Nologin CSIRT - RFC 2350 - ES

noviembre,2024

Índice

1 Información del documento 4
1.1 Objeto 4
1.2 Fecha de actualización 4
1.3 Lista de distribución 4
1.4 Ubicación del documento 4
2 Información de contacto 5
2.1 Datos de identificación 5
2.2 Equipo CSIRT 5
2.2.1 Miembros 5
2.2.2 Horario de atención 5
2.2.3 Puntos de contacto para la comunidad 6
3 Constitución 7
3.1 Misión 7
3.2 Circunscripción 7
3.3 Autoridad 7
4 Políticas 8
4.1 Tipo de incidentes y nivel de soporte 8
4.2 Cooperación, Interacción y divulgación de la Información 8
4.3 Comunicación y Autenticación 9
5 Servicios proporcionados 10
5.1 Servicios reactivos 10
5.2 Servicios proactivos 10
5.2.1 Ciberinteligencia y alertas 10
5.2.2 Sensibilización y concienciación 10
5.2.3 Gestión de vulnerabilidades y auditorías 11
5.2.4 Desarrollo de la ciberseguridad 11
5.3 Formas de notificación de incidentes 11

1 Información del documento

1.1 Objeto

Este documento describe el servicio proporcionado por el Equipo de Respuesta a Incidentes de Seguridad Informática de Nologin (en adelante "Nologin-CSIRT") con el fin de establecer su marco de trabajo y actuación, estructura organizativa y formas de contacto. El formato para dicho propósito cumple con con el estándar RFC 2350 https://www.ietf.org/rfc/rfc2350.txt.

1.2 Fecha de actualización

Este documento se ha actualizado por última vez el 7 de noviembre de 2024.

1.3 Lista de distribución

No existe un canal de distribución para notificar cambios en este documento. Ante cualquier duda, por favor, contacte a través de https://nologin.es/es/contact .

1.4 Ubicación del documento

El documento se encuentra disponible en https://www.nologin.es/es/cybersecurity-incident-management-csirt-as-a-service .

2 Información de contacto

2.1 Datos de identificación

- **Nombre del equipo**: Nologin-CSIRT
- **Dirección**: Avenida Ranillas, 1D, Planta 3, Av. Ranillas, 1D, of. 3G, 50018 Zaragoza
- **Zona horaria**: CET / CEST
- **Número de teléfono**: +34 976 51 24 33
- **Número de fax**: No existe
- **Otras comunicaciones**: No existe
- **Direcciones de correo electrónico**:
  - Gestión de incidentes para la comunidad circunscrita: incident.csirt@nologin.es
  - Notificación de información de interés para el CSIRT: communication.csirt@nologin.es
- **Claves públicas y cifrado de información**: Claves PGP disponibles en RedIRIS
  - incident.csirt@nologin.es: 093432C8A7858FFDF1A432977385A8FB0907BB78
  - communication.csirt@nologin.es: 76261009EAC4ACD43D28D273BEF5A84DB9D08E1E

2.2 Equipo CSIRT

2.2.1 Miembros

El equipo CSIRT de Nologin está constituido por analistas de ciberseguridad agrupados en varios niveles acorde a sus funciones y nivel de análisis. Todos ellos están gestionados por el Responsable del servicio CSIRT y por el Responsable de Ciberseguridad de Nologin.

Así, el servicio proporcionado por Nologin-CSIRT consta de los siguientes niveles:

- Reponsable de seguridad
- Responsable del CSIRT
- Expertos en seguridad de la información (Nivel 3)
- Especialistas en respuesta a incidentes (Nivel 2)
- Analistas de ciberseguridad (Nivel 1)

2.2.2 Horario de atención

El equipo CSIRT de Nologin está disponible en los siguientes horarios:

- Consultas sobre servicios de ciberseguridad: Horario de oficina (8:00 h - 18:00 h).
- Incidentes de ciberseguridad: horario extendido (24x7x365).

