CONSTITUCIÓN CSIRT-GMS

Contenido

1. INFORMACIÓN DEL DOCUMENTO

Este documento contiene una descripción de CSIRT-GMS según el RFC 2350. Se proporciona información básica sobre el CISRT-GMS en sus responsabilidades y servicios prestados.

1.1 Fecha de última actualización

La última actualización de la documentación se realizó el 30 de noviembre de 2023 como su versión 4.0

1.2 Lista de distribución

Se cuenta con una lista de distribución públicas para comunicaciones y notificaciones relacionados a eventos y/o incidentes de seguridad de la información a través de csirtgms@gmsseguridad.com

1.3. Ubicación del documento

La versión actual de este documento está disponible en https://gmsseguridad.com/csirt-quienes-somos/

1.4. Identificación del documento

Título: Constitución CSIRT-GMS_v4.0.pdf

Versión: 4.0.

Fecha del documento: 30 de noviembre de 2023

Caducidad: este documento es válido hasta que sea reemplazado por una versión posterior.

2. INFORMACIÓN DE CONTACTO

2.1. Nombre del equipo

CSIRT-GMS

2.2. Dirección Postal

CSIRT-GMS
Avenida Naciones Unidas y Avenida Río Amazonas.
Edificio “La Previsora” oficinas 11B.
CP: 170507
Quito, Ecuador

2.3. Zona horaria

América/Guayaquil (GMT-0500)

2.4. Teléfono

+593 23993000 opción 4

2.5. Fax

No disponible.

2.6. Otros medios de comunicación

No disponible.

2.7. Dirección de correo electrónico

csirtgms@gmsseguridad.com.

2.8. Claves públicas

CSIRT-GMS tiene la clave PGP cuyo KeyID es: 0xEF8E0613.

Fingerprint: 2866 C3A0 EE74 6232 A7F9 1A17 ABB8 D48F EF8E 0613

Esta clave y firma pueden ser encontradas en servidores de claves públicos y puede ser utilizada para enviarnos mails confidenciales a csirtgms@gmsseguridad.com

2.9. Miembros del Equipo

Eduard Gutierrez, Gerente Regional de SOC - IT

Equipo CSIRT-GMS (Operadores, Analistas, Especialistas en Respuesta a Incidentes)

2.10. Otra información

Toda la información sobre el CSIRT-GMS se encuentra disponible en https://gmsseguridad.com/csirtquienes-somos/

2.11. Formas de contacto

El método de contacto recomendado se establece a través de correo electrónico a csirtgms@gmsseguridad.com. Los emails serán recibidos por el Equipo de Especialistas de GMS de forma inmediata. En caso de no contar con acceso a correo electrónico, se recomienda como segunda opción el uso de nuestro canal de comunicación por teléfono en horarios de operación.

Los horarios de operación del CSIRT-GMS son de lunes a viernes de 8AM a 6PM.

3. CONSTITUCIÓN

3.1. Propósito y misión

Propósito

El CSIRT-GMS se constituye como un CSIRT comercial de carácter mixto, cuyos propósitos se

basan en los siguientes puntos:

- Apoyar a sus miembros en la implementación de medidas preventivas y proactivas en temas de seguridad de la información, para evitar riesgos asociados a sus activos críticos de información.
- Apoyar a sus miembros en la investigación forense y respuesta a incidentes bajo solicitud.
- Apoyar a otros equipos de seguridad de la información como punto de contacto con fuentes de inteligencia nacionales e internacionales de información ante escenarios de respuesta a incidentes.

3.2. Misión

Prestar servicios de investigación y análisis en la contención, resolución y prevención de escenarios.

3.3. Miembros

Miembros externos: Los miembros del CSIRT-GMS son todos sus clientes que realicen la contratación del servicio bajo necesidad.

Miembros internos: Se cuenta con el apoyo interno a nuestro patrocinador Grupo Microsistemas Jovichsa S.A. (GMS Seguridad de la Información).

3.4. Auspicios y afiliados

El equipo CSIRT-GMS es patrocinado por Grupo Microsistemas Jovichsa S.A. (GMS Seguridad de la Información).

