



INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 8



9 DE NOVIEMBRE DE 2023
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Ejercicio 1	¡Error! Marcador no definido.
Ejercicio 2	¡Error! Marcador no definido.
Ejercicio 3	¡Error! Marcador no definido.
Ejercicio 4	7

Enunciado.

Incibe en su página web provee de una serie de métodos para que las empresas puedan notificarles los incidentes. Estos procedimientos se encuentran en la web.

<https://www.incibe.es/protege-tu-empresa/reporta-tu-incidente>.

Claves públicas para reportar incidentes :

<https://educacionadistancia.juntadeandalucia.es/profesorado/mod/url/view.php?id=546896>

CCN-CERT Notificación de Incidentes : <https://www.ccn-cert.cni.es/gestion-de-incidentes/notificacion-de-incidentes.html>

Como ejercicio, se propone que examines los distintos modos de notificar los incidentes propuestos, y generes un esquema informativo donde se expliquen los pasos para realizarlo.

Partes del Informe a realizar :

1º.- Cómo se notifican los incidentes al INCIBE y al Centro Criptológico Nacional .- Pasos a seguir .-

2º.- Como se van a notificar los incidentes en nuestro Centro Educativo .- Formulario + E-mail.-

Cómo se notifican los incidentes al INCIBE y al Centro Criptológico Nacional.

Para reportar los incidentes al incibe, podemos hacerlo desde la pagina

<https://www.incibe.es/empresas/te-ayudamos/reporta-tu-incidente> .

Después tiene 4 tipos de incidentes, mediante fraude, ransomware, botnet y “denuncia tu incidente”

Fraude

Si te has visto afectado por un caso de fraude electrónico, puedes reportarlo al equipo de respuesta a incidentes de INCIBE-CERT, aportando:

- Una descripción detallada del incidente y tus datos de contacto.
- El correo sospechoso junto con sus cabeceras y ficheros adjuntos.

De esta forma, el equipo de respuesta a incidentes identificará mejor tu caso y te ayudará a resolverlo.

Ransomware

Si te has visto afectado por un ataque de tipo ransomware, puedes reportarlo al equipo de respuesta a incidentes de INCIBE-CERT, aportando:

- Una descripción detallada del incidente y tus datos de contacto.

- La nota de rescate original (ransom note) en el formato en el que se encuentre en su equipo. - Si no dispones de ella o no localizas el archivo, envía una captura de pantalla donde se visualice el contenido de la nota.

- Dos archivos cifrados por el ransomware (que no contengan datos de carácter personal, cuyos originales fueran formato Word o Excel y ocupen menos de un MB).

Si la incidencia afecta a datos de carácter personal, el incidente tiene que ser notificado antes de 72 horas por parte del «Responsable del tratamiento» a la «Autoridad de control competente». La autoridad competente para resolver cuestiones legales relacionadas con el RGPD es la AEPD (Agencia Española de Protección de Datos) o las análogas Autoritat Catalana de Protecció de Dades, de Cataluña, y Datuak Babesteko Euskal Bulegoa, del País Vasco.

También es recomendable que denuncies el incidente para que se investigue el origen del delito. Así colaboras en las labores de prevención a otras empresas y en las acciones para capturar al ciberdelincuente.

Botnet

Si has recibido una notificación de tu operador de servicios de Internet indicándote que perteneces a una botnet, o crees que puedes sufrir este tipo de incidente, puedes reportarlo al equipo de respuesta de incidentes de INCIBE-CERT, aportando:

- Una descripción detallada del incidente y tus datos de contacto.
- La dirección IP pública y fecha y hora de la detección (ejemplo de fecha y hora: 2019-10-30 T 10:45 UTC)
- El nombre de la botnet.

