EDATA CSIRT

RFC 2350

+51 1 476 0808
Av. Guardia Civil 1292 - San Isidro – Perú
ventas@electrodata.com.pe
electrodata.com.pe

Índice de contenido

+51 1 476 0808
Av. Guardia Civil 1292 - San Isidro – Perú
ventas@electrodata.com.pe
electrodata.com.pe

1. INFORMACIÓN DEL DOCUMENTO

1.1. Fecha de la última actualización

Versión 1.0, publicada el 15.Mayo.2024

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@edata.pe)

1.3. Ubicación del documento

La última versión del documento se encuentra publicada en:

English: http://www.electrodata.com.pe/csirt/rfc2350-EN.pdf

Español: http://www.electrodata.com.pe/csirt/rfc2350-ES.pdf

2. INFORMACIÓN DE CONTACTO

2.1. Nombre del equipo

Equipo de respuesta a incidentes de seguridad tecnológica - EDATA CSIRT

2.2. Zona horaria

GMT –5 (Lima-Perú)

2.3. Otras telecomunicaciones

Formulario Web: https://www.electrodata.com.pe/contacto/

2.4. Correo electrónico (método preferido)

Reporte de incidencias: csirt@edata.pe

Información de carácter general sobre ciberseguridad y consultas: soc@electrodata.com.pe

Información sobre cualquier otro servicio contratado: servicedesk@electrodata.com.pe (no debe ser usado para reportar incidencias de seguridad)

2.5 Comunicación segura

El correo electrónico: csirt@edata.pe, tiene el siguiente PGP key asociado.

Llave púbica: PE_0x553BD2FD_public.asc

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. Otra información

La información general de los servicios la podrá encontrar publicadas en el siguiente portal: https://www.electrodata.com.pe/

2.8. Puntos de contacto con el cliente

El método preferido para comunicarse con EDATA CSIRT en caso de incidentes cibernéticos por parte de sus clientes es mediante mensajes de correo electrónicos con EDATA CSIRT. El mensaje de correo electrónico enviado a dicha dirección será comunicado al responsable, o se reenviará automáticamente a la persona de respaldo adecuada, de inmediato.

Si necesitas asistencia urgente por un incidente crítico, agregue la palabra [URGENTE] al inicio del asunto del mensaje para

poder activar los flujos de emergencia. Si no es posible o por razones de confidencialidad, puede contactar al EDATA CSIRT por teléfono.

2.9. Horarios de atención

Los servicios de respuesta a incidentes están disponibles 24x7x365 y se atenderán de acuerdo a los acuerdos de nivel de servicio para cada caso. El triaje inicial determinará si la incidencia es crítica y se mantendrá activa en el formato 24x7 o podrá ser derivada al horario de funcionamiento regular.

El horario de funcionamiento regular de EDATA CSIRT para otros servicios o para incidentes no críticos, está restringido al horario comercial habitual de 09:00-18:00 de lunes a viernes, excepto días feriados.

Durante los días de feriados nacional solo se atenderá incidencias críticas.

3. CARTA

3.1. Misión

Proteger proactivamente los activos digitales y la integridad de la infraestructura de nuestra empresa y la de nuestros clientes mediante la detección, respuesta y apoyo en la mitigación eficaz de amenazas cibernéticas. Nuestro compromiso es salvaguardar la confidencialidad, integridad y disponibilidad de la información crítica, garantizando la continuidad del negocio y la confianza de nuestros clientes y socios.

3.2. Visión

Ser reconocidos como líderes en la defensa contra las amenazas cibernéticas, destacándonos por nuestra capacidad para anticipar y responder rápidamente a los incidentes de seguridad utilizando todos nuestros recursos, logística y conocimiento especializado. Impulsados por la innovación y la excelencia técnica, colaborando estrechamente con nuestros clientes, compartiendo nuestro conocimiento para fortalecer la postura de seguridad de nuestra organización y de nuestros clientes

3.3. Comunidad Atendida

Atenderemos a los clientes internos y externos de Grupo ELECTRODATA, tanto del sector público como privado, que hayan suscrito o formalizado algún acuerdo de servicios de CyberSOC, los clientes externos pueden estar físicamente localizados dentro del territorio peruano así como también atenderemos a clientes de otros países de la región latinoamericana.

