RFC-2350 ENOC-CSIRT

Versión 1.0

Control de Versiones

Autor	versión	Fecha de aprobación	Cambios realizados
ENOC-CSIRT	1.0	13 septiembre 2019	Creación del Documento

Índice

1. Difusión

1.1. Destinatarios del documento

El presente documento tiene como público objetivo los clientes del ENOC-CSIRT, otros CSIRT constituidos, organizaciones con un interés legítimo en los servicios provistos y el público en general. En atención a ello puede ser distribuido libremente, estando sujeto exclusivamente a controles de copyright.

1.2. Introducción

En el presente documento se describen los servicios prestados por el ENOC-CSIRT conforme al modelo RFC 2350 de IETF disponible en: https://www.ietf.org/rfc/rfc2350.txt

1.3. Fecha de la última actualización

La versión actual de este documento es la versión 1.0 y se lanzó el 13 de septiembre del 2019.
Listas de distribución para notificaciones
Se ha creado una lista de distribución privada para informar a los abonados a los servicios de ENOC-CSIRT sobre los cambios realizados en este documento.

1.4. Localizaciones en las que se puede acceder al documento

La versión actual de este documento está disponible en el sitio web público de ENOC-CSIRT:

https://ednon.com/enoc-csirt/rfc2350_enoc-csirt.pdf

1.5. Autenticación del documento

Este documento ha sido firmado con la clave PGP de ENOC-CSIRT. La firma de dicha clave se encuentra disponible en la página web del ENOC-CSIRT:

https://ednon.com/enoc-csirt/comunicaciones

1.6. Identificación del documento

Título: RFC 2350 ENOC-CSIRT
Versión: 1.0
Fecha del documento: 01/09/2019
Fecha de expiración: Este documento será válido mientras no se publiquen nuevas versiones del mismo.

2. Información de contacto

2.1. Nombre del equipo

ENOC-CSIRT

2.2. Dirección

Rúa dos Postes numero 10
15703 Santiago de Compostela
A Coruña (Galicia)
España

2.3. Zona horaria

Europa Central (CET/CEST)

2.4. Teléfonos de contacto

Fijo: +34 981552700 extensión 272

2.5. Número de fax

No se dispone de número de fax.

2.6. Direcciones de correo electrónico

Comunicación y gestión de incidentes: csirt@ednon.com
Otras comunicaciones: enoc_csirt@ednon.com

2.7. Otros medios de comunicación

No se han definido a fecha de publicación del presente documento.

2.8. Claves públicas y cifrado

ENOC-CSIRT emplea para las comunicaciones relacionadas con gestión de incidentes la dirección csirt@ednon.com la siguiente clave PGP:

ID: BD70 253F D045 BD1B
Fingerprint: 5B62 38F3 B203 167F 03A4 5C28 BD70 253F D045 BD1B

Esta clave se encuentra disponible en servidores PGP de libre acceso y 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 se emplea La dirección enoc_csirt@ednon.com asociada a la siguiente clave PGP:

ID: FA07 2768 7F13 0ECF
Fingerprint: 6028 AB4A B5BC 5E80 A614 F74A FA07 2768 7F13 0ECF

2.9. Componentes del equipo

En la fecha de publicación de este documento el equipo se encuentra constituido por analistas de seguridad dedicados a tiempo completo.
Por razones de privacidad el listado de personal perteneciente al equipo no se publica en este documento, por favor contáctenos directamente si necesita más información.