Denuncia tu incidente

Además de notificar el incidente al equipo de respuesta a incidentes de INCIBE-CERT para que te ayuden a resolverlo, también puedes interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado en cualquier comisaría o a través de sus diferentes portales web:

*Policía
Nacional*



*Guardia
Civil*



Ertzaintza



*Mossos
d'Esquadra*



*Policía
Foral*



*Brigada de
Investigación
Tecnológica de la
Unidad de
Investigación
Tecnológica (UIT)
de la Policía*

*Grupo de Delitos
Telemáticos (GDT)
de la Guardia Civil*

*Sección Central de
Delitos en
Tecnologías de la
Información
(SCDTI) de la
Ertzaintza*

Para notificar un incidente en el Centro Criptológico Nacional podemos hacerlo desde la página <https://www.ccn-cert.cni.es/es/gestion-de-incidentes/notificacion-de-incidentes.html>

Son varias las vías para notificar un incidente al CCN-CERT:

- Herramienta LUCIA para aquellas entidades del ámbito del Esquema Nacional de Seguridad.
- A través del correo electrónico Incidentes (incidentes@ccn-cert.cni.es)
- Se aconseja ofrecer una descripción lo más detallada posible del incidente y la información de contacto (al menos una dirección de correo y un teléfono). En este caso, se deberán cifrar los mensajes y autenticar la identidad. En nuestro sitio Web, encontrará nuestra clave PGP/GPG.

Herramienta lucia

LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) es una herramienta desarrollada por el CCN-CERT para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Con ella se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora.

LUCIA ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el seguimiento del mismo. El sistema permite, además, automatizar las tareas e integrarse con otros sistemas ya implantados.

Con la herramienta LUCIA, el organismo podrá gestionar tres tipos de ciberincidentes:

- Los incidentes propios del Organismo
- Los provenientes del Sistema de Alerta Temprana de Red SARA (SAT-SARA).
- Los provenientes del Sistema de Alerta Temprana de Internet (SAT-INET).

Las claves para la gestión de ciberincidentes son:

1. Disponer de herramientas, mecanismos, y procedimientos de detección que alerten al organismo de comportamientos anómalos en sus sistemas y redes. Para ello, se recomienda la adhesión al Sistema de Alerta Temprana (SAT) del CCN-CERT.
2. Es fundamental identificar la amenaza, la peligrosidad potencial y prevenir de esta manera el posible impacto sobre el servicio.
3. El organismo debe conocer su grado de madurez para responder al incidente en base a la tipología y peligrosidad definidos en la guía CCN-STIC 817.
4. Actuar con prontitud, sin dilación indebida. Notificar el incidente a la autoridad competente a través del CSIRT de referencia para establecer una comunicación directa. En el caso del sector Público, los organismos víctimas de posibles ciberincidentes deberán notificar al CCN-CERT. La notificación es un paso fundamental: el incidente puede estar afectando a otro organismo de forma simultánea.
5. Priorización y ejecución de procedimientos y medidas para evitar la propagación del incidente. El procedimiento de notificación de incidentes tiene que ser una realidad dentro del

marco normativo que desarrolla el plan de implantación para dar respuesta a la política de seguridad del organismo.

6. Recopilar toda la información del incidente. Revisar los eventos de seguridad y determinar los activos internos que han sufrido el intento de ataque y lo que es más importante priorizar en base a la peligrosidad y el contexto (triaje).

7. Documentar el incidente y las acciones llevadas a cabo en el momento de su detección.

8. Contener y mitigar la amenaza. Llevar a cabo labores de investigación, auditoría, bastionado, análisis forense e ingeniería inversa.

9. Restauración de sistemas y servicios siguiendo un plan establecido. Se determinará técnicamente el riesgo de reconexión de un sistema indicando los procedimientos a seguir y las salvaguardas a implementar para reducir el impacto para, en la manera de lo posible, evitar que se den de nuevo las circunstancias que lo propiciaron.

10. Resolución y cierre del incidente. Determinar el impacto del ciberataque y revisar y reforzar las políticas y medidas de seguridad necesarias.

Desde aquí podemos ver la documentación, acceder al sistema Lucia y descargar las claves PGP.

Documentación y descargas

- [Claves para la gestión de ciberincidentes \(infografía\)](#)
- [Compartir información, crear comunidad: cómo la notificación de incidentes contribuye a mejorar la ciberseguridad nacional \(infografía\)](#)
- [Cómo agilizar la gestión y notificación de ciberincidentes con LUCÍA \(infografía\)](#)

[Sistema LUCIA y actualizaciones](#) | contraseña: LUCIA

Contacto: lucia@ccn-cert.cni.es

Clave PGP [Descargar](#)

FINGERPRINT 05BF 19A8 3D73 2273 A0E3 5D6F 6B3E DCBF 4038 36FE

Podemos usar el sistema lucia (la contraseña es : LUCIA)



