Expectativas para la Respuesta a Incidentes de Seguridad Informática de BUSINESS IT

CSIRT – BUSINESS IT

RFC 2350

expertos@grupobusiness.it
www.GrupoBusiness.it

INDICE

CSIRT – BUSINESS IT

RFC 2350

1. Información del documento

1.1. Fecha de última actualización

La versión 02 del documento RFC 2350 de CSIRT – BUSINESS IT fue publicado el 24 de Febrero del 2025.

1.2. Lista de distribución de notificaciones

No existe un canal de distribución por mensaje de correo electrónico para notificar cambios en este documento. Los cambios son anunciados por medio de notificaciones en: www.grupobusiness.it/csirt

Cualquier pregunta o comentario, por favor diríjase a la siguiente dirección de correo electrónico: csirt-latam@grupobusiness.it

1.3. Ubicaciones donde se puede encontrar este documento

La última versión de este documento se encuentra publicada en:

Idioma	URL del documento
ESPAÑOL	https://standprocesos.blob.core.windows.net/csirt/BIT-D-MS-02%20EXPECTATIVAS%20CSIRT%20-%20ESP.pdf
ENGLISH	https://standprocesos.blob.core.windows.net/csirt/BIT-D-MS-02%20EXPECTATIVAS%20CSIRT%20-%20ING.pdf

2. Información de contacto

2.1. Nombre del equipo

"CSIRT – BUSINESS IT": Equipo de Respuesta a Incidentes de Seguridad Informática de BUSINESS IT.

2.2. Dirección

Julio Alarcón Ayala S/N entre Japón y Pereira, Edificio Zaigen, Piso 9. Quito, Ecuador.

2.3. Zona horaria

UTC-5 Quito/Ecuador.

2.4. Número de teléfono

+593 (02) 6002741, preguntar por CSIRT-BUSINESS IT

2.5. Dirección de correo electrónico

Intercambio de información relacionado con incidentes: csirt-latam@grupobusiness.it.
Otras direcciones de correo electrónico para contactar a CSIRT-BUSINESS IT

2.6. Claves públicas y otra información de cifrado

PGP se utiliza para intercambios de información funcionales entre CSIRT-BUSINESS IT y otro equipos o interesados (informes de incidentes, alertas, etc.)

2.7. Miembros del equipo

La lista completa de los miembros del equipo de CSIRT-BUSINES IT no está disponible públicamente. Los miembros del equipo se identificarán ante la parte informante o cliente con su nombre completo en una comunicación oficial sobre un incidente.
La gestión, enlace y supervisión de CSIRT-BUSINESS IT están cargo del Cyber Security Manager y del Incident Responder & Forensic.

2.8. Puntos de contacto con el cliente

El método preferido para comunicarse con CSIRT-BUSINESS IT es mediante mensajes de correo electrónico con la dirección csirt-latam@grupobusiness.it.
El mensaje de correo electrónico enviado a dicha dirección será comunicada al responsable, o se reenviará automáticamente a la persona de respaldo adecuada, de inmediato. Si necesita asistencia urgente, escriba "urgente" en la línea de asunto.
Si no es posible (o no es aconsejable por razones de seguridad) utilizar el correo electrónico, se puede contactar a CSIRT-BUSINESS IT por teléfono durante el horario habitual de oficina. Los mensajes telefónicos se revisan con menos frecuencia que el correo electrónico.
El horario de funcionamiento de CSIRT-BUSINESS IT está generalmente restringido al horario comercial normal (de lunes a viernes de 08:30 a 18:00 horas, excepto los días feriados).
En caso de incidente crítico la operación podría ser en el formato 24x7.

3. Carta

3.1. Misión

BUSINESS IT considera la información digital como un activo esencial que debe ser protegido y monitoreado oportunamente debido a la rápida evolución de amenazas cibernéticas para garantizar la continuidad del negocio de las organizaciones. Los ciberataques a menudo comprometen datos personales y comerciales, por lo que es crucial responder de manera rápida y efectiva ante violaciones de seguridad.

