RFC 2350 — CSIRT DICOFRA

Versión 1.0 — Octubre 2025

1. Información del Documento

1.1 Fecha de última actualización: 27 de octubre de 2025

1.2 Lista de distribución para notificaciones: csirt@dicofra.com.mx

1.3 Ubicación donde puede encontrarse este documento:

https://www.dicofra.com/servicios-csirt

1.4 Autenticidad e integridad: Este documento se publica en el dominio oficial de DICOFRA y está firmado digitalmente utilizando la clave PGP del CSIRT DICOFRA.

2. Información de Contacto

2.1 Nombre del equipo: CSIRT DICOFRA

2.2 Dirección: Av. Insurgentes Sur 945-Planta baja y Piso 4, Cd. de los Deportes, Benito Juárez, 03100 Ciudad de México, CDMX

2.3 Zona horaria: GMT-6 (America/Mexico_City)

2.4 Teléfono: +52 55 4884 1547

2.5 Fax: No aplica

2.6 Otros medios de comunicación: Microsoft Teams / Zoom (previa solicitud)

2.7 Correo electrónico: csirt@dicofra.com.mx

2.8 Claves públicas y cifrado: El CSIRT utiliza PGP para comunicaciones seguras. Clave pública disponible en https://www.dicofra.com/servicios-csirt

2.9 Miembros del equipo: Los nombres y roles no se publican por razones de seguridad.

2.10 Otra información: Miembro de la División de Operaciones Cibernéticas de DICOFRA (Seguridad Ofensiva y Defensiva). Coordina con los equipos internos Blue Team, Red Team y Purple Team.

2.11 Punto de contacto con clientes:

Atención por correo electrónico: csirt@dicofra.com.mx.

Horario laboral habitual: lunes a viernes de 09:00 a 18:00 (CST).

Atención 24/7 a través de: soc@dicofra.com.mx Atención de emergencias disponible por correo electrónico.

3. Mandato del Equipo

3.1 Declaración de misión:

El **CSIRT de Dicofra** tiene como misión proteger la infraestructura tecnológica, la información y los sistemas tanto de la organización como de sus clientes. A través de la detección, análisis, respuesta y mitigación de incidentes de seguridad informática, el CSIRT trabaja para garantizar la **confidencialidad, integridad y disponibilidad** de los activos digitales.

Nuestro equipo se compromete a ofrecer servicios de alta calidad en la gestión de incidentes, el manejo de vulnerabilidades y la mejora continua de las defensas de ciberseguridad. Además, el CSIRT actúa como un recurso estratégico para la organización y sus clientes, asesorando en la implementación de medidas de seguridad y ayudando a prevenir futuros incidentes mediante un enfoque proactivo y coordinado.

3.2 Población atendida:

El CSIRT de Dicofra tiene una **constituencia** bien definida que abarca tanto a la organización interna como a clientes externos que solicitan servicios de ciberseguridad. A continuación, se detalla la constituencia del equipo:

- **Interna**: Todos los empleados, sistemas de información y redes internas de **Dicofra**, incluyendo datos sensibles y la infraestructura tecnológica interna. El equipo es responsable de proteger la infraestructura tecnológica interna, respondiendo a incidentes que puedan comprometer la confidencialidad, integridad y disponibilidad de los sistemas de la organización.
- **Externa**: **Clientes externos** que contraten asistencia para la gestión de incidentes de seguridad informática. Esto puede incluir organizaciones asociadas, clientes comerciales y cualquier entidad que contrate los servicios de ciberseguridad ofrecidos por **Dicofra**.

3.3 Patrocinio / Propiedad:

Dirección y control de franquicias S.A. de C.V. (DICOFRA) es propietaria y patrocinadora del CSIRT DICOFRA.

3.4 Autoridad:

El CSIRT tiene la **autoridad otorgada por la alta dirección de Dicofra** para actuar tanto sobre su constituencia interna como externa, bajo los siguientes parámetros:

Para la constituencia interna (Dicofra):

El CSIRT tiene plena autoridad para:

- Imponer medidas de seguridad y tomar acciones directas, como la desconexión de sistemas o la implementación de parches críticos en caso de identificar riesgos.
- Acceder a todos los sistemas y datos internos necesarios para la investigación, respuesta y mitigación de incidentes de seguridad.
- Escalar incidentes a la alta dirección o a otras áreas clave de la organización para coordinar respuestas inmediatas.

