RFC 2350

BIGFIVE B5, S.R.L.

Versión: Primera
Clasificación: Publico
Fecha de Creación: 2025

Contenido

1. INFORMACIÓN DEL DOCUMENTO

1.1. Fecha de la última actualización

15 de julio de 2025

1.2. Lista de distribución para notificaciones

Los cambios a este documento y las notificaciones de seguridad son distribuidos mediante la lista de correo csirt@bigfive.net, la cual incluye a los miembros del equipo de respuesta a incidentes.

Consultas adicionales pueden dirigirse a info@bigfive.net.

1.3. Ubicación del documento

La última versión de este documento está disponible en el sitio web oficial de BigFive: https://www.bigfive.net

2. INFORMACIÓN DE CONTACTO

2.1. Nombre del equipo

BIGFIVE – CSIRT

2.2. Zona horaria

GMT –4

2.3. Otras telecomunicaciones

Contacto –

Central Telefónica: (809) 745-3252

Canales alternativos: Grupos de Teams autorizados

2.4. Correo electrónico

Reporte de incidentes: csirt@bigfive.net

Consultas generales: info@bigfive.net

2.5 Comunicación segura

BigFive emplea mecanismos de cifrado extremo a extremo. Aunque actualmente no se utiliza PGP de forma generalizada, se aplican protocolos TLS, cifrado AES y plataformas seguras para la transmisión de información crítica.

2.6. Miembros del equipo.

Serán identificables en comunicaciones oficiales el Líder, los Gerentes y los directores del CSIRT.

2.7. Otra información

La información general sobre los servicios se publica directamente en el sitio web de BigFive.

2.8. Puntos de contacto con el cliente

El canal oficial de contacto del CSIRT de BigFive es el correo csirt@bigfive.net. Todos los reportes de incidentes deben enviarse a esta dirección incluyendo el asunto detallado y, en casos críticos, la palabra clave “URGENTE” al inicio del título del mensaje.

El equipo de respuesta está disponible en modalidad 24/7, de acuerdo con los niveles de servicio contratados. Los mensajes son redirigidos automáticamente al analista responsable o su respaldo operativo según la matriz de turno vigente.

Para mantener trazabilidad, se recomienda que toda comunicación inicial sea electrónica. En situaciones excepcionales o por razones de confidencialidad, puede contactarse telefónicamente al número oficial o a través de grupos de Teams autorizados.

En BigFive se mantiene una matriz de escalamiento privada, gestionada por el Coordinador del CSIRT, que garantiza una respuesta adecuada a cada nivel de criticidad.

3. CARTA

3.1. Misión

Proteger la integridad, confidencialidad y disponibilidad de la información de nuestros clientes mediante servicios de ciberseguridad gestionada de clase mundial, inteligencia de amenazas, monitoreo 24/7, automatización avanzada, respuesta efectiva y resiliencia.

3.2. Visión

Ser el aliado de ciberseguridad más confiable e innovador de la región, anticipando, neutralizando y transformando los riesgos cibernéticos en ventajas estratégicas mediante inteligencia artificial y un equipo élite de expertos.

3.3. Comunidad Atendida

Clientes internos y externos, tanto del sector público como privado, incluyendo clientes internacionales de Latinoamérica.

3.4. Patrocinio y / o Afiliación

El CSIRT es patrocinado por BigFive. Actualmente no está afiliado a ninguna red formal, pero se encuentra evaluando su incorporación mediante el CSRC.

3.5. Autoridad

El CSIRT de BigFive actúa como unidad técnica especializada, con capacidad de ejecución operativa dentro del alcance de los servicios contratados y conforme a los procedimientos aprobados por la Dirección de Seguridad de la Información.

Su autoridad se basa en principios de colaboración técnica con las áreas responsables de los activos afectados, privilegiando el consenso para actuar. No obstante, en escenarios de alta criticidad (Ej. ransomware, fuga de datos, sabotaje activo), puede activar protocolos de contención inmediatos, conforme a las directrices del Plan de Respuesta a Incidentes de Seguridad.

