URUDATA CIBERSEGURIDAD

TLP:CLEAR

CSIRT Urudata Ciberseguridad

RFC 2350

TLP:CLEAR

URUDATA CIBERSEGURIDAD

TLP:CLEAR

Índice

TLP:CLEAR

TLP:CLEAR

1. Información del documento

Este documento contiene una descripción de Urudata Ciberseguridad como se implementa según la RFC 2350. Proporciona información básica sobre Urudata Ciberseguridad, sus canales de comunicación, sus roles, responsabilidades y los servicios ofrecidos.

1.1. Fecha de última actualización

Versión 1, creada el 07/01/2024.

1.2. Lista de distribución para notificaciones

No existe una lista de distribución para notificaciones ante modificaciones de este documento. Este documento se mantiene actualizado en la ubicación especificada en 1.3 - "Dónde encontrar este documento". Para consultar por actualizaciones puede comunicarse con el correo electrónico de Urudata Ciberseguridad.

1.3. Dónde encontrar este documento

La versión actual y más reciente de este documento está disponible en el sitio web de Urudata Ciberseguridad. Su URL es: https://www.urudataciberseguridad.com/

Por favor, asegúrese de estar utilizando la última versión.

1.4. Autenticación del documento

Este documento ha sido firmado con la clave PGP de **Urudata Ciberseguridad.** La firma está disponible en el sitio web de Urudata Ciberseguridad. Su URL es: https://www.urudataciberseguridad.com

1.5. Identificación del documento

- Título: **Urudata Ciberseguridad RFC 2350**
- Versión: 1.0
- Fecha del Documento: 07-01-2024
- Caducidad: Este documento es válido hasta ser reemplazado por una versión posterior.

2. Información de contacto

Esta sección describe cómo contactar a Urudata Ciberseguridad.

2.1. Nombre del equipo

Nombre completo: Urudata Ciberseguridad.

Urudata Ciberseguridad es el nombre comercial del Centro de Operaciones de Seguridad de Urudata Ciberseguridad.

2.2. Dirección

Urudata Ciberseguridad.

Santiago de Chile 1322, Oficina 1001, Montevideo, Uruguay.

2.3. Zona horaria

GTM-3, hora local de Montevideo.

2.4. Número de Teléfono

+598 2419 6457 interno 260

2.5. Dirección de correo electrónico

Si necesita notificarnos acerca de un incidente de seguridad de la información o amenaza de ciberseguridad contra o involucrando a Urudata Ciberseguridad, por favor contáctenos a través de: csirt@urudata.com

2.6. Información, cifrado y llaves públicas

ID de Clave: 0xB0635BFD
Huella Digital: 86C5 7084 5CCA 88BE F43A 2784 6A24 EEB6 B063 5BFD

La clave deberá ser utilizada siempre que la información deba ser enviada a Urudata Ciberseguridad de manera segura, y la misma se encuentra disponible en https://keyserver.ubuntu.com/. Utilizando el ID de la clave se puede obtener la llave pública.

- Por favor, utilice esta clave cuando desee/necesite encriptar mensajes que envíe a Urudata Ciberseguridad.
- Cuando corresponda, Urudata Ciberseguridad firmará mensajes.
- Cuando corresponda, firme sus mensajes utilizando su propia clave.

2.7. Miembros del equipo

- Gerente de Ciberseguridad: Fernando Franceschi
- Gerente de Operaciones: José Callero
- Gerente de Consultoría: Claudio López
- Manager: Luis Tognola
- El equipo del CSIRT está compuesto por técnicos y analistas de ciberseguridad.

2.8. Otra información

Información general de Urudata Ciberseguridad se puede encontrar en: https://www.urudataciberseguridad.com

2.9. Puntos de Contacto

El método principal para contactar a Urudata Ciberseguridad es enviar un correo electrónico a la siguiente dirección: ciberseguridad@urudata.com. Para contactarse por incidentes de seguridad, contactarse con csirt@urudata.com

Si es necesario, los casos urgentes pueden ser reportados por teléfono al +598 2419 6457 interno 260. El horario de operación de Urudata Ciberseguridad es 24x7x365.

3. Estatuto

Esta sección describe el mandato de Urudata Ciberseguridad.

3.1. Propósito

Urudata Ciberseguridad fue creado en el año 2023 dentro de la organización Urudata S.A. con el fin de brindar servicios especializados tanto para la organización anfitriona como para clientes externos. El mismo es un equipo privado que brinda servicios de seguridad, principalmente en Uruguay.

Ante las cada vez más diversas amenazas que surgen en el mundo de la informática, y que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información de las empresas, Urudata Ciberseguridad surge para dar respuesta a estos retos, poniendo a disposición a sus técnicos altamente capacitados y experimentados en lo que a seguridad de la información refiere y a los sistemas y servicios necesarios para proteger los sistemas de información de sus clientes.