CCN LUCIA		Descargar
Todos los archivos		
Nombre	Tamaño	Modificado
Actualizaciones	3.8 MB	hace 3 años
CLAVE PGP	4 KB	hace 3 años
Documentacion	7.1 MB	hace 6 meses
LUCIA DEMO	3.4 GB	hace un mes
LUCIA Hyperv	2.4 GB	hace 3 años
LUCIA IVM	2.3 GB	hace 3 años
LUCIA NUBE	943 KB	hace 4 meses
LUCIA NUTANIX	2.3 GB	hace 3 años
LUCIA PROMIX	2.4 GB	hace 3 años
LUCIA VMWARE ESX	2.5 GB	hace 3 años
Presentacion LUCIA.pdf	1.7 MB	hace 3 años

10 carpetas y 1 archivo 15.3 GB

Podemos ver las claves publicas PGP:

```

PUBLIC-CCN-CERT LUCIA.asc
C: > Users > cdiaz > Downloads > PUBLIC-CCN-CERT LUCIA.asc
1  |-----BEGIN PGP PUBLIC KEY BLOCK-----
2
3  mQMuBGHv1twRCAD7rz/B10aQpWjI/SDqQoP0pyqy7q0aD94XrRPNyweHpv90+bHC
4  Lu6XuiZK307r/pOuywnArHK6oK2FXt4ShpENIGM6mqCm1cjTlxcIcb5LE2jlyeR
5  R5/e9iBXhc6sL1wM4jnv98tm7ZyLMSM18PI0iemEepd/yqCC9aGix+LAY7gl+poz
6  JIn1mAntwL97nCvB6V14N3SOCiG5+n9Wwd+bHXRRo179wLK9Ziv0E5ZQbOS/UZwu
7  cmRXgFvQHPzdV6uCnJ/RIA8Yh5ezimkVXS8mneTwIy8Wk7YQBRe6jBVu7oJg61b
8  oWlH+tw8y0uiWMGS8k0myxAK5X/GQ7RzfUjkVAQD/hdGhmMKWgJzqZXWQBSJLLode
9  XJao13DD3EFZVP7swf/e38Sug5fzGLLHddxavzrdMUTFcFuh1NXHvKQcoYnoALM
10 QstDCv9E8cqtU8ij0iRWAAT9bHfVlnEGgD6wOy8ftvn6nh+zMko2y+ElcB0jzM+
11 LHNzWJAftipEdflbywxNJXwSA2lVSvutF2wk7/8ci81ZzYJGoZSNOLNnmftfZ7tx
12 yc6Ij8N08tqh0oNlKxkbogaecOgoV4K/SUZTu/v/QYP1lmCu79xd8ibvHnNsEVQ
13 14Jeggip03LyfPOKX83CDhr1SRaXP8GMJTD3GHax6ke6wIfaa8neppmdfLLPqii/
14 CUznKuxhu0xqUqqefdcTVgOPP1w78fLX6rQ6K5x5AgA13Buu/O299vo3RLt9j8b
15 Gh59Y8pyM72u0+WD9p09p+Y9X9t7t/cjEsCY0dfu5xqJl8t1SE1FMX5HXsadbWz
16 OeawUiJjA7rM9+61Pew8tHgRS3yR8L4IediG3/SFY3GfiEPNBowdC1126IN1xE1p
17 +dU+rSwl/qB0043HJ3cNPCNcIF4aKWeHX0yIPkyX7yn0hznzWsQYzyTxIcHUhTxx
18 aF++uRLlu+M4Byll/0isb8D80KjF93pToAFW0DxxVPw6EWSrFnswh2Sj0pIKbXnA
19 mPVj730pPCv80+m/Bo4wLQLYAUOIHU4HIF2bkxvHght4Vs7Kw7RweBx4hjP7RIe
20 2bQnTFVDSUEgmJAYMi0yMDIzIDxsdlWnpYUBjY24tY2YdC5jbmkuZXm+iQCyBBAR
21 CABABQJh79bcBQkdyIAAMBSAAAAACAAB3ByZWZlcnJlZC1lbWVpbC1lbmNvZGlu
22 Z0BwZ3AuY29tcGdwbWltZQQLCQgHAhKBRRSDAAAAAXYCAQUeAQAAAAQVQgKAAoJ
23 EGs+3L9A0Db+A5oA/jbothh8DzW/B6Ae4BzsfNZUXoPHzc5nn29vGa6e84lTAPOs
24 Dckez/ML1NaAgofDAaE2ql0KcVP+ZZ6LK/Csgfksi7KEDQRh79bcEBAA+Rigflog
25 YXpDkXcBWyHhuxh7M1FHw7Y4KN5xsncegs5D/jRps2MEpT13wCFkiAtRXlKZmp
26 nwd00//jocwWIE6YzbjYDe4QXau2FxxR2FDKlIdDKb6V6FYrOHhcC9v4TE3V46pG
27 zPvOF+ggqRRh44SpT9GDhKh5tu+Pp0NGCMbHXdXJDhK4sTw6I4TZ5d0khNh9tvr
28 JQ4X/fay98h8ebByHTh1+/bBc8SDESYrQ2DD4+jWcv2hKCYLrqmus2UPogBTAA8
29 1qujEh76DyrOH3SET8rzF/OkQ0nX0ne2Q10CNSEmy2henXyYQCqNfi3t5F159dSS
30 T5sYjvwqp0t8MvZCV7cIfwgXcqK61q1C8wXo+VMROU+28W65S2gg2gGnVqMU6Y9A
31 VFPQ88bLQ6mUrfdmZIZJ+AyDvWxPf9Sh01D49V1f3HZSTZ09jdvomeFXklN/biu
32 de/F/Ha8g8VHMGHOfm1m/xX5U/2RXscBqtNbno2gpXI61Brwv0YAWCv19Ij9WE5J
33 280gtJ3kkQc2azNs0A1FHQ98iLMcFfstjvbyzSPAQ/ClwxiNjrtVjLhdONM0/XwX
34 V00jHRhs3jMhLUUq/zzhsS1AGBNfISnCNLWhsQDgcgHXKrKlQzZlp+r0ApQmwJG
35 0wg9ZqRdQZ+cFL2JSyIZJrqr017DVes91hcAaGIP/jr7CG3ELarNYUvwmVTT1cHr
36 ACSNFeUNERYP18eVmxe0si5dnpu7230eLH+bhhH10bMgh7y0aF30iOLTKa9FvHBX
37 bGPVWmWanzfHTLobMPEfSpC/z8cXJT5QNrv5+cH7sZhx6CXq5k1kr1deoRY7VSCe
38 30f6m+udhucvdxcd763+-09-16-05+-+7-76-13-16-03-06-13-