3.5. Autoridad

El CSIRT-GMS opera bajo el auspicio y bajo la dirección del Gerente Regional de SOC y Consultoría de GMS Seguridad de la Información. Para solicitar más información sobre la autoridad del CSIRT-GMS contactar con su director.

El CSIRT-GMS trabaja en colaboración con los administradores de sistemas y usuarios de GMS y, en la medida de lo posible, evitar las relaciones autoritarias. Sin embargo, si las circunstancias lo justifican, el CSIRT-GMS apelará para ejercer su autoridad, directa o indirecta, según lo definan las políticas internas de la organización.

4. POLÍTICAS

4.1. Tipos de incidentes y nivel de soporte

Los miembros del CSIRT-GMS reportarán toda actividad asociada a incidentes de seguridad de la información a través del correo electrónico csirtgms@gmsseguridad.com o a través del registro del formulario disponible aquí. El Coordinador del CSIRT-GMS debe gestionar todo requerimiento que ingrese con el canal de comunicación mencionado considerando:

- Validar la membresía del solicitante para la gestión del incidente reportado.
- Para los miembros se procederá con la asignación de un técnico líder de respuesta a incidentes para la gestión del incidente reportado. Para los reportes que procedan de no miembros, el Coordinador del CSRIT validará la posibilidad de apoyo para él envió

de información acerca de indicadores de compromiso asociados al incidente reportado.

- Adicionalmente a la asignación del líder de respuesta a incidentes, el Coordinador del CSIRT establecerá la clasificación del incidente considerando:
  - Incidentes de relevancia crítica:
    - Ataques de Ransomware.
    - Infección de malware.
    - Accesos no autorizados como usuarios administradores.
  - Incidentes de relevancia alta:
    - Accesos no autorizados como usuarios sin privilegios.
    - Ataques de denegación de servicio dirigidos.
    - Comportamiento malicioso desde la red interna.
    - Secuestro de servicio web de la organización.
    - Ataques de SCAM.
  - Incidentes de relevancia media:
    - Ataques a través de correo electrónico (SPAM, ingeniería social, chantaje por email, Spoofing, Phishing).
    - Ataques de malware a dispositivos móviles.
    - Fuga de información.
    - Nuevos escenarios de riesgo no identificados.
  - Incidentes de relevancia baja:
    - Abuso interno de activos de información (Generación de tráfico elevado de red, intentos de acceso por fuerza bruta).
    - Ataques contra la marca de la organización.

Los nuevos escenarios de seguridad de la información no identificados tendrán una categorización inicial de relevancia Medio. Sin embargo, en caso de ser necesario y según lo disponga el Coordinador del CSIRT, se puede recategorizar su nivel de riesgo y afectación.

Se debe considerar que el CSIRT-GMS no dará soporte directo a usuarios finales, sino, que mantendrá puntos de contacto o responsables de comunicación con los administradores de sus respectivos suscriptores para la generación de requerimientos. Adicionalmente queda fuera de las responsabilidades del CSIRT-GMS la capacitación del personal de sus suscriptores en el acompañamiento y apoyo en la gestión de incidentes de seguridad de la información.

El CSIRT-GMS ejecutara comunicaciones a los administradores de sus respectivos suscriptores sobre vulnerabilidades potenciales y amenazas latentes en la región según se definan los acuerdos de trabajo.

4.2. Cooperación, interacción y publicación de información

El CSIRT-GMS podrá colaborar con otros CSIRT y CERT nacionales o internacionales, así como con otros terceros afectados en la medida en que los acuerdos de trabajo lo definan o bajo la

autorización del Coordinador del CSIRT. La información generada por los servicios del CSIRT-GMS se puede compartir con sus suscriptores y las entidades Grupo Microsistemas Jovichsa S.A, Grupo Microsistemas Perú SAC, Grupo Microsistemas Colombia S.A.S, así como con los proveedores y partners de servicios de ciberseguridad, según sea necesario.

El intercambio de información se realizará con el cumplimiento de obligaciones contractuales, legales y éticas definidas con sus suscriptores, principalmente con el ofuscamiento de información para la protección de entidad de nuestros suscriptores. Información como Indicadores de compromiso, perfilamiento de atacantes y posibilidades de explotación de vulnerabilidades se podrán compartir según lo defina el Coordinador del CSIRT.