2.10. Horas de funcionamiento

El ENOC-CSIRT funciona siguiendo los siguientes horarios:

Habitualmente. De lunes a jueves, de 8:00 h a 17:30 h y viernes, de 8:00 h. a 15:00 h
Temporada de verano. De lunes a viernes, de 8:00 h a 15:00 h

**El servicio está cerrado los días festivos oficiales.*

2.11. Información adicional

Más información relacionada con el ENOC-CSIRT puede ser consultada en el sitio web:

https://ednon.com/enoc-csirt

2.12. Puntos de contacto

Se han establecido los siguientes medios de contacto durante las horas de operación del servicio.
Para comunicaciones no relacionadas con incidencias se empleará el correo electrónico dirigido a:

enoc-csirt@ednon.com

Para comunicación y gestión de incidentes los medios de contacto asignados son el correo electrónico dirigido a:

csirt@ednon.com

Y/o llamadas telefónicas a los números indicados anteriormente.

3. Objetivos

3.1. Misión

ENOC-CSIRT es un CSIRT privado dedicado a organismos y empresas, públicos y privados, que se crea por mandato de la Dirección de EDNON S.L., con la misión de proveer servicios de seguridad y proteger los sistemas de información de los distintos departamentos de la organización y clientes externos a la misma, siendo ambos referidos en adelante como los beneficiarios, ante incidentes de seguridad que pudiesen llegar a afectar la integridad, confidencialidad o accesibilidad de la información y/o dañar las operaciones o reputación de los afectados. Dichos servicios están disponibles a clientes externos a EDNON S.L. mediante suscripción, la cual puede ser realizada a la totalidad o parte de los servicios ofertados.

Para lograr estos objetivos ENOC-CSIRT realiza, entre otras, las siguientes tareas:

- Recopilación y análisis de información de distintas fuentes disponibles relativa a nuevas vulnerabilidades y amenazas.
- Comunicación a los beneficiarios de la inteligencia generada que resulte relevante para su contexto de operaciones.
- Distribución de información técnica sobre incidentes con otros centros de respuesta a incidentes para así mejorar la respuesta conjunta ante los mismos.
- Realización de tareas proactivas y preventivas para la mejora de la seguridad de sus beneficiarios.
- Monitorización de eventos de seguridad y detección de incidentes.
- Dar apoyo a los beneficiarios en la coordinación y gestión de las respuestas a los incidentes de seguridad que pudiesen llegar a afectarles.

Para lograr estos objetivos ENOC-CISRT se adhiere desde su creación a los siguientes valores:

- Cumplimiento de la normativa legal aplicable a los servicios suministrados.
- Aplicación de las mejores prácticas comúnmente reconocidas en el sector, adhiriéndose y tomando como referencia para sus operaciones el CSIRT *Code of Practice* versión 2.4, disponible en *https://www.trusted-introducer.org/TI-CCoP.pdf*
- Establecimiento de estrictos requisitos de comportamiento ético y confidencialidad para todo el personal perteneciente al servicio.
- Promocionar el uso de buenas prácticas entre sus beneficiarios.
- Proporcionar una capacidad de respuesta eficaz y eficiente en caso de incidentes.
- Definición y ejecución de procesos de auditoria continua de Calidad y Seguridad sobre los servicios suministrados tomando como referencia para las mismas metodologías y estándares comúnmente reconocidos en el sector.
- Creación y mantenimiento de procesos de comunicación y evaluación periódicos de las necesidades de los clientes internos y externos de los servicios dentro de un proceso de mejora continua de los mismos.

3.2. Circunscripción

Los servicios proporcionados por ENOC-CSIRT están dirigidos a todos los departamentos internos de EDNON S.L. y a las empresas e instituciones externas a la empresa que se suscriban a los mismos.

3.3. Afiliación

ENOC-CSIRT forma parte del grupo de operaciones de EDNON S.L. Asimismo, mantiene relaciones con distintos CSIRT y organizaciones relacionadas dentro del ámbito nacional español y europeo.

3.4. Autoridad

ENOC-CSIRT opera, dentro de EDNON S.L. bajo la autoridad del Responsable de la Seguridad de la información corporativo y de la Dirección de la empresa.
En referencia a sus clientes externos ENOC-CSIRT actúa como asesor de los equipos de seguridad de dichos clientes y no dispone de autoridad sobre los mismos, por lo cual la implementación de las recomendaciones que se proporcionen será exclusivamente responsabilidad del cliente.