En este contexto, el CSIRT-BUSINESS IT tiene la misión de apoyar a las organizaciones de la comunidad atendida por BUSINESS IT. Esto incluye coordinación para seguir con el plan de respuesta a incidentes en todas sus fases.

3.2. Comunidad atendida o circunscripción

La circunscripción de CSIRT-BUSINESS IT son los clientes internos y externos de BUSINESS IT, con los cuales se hayan suscrito o formalizado algún acuerdo de servicio que BUSINESS IT provee como Respuesta a Incidentes de Seguridad Informática. Los incidentes atendidos por CSIRT-BUSINESS IT serán aquellos que afecten a las redes, sistemas y aplicativos de los clientes internos y externos de BUSINESS IT conforme a los servicios que preste el CSIRT, especificados en la sección 5 denominado "Servicios" del presente documento.

Sin embargo, se debe tener en cuenta que, sin perjuicio de lo anterior, los servicios de CSIRT-BUSINESS IT se prestarán para los sistemas en los centros de procesamiento de datos de BUSINESS IT y otras ubicaciones de los clientes internos y externos de BUSINESS IT que están dentro del alcance de los servicios proporcionados, como infraestructura en la nube. CSIRT-BUSINESS IT puede actuar, siempre y cuando se proporcione un acceso remoto seguro a la infraestructura donde se ha producido el incidente.

3.3. Patrocinio y/o afiliación

CSIRT-BUSINESS IT está patrocinado por la Unidad de Negocio de Infrastructure & Managed Services de BUSINESS IT.

CSIRT-BUSINESS IT busca estar afiliado a instituciones alrededor del mundo con la finalidad de colaborar y compartir información de incidentes de seguridad informática.

CSIRT-BUSINESS IT está conformado de la siguiente manera:

- Cyber Security Manager que depende de la Unidad de Negocio de Infrastructure & Managed Services de BUSINESS IT, a cargo de CSIRT-BUSINESS IT.
- El Líder de CSIRT-BUSINESS IT, a cargo del Incident Responder & Forensic de BUSINESS IT.
- Analistas y Especialistas del área de Ciberseguridad.

3.4. Autoridad

CSIRT-BUSINESS IT opera bajo los auspicios y con la autoridad delegada por la Unidad de Negocio de Infrastructure & Managed Services de BUSINESS IT.

CSIRT-BUSINESS IT trabaja en cooperación con las demás áreas de BUSINESS IT, así como con los clientes internos y externos. En la medida de lo posible se evita relaciones autoritarias. No obstante, si las circunstancias lo ameriten, CSIRT-BUSINESS IT recurrirá

al Delivery Manager y al Chief Business Officer para que ejerza sus facultades, directa o indirectamente, según sea necesario.

Los miembros de la comunidad de BUSINESS IT que deseen apelar las acciones de CSIRT-BUSINESS IT deben comunicarse con el Cyber Security Manager. Si este recurso no es satisfactorio, el asunto puede remitirse al Delivery Manager de la Unidad de Negocios de Infrastructure & Managed Services de BUSINESS IT.

4. Políticas

CSIRT-BUSINESS IT 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

CSIRT-BUSINESS IT está autorizado para atender cualquier tipo de incidentes de seguridad informática que se produzcan en su comunidad atendida o circunscripción y que forme parte de los servicios que brinde.

CSIRT-BUSINESS IT puede actuar a petición de los interesados de su comunidad atendida o circunscripción o puede actuar si alguno de sus integrantes se ve involucrado en un incidente de seguridad informática. Tenga en cuenta que no se brindará soporte directo a los usuarios finales; se espera que estos se comuniquen con su administrador de sistema, administrador de red, jefe de proyecto, jefe de departamento de tecnologías de la información, oficial de seguridad de la información o puestos similares para obtener ayuda, CSIRT-BUSINESS IT apoyará a estas últimas personas.