4.3. Comunicación y autenticación

Los niveles de intercambio de información dependerán de su destinatario, el CSIRT-GMS identifica los siguientes niveles de comunicación:

- Intercambio de información propia del suscriptor: Cuando el CSIRT-GMS establezca un intercambio de información de indicadores de compromisos (informes y/o reportes) y alertas del propio suscriptor se aceptará como envió seguro el uso de correos electrónicos sin encriptar.
- Intercambio de información consolidados y nuevas amenazas: Cuando el CSIRT-GMS realice un intercambio de información de indicadores de compromiso regionales o nuevas amenazas detectadas a través de reportes consolidados se considera como envió seguro el uso de correo electrónico sin encriptar.
- Intercambio de información con CSIRT/CERT regionales: Cuando el CSIRT-GMS establezca un intercambio de información sobre incidentes y/o indicadores de compromiso sobre escenarios de riesgo actuales, lo debe realizar a través de correos electrónicos encriptados.

El cumplimiento de esta política se realizará desde el correo oficial del CSIRT-GMS csirtgms@gmsseguridad.com así como con el uso de correos institucionales del personal que forma parte del proceso (Operadores, Analistas, Coordinadores, Gerentes, Consultores de Seguridad de la Información).

Se prohíbe el intercambio de información del CSIRT por medios no oficiales como: redes sociales, correos electrónicos personales o dispositivos de almacenamiento externo no autorizados.

5. SERVICIOS

Los servicios prestados por el CSIRT-GMS se dividen en dos grandes grupos: Respuesta a incidentes y actividades proactivas para resolución de incidentes.

5.1. Respuesta a Incidentes

La respuesta a incidentes busca proporcionar disponibilidad para coordinar la contención, erradicación y recuperación de los incidentes relacionados con la seguridad de la información y consiste en experiencia, herramientas y otras capacidades para actuar, analizar y comunicarse con las partes interesadas y los medios de comunicación.

5.1.1 Respuesta a Incidentes

- Monitoreo 24/7 de activos críticos de información a través de los logs que estos

generen.

- Detección de amenazas, indicadores de compromiso y vulnerabilidades asociados a los activos de información que formen parte del alcance de monitoreo.

5.1.2 Resolución de incidentes

- Brindar asesoramiento a los suscriptores a eliminar las vulnerabilidades o brechas de seguridad que permitieron la ejecución del incidente y proteger los sistemas de los efectos de los incidentes.
- Evaluar qué acciones son más adecuadas para proporcionar los resultados deseados con respecto a la resolución del incidente.
- Acompañamiento en la contención y erradicación de artefactos, malware y/o comunicaciones asociadas al incidente de seguridad de la información.

5.1.3 Análisis forense

- Proporcionar asistencia en la recopilación de pruebas y la interpretación de datos para identificar el escenario de riesgo usado en el incidente.
- Realizar la investigación en base a las evidencias sobre las brechas de seguridad y/o actores asociados al incidente de seguridad de la información materializada en la organización.

6. FORMULARIOS DE REPORTE DE INCIDENTES

Para informar sobre algún incidente asociado a la comunidad del CSIRT-GMS, se debe enviar una comunicación a csirtgms@gmsseguridad.com o registrar el reporte de incidentes desde el formulario disponible en el servicio web del CSIRT-GMS

7. AVISO LEGAL

Considerando los controles y precauciones en la preparación de información, notificaciones y alertas, el CSIRT-GMS no asume responsabilidad por errores, omisiones o daños resultantes de la información aquí contenida.

8. HISTORIAL DE CAMBIOS

Versión	Motivo de Cambio	Realizado por	Aprobado por	Fecha
1.0	Creación de documento	Coordinador de Consultoría	Gerente Regional de SOC y Consultoría	19/3/2021
2.0	Revisión de documento	Coordinador de SOC	Gerente Regional de SOC	05/01/2022
3.0	Actualización de documento	Coordinador de SOC	Vicepresidente de Operaciones	07/07/2023
4.0	Actualización de documento	Coordinador de SOC	Gerente Regional de SOC - IT	30/11/2023