Urudata Ciberseguridad establece como objetivo asistir a sus clientes en las siguientes actividades:

- Mejora de la postura de seguridad mediante consultorías.

- Análisis y evaluación de riesgos.
- Reducir la superficie de ataque.
- Monitoreo y respuesta de a incidentes.
- Asesoría en respuesta de incidentes
- Implementar sistemas de detección y alerta de eventos de seguridad que permitan realizar detecciones tempranas de incidentes o posibles incidentes.

Urudata Ciberseguridad se encuentra en la búsqueda constante de mantener los mejores estándares de calidad y para ello está siempre en búsqueda de adoptar las mejores prácticas

- Urudata Ciberseguridad cuenta con las políticas y procedimientos necesarios para asegurar los procesos adecuados y el cumplimiento de la normativa legal.
- Aplica las mejores prácticas comúnmente conocidas en el sector de la Ciberseguridad.
- Establece acuerdos de comportamiento y de confidencialidad para todo el personal.

3.2. Constituyentes

Urudata Ciberseguridad brinda servicios a sus clientes y a su organización anfitriona, Urudata S.A., incluyendo sus usuarios, sistemas, aplicaciones y redes.

3.3. Afiliación

Urudata Ciberseguridad forma parte de Urudata S.A, su organización anfitriona, brindando servicios especializados en ciberseguridad.

3.4. Autoridad

Urudata Ciberseguridad participa y puede coordinar la respuesta a incidentes de seguridad únicamente a petición de sus constituyentes, por lo cual Urudata Ciberseguridad opera con el auspicio y la autoridad delegada por sus constituyentes.

Urudata Ciberseguridad actúa principalmente como un asesor en relación con los equipos de seguridad de sus constituyentes, y puede no tener ninguna autoridad para exigir acciones específicas. La implementación de las recomendaciones no es responsabilidad de Urudata Ciberseguridad, sino únicamente de aquellos a quienes se les hicieron las recomendaciones.

3.5. Responsabilidades

Las responsabilidades de Urudata Ciberseguridad están claramente definidas en las condiciones contractuales establecidas con cada uno de sus constituyentes. Estas incluyen:

- Proveer servicios de monitoreo y detección de incidentes de seguridad.
- Coordinar y asesorar en la respuesta a incidentes de ciberseguridad cuando sea solicitado.
- Informar sobre amenazas de seguridad emergentes y proporcionar recomendaciones estratégicas y operativas.

La implementación de las recomendaciones hechas por Urudata Ciberseguridad es responsabilidad exclusiva de los constituyentes.

4. Políticas

Esta sección describe las políticas de Urudata Ciberseguridad.

4.1. Tipos de incidentes y nivel de soporte/servicio.

Urudata Ciberseguridad presta a sus clientes servicios de detección, análisis y respuesta a incidentes de seguridad que puedan afectar la confidencialidad, integridad y/o disponibilidad de la información de sus clientes.

Urudata Ciberseguridad abarca los tipos de incidentes de seguridad informática que ocurren o amenazan con ocurrir en su conjunto de clientes.

El nivel de apoyo brindado por el Urudata Ciberseguridad variará según el tipo y la gravedad del incidente o problema, el nivel de soporte prestado en cada caso dependerá de lo establecido contractualmente con cada cliente de Urudata Ciberseguridad.

4.2. Cooperación, interacción y divulgación de información

Urudata Ciberseguridad considera de gran importancia la coordinación operativa y el intercambio de información entre organismos similares (SOC, CSIRT, CERT) y con otras organizaciones, que puedan ayudar a prestar sus servicios o que proporcionen beneficios para ambas partes

Dado esto, el Urudata Ciberseguridad intercambia información necesaria con las partes afectadas, así como otros organismos similares. Sin embargo, no se intercambian datos personales ni generales a menos que se autorice explícitamente.

Urudata Ciberseguridad protegerá la privacidad de sus clientes. Toda la información entrante es tratada de forma confidencial por Urudata Ciberseguridad, independientemente de su prioridad.

Todos los datos sensibles (como datos personales, configuraciones del sistema, vulnerabilidades conocidas con sus ubicaciones) se almacenan en un entorno seguro y se cifran si deben transmitirse a través de un entorno no seguro.

Urudata Ciberseguridad admite el protocolo de semáforo de intercambio de información versión 2.0. La información que llegue con las etiquetas blanco, verde, ámbar o rojo será manejada apropiadamente. Los detalles se encuentran en el siguiente enlace: https://www.first.org/tlp/

4.3. Comunicación y autenticación

Tal como se vio en el punto 2, la comunicación con Urudata Ciberseguridad se realizará en los canales allí descriptos, siendo el correo electrónico el principal medio de intercambio de información de manera confidencial y protegida.