2.2.3 Puntos de contacto para la comunidad

Se han habilitado las direcciones de correo electrónico mencionadas previamente para el tratamiento de incidentes y de consultas CSIRT.

3 Constitución

3.1 Misión

El CSIRT de Nologin es un equipo privado de respuestas ante cibericidentes que opera tanto en organismos públicos como en empresas privadas. Su creación se corresponde con el mandato de la Dirección de Nologin S.L.U. con el fin de proveer servicios de ciberseguridad orientados a la gestión del ciclo de vida de un ciberincidente, apoyando así a los clientes a actuar de la forma correcta y rápida para minimizar el impacto y evitar las pérdidas en el negocio y servicio.

Nologin ofrece tanto el conocimiento de sus técnicos expertos como el liderazgo de sus responsables para gestionar de la forma correcta un incidente de ciberseguridad. Además, Nologin-CSIRT también cuenta con servicios de ciberseguridad que ayudan a actuar en aquellos incidentes que afectan a la integridad, confidencialidad o accesibilidad de la información.

Además, Nologin-CSIRT también ofrece servicios proactivos que ayudan a las empresas a gestionar la ciberseguridad de forma previa a la detección de ciberincidentes. Dichos servicios son:

- Administración, operación y mejora de herramientas de ciberseguridad acorde al negocio y a la operativa del cliente.
- Respuestas automáticas basadas en herramientas SOAR para disminución de tiempos de respuesta y minimización de impactos.
- Comunicaciones de ciberinteligencia para prevenir y evitar ataques inminentes.
- Búsqueda de amenazas avanzadas y gestión del ciclo de vulnerabilidades.
- Monitorización de eventos de seguridad y detección de incidentes.
- Integración de productos y servicios para un enriquecimiento de la información.
- Acomodación a estándares y normativas.

3.2 Circunscripción

Los servicios proporcionados por Nologin-CSIRT están dirigidos a entidades, tanto públicas como privadas, que decidan optar por la contratación de los mismos. Los servicios anteriormente comentados se acomodorán al cliente tras la contratación para optimizar los resultados y garantizar la ciberseguridad desde un punto de vista más “ad-hoc”.

3.3 Autoridad

Nologin-CSIRT opera dentro de Nologin S.L.U. y bajo la autoridad del Responsable de Seguridad y de la Dirección de la empresa.

4 Políticas

4.1 Tipo de incidentes y nivel de soporte

El equipo Nologin-CSIRT trabaja de forma continua en la respuesta ante cualquier ciberincidente que sea notificado, ya sea de forma manual o automática, por alguno de sus servicios o entidades adscritas. Dicha respuesta se lleva a cabo dentro del marco establecido por el CCN en la guía CCN-STIC-817 para garantizar la uniformidad y el correcto tratamiento.

Acorde a un sistema de escalados por niveles, los incidentes de analizan y priorizan acorde a la gravedad determinada en el análisis inicial, según las recomendaciones del CCN-CERT, el negocio del cliente y la base de conocimientos en materia de ciberseguridad con la que cuenta Nologin-CSIRT.

Según dicha categorización inicial, se determina el escalado y el tiempo de respuesta. Las empresas y entidades adscritas a los servicios de Nologin contarán, de forma previa, con unos acuerdos en el nivel de servicio que garantizarán la respuesta acorde a la categorización del incidente, la cual estará determinada, entre otras cosas, por la tipología del ataque, el impacto, la severidad, la veracidad de los indicadores y los sistemas implicados, entre otros parámetros.

De esta manera, el Nologin-CSIRT gestiona todo el ciclo de vida del incidente, desde el primer tratamiento hasta las acciones de remediación finales.

4.2 Cooperación, Interacción y divulgación de la Información

La información que maneja Nologin-CSIRT es confidencial y privada, y solo se trata para el objeto de los servicios contratados, acorde a las políticas internas de Nologin (apoyadas por la certificación ENS Nivel Medio e ISO 27001) y a la normativa RGPD.