4. Políticas

4.1. Tipos de incidentes gestionados y nivel de soporte proporcionado

El ENOC-CSIRT da soporte a los incidentes de información que puedan afectar a la integridad, disponibilidad y confidencialidad de la información gestionada por los sistemas y procesos de los beneficiarios de sus servicios. De modo general los tipos de incidentes soportados se corresponden con las tipologías de incidentes de seguridad publicadas por el Centro Criptológico Nacional de España, CCN-CERT, que pueden consultarse entre otros en el documento:

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

Todos los incidentes confirmados son clasificados según su tipología y gravedad de acuerdo a las recomendaciones del CCN-CERT, priorizándose las respuestas en base a los resultados de dicha clasificación.
El ENOC-CSIRT no da soporte directo a usuarios finales externos a EDNON S.L., considerando que estos contactaran con sus servicios de seguridad propios. Todas las comunicaciones entre el ENOC-CSIRT y sus beneficiarios externos serán canalizadas a través de los interlocutores definidos en el contrato de servicio.
El nivel de soporte proporcionado puede estar sujeto a variación según las condiciones contractuales del servicio y la tipología, impacto, severidad y/o complejidad del incidente, como resultado de los cuales puede llegar a ser necesaria la intervención de CSIRT de alcance superior asociados a distintas administraciones y/o servicios del estado.

4.2. Cooperación, interacción y distribución de información

Durante la ejecución de su misión, el ENOC-CSIRT puede interactuar con otras organizaciones, como otros equipos CERT o CSIRT, proveedores, analistas y generadores de inteligencia, etc.
Dentro del ámbito nacional español se han establecido dos CERT de referencia a los que deben ser comunicados los incidentes relevantes de seguridad de la información y sistemas, limitándose sus competencias según la tipología de las organizaciones afectadas por los accidentes. Estos organismos son los siguientes:

- Para los ciudadanos, organismos y empresas del sector privado se ha designado como referencia a INCIBE-CERT. *https://incibe-cert.es*

- Para los organismos y empresas públicas se ha designado como referencia al CCN-CERT. *https://ccn-cert.cni.es*

A fecha de la aprobación del presente documento no se han establecido formalmente relaciones de cooperación con otros CSIRT/CERT a nivel español o europeo, más allá de las obligatoriamente establecidas por la normativa legal española. Aun así, se han iniciado los contactos necesarios y en el medio plazo se prevé el establecimiento de relaciones formales con distintos CSIRT autonómicos y sectoriales a nivel español para la mejora de los servicios de respuesta y distribución de información sobre amenazas.
En referencia a la información que pueda ser compartida con otros actores, el ENOC-CSIRT aplica las siguientes directrices de manejo y selección de la misma:

- Aplicar en todo momento las medidas técnicas y legales indicadas en este documento 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.

- Respetar el nivel de confidencialidad asignado a la información por su propietario.

- No compartir información confidencial con otras partes sin un acuerdo y autorización previos del propietario de la misma. Esta directriz aplica en todos los supuestos en los que no exista una obligación legal o normativa superior que obligue a compartir la información

.

- 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 la normativa 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 cliente propietario de la misma notifique la denegación del permiso para ello. Esta directriz aplica en todos los supuestos en los que no exista una obligación legal o normativa superior que obligue a compartir la información.

4.3. Operaciones

El ENOC-CSIRT opera de acuerdo a la normativa legal española y se adhiere al **CSIRT Code of Practice** versión 2.4, disponible en *https://www.trusted-introducer.org/TI-CCoP.pdf*.

