WIN CSIRT RFC-2350

1. Acerca de este documento

1.1 Fecha de última actualización: Esta es la versión 2.0 del 22/09/2023

1.2 Lista de distribución para notificaciones: Los cambios a este documento no se distribuyen por una lista de correo. Cualquier pregunta o comentario específico, por favor diríjase a la dirección de correo csirt@winempresas.pe (Esta lista de correo es moderada).

1.3 Ubicación del documento: La última versión del documento se encuentra publicada en:

English: https://winempresas.pe/files/csirt/rfc/english/WIN-CSIRTdescription.pdf

Español: https://winempresas.pe/files/csirt/rfc/spanish/WIN-CSIRTdescription.pdf

2. Información de contacto

2.1 Nombre del equipo: WIN CSIRT Equipo de respuesta a incidentes de seguridad informática de WIN EMPRESAS.

2.2 Dirección: Oficina principal: Av. Jose Gálvez Barrenechea 645 – San Isidro – Lima - Perú

2.3 Zona horaria: UTC -5. Lima/Perú.

2.4 Correo electrónico: Información e incidentes csirt@winempresas.pe

Huella digital	A835862C72AF839966F6DCFF6266A87D7BD98FFB
KEY ID	6266 A87D 7BD9 8FFB

2.5 Teléfono: +51 01 680-9866

2.6 Miembros del equipo: Una lista completa de los miembros del equipo no está disponible públicamente. Los miembros del equipo se identificarán ante la parte informante con su nombre completo en una comunicación oficial sobre un incidente.

2.7 Puntos de contacto con el cliente:

- Correo electrónico -> Método preferido
- Teléfono -> Método secundario

En caso de requerir asistencia urgente, ponga **"urgente"** en el asunto. Si no es posible (o no es aconsejable por razones de seguridad) utilizar el correo electrónico, se puede contactar con el WIN CSIRT por teléfono durante el horario de atención establecido. Los mensajes telefónicos se comprueban con menos frecuencia que el correo electrónico.
El horario de funcionamiento del WIN CSIRT se limita generalmente a las horas normales de oficina (09:00-18:00 de lunes a viernes, excepto los días festivos). Sin embargo, en caso de incidente crítico o servicio contractual, el funcionamiento es 24*7*365.
Si es posible, cuando envíe su informe, utilice el formulario mencionado en la sección 6.

3. Carta

3.1 Misión:

La misión del WIN CSIRT es apoyar activamente a las actividades de ciber resiliencia de nuestros clientes internos y externos. Para lograrlo, tenemos los siguientes objetivos:

- Ayudar a nuestros clientes a reforzar sus capacidades de detección temprana para reducir los riesgos de ciberseguridad mediante la aplicación de controles y medidas proactivas.
- Ayudar a la comunidad de clientes de WIN EMPRESAS a responder a estos incidentes cuando se produzcan.
- Apoyar a las actividades de recuperación de las operaciones de nuestros clientes para que puedan alcanzar sus objetivos empresariales en materia de seguridad de la información y continuidad del negocio.

3.2 Comunidad atendida:

La jurisdicción del WIN CSIRT son: clientes internos y externos, del sector público o privado. Sin embargo, se debe tener en cuenta que, a pesar de lo anterior, los servicios de WIN CSIRT se prestarán principalmente para los sistemas de los centros de datos de WIN EMPRESAS y otras ubicaciones de los centros de datos o computo de los clientes que estén suscritos para los servicios CSIRT que brindamos. En el área de Lima metropolitana y Callao. Para otras ubicaciones más alejadas y/o en el contexto de una pandemia o similar; podemos actuar, siempre y cuando se nos proporcione un acceso remoto seguro a la infraestructura donde se ha producido el incidente.

3.3 Patrocinio: WIN CSIRT está patrocinado por WIN EMPRESAS.

3.4 Autoridad: WIN CSIRT opera bajo los auspicios de WIN EMPRESAS y con autoridad delegada por esta. WIN CSIRT espera trabajar en cooperación con los administradores de sistemas y los usuarios de WIN EMPRESAS y con los equipos correspondientes de clientes y, en la medida de lo posible, evitar las relaciones autoritarias. Sin embargo, si las circunstancias lo justifican, el WIN CSIRT apelará a WIN EMPRESAS para ejercer su autoridad, directa o indirecta, según sea necesario.

Todos los miembros del WIN CSIRT pertenecen al equipo de ciberseguridad y comunicaciones de la unidad de negocio Cloud de WIN EMPRESAS, y tienen todas las facultades y responsabilidades asignadas de acuerdo con los sistemas que administran o en su defecto, son miembros de la dirección de WIN EMPRESAS.

Los miembros de la comunidad que deseen apelar a las acciones del WIN CSIRT deben ponerse en contacto con el jefe de servicios de ciberseguridad y comunicaciones. Si este recurso no es satisfactorio, el asunto puede remitirse al gerente de operaciones Cloud y Servicios.

