/sat.asc

2.7 Miembros del equipo

Oscar Atienza
Oscar.atienza@nunsys.com
Key ID: 104AD6A0
Fingerprint D2DDACAB8FD56098967FCFA0219D0B04104AD6A0

María José Montes
mariajose.montes@nunsys.com
Key ID: EC835DA3
Fingerprint 27781C0EA6F4B197F792F1D83BCF410BEC835DA3

Néstor Jarque
Nestor.jarque@nunsys.com
Key ID: EE3BC7CE
Fingerprint 0E6B0BEB5593CE40E87DF4D408BFEABBEE3BC7CE

Nafees Muhammad
nafees.muhammad@nunsys.com
Key ID: 2C6700C0
Fingerprint 0E6B0BEB5593CE40E87DF4D408BFEABBEE3BC7CE

Agustin Domenech
agustin.domenech@nunsys.com
Key ID: 9FBEBC5F
Fingerprint D4E482E353F9F29763E456BAA1B5148B9FBEBC5F

David Blasco
david.blasco@nunsys.com
Key ID: 732A23ED
Fingerprint 1D29F7CB9FF65E80F4035A217E3E4E5D732A23ED

Manuel del Olmo
Manuel.deolmo@nunsys.com
Key ID: 3148A951
Fingerprint EF4CDBCBE4642159AA5C504B4184D9AA3148A951

Juan Antonio Vicent
juanantonio.vicent@nunsys.com
Key ID: 5740F93C
Fingerprint 7E234B4AFE60B7048CF27F60CCACFA565740F93C

Arturo Raga
arturo.raga@nunsys.com
Key ID: CB844621
Fingerprint A1D3D617EDF58EDCA4DE1D0E966D5BFECB844621

Carlos José Hernandez
carlosjose.hernandez@nunsys.com
Key ID: E3CFDACA
Fingerprint A8C9979878C07D2925D7C4594ECDA2F4E3CFDACA

Lorena Penalba
lorena.penalba@nunsys.com
Key ID: BA6A4C0D
Fingerprint E2CF65D73B6CB98B98D3075FA2B61C41BA6A4C0D

Antonio José Escabias
antoniojose.escabias@nunsys.com
Key ID: 37B1E061
Fingerprint BFB93BE667EDDA0DE34E6F8A09D0857437B1E061

2.8 Puntos de contacto con los clientes

El método preferido para reportar y gestionar las incidencias de seguridad es por correo electrónico.

Por favor, escríbenos a sat@nunsys.com usando la clave pública. Esto creará un caso en nuestro sistema de tickets y nuestro equipo se encargará de gestionarlo.

3 ESTATUTOS

3.1 Misión

NUNSYS-CERT es un Centro de respuesta ante incidentes de seguridad, establecida por el Directorado de NUNSYS S.L., que tiene como misión proveer servicios de ciberseguridad con el objetivo de proteger contra incidencias de seguridad que podrían tener un impacto en la confidencialidad, integridad y disponibilidad de sus propios servicios de información, así como clientes externos, afectando a sus procesos o reputación.

3.2 Ámbito de actuación

NUNSYS-CERT ofrece servicios de seguridad de la información para infraestructuras críticas, instituciones educativas, instituciones o corporaciones públicas además de analizar eventos, coordinar soluciones técnicas, garantizar que la información necesaria sea transmitida y formar a otros equipos o individuos en la gestión de incidencias de seguridad.

Nuestros servicios de seguridad se proporcionan a clientes finales tales como empresas privadas (industria, infraestructuras críticas, integradores, otros proveedores de telecomunicaciones, etc) y entidades públicas (ayuntamientos, hospitales, universidades, etc.)

3.3 Accionariado y/o afiliación

NUNSYS-CERT forma parte del Departamento de Sistemas de Nunsys S.L. dentro de su división de operaciones. Es miembro de TF-CSIRT Trusted Introducer y CSIRT.ES, colaborando activamente con otros CSIRTs y empresas de ciberseguridad.

3.4 Autoridad

NUNSYS-CERT opera, como departamento dentro de Nunsys S.L., bajo la autoridad del responsable técnico de ciberseguridad y Director de operaciones (COO) de la empresa.

NUNSYS-CERT se relaciona con sus clientes externos como asesor, por lo que no tiene autoridad sobre ellos. Es responsabilidad únicamente del cliente adoptar las recomendaciones y medidas propuestas por este CERT.

4 POLÍTICAS

4.1 Tipos de incidentes y nivel de soporte

En general, NUNSYS-CERT soporta los tipos de incidentes recopilados por CCN-CERT, en su documento "CCN-STIC 817 Cyberincident Management", y que puedan tener un impacto en la confidencialidad, integridad o disponibilidad de los activos de sus clientes, tanto internos como externos.

Todos los incidentes confirmados se clasifican según su tipología y severidad, según las recomendaciones de CCN-CERT, con prioridad a respuestas basadas en los resultados de esta clasificación.

El nivel de soporte puede variar dependiendo de las condiciones contractuales del servicio y el tipo, impacto, severidad y/o complejidad del incidente, que puede implicar la necesidad de escalarlo y la intervención de CSIRTs con más amplitud asociados con diferentes administraciones gubernamentales y/o servicios.