Durante la ejecución de su misión, dentro de RNS o First, el Nologin-CSIRT puede interactuar con otras organizaciones, como otros equipos CERT o CSIRT o servicios de inteligencia, con el fin de mejorar sus servicios y los de otras entidades y, por ende, la ciberseguridad de todos los clientes finales.

En 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:

- INCIBE-CERT: Para los ciudadanos, organismos y empresas del sector privado.
- CCN-CERT: Para los organismos y empresas públicas.

4.3 Comunicación y Autenticación

El Nologin-CSIRT utiliza un sistema de etiquetado interno de la información para distribuir de forma correcta y proporcionada la información por los diferentes canales habilitados. De esta manera, se garantiza que la confidencialidad y la integridad de la información no se ven comprometidas acorde a sus políticas internas, al Reglamento General Europeo de Protección de Datos (GDPR) y a la directiva NIS2 europea.

5 Servicios proporcionados

Los servicios proporcionados por Nologin-CSIRT se pueden dividir en dos:

- Actividades reactivas
- Actividades proactivas

5.1 Servicios reactivos

Los servicios reactivos ofrecidos por el CSIRT de Nologin garantizan la respuesta completa a un ciberincidente. Para cumplir con este propósito, Nologin-CSIRT coordina todo el ciclo de vida del incidente, además de responder técnicamente a las necesidades que plantee dicho incidente.

Así, Nologin monitoriza, detecta, clasifica, categoriza, analiza, coordina y responde a los ciberincidentes (servicios de monitorización y DFIR). Esta gestión completa del incidente por parte de Nologin garantiza una correcta coordinación de la contención y de la recuperación, lo que minimiza el impacto y asegura el negocio.

5.2 Servicios proactivos

Los servicios proactivos están orientados a mejorar y asegurar los recursos disponibles con el fin de evitar y prevenir posibles incidentes futuros.

5.2.1 Ciberinteligencia y alertas

Nologin-CSIRT cuenta con servicios internos que analizan de forma continua el ciberespacio con el fin de encontrar cualquier información que pueda afectar a la seguridad de los clientes. Este servicio genera alertas tempranas junto a las recomendaciones necesarias si se determina, tras un primer análisis, que es necesario actuar.

5.2.2 Sensibilización y concienciación

El cumplimiento de las políticas internas, así como la sensibilización en materia de ciberseguridad, son esenciales para eliminar de las organizaciones los problemas de seguridad ocasionados por malas prácticas.

Nologin-CSIRT también analiza el negocio y la estructura de los clientes para ofrecer campañas de concienciación adecuadas que minimicen el riesgo ante posibles ataques.

5.2.3 Gestión de vulnerabilidades y auditorías

Nologin-CSIRT realiza un estudio completo del servicio de los clientes para realizar tareas de auditoría y descubrimiento de vulnerabilidades con las que solucionar los problemas de seguridad existentes antes de que sean explotados por actores maliciosos.

Además de ofrecer la categorización necesaria con la que priorizar todos los hallazgos, Nologin-CSIRT ofrece recomendaciones para su mitigación, y apoyo durante el mismo.

5.2.4 Desarrollo de la ciberseguridad

Nologin-CSIRT está en constante formación para adaptar la ciberseguridad del cliente a las nuevas tendencias, de tal forma que se garantice la seguridad en todo momento.

Este objetivo se lleva a cabo mediante el análisis de nuevas amenazas junto con el análisis del servicio del cliente. El resultado son mejoras proactivas en las herramientas (nuevas monitorizaciones, automatización de las respuestas, arquitecturas de seguridad, etc.), así como el diseño e implantación de nuevas soluciones que se adapten a cada escenario planteado.

5.3 Formas de notificación de incidentes

La notificación de incidentes puede realizarse mediante:

- **Buzón de correo específico**: incidentes@ccn-cert.cni.es
- **Sistema ITSM** habilitado durante el proceso de adhesión
- **Teléfonos**: proporcionados durante el proceso de adhesión o el apoyo a incidentes