El nivel de soporte brindado por CSIRT-BUSINESS IT variará según el tipo y la gravedad del incidente o problema, el tipo de interesado de su comunidad atendida o circunscripción, el tamaño de la comunidad de usuarios afectada y los recursos disponibles de CSIRT-BUSINESS IT para gestionar el incidente en ese momento, aunque en todos los casos alguna respuesta se realizará en el plazo de un día hábil.

CSIRT-BUSINESS IT maneja diferentes tipos de incidentes clasificados según su nivel de criticidad y la priorización de atención con base en una matriz de impacto y urgencia,
el nivel de apoyo de CSIRT-BUSINESS IT dependerá de ambos factores y de la gravedad que determine el personal del equipo, conforme a la Política de Gestión de Incidentes de CSIRT-BUSINESS IT.

Si bien CSIRT-BUSINESS IT entiende que existe una gran variación en el nivel de experiencia del administrador del sistema en BUSINESS IT y/o del administrador del sistema de su comunidad atendida o circunscripción, y aunque CSIRT-BUSINESS IT se esforzará por presentar información y asistencia en un nivel apropiado para cada persona, CSIRT-BUSINESS IT no puede capacitar a los administradores del sistema sobre

la marcha y no puede realizar el mantenimiento del sistema en su nombre. En la mayoría de los casos, CSIRT-BUSINESS IT proporcionará indicaciones y recomendaciones sobre la información necesaria para implementar las medidas apropiadas.

4.2. Cooperación, interacción y divulgación de información

CSIRT-BUSINESS IT cooperará e interactuará con otras organizaciones en el ámbito de la seguridad de la información, ciberseguridad y protección de datos personales enfocado en los temas relacionados con la respuesta a incidentes de seguridad, en especial con otros IRTs (Equipos de Respuesta a Incidentes), SIRTs (Equipo de Respuesta a Incidentes de Seguridad), CIRCs (Centros de Respuesta a Incidentes Informáticos), CSIRTs (Equipos de Respuesta a Incidentes de Seguridad Informática), CERTs (Equipos de Respuesta ante Emergencias Informáticas), PSIRTs (Equipos de Respuesta a Incidentes de Seguridad de Productos), NCSCs (Centros Nacionales de Ciberseguridad) o ISACs (Centro de Análisis e Intercambio de Información). Esta cooperación también incluye y, a menudo, requiere el intercambio de información sobre incidentes y vulnerabilidades de seguridad.

No obstante, CSIRT-BUSINESS IT protegerá la privacidad de los interesados de su comunidad atendida o circunscripción y, por lo tanto (en circunstancias normales), transmitirá información únicamente de forma anónima. Salvo autorización expresa, no se divulgará la identidad o información vital de las víctimas de incidentes de seguridad informática.

CSIRT-BUSINESS IT opera en el marco legal ecuatoriano, por lo tanto, CSIRT-BUSINESS IT puede verse forzado a revelar cierta información para cumplir con alguna obligación legal o una orden judicial expresa, la que tendría que brindarse en coordinación y previo análisis con la parte legal de BUSINESS IT.

CSIRT-BUSINESS IT maneja diverso tipo de información, aquella información de naturaleza muy sensible (restringido, confidencial, secreto o estrictamente secreto) solo se comunica y almacena en un entorno seguro y en caso de ser necesario utiliza mecanismos criptográficos. Toda la información suministrada y provista por CSIRT-BUSINESS IT será utilizada para ayudar a resolver los incidentes de seguridad.

La cooperación, interacción y divulgación de información se realiza conforme a la Política de Transferencia de Información y Política de Clasificación de la Información de CSIRT-BUSINESS IT.

CSIRT-BUSINESS IT utiliza el protocolo TLP para el intercambio de información, así como mecanismos de comunicación segura mediante el uso de controles criptográficos

4.3. Comunicación y autenticación

La comunicación a través de mensajes de correo electrónico no cifrados no se considerará seguro, sin embargo, es suficiente para la transmisión de datos de baja

sensibilidad o datos no sensibles. Tenga en cuenta que los datos sensibles que conforman información de naturaleza muy sensible (restringido, confidencial, secreto o estrictamente secreto) deben cifrarse antes de la transmisión, lo que incluye transferencia de archivos.