Las acciones del CSIRT están respaldadas por los lineamientos del Comité de Seguridad de la información o la Alta Gerencia cuando se requiere coordinación interdepartamental o escalamiento estratégico.

En caso de desacuerdo, se establece un canal de apelación escalonado: Líder del CSIRT → Gerente de SOC → Alta Gerencia. Toda gestión debe canalizarse a través del correo oficial del CSIRT.

4. POLÍTICAS

4.1 Principios generales

El CSIRT de BigFive gestiona los incidentes conforme a principios de inmediatez, trazabilidad, proporcionalidad y conservación del conocimiento, alineados con la norma ISO/IEC 27035.

4.2 Notificación de incidentes

Todos los incidentes o sospechas deben ser notificados sin dilación por el personal autorizado, a través de los canales oficiales del CSIRT.

4.3 Clasificación y evaluación

Los incidentes se evalúan según criterios técnicos objetivos que permiten determinar su naturaleza, severidad y alcance. Se aplican escalas internas con posibilidad de ajuste según evolución del caso.

4.4 Priorización de respuesta

Se prioriza la atención considerando impacto, urgencia, procesos afectados, usuarios involucrados y compromisos legales o contractuales.

4.5 Registro y documentación

Todo incidente es documentado en sistemas seguros que aseguran su trazabilidad y conservación. Los registros deben ser suficientes para su análisis posterior.

4.6 Conservación de evidencia

Se garantiza la preservación íntegra de evidencias digitales, conforme a prácticas forenses reconocidas, asegurando su validez técnica y jurídica.

4.7 Escalamiento

BigFive mantiene una matriz formal de escalamiento según el nivel de criticidad, exposición externa y duración estimada del impacto. Esta define las instancias responsables de la resolución.

4.8 Comunicación externa

Si un incidente afecta a terceros, se activa el protocolo de comunicación pública, bajo evaluación del Líder de Incidentes y demás responsables designados.

4.9 Monitoreo e inteligencia

El CSIRT mantiene capacidades de monitoreo continuo e inteligencia de amenazas, apoyado en análisis interno y fuentes externas para detección temprana.

4.10 Capacitación y mejora continua

El personal clave recibe formación periódica. Se realizan ejercicios prácticos, análisis post mortem y propuestas de mejora para reforzar la capacidad de respuesta.

4.11 Coordinación con partes externas

BigFive mantiene relaciones operativas con autoridades, proveedores y otros CSIRT bajo marcos formales y confidenciales, promoviendo el intercambio técnico responsable.

5. SERVICIOS

5.1 Servicios Proactivos

- Monitoreo de alertas y amenazas
- Gestión de herramientas de seguridad (parches, actualizaciones)
- Inteligencia de amenazas (Threat Hunting)
- Evaluación de riesgos tecnológicos
- Difusión de boletines y capacitaciones

5.2 Servicios Reactivos

- Gestión de incidentes (análisis, respuesta y coordinación)
- Contención y remediación
- Análisis forense digital

5.3 Evaluación de Seguridad

- Descubrimiento de activos
- Escaneo de vulnerabilidades IT/OT
- Simulaciones de adversario (Red Team)
- Seguimiento a acciones preventivas

5.4 Concientización

- Gestión de plataformas de phishing
- Capacitaciones para reducir el riesgo humano

5.5 Boletines de Seguridad

- Envío periódico de alertas con vulnerabilidades relevantes

6. FORMULARIOS DE NOTIFICACIÓN DE INCIDENTES

Enviar un correo a csirt@bigfive.net con la siguiente información:

- Nombre completo
- Correo
- Teléfono
- Empresa
- Dirección de empresa
- Asunto
- Descripción del incidente
- Nivel de criticidad

Actualmente no se cuenta con un formulario automatizado.

7. DESCARGOS DE RESPONSABILIDAD

BigFive no asume responsabilidad legal por errores u omisiones en la información contenida en este documento o en las alertas emitidas por el CSIRT, aun cuando se hayan aplicado los más altos estándares de revisión y actualización.