También colaboramos con otros grupos de respuestas a incidencias locales, regionales o internacionales, sean del sector gobierno o privados.

3.4. Patrocinio y / o Afiliación

EDATA CSIRT está patrocinado por el Grupo ELECTRODATA y está autorizado a atender todos los tipos de incidentes relacionados con ciberseguridad IT y OT relacionados a los servicios que brinda a sus clientes, y cuando se requiere a la industria tecnológica en general.

EDATA CSIRT tiene como objetivo estar afiliado a instituciones alrededor del mundo para colaborar, compartir información y dar soporte a incidentes de ciberseguridad.

3.5. Autoridad

EDATA CSIRT colabora estrechamente con los administradores y usuarios de los sistemas de Grupo ELECTRODATA, y con los clientes internos y externos, promoviendo relaciones de cooperación y no de autoridad cuando sea posible. Sin embargo, si las circunstancias lo justifiquen, el EDATA CSIRT apelará a Grupo ELECTRODATA para ejercer su autoridad directa o indirecta, según sea necesario.

Adicionalmente, EDATA CSIRT realiza las acciones que requieran sus clientes a nivel operativo y técnico, teniendo siempre la potestad principal y última decisión sobre las acciones a realizar.

Se deja la potestad de que los clientes o miembros de la comunidad puedan apelar a las acciones del EDATA CSIRT poniéndose en contacto con el Coordinador del SOC. En caso de que no se encuentre disponible o se requiere un escalamiento, se debe comunicar con el Gerente del CyberSOC. En cualquier caso, la comunicación se debe iniciar a través de los canales de comunicación establecidos.

4. POLÍTICAS

EDATA CSIRT definirá sus políticas y procedimientos para la operación y la gestión de incidentes a lo largo de todo su ciclo de vida. No obstante, conforme a lo establecido en el RFC 2350, se describe lo siguiente:

4.1. Tipos de incidentes y nivel de soporte

El EDATA CSIRT puede abordar cualquier incidente de ciberseguridad dentro de su comunidad atendida o área de alcance, si está dentro de los servicios que ofrece. Puede intervenir cuando los miembros de su comunidad lo soliciten o cuando alguno de ellos esté involucrado en un incidente de seguridad informática.

EDATA CSIRT no ofrece soporte directo a los usuarios finales; se espera que estos se comuniquen con sus departamentos correspondientes para obtener ayuda, y EDATA CSIRT brindará apoyo a esos departamentos. El nivel de asistencia proporcionado por EDATA CSIRT variará según la naturaleza y la gravedad del incidente, el tipo de interesado dentro de su comunidad a entidad, el tamaño de la comunidad de usuarios afectados y los recursos disponibles en ese momento, así como los acuerdos de servicio comprometidos.

El nivel de soporte que entrega EDATA CSIRT variará de acuerdo a la severidad del incidente, el impacto generado y en caso de clientes, del acuerdo de servicio contratado.

Para la priorización se tomará en cuenta el impacto en las partes y el riesgo que genera el incidente. En la mayoría de los casos, EDATA CSIRT ofrecerá apoyo en la priorización del

incidente y en caso no sea crítico recomendará medidas apropiadas para su gestión.

4.2. Cooperación, interacción y divulgación de información

EDATA CSIRT colabora con otros equipos especializados en la mejora de la seguridad, para ello puede compartir la naturaleza de los incidentes detectados en el ejercicio de sus funciones y los métodos de actuación llevados a cabo para su resolución. No obstante, se considera información confidencial cualquier dato que pueda comprometer los sistemas de información o identificar a nuestros clientes no compartiendo ningún tipo de información relevante a los mismos, salvo consentimiento previo, en cuyo caso se utilizará un método de seguridad para garantizar su confidencialidad e integridad.