CSIRT-BUSINESS IT utilizará correo cifrado PGP de extremo a extremo siempre que sea posible. La autenticación se proporciona a través de firmas PGP mediante las claves mencionadas.

5. Servicios

CSIRT-BUSINESS IT asistirá a su comunidad atendida o circunscripción en el manejo de los aspectos técnicos y organizacionales de los incidentes. En particular, prestará asistencia o asesoramiento con respecto a los siguientes aspectos de la gestión de incidentes en servicios reactivos y proactivos:

5.1. Servicios reactivos

Estos servicios se activan como consecuencia de incidente, lo que viene a ser el componente central en el trabajo de CSIRT-BUSINESS IT para el manejo de incidentes de su comunidad atendida o circunscripción:

5.1.1. Clasificación de incidentes

CSIRT-BUSINESS IT clasifica los incidentes según su nivel de criticidad y la priorización de atención viene a estar dada con base en una matriz de impacto y urgencia. Asimismo, se realiza la investigación para concluir si efectivamente ocurrió un incidente, determinar el alcance de este, y evaluar y comparar el incidente con la información histórica.

5.1.2. Coordinación de incidentes

Este servicio tiene como objetivo la coordinación de la respuesta a incidentes de seguridad informática con otros equipos a nivel local, regional y global, los proveedores de servicio de internet, las empresas de telecomunicaciones y otros organismos públicos y privados (fuerzas del orden y ámbito legal), según corresponda. Coordinaciones que se realizan en estrecha relación con las partes afectadas. Parte del objetivo es determinar la causa raíz del incidente y que vulnerabilidad fue explotada, para ello se realizan los contactos con sitios que pueden verse involucrados en el incidente.

También, de ser el caso, se realizan las coordinaciones con los medios a través de los lineamientos descritos en el “Manual de Comunicación en Crisis”, que pertenece a la Dirección de Marketing de BUSINESS IT.

Además, si es aplicable, se debe gestionar la elaboración de los anuncios para los

usuarios finales de las partes interesadas.

5.1.3. Resolución de incidentes

Este servicio tiene por objetivo manejar un incidente mediante el proceso de respuesta a incidentes que involucra las fases de preparación; detección y análisis; contención, erradicación y recuperación; y actividades después de ocurrido un incidente.

CSIRT-BUSINESS IT proporcionará la asistencia técnica mediante el análisis de sistemas comprometidos, recomendaciones para la erradicación y eliminación de la causa del incidente y para asegurar los sistemas afectados.

También, CSIRT-BUSINESS IT recopilará estadísticas sobre los incidentes que ocurran dentro de su comunidad atendida o circunscripción, o que se vean involucrados de alguna forma; y según sea necesario, notificará a la comunidad para protegerse contra los ataques conocidos.

Tenga en cuenta que CSIRT-BUSINESS IT tiene por función la coordinación de respuesta a incidentes con información en parte provista por la comunidad atendida o circunscripción, sin coacción. En ese sentido, es probable que no siempre sea posible llegar a una resolución exitosa de todos los incidentes, ya que la resolución real depende de las correctas acciones que realice y ejecute la parte interesada.

5.2. Servicios proactivos

Estos servicios tienen por finalidad proveer información oportuna para ayudar a proteger la infraestructura de red de la comunidad atendida o circunscripción, anticipándose a los ataques cibernéticos. Por lo tanto, el éxito o implementación oportuna de los servicios reducirá el número de incidentes futuros.

CSIRT-BUSINESS IT coordina y mantiene los siguientes servicios en la medida de lo posible en función de sus recursos:

5.2.1. Avisos y alertas

Este servicio tiene como objetivo alertar y avisar proactivamente sobre ciberataques o interrupciones, vulnerabilidades de seguridad, alertas de intrusión, malware, virus informáticos, comportamientos anómalos y brindar recomendaciones para abordar el problema a la parte interesada de su comunidad atendida o circunscripción. Se realiza a través de:

- Correlación de eventos,
- Monitoreo,
- Análisis avanzados e investigaciones y respuestas automatizadas,
- Uso de inteligencia artificial,
- Responder de manera más inteligente y rápida

5.2.2. Análisis de vulnerabilidades

El análisis de vulnerabilidades es el proceso de identificar los sistemas en la red que tiene vulnerabilidades conocidas o identificadas, como fallas, brechas de seguridad, exploits, puntos de entrada de acceso inseguros y los errores de configuración del sistema.