```

Como se van a notificar los incidentes en nuestro Centro Educativo. Formulario + E-mail.

Lo primero que vamos a hacer es irnos a la página web oficial del centro:

The screenshot shows the homepage of the IES Celia Viñas website. At the top, the school's name "IES CELIA VIÑAS" is displayed in large, bold letters, with "INSTITUTO HISTÓRICO EDUCATIVO ANDALUZ" underneath in a smaller font. Below this is a dark navigation bar with white text links: "CONÓCENOS", "INFORMACIÓN EDUCATIVA", "DEPARTAMENTOS", "PLANES Y PROYECTOS", "NOTICIAS", and "SECRETARÍA". A secondary row of links includes "BACHILLERATO INTERNACIONAL", "AUXILIARES DE CONVERSACIÓN", and "SCIENTIA OMNIBUS PORTUS". The main content area features three news items. The first, titled "Un alumno del IES Celia Viñas, medalla de oro en el campeonato Andalucía Skills", includes a graphic of a person climbing stairs and a date of "28 octubre, 2023". The second, "Reuniones Iniciales con las familias", features a graphic of a chalkboard and a date of "23 octubre, 2023". The third item, "MOODLE CENTROS", is partially visible on the right. The school's logo, a stylized building, is on the right side of the page.

Si bajamos a pie de página podemos ver las distintas formas de contactar con el centro educativo:

The footer is a dark grey rectangular box containing white text. It provides the following contact details: "© IES Celia Viñas | Instituto Histórico Educativo Andaluz", "C/ Javier Sanz 15 | 04004 Almería (España)", and "Teléfono: (+34) 950 15 61 51 | Email: 04001151.edu@juntadeandalucia.es".