4. Políticas

4.1 Tipos de incidentes y nivel de soporte

El WIN CSIRT se encarga de abordar diversos tipos de incidentes y los evalúa de acuerdo a criterios de peligrosidad o criticidad que son discutidos con los clientes. El nivel de asistencia brindada dependerá de ambos factores y de la gravedad determinada por el personal del WIN CSIRT.

Los recursos, que influyen en el nivel de apoyo del WIN CSRIT, se asignarán de acuerdo con las siguientes prioridades enumeradas en orden decreciente:

- Amenazas a la seguridad física de las personas.
- Ataques masivos o a nivel de sistema a cualquier Sistema de Información de Gestión, o a cualquier parte de la infraestructura de la red troncal.
- Ataques masivos o de sistema a cualquier máquina de servicio público de gran tamaño, ya sea multiusuario o de uso exclusivo.
- Compromiso de las cuentas de servicios confidenciales restringidos o de las instalaciones de software, en particular las utilizadas para las aplicaciones de WIN EMPRESAS que contienen datos confidenciales, o las utilizadas para la administración del sistema.
- Ataques de denegación de servicio a cualquiera de los tres elementos anteriores.
- Cualquiera de los anteriores en otros sitios, con origen en WIN EMPRESAS.
- Ataques a gran escala de cualquier tipo, por ejemplo, ransomware, ataques de sniffing, ataques de "ingeniería social", ataques de cracking de contraseñas.

- Amenazas, acoso y otros delitos relacionados con cuentas de usuario individuales.
- Compromiso de cuentas de usuarios individuales en sistemas multiusuario y de sistemas de escritorio.
- Falsificación y tergiversación, y otras violaciones de la normativa local relacionadas con la seguridad, por ejemplo, falsificación de páginas web, netnews y de correo electrónico, uso no autorizado de bots.
- Denegación de servicio en cuentas de usuarios individuales, por ejemplo, mailbombing.

Los tipos de incidentes distintos de los mencionados anteriormente se priorizarán en función de su gravedad y alcance aparentes.

4.2 Cooperación, interacción y divulgación de información:

WIN CSIRT tomarán las medidas adecuadas para proteger la información e identidad de los miembros de nuestra comunidad atendida. La información será tratada con absoluta confidencialidad de acuerdo con su clasificación. Sin embargo, se compartirá libremente la información cuando esto ayude a otros a resolver o prevenir incidentes de seguridad.

4.3 Comunicación y Autenticación

Los medios de comunicación disponibles con WIN CSIRT son las siguientes:

- Correo electrónico y teléfono descritos anteriormente.
- El proceso de autenticación se realiza mediante PGP como mecanismo de autenticación.

5. Servicios

WIN CSIRT brinda servicios proactivos y reactivos. Los servicios proactivos buscan anticiparse a cualquier incidente con la finalidad de prevenirlos y los servicios reactivos son los que se concentran en monitorear, analizar, categorizar, contener y responder a las ciber amenazas. A continuación, se encuentra una breve descripción de los servicios disponibles:

5.1 Servicios Proactivos:

5.1.1 Gestión de Vulnerabilidades

WIN CSIRT analizará las actuales y nuevas vulnerabilidades para fortalecer la seguridad de la información y reducir el riesgo de brechas de seguridad en las organizaciones colaboradoras.

- Descubrimiento / Investigación de vulnerabilidades

- Toma de reporte de vulnerabilidades
- Análisis de vulnerabilidad
- Coordinación de vulnerabilidades
- Divulgación de vulnerabilidades
- Respuesta de vulnerabilidades

5.1.2 Transferencia de conocimiento

A los miembros del WIN CSRIT se les compartirá y transmitirá información, experiencia; a través de conferencias internas y externas.

- Sensibilización
- Formación y educación
- Ejercicios

5.2 Servicios Reactivos:

5.2.1 Gestión de eventos de seguridad de la información

WIN CSIRT monitoreará y analizará eventos de seguridad que ocurren en los sistemas de información y redes de una empresa o entidad colaboradora.

- Monitoreo y detección
- Análisis de eventos

5.2.2 Gestión de incidentes de seguridad de la información

WIN CSIRT identificará, analizará, monitoreará, y responderá incidentes de seguridad para que no haya afectación de la integridad, disponibilidad e integridad de los activos de datos de una organización.

- Recepción de notificación del informe de incidentes de seguridad de la información
- Análisis de artefactos y pruebas forenses
- Mitigación y recuperación
- Coordinación de incidentes de seguridad de la información
- Apoyo en la gestión de crisis

6. Formularios de notificación de incidentes

Para reportar e informar incidentes se debe enviar comunicación a: csirt@winempresas.pe

También se encuentra disponible un Formulario interno de notificación de incidentes denominado: Formulario de informe de seguridad WIN CSIRT

7. Descargos de responsabilidad

WIN CSIRT tomará todas las precauciones en la preparación de información, notificaciones y alertas. Sin embargo, no asume responsabilidad por errores u omisiones, o por daños como resultado del uso de la información contenida en el mismo.