softeng
Maximize the cloud.
Securely.

TOP PARTNER CLOUD
Microsoft

Maximiza el poder de la nube.
Avanza con seguridad.

RFC 2350
Softeng-CSIRT

17 de marzo de 2022

Índice

Sobre este documento

Introducción

El presente documento cumple con el estándar RFC 2350 publicado en:

- https://www.ietf.org/rfc/rfc2350.txt

Fecha de última actualización

El presente documento se encuentra publicado en la versión **1.0**, cuya fecha de última actualización es del **17 de marzo de 2022**.

Ubicaciones dónde puede encontrarse el presente documento

El presente documento es accesible públicamente en la página web de Softeng, concretamente, en el siguiente enlace:

- https://www.softeng.es/areas-de-especializacion/security/softeng-csirt.

Información de contacto

Nombre del equipo

El equipo CSIRT de Softeng se denomina **Softeng-CSIRT.**

Dirección postal

La dirección postal es la siguiente:

- C/ Pau Claris, 162-164, 2-6, 08037, Barcelona.

Zona horaria

La zona horaria es la siguiente:

- Hora central europea (CET/CEST).

Teléfono de contacto

El teléfono de contacto es el siguiente:

- +34 932 37 59 11.

Direcciones de correo electrónico de contacto

Las direcciones de correo electrónico de contacto son las siguientes:

- Comunicaciones generales: csirt@softeng.es.
- Notificación de incidentes: incidentes.csirt@softeng.es.

La huella digital y la clave PGP pública están especificadas en el apartado **"Información de cifrado".**

Otros canales de comunicación

No se dispone de otros canales de comunicación adicionales a los indicados en los apartados **"Teléfono de contacto"** y **"Direcciones de correo electrónico de contacto"** del presente documento.

Información de cifrado

Softeng-CSIRT pone a disposición una clave PGP pública para cifrar todas aquellas comunicaciones entrantes y salientes de las direcciones de correo electrónico especificadas en el apartado **"Direcciones de correo electrónico de contacto"** que, por su nivel de confidencialidad, así lo requieran, y cuya huella digital es la siguiente:

- FB25 F81F F502 6714 9C8E 532B 1279 F37F 0147 B357.

La clave PGP pública se puede encontrar en el siguiente enlace:

- https://www.softeng.es/areas-de-especializacion/security/softeng-csirt.

Composición del equipo

Softeng-CSIRT se encuentra compuesto por personal interno de Softeng que desempeña los siguientes perfiles:

- Analistas de seguridad (nivel 1).
- Analistas de seguridad (nivel 2).
- Analistas de seguridad (nivel 3).
- Ingenieros de seguridad.
- Cazadores de amenazas (*threat hunters*).
- Analistas de inteligencia de amenazas (*threat Intelligence*).
- Investigadores forenses.
- Coordinador del equipo.
- Administrador técnico del equipo.
- Responsable de ciberseguridad.

La información sobre la identidad de los miembros que desempeñan estos perfiles, así como cualquier otro dato relacionado con estos, es confidencial y no se publica en el presente documento.

Horario establecido

El horario de trabajo establecido para Softeng-CSIRT es de 24 horas, 7 días a la semana y 365 días al año.

Información adicional

Cualquier información adicional relativa a Softeng-CSIRT, se puede consultar en la página web de Softeng, concretamente, en el enlace:

- https://www.softeng.es/areas-de-especializacion/security/softeng-csirt.

Para cualquier duda y/o pregunta, es posible utilizar los canales de comunicación especificados en los apartados **"Teléfono de contacto"** y **"Direcciones de correo electrónico de contacto"** del presente documento.

Constitución

Misión

Las empresas 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 ciberseguridad.

A esta nueva realidad de las organizaciones se suma que las amenazas son cada vez más sofisticadas y diversas, estando todos cada vez más expuestos al cibercrimen. Este hecho, unido a la necesidad de cumplimiento de ciertas obligaciones legales, hace cada vez más necesario que las empresas dispongan de un equipo dedicado para la respuesta ante incidentes de seguridad informática.

En Softeng, conocedores de esta necesidad y gracias a nuestra experiencia en soluciones y servicios de ciberseguridad, ofrecemos a nuestros clientes un servicio de CSIRT 24×7 que permite disponer de una visión y gestión centralizada de las amenazas de ciberseguridad. Nuestro servicio cuenta con una estructura organizativa y procedimientos asociados, que, unidos a nuestro equipo técnico especializado, permiten a nuestros clientes disponer de la máxima protección en sus activos de negocio (identidad, dispositivos, servidores, infraestructuras, aplicaciones y servicios). De este modo, acompañamos a nuestros clientes maximizando el poder de la nube de Microsoft para impulsar la innovación digital con seguridad e inteligencia.