4.2 Cooperación, interacción y revelación de información

NUNSYS-CERT, en ejercicio de su misión, puede cooperar e interactuar con otras organizaciones, tales como otros CERT o CSIRT. Dentro del territorio nacional español, se han establecido dos CERTs a los cuales hay que reportar los incidentes de seguridad de la información relevantes. Estas entidades son las siguientes:

- INCIBE-CERT: para ciudadanos, organizaciones y empresas en el sector privado.
- CCN-CERT: para entidades y empresas públicas

NUNSYS-CERT forma parte de foros conocidos a nivel nacional e internacional, cuyo objetivo es promover la cooperación y Coordinación entre los CSIRTs para actuar contra los problemas de seguridad informática. Estos foros son los siguientes:

- CSIRT.ES
- TF-CSIRT Trusted Introducer

Si es necesario compartir información con otros actores, NUNSYS-CERT seguirá la siguiente guía:

- Compartir solo información relevante para controlar el incidente, respetando el nivel de confidencialidad establecido por el propietario.
- Aplicar en todo momento las medidas técnicas y legales necesarias para la protección de la información.
- Anonimizar la información compartida al máximo.
- No compartir información confidencial con otros sin acuerdo y autorización previa del propietario, a menos que exista una obligación legal o regulatoria mayor para ello.
- No compartir información personal. Si es necesario, se realizará teniendo en cuenta la ley española de protección de datos personales y solicitando autorización previa de su propietario.

4.3 Comunicación y autenticación

NUNSYS-CERT trata la información con absoluta confidencialidad, aplicando las medidas necesarias para su protección, tal y como se establece en la Política de clasificación de la información y considerando entre otras leyes y reglamentos:

- Regulación EU 2016/679 Reglamento general de protección de datos
- Ley orgánica 3/2018 Protección de datos personales y Garantía de derechos digitales
- Real Decreto 3/2010 y 951/2015 Esquema de seguridad nacional
- Real Decreto 704/2011 Protección de infraestructuras críticas

Para el objetivo de información no considerada sensible, la transmisión por correo electrónico o por la red, no siendo considerado un medio particularmente seguro, será suficiente. En caso de tratarse de información sensible, la comunicación por correo electrónico requerirá cifrado, para lo cual se utilizará las llaves PGP de remitentes y destinatarios; similarmente, para la transmisión de archivos por la red, estos se cifrarán previamente.

Las líneas telefónicas se consideran lo suficientemente seguras para su uso incluso sin cifrado.

5 SERVICIOS

5.1 Respuesta ante incidentes

NUNSYS-CERT proporciona servicios de monitorización, detección, análisis, clasificación, coordinación y soporte 24x7x365 en respuesta a incidentes de seguridad, siempre en colaboración estrecha con los diversos actores implicados, con el objetivo de mejorar la capacidad de mitigación.

5.1.1 Triaje de incidentes

- Investigar si un incidente realmente ha ocurrido
- Identificar su alcance

5.1.2 Coordinación de incidentes

- Identificar y contactar con las empresas implicadas
- Proporcionar contacto con terceros, incluyendo las fuerzas de seguridad, si es necesario.
- Solicitar y/o escribir informes según las organizaciones implicadas, el tipo de incidente y severidad.
- Cuando sea apropiado, generando comunicación con los accionistas.

5.1.3 Resolución de incidentes

- Proporcionar asistencia técnica a las organizaciones implicadas
- Recomendar acciones enfocadas a erradicar la causa raíz del incidente y su impacto.
- Llevar a cabo investigaciones forenses, recopilando pruebas e interpretando la información si es necesario.

5.2 Servicios proactivos

5.2.1 Anuncios y alertas

NUNSYS-CERT recopila y distribuye inteligencia sobre amenazas emergentes, indicadores de compromiso, campañas maliciosas, etc, así como guías y recomendaciones sobre las acciones a tomar para su prevención y respuesta.

5.2.2 Gestión de vulnerabilidades

Monitorización y mejora continua de los Sistemas de seguridad de la información (red, aplicaciones, infraestructura, etc) a través de la ejecución periódica de análisis con el objetivo de identificar, cuantificar y clasificar las vulnerabilidades del sistema.

5.2.3 Análisis/auditoría de seguridad

Revisión de la gestión de la seguridad de la información y servicio de mejora según los estándares reconocidos internacionalmente, marcos y buenas prácticas, así como servicios de pentesting.

5.2.4 Desarrollo de herramientas de seguridad

NUNSYS-CERT colabora con el departamento de I+D de Nunsys S.L. en el Desarrollo de herramientas y servicios enfocados a mejorar la gestión de la seguridad de la información de sus accionistas, tanto internos como externos.

5.2.5 Formación y concienciación

Como primera barrera de defensa en la prevención de incidentes, NUNSYS-CERT proporciona servicios de concienciación y formación en todas las áreas de la seguridad de la información, tales como la ciberseguridad, privacidad o respuesta ante incidentes.

5.2.6 Retención de registros

Los registros de los incidentes de seguridad gestionados se guardarán. Esta información será considerada confidencial. Sin embargo, se pueden generar informes estadísticos anonimizados y pueden ser compartidos con la comunidad.

6 CÓMO REPORTAR UN INCIDENTE

Para reportar y gestionar incidentes de seguridad, el método preferido es el correo electrónico, tal y como se establece en el punto 2.8 de este documento.
Esto se realiza usando formatos de notificación acordados con las partes interesadas. En ausencia de un formato o de una comunicación externa con terceros, será necesario incluir en esta comunicación al menos la siguiente información:

- Datos de identificación (nombre del remitente, organización, etc)
- Detalles de contacto (dirección de correo electrónico y número de teléfono)
- Clave PGP (en caso de disponer de ella)
- Breve resumen del incidente
- Sistemas afectados e impacto inicial estimado
- Información técnica relevante (direcciones IP, cabeceras de correo electrónico, etc.)

7 DESCARGO DE RESPONSABILIDAD

NUNSYS-CERT toma todas las precauciones en la preparación de información, notificación, alertas e informes sin asumir ninguna responsabilidad por errores, omisiones o daños resultantes del uso de la información proporcionada.