Para la constituencia externa (clientes):

El CSIRT tiene la autoridad definida por los acuerdos contractuales con los clientes. Dependiendo de los términos del contrato o SLA, el CSIRT puede:

- Proporcionar recomendaciones para la contención y resolución de incidentes.
- Asesorar en la implementación de medidas correctivas y preventivas.
- Escalar incidentes críticos a los responsables de seguridad del cliente o a terceros autorizados (por ejemplo, reguladores o proveedores de servicios externos).
- En situaciones en las que el contrato lo permita, el CSIRT puede tomar medidas directas en los sistemas del cliente con su aprobación previa, garantizando siempre la protección de la infraestructura y los datos del cliente.

Nota: En todos los casos, el **alcance de la autoridad** sobre los clientes externos será definido en los contratos o acuerdos de servicio, y la ejecución de medidas siempre se hará conforme a dichos acuerdos.

4. Políticas

4.1 Manejo y clasificación de la información

El **CSIRT DICOFRA** administra toda la información relacionada con incidentes de seguridad bajo los principios de **confidencialidad, integridad y disponibilidad**, conforme a la *Política de CSIRT*.
Toda la información se clasifica utilizando el **Traffic Light Protocol (TLP)**: **RED, AMBER (+STRICT), GREEN y WHITE**, en su idioma original.
La información se considera **confidencial por defecto** y sólo se comparte con personal autorizado, otros CSIRT acreditados o clientes afectados, bajo el principio de **"Need to Know"**.
La evidencia digital se almacena de manera controlada y cifrada, manteniendo la cadena de custodia. Su eliminación se realiza mediante **borrado seguro o destrucción física**, según los plazos de retención establecidos en la *Lista Maestra de Control de Información Documentada*.

4.2 Política de cooperación y coordinación

De acuerdo con la *Política Cooperación con otros equipos CSOC*, el **CSIRT DICOFRA** mantiene relaciones de colaboración con otros CSIRT, CERT nacionales e internacionales y organizaciones del ecosistema de ciberseguridad, incluyendo **FIRST** y **CSIRTMX**.
La cooperación se rige por acuerdos **NDA y SLA**, bajo los principios de **Need to Share / Need to Protect**, garantizando la confidencialidad de los datos compartidos.
Las actividades de cooperación incluyen el intercambio de indicadores de compromiso (IoCs), tácticas, técnicas y procedimientos (TTPs), reportes técnicos, análisis de malware y alertas coordinadas.

4.3 Política de comunicación y divulgación

La comunicación pública o externa durante la atención de incidentes se rige por la *Política de Comunicación ante Incidentes CSIRT*.

Cualquier información sensible o relacionada con un incidente se mantiene confidencial y sólo se divulga una vez mitigado, con autorización de la **Dirección General**.
Los canales oficiales del CSIRT son:

- **Correo:** csirt@dicofra.com.mx
- **Sitio web:** https://www.dicofra.com/servicios-csirt
- **Llave PGP:**

  -----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGk3K8MBEACv9qIqmiUabOV6OQC0aRkYIFXMjann1BtSr+9F6Rl74GLe2sTR