Corresponde a la evaluación de vulnerabilidades de la infraestructura de red, equipos, software, aplicaciones y otros dispositivos de red con fines de brindar recomendaciones para las correcciones oportunas.

5.2.3. Evaluación de seguridad (bechmarks y hardening o endurecimiento informático)

El "Hardening" o endurecimiento informático es una serie de técnicas, herramientas y mejores prácticas para reducir vulnerabilidades en sistemas tecnológicos, cuyo objetivo es reducir riesgos de seguridad eliminando posibles vectores de ataque y la materialización de la superficie de ataque (Attack Surface) sobre algún sistema.

El servicio corresponde a la evaluación de configuraciones que permite analizar y supervisar el estado de seguridad de los sistemas de información y la eficacia de los controles. El servicio se brinda mediante el acceso a un conjunto de recursos y herramientas de seguridad cibernética para implementar los controles de seguridad crítica, que comprende un conjunto prioritario de buenas prácticas en seguridad cibernética, así como las acciones defensivas que puedan ayudar a prevenir los ciberataques más peligrosos y con mayor impacto; y en ese sentido, apoyar el cumplimiento de una serie de múltiples marcos de seguridad de la información y ciberseguridad. La evaluación de seguridad corresponde a líneas base de configuración y mejores prácticas para configurar un sistema de forma segura. Cada una de las recomendaciones de orientación hace referencia a uno o más controles de buenas prácticas internacionales que se desarrollaron para ayudar a las organizaciones a mejorar sus capacidades de defensa cibernética.

5.2.4. Entrenamiento y concientización

Los miembros de CSIRT-BUSINESS IT impartirán seminarios, charlas y cursos periódicos o a requerimiento según los recursos disponibles, sobre temas relacionados con la seguridad informática; estos seminarios, charlas y cursos estarán abiertos a los clientes, administradores de los sistemas que administra BUSINESS IT o también puede ser un evento público según comunicación oportuna.

5.2.5. Envío de boletines, comunicados o anuncios

Este servicio tiene como objetivo brindar información sobre el panorama de amenazas, vulnerabilidades publicadas, ataques en curso, indicadores de compromiso, nuevas herramientas, técnicas de ataque o artefactos de ataque, medidas de seguridad y protección, entre otros, para remitir las alertas de manera

general y la ruta de acción recomendada, los que son necesarios para proteger los sistemas y las redes de su comunidad atendida o circunscripción.

5.2.6. Servicios de información

Estos servicios contemplan:

- Lista de contactos departamentales de seguridad, administrativos y técnicos. Estas listas estarán disponibles a través de canales comúnmente disponibles.
- Listas de correo para informar a los contactos de seguridad sobre nueva información relevante para sus entornos informáticos. Estas listas estarán disponibles solo para clientes y los administradores de los sistemas que opera BUSINESS IT.
- Repositorio de herramientas de seguridad y documentación para uso de los administradores de sistemas. Siempre que sea posible, se proporcionarán versiones precompiladas y listas para instalar.

6. Formulario para reportar incidentes

Para reportar incidentes, sírvase remitir un mensaje de correo electrónico a la cuenta csirt-latam@grupobusiness.it. A la fecha de versión del presente documento aún no se han desarrollado formularios para informar incidentes a CSIRT-BUSINESS IT.

7. Descargos de responsabilidad

Si bien CSIRT-BUSINESS IT tomará todas las precauciones en la preparación de información, notificaciones y alertas, CSIRT-BUSINESS IT no asume ninguna responsabilidad por errores u omisiones, o por daños que resulten del uso de la información contenida en el mismo.