Softeng-CSIRT es un equipo de respuesta ante incidentes de seguridad (CSIRT), de ámbito privado, constituido por Softeng para detectar, investigar, mitigar y responder ante las amenazas de ciberseguridad de la propia compañía (CSIRT interno) como de otras compañías externas a las que Softeng presta servicio (CSIRT comercial), poniendo a disposición de Softeng y de sus clientes los servicios de seguridad requeridos para proteger los Sistemas de Información y activos ante amenazas que puedan poner en juego su integridad, confidencialidad y/o disponibilidad.

Circunscripción

Los servicios proporcionados por Softeng-CSIRT están dirigidos a la propia compañía a la que pertenece, Softeng, así como a sus clientes, compañías privadas que deciden contratar los servicios de acompañamiento de Softeng.

Autoridad

Softeng-CSIRT ejerce sus funciones, dentro de la propia compañía, bajo la autoridad del responsable del departamento de sistemas y seguridad de Softeng. En cuanto a las compañías externas que son clientes de Softeng, Softeng-CSIRT ejerce funciones de consultoría de seguridad y no dispone de autoridad sobre los mismos.

Políticas

Tipología de incidentes y nivel de soporte

Softeng-CSIRT proporciona servicios de detección, investigación, clasificación y respuesta ante incidentes de seguridad que puedan afectar a la integridad, disponibilidad y/o confidencialidad de las infraestructuras TI de los clientes de Softeng.

La tipología de incidentes gestionados se corresponde con lo establecido por el **Centro Criptológico Nacional de España (CCN),** tomando como referencia el documento **"Gestión de ciberincidentes"** de la **Guía de seguridad de las TIC, CCN-STIC 817**, en el ámbito del **Esquema Nacional de Seguridad (ENS)**. Este documento se puede consultar en el siguiente enlace:

- 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 lo establecido en el documento, los incidentes se clasifican según su tipología y severidad, priorizando la respuesta en base a los resultados de esta clasificación.

El nivel de soporte proporcionado por Softeng-CSIRT dependerá de las condiciones contractuales del servicio establecidas con cada cliente y de la tipología, impacto, severidad y/o complejidad de los incidentes. Del mismo modo, el nivel de interlocución durante la gestión de los incidentes, los canales a utilizar y la información que puede o no puede ser intercambiada con otros interlocutores también dependerá de las condiciones contractuales del servicio establecidas con cada cliente.

Cooperación, interacción y distribución de información

Softeng-CSIRT interactúa, diariamente, con otras organizaciones, como autoridades legales, otros equipos CSIRT, proveedores y/o equipos de inteligencia de amenazas, con los que intercambia distinta información según el tipo de organización y las relaciones que mantienen con Softeng-CSIRT.

De entre estas organizaciones, es posible destacar las siguientes, debido a su relevancia en el ámbito de ciberseguridad nacional:

- **CCN-CERT** (https://www.ccn-cert.cni.es), para comunicar incidentes relevantes de seguridad de la información y sistemas que afectan a organismos y empresas públicas.
- **INCIBE-CERT** (https://www.incibe-cert.es), para comunicar incidentes relevantes de seguridad de la información y sistemas que afectan a ciudadanos, organismos y empresas privadas.
- **AEPD** (https://www.aepd.es/es), para comunicar incidentes relevantes que pongan en riesgo o provoquen la filtración de datos de carácter personal, protegides por el Reglamento de Protección de datos (RGPD) europeo y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- **Microsoft Security Response Center** (https://www.microsoft.com/en-us/msrc) para reportar nuevos incidentes, amenazas, vulnerabilidades, muestras de phishing, malware, ransomware, APT, comportamientos sospechosos, etc. cuando no se detectan por parte de los productos de Seguridad de Microsoft 365 o Azure, con el objetivo de mejorar la detección de la BBDD de inteligencia de amenazas de Microsoft (Microsoft Threat Intelligence) y de este modo, nutrir a todos los clientes de Microsoft 365 y Azure con dichas detecciones para evitar brechas de seguridad.

Además, es fundamental para Softeng-CSIRT establecer relaciones formales de cooperación, interacción y distribución de la información con otros equipos CSIRT, por lo que, en el momento de redacción de este documento, se ha iniciado el proceso para formar parte de diferentes comunidades de intercambio de información de amenazas, tales como:

- **FIRST:** https://www.first.org.
- **TF-CSIRT**: https://www.trusted-introducer.org.
- **CSIRT.es**: https://www.csirt.es.
- **Red Nacional de SOC**: https://rns.ccn-cert.cni.es.
- **Foro Nacional de Ciberseguridad**: https://foronacionalciberseguridad.es.
- **APWG (Anti Phishing Working Group):** https://apwg.org.