4.3. Comunicación y autenticación

El método preferido de comunicación es por correo electrónico. La utilización de correos electrónicos no cifrados no se valora como un medio seguro de comunicación. No obstante, resulta adecuado para la transmisión de datos de baja sensibilidad o información no delicada. Es importante tener en cuenta que los datos sensibles, que abarcan información de carácter altamente confidencial (restringido, confidencial, secreto o estrictamente secreto), deben ser cifrados antes de su transmisión, lo cual también aplica para la transferencia de archivos.

5. SERVICIOS

5.1. Respuesta a incidentes

EDATA CSIRT asistirá a sus clientes y comunidad asociada en el manejo de los incidentes. Para esto ofrece asistencia técnica de sus recursos especializados en los tiempos y alcance de acuerdo a los servicios comprometidos en los contratos específicos con clientes.

También ofrece recomendaciones y soporte en la gestión de los incidentes.

5.2. Solución de incidentes

Aplica para los casos cuando se tiene una solicitud formal de asistencia en la solución de los incidentes. EDATA CISRT puede, en la medida de sus posibilidades, participar en la solución del incidente de la siguiente manera:

- Asistencia técnica especializada, para la contención de la amenaza y remediación de los sistemas y servicios críticos.
- Delimitación de la superficie de ataque.
- Segmentación de redes y aseguramiento de accesos.
- Recomendaciones para aseguramiento de sistemas críticos.
- Despliegue de controles de seguridad para mitigar el riesgo.
- Otras según el caso.

5.3. Actividades proactivas

5.3.1. Gestión de vulnerabilidades

Descubrimiento, análisis, comunicación, y soporte en la respuesta a la mitigación de las vulnerabilidades en los entornos IT y OT.

Seguimiento de acciones preventivas para fortalecer la postura de seguridad.

5.3.2. Boletines de seguridad

Publicación y envío regularmente de boletines de ciberseguridad generales, con los avisos de las últimas vulnerabilidades de los principales fabricantes o proveedores tecnológicos. Incluye recomendaciones para tomar acciones correctivas inmediatas.

5.3.3. Sensibilización y entrenamiento de ciberseguridad

Promovemos el conocimiento interno a través de capacitación y entrenamiento constante a nuestros equipos, y extendemos esto a nuestros clientes y socios.

Publicamos diferentes tópicos de seguridad y promovemos nuestra participación en conferencias, en particular sobre temas relacionados a posibles amenazas a nuestros clientes y comunidad de atención.

5.3.4. Seguridad gestionada

En el caso de que exista un contrato de seguridad gestionada se incluye el monitoreo proactivo y gestión de herramientas de ciberseguridad. Se actúa de manera proactiva en caso de amenazas para reducir la posibilidad de incidentes críticos que generen impacto en las operaciones y negocios del cliente.

Se incluye entre otras actividades:

- Gestión y administración de herramientas y soluciones de seguridad, que incluye su configuración y soporte que incluye las actualizaciones de versiones y aplicación de parches.
- Correlación de eventos y threat hunting.
- Gestión de vulnerabilidades.
- Validación de amenazas cuando sea parte del servicio contratado.
- Evaluación de riesgo según criticidad de los activos.

6. FORMULARIOS DE NOTIFICACIÓN DE INCIDENTES

Para reportar incidentes, por favor envíe un correo electrónico a la dirección csirt@edata.pe

Al notificar un incidente, es necesario proporcionar la siguiente información:

- Nombre de usuario que reporta.
- Nombre del cliente.
- Número telefónico de contacto.

- Correo electrónico.
- Descripción del incidente (indicar el impacto generado)

7. DESCARGOS DE RESPONSABILIDAD

Si bien se tomarán todas las precauciones en la preparación de la información, notificaciones y alertas, CISRT EDATA no asume ninguna responsabilidad por errores u omisiones, ni por daños resultantes del uso de la información proporcionada durante la ejecución de sus servicios.