4.4. Comunicación y autenticación

El ENOC-CSIRT aplica a la información que maneja las medidas de protección correspondientes a su naturaleza y clasificación, tomando como referencia, entre otros, la normativa española de protección de datos personales, el Esquema Nacional de Seguridad del Gobierno de España y la directiva NIS europea.
Asimismo, en las comunicaciones y documentación se emplea interna y externamente el protocolo FIRST TLP v1.1 para la clasificación y etiquetado de los documentos.
Considerando los tipos de información con los que trata el ENOC-CSIRT, los teléfonos se considerarán lo suficientemente seguros como para usarse incluso sin cifrar. 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 confidenciales por correo electrónico, se cifrarán empleando para ello las claves PGP de los emisores y receptores de los mismos. Las transferencias de archivos de red se considerarán similares al correo electrónico para estos fines, por lo cual los datos confidenciales deben cifrarse para su transmisión.
Cuando sea necesario establecer una relación de confianza, y antes de revelar información confidencial, la identidad de la otra parte se determinará con un grado razonable de confianza empleando para ello, dentro de lo posible, las referencias de terceras personas y/o organismos conocidos y de confianza como medio de acreditación. De lo contrario, se utilizarán los métodos apropiados, como la búsqueda de los miembros de FIRST o la base de datos de ***Trusted Introducer*** y realizando una devolución de llamada telefónica o un correo electrónico para garantizar la identidad de las otras partes.

5. Servicios proporcionados

5.1. Sensibilización y concienciación

El ENOC-CSIRT proporciona estos servicios mediante la participación en jornadas formativas e informativas junto con el envío de comunicaciones a sus beneficiarios donde se abordan noticias sobre buenas prácticas relativas a la seguridad de la información, incidentes de seguridad recientes, nuevas vulnerabilidades, análisis e informes sobre malware, etc.

5.2. Alertas y avisos

El ENOC-CSIRT distribuye información de inteligencia en relación a campañas maliciosas detectadas, nuevas amenazas, indicadores de compromiso, etc., así como recomendaciones sobre las acciones a tomar en respuesta a los mismos.

5.3. Revisiones y auditorías de seguridad

El ENOC-CSIRT proporciona servicios de revisión y mejora de la gestión de la seguridad de la información atendiendo a marcos de trabajo (*frameworks) reconocidos*, así como análisis de vulnerabilidades y *pentesting*.

5.4. Monitorización y gestión de incidentes

El ENOC-CSIRT proporciona servicios de motorización, detección, análisis, clasificación, coordinación y apoyo en la respuesta a incidentes de seguridad.
Estos servicios se proporcionan mediante el apoyo y colaboración con otros grupos IT de los beneficiarios.

5.5. Desarrollo de soluciones de seguridad

El ENOC-CSIRT colabora con el departamento de desarrollo de soluciones de EDNON S.L., **EDNON labs_** para el desarrollo de servicios y herramientas, para uso interno y comercialización, con el objetivo de lograr mejoras en la gestión de la seguridad de la información de sus beneficiarios.

6. Formularios de respuesta a incidentes

Para las comunicaciones del servicio se emplean formatos acordados entre las partes participantes y/o reconocidos de modo general por el sector. En los casos en los cuales el origen de una comunicación sea externo y no exista un formato previamente acordado de notificación, se recomienda incluir en la misma al menos los siguientes datos:

- Datos de identificación. Nombre del remitente, organización, dirección, etc.
- Datos de contacto. Dirección de correo electrónico y teléfono si está disponible.
- Clave PGP si estuviese disponible.
- Breve resumen del incidente comunicado.
- Medio de detección del incidente.
- Sistemas afectados e impacto inicial estimado.
- Información técnica relevante sobre el incidente. Cabeceras de correo, direcciones IP, muestras y artefactos asociados al incidente o información sobre los medios disponibles para compartirlos.

Siempre que sea posible, los incidentes deben comunicarse por correo electrónico utilizando la dirección previamente indicada en este documento.
Asimismo, ENOC-CSIRT ha desarrollado modelos propios de informes para la gestión y análisis de los incidentes y la comunicación de los resultados a sus beneficiarios.

7. Descarga de responsabilidad

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