Por otra parte, Softeng ya es miembro de **ISMS Forum**. Esta información se puede consultar en el siguiente enlace:

- https://www.ismsforum.es/miembros/lista-miembros.php.

Softeng-CSIRT, cumpliendo, además, con las políticas de seguridad de la información implementadas en Softeng, hará uso del protocolo **FIRST TLP v2.0 (Traffic Light Protocol)** para la clasificación y etiquetado de la información:

- https://www.first.org/tlp.

Los propietarios de la información serán los responsables de clasificarla, e indicar cómo y con quién se puede compartir en base a dicha clasificación.

Como medidas de seguridad y privacidad adicionales en la gestión de la información compartida, Softeng-CSIRT se compromete a:

- Aplicar, en todo momento, medidas de clasificación y cifrado para la protección de la información.
- Anonimizar, dentro de lo posible, la información compartida y seleccionando, únicamente, aquella más relevante.
- Respetar el grado de confidencialidad asignado a la información.
- No compartir información confidencial con otras partes sin un acuerdo y/o autorización por parte del propietario de esta.
- Proteger la privacidad de la información personal. Aunque de modo general no se compartirá información personal, si fuese necesario hacerlo, y dentro de las directrices y normes recogidas en las normatives europea y española de protección de datos personales, se solicitará la autorización expresa de los propietarios de esta.
- Detener la distribución de información en el momento en el que los propietarios de esta notifiquen la denegación del permiso para ello, salvo en los supuestos casos en que exista una obligación legal o normativa superior que obligue a compartir dicha información.

Comunicación y autenticación

Tal y como se ha indicado en los apartados **"Teléfono de contacto"** y **"Direcciones de correo electrónico de contacto"** del presente documento, los canales de comunicación de Softeng-CSIRT son mediante correo electrónico y teléfono, siendo, el primero, el utilizado como canal principal:

- **Comunicación por correo electrónico:** Este canal de comunicación podrá ser empleado sin cifrar para la transmisión de información no sensible, siendo responsable de determinar la sensibilidad de la información que se requiere transmitir, el remitente de los correos electrónicos. Para la transmisión de información sensible, se utilizarán claves PGP para la firma y el cifrado de los correos electrónicos. Las claves PGP se pueden consultar en el apartado "Información de cifrado" del presente documento.
- **Comunicación por teléfono:** Este canal de comunicación siempre tendrá que ser empleado sin cifrar para la transmisión de información no sensible, puesto que se considera lo suficientemente seguro para la transmisión de este tipo de información.

Servicios

Tal y como se ha indicado en el apartado **"Políticas"** del presente documento, Softeng-CSIRT proporciona servicios de detección, investigación, clasificación y respuesta ante incidentes de seguridad que puedan afectar a la integridad, disponibilidad y/o confidencialidad de las infraestructuras TI de los clientes de Softeng.

Estos servicios se proporcionan mediante el apoyo y colaboración de los beneficiarios, en este caso, los clientes de Softeng mediante servicios gestionados, ayudando a nuestros clientes desplegando soluciones para proteger, detectar y responder frente a las amenazas de seguridad en las diferentes superficies de ataque de las empresas. A continuación, se detallan los servicios prestados desde Softeng-CSIRT.

Gestión y respuesta ante incidentes

Detección de incidentes

- Implantación de servicios y configuraciones que permitan generar incidentes de seguridad cuando se detecten posibles amenazas.
- Implantación de sistema SIEM (Security Information and Event Management) para la concentración y recepción de todos los incidentes de seguridad.

Investigación de incidentes

- Verificación de la existencia, causa inicial y alcance de los incidentes.
- Notificación a los clientes de Softeng de toda la información relativa a los incidentes que afectan a su organización.
- Notificación a las posibles partes interesadas de la existencia de los incidentes, si fuese necesario, y según lo establecido en el apartado **"Cooperación, interacción y distribución de información"** del presente documento.

Clasificación de incidentes

- Determinación de si los incidentes se tratan de positivos malignos, positivos benignes o falsos positivos.
- Priorización de la respuesta ante incidentes en función de la causa, alcance y clasificación de estos.

Respuesta ante incidentes

- Implementación de acciones manuales y/o automáticas necesarias para la prevención y/o mitigación de los incidentes.

Análisis de vulnerabilidades y sistema de alerta temprana

- Softeng-CSIRT proporciona servicios de detección, análisis y notificación de las vulnerabilidades aplicaciones y sistema operativo que afecten a los dispositivos de usuario, servidores y dispositivos de red de los clientes de Softeng.
- Estos Servicios de proporcionan de manera proactiva con el objetivo de que los clientes conozcan las vulnerabilidades que afectan a sus sistemas y las puedan corregir antes de que la explotación de estas por parte de un atacante pueda provocar un incidente de seguridad mayor.