Para el intercambio de información, Urudata Ciberseguridad también reconoce y soporta el protocolo TLP (Traffic Light Protocol) en su versión 2.0 (https://www.first.org/tlp/)

5. Servicios

5.1. Gobernanza

- Guía a la organización a la hora de desarrollar e implementar políticas, guías y procedimientos de seguridad.

5.2. Gestión del cumplimiento

- Soporte a la empresa en el proceso de alineación/cumplimiento con todas las regulaciones y normas relevantes, como ser ISO27001, NIST CSF, Marco de Ciberseguridad de AGESIC, PCI DSS, GDPR, etc.

5.3. Análisis y evaluación de riesgos

- Evaluación exhaustiva de riesgos.
- Identificación de vulnerabilidades, posibles amenazas y el impacto de estas en la empresa.
- Análisis de controles necesarios para mitigar los riesgos existentes.

5.4. Consultoría en respuesta de incidentes

- Apoyo a la empresa al desarrollar un plan de respuesta a incidentes, para que esté preparada ante la existencia de eventos que comprometan su seguridad, y poder responder y recuperarse de manera ágil y efectiva, mitigando el impacto de estos y las pérdidas ocasionadas.

5.5. Auditorías de seguridad en infraestructura

- Proceso de análisis de vulnerabilidades sobre infraestructura, a fin de detectar debilidades y definir los controles correctivos necesarios.

5.6. Auditoría en seguridad en aplicaciones

- Evaluación de vulnerabilidades en aplicaciones de forma de detectar fallas en la codificación que lo hagan pasible de ataques, previniendo incidentes que puedan comprometer la confidencialidad, integridad y/o disponibilidad de la información.

5.7. Seguridad ofensiva

- Realización de pruebas de penetración, emulando el comportamiento de un atacante, permitiendo con esto identificar vulnerabilidades y promover mejoras en el establecimiento de una estrategia defensiva.

5.8. Servicio de Asesoría en Seguridad (SAS)

- Asesorar a la organización en estrategias de seguridad operativa, así como acompañar a los proyectos e iniciativas que surjan de dichas recomendaciones.
- Seguimiento periódico del estado de las actividades relacionadas a la operación de seguridad que permite detectar desvíos y demoras, de forma de poder tomar las acciones correctivas correspondientes.

5.9. Monitoreo y respuesta a Incidentes (SOC/CSIRT)

- Servicios de seguridad gestionados continuos (7x24x365) tanto para ayudar a la empresa a monitorear su infraestructura de TI en busca de posibles amenazas (SOC) así como responder rápidamente a cualquier incidente (CSIRT).

5.10. Concientización de seguridad

- Capacitación y concientización de seguridad a los empleados, de manera didáctica (no técnica) para ayudarles a comprender la importancia de la ciberseguridad, cómo identificar posibles amenazas y protegerse de las mismas.

5.11. Presentaciones ejecutivas

- Presentaciones a la alta dirección y gerencias, visualizando los aspectos superlativos de la ciberseguridad, reconocimiento de amenazas y estado actual en el mundo y en concreto al rubro desarrollado, y el estado actual de la empresa ante ese escenario.

6. Comunicación y reporte de Incidentes

Cuando un cliente detecta un evento o incidente de seguridad, se lo reportará a Urudata Ciberseguridad a través del correo csirt@urudata.com. En el intercambio de esta información se utilizarán las medidas de protección pertinentes, mediante el uso de claves PGP.

Estas medidas tendrán en cuenta tanto la clasificación de la información, como los acuerdos que se hayan establecido con cada cliente al inicio de la prestación del servicio.

A la hora de reportar un incidente de seguridad se solicita que se provea la siguiente información:

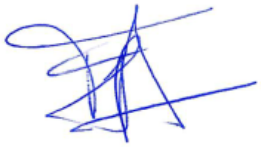
- Descripción de lo sucedido.
- Usuario/s afectados.
- Fecha y hora del incidente.
- Fecha y hora de la detección del incidente.
- Recursos afectados.

7. Exclusiones de responsabilidad

Urudata Ciberseguridad tomará todas las precauciones en la elaboración de información, notificaciones y alertas. Urudata Ciberseguridad no asume ninguna responsabilidad por errores o mal uso que se realice de la información proporcionada durante la ejecución de sus servicios.

8. Aprobación

Este documento ha sido aprobado por:



Fernando Franceschi
Gerente de Ciberseguridad 18/09/2024

Fecha de Revisión: Próxima revisión programada para el 18/03/2025.