Análisis de vulnerabilidades

- Implementación de sistema de análisis de vulnerabilidades de dispositivos de usuario, servidores y dispositivos de red.
- Contraste de las vulnerabilidades detectadas con la información publicada por el organismo NIST (National Institute of Standards and Technology).
- Notificación a los clientes de Softeng de toda la información relativa a las vulnerabilidades que afectan a su organización.
- Panel personalizado de vulnerabilidades integrando los dispositivos de usuario, servidores y dispositivos de red.

Sistema de alerta temprana

- Notificación a los clientes de Softeng de aquellas vulnerabilidades más críticas y de día cero que afectan a su organización.

Búsqueda de amenazas (*threat hunting*)

Softeng-CSIRT proporciona servicios de detección proactiva de amenazas en las infraestructuras TI de los clientes de Softeng, mediante la ejecución recurrente de búsquedas de posible actividad maliciosa y la notificación a los clientes de Softeng de aquellos resultados más relevantes.

Se dispone de más de 250 casos de uso para realizar búsquedas y se incluye un panel de búsqueda personalizado disponible para los cazadores de amenazas (*threat hunters*).

Inteligencia de amenazas (*threat intelligence*)

Softeng-CSIRT proporciona servicios de inteligencia de amenazas en las infraestructuras TI de los clientes de Softeng, con el objetivo de identificar artefactos maliciosos, conocidos como indicadores de compromiso (IOCs) y de generar incidentes cuando se detecte actividades inusuales en las que estén involucrados estos IOCs.

Para ello, Softeng-CSIRT se vale de la plataforma de inteligencia contra amenazas de Softeng (https://ti.softeng.es), del protocolo TAXII (Trusted Automated eXchange of Intelligence Information) y del lenguaje STIX (Structured Threat Information eXpression). En esta plataforma, se concentra miles de IOCs de distintas fuentes que se van actualizando diariamente.

El uso de esta plataforma está limitado a ciertas IPs, no es accesible públicamente al exterior. En el caso de requerir acceso para el intercambio de información de amenazas, se debe solicitar el acceso a Softeng-CSIRT para añadir las IPs a las ACLs pertinentes.

Vigilancia digital

Softeng-CSIRT proporciona servicios de detección de activos corporativos de los clientes de Softeng expuestos a Internet (Web, Deep Web y Dark Web), con el objetivo de reducir las vulnerabilidades de estos, los riesgos de sufrir un incidente de seguridad y mejorar la reputación digital de la compañía.

Simulación de ataque

Softeng-CSIRT proporciona servicios de preparación, ejecución y supervisión de ataques simulados de suplantación de la identidad (*phishing*) en la organización de los clientes de Softeng, con el objetivo de detectar aquellos usuarios con una baja cultura de ciberseguridad y que son más susceptibles de ser vulnerados bajo un ataque real.

Además, se dispone de una plataforma propia creada con tecnología Microsoft basada en píldoras formativas para formar y concienciar a los usuarios, que nos permite identificar el nivel de formación de cada uno de ellos y el nivel de trampas de visualización de videos que nos permite cuadrar estos datos con los datos de la simulación de ataque.

Informe de seguridad trimestral

Softeng-CSIRT elaborará un entregable que se presentará en una reunión trimestral con los clientes de Softeng para revisar el análisis de los servicios proporcionados y de la postura de seguridad de la organización.

Formulario de notificación de incidentes

Los clientes de Softeng notificarán a Softeng-CSIRT mediante correo electrónico cuando detecten un evento o incidente de seguridad en su organización. La dirección de correo electrónico que se empleará es la dirección de correo de incidentes que figura en el apartado "Direcciones de correo electrónico de contacto" del presente documento y los mensajes enviados tendrán que estar cifrados mediante cifrado PGP, tal y como se indica en el apartado "Información de cifrado" del presente documento.

Los mensajes deberán de acompañarse del formulario de notificación de incidentes cumplimentado, que se puede encontrar en el siguiente enlace:

- https://www.softeng.es/areas-de-especializacion/security/softeng-csirt.

Este procedimiento tendrá en cuenta tanto la clasificación de la información como los acuerdos que se hayan establecido entre Softeng y cada cliente en el inicio de la prestación de los servicios.

Exención de responsabilidad

Aunque se tomarán todas las precauciones en la elaboración de la información, notificaciones y alertas, Softeng-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.

softeng

Maximize the cloud.
Securely.

hola@softeng.es
+34 93 237 59 11