ML7F+C7dq6PCbMWImvVh3XEqWbu7o/MBsOAAdFbiW7r0NQSUveb2jKuD2U4Uh
mMJ

ced7zvSPs6Gts+XGBqVb+rWmsHRAi9RjqtKdGpaGXgNsc+SGUjhUa0lz/Fcn+7Ey

NU3dOYNArNd1h9e7pAqFIpYdec7Um/2J1G8dt1Udszh30AkgexyHOJeFh4heD7Bw

8MvzwcBiSq2jJVBUi5JvhwyAybx/jBXyRnawTYmRprPHitduXsFs0eFVtAvjxbda

qD/dQ184BHKDJ8NnQKvBsCvwr43SvYwaSffrdi/jQDhbsLuP72PIHeveaFIniSxE

f74s5EAgYwgGPiW59K549H+nnH2ygn1cLjtPWXiJdnV7GCMxJu1bOcLTPtQvSQDh

Qj6k3G/wZVM9yq72Tig5cqY9KtTwCuUBQuAqf6YNu0kTxWOEGi6Ks77FdZtQNu5T

f/2scPKJZFMg0s+jg9P5kMRk2ZrDBYBtlOHqyhDhAsRh9/+w9IQX0qp/DFOBOcTs

XDEKk2A2R0f9gVKshDWLrHjJ7q9nbrc6tZGDWepXu8Q4vwr7T4rhnbsEr43DGGbm

LrqHAus9CBhYrLJ632SZ0waCZQeckeCBqTzwuk8kjlgHXoxYRok1xyihaQARAQAB

tCRjc2lydCBkaWNvZnJhIDxjc2lydEBkaWNvZnJhLmNvbS5teD6JAlcEEwEIAEEW

IQQ5I1yIj0dAN6J35Itfsbs9h0XLtwUCaTcrwwIbAwUJA8JNXQULCQgHAgIiAgYV

CgkICwIEFgIDAQIeBwIXgAAKCRBfsbs9h0XLt031EACSupfoJXUG+/absTFFTjpe

CaOGLo+eQlTNpbiRestLiRHdG4b1Jjyr68u4AziWzTIALFvaJHPAGzvrBiYMk8t2

+6su9kBCGOM+FO68329LABYrajSB77BygYXn8HQpeTLBqx9SWThlgGTDMagm48C
D

JDoqc43jRMF78IjdXnpfSz/gg7xhn9vZgL3hTYtrWN1HqLduYRKL0EjaQEZ+JcCF

m0USpSrqiOVDiHOVsUzRhCJvjPzUEmiE4vTjKzoPibYTsxJ6+fn4w7+yd6lGubSm

zMoexUpPECiu6rdzTD5BaVtn0SPDl/xNwJ8s2NBUkIG7XYwSWwjhVbBM2BL7XP3b

LXVVoztFIcTkiQXaJxZ2pz7ThNRRES51sao4IohyUzkdDkHxS0OgD1lkVtQaTB8L

2mGTMA3xXSxm50C0i/Q5dw19Y4VmkGsDuAJoDQ6DHYvmEBAP/Yb2NV/retyl/jQ
l

/heBAiijoe4lYnSfvXa3WQA7Z4/9XXRWa99pF6zZsddouII/vlTvPJXOpErbLTDp

XUQEkJ7rc1BMKY+DpNInId1oaBKH8wYcBs88tnr1VojX2JOcrHR1Grtb0bZm5JlQ

M0/nhF++l1B2qPhC4d+bpQf0pSmMPv1TeTeDDcg72pjo8QZhAsDIBxUvkaiVSbiw

vUPZMqslNq+PptFix3wsxbkCDQRpNyvDARAAt8k57ty46i3CLlBv9EKwXou5ejwK

5RfPQ8VzKUne+7/QRp456f2dYQ40ZY7Dxd+t8S9WYRPA08H63Y1Oy1CKB0x6tsvd

fpoPeBZyEVfmGdBqkAD53WM4thNKDLuplTCA0sJXk4pyAbaibY4gMmXjY4g2EJIs

sDxEo4nLSl72+L7vmTxnY1cZrtC1QvDTumL+bdNXBzIFxZEsn2WKp76mjOmDJsri

qqnA0DYHJdYSEzzO7TMG0O8om9NMxn1P31JegivM420xcMTvgvuwN2thjqI4lTkJ

5ecUuK3fLN8bZzk4j9Ozp4ol2hZU/ErYWuKNdfA+wELeAOtL138ZxOggfGJwQv9B

IDJZdJEDRwiaCc/pi/dqGWs8KiQl7TkvhsMRThp8aEVi6ozhK+cli6W2XU+U1SWD

36Gqox7uVWCUmk5Z1eeJrOifu1S3Nd/EMmBAIFxb63Yx/M6/G5w5Vwy1ucNmNRc
I

NuS4BSrjNpSSWPrLJgw4qSXwuci1B3nLpmEgzmPa1kfpJWJNlEjP8wr1s5PSmOvY

Rn+0yZxZfiqg1hROobOhXmNmHeU1NDz1jaHagR7CH5N/Tp4K+nZsU6Jz5Er2e9DL

uLeFlKTYokvruW1eisfB8EioK06NNm1OmEn1Iub8HPOYpwOMEKRfSQ9NTVyJ7Vu/

kf7btK2O22DiQVEAEQEAAYkCPAQYAQgAJhYhBDkjXIiPR0A3onfki1+xuz2HRcu3

BQJpNyvDAhsMBQkDwk1dAAoJEF+xuz2HRcu3UsMQAICweqWxPSF/KLlht1RTMg7
2

N74fk/Ka7jauh9ZqOWV18zISuuA9jWftx3aW7fNSRu5ZUH//VwhAXPLQIX0RJdQz

Fuh79/jKRoFfoGOjwMYtIoCwyD1WrBsXlmewUAJOdVeGUt5zyR9dbIx9f2pe+zQK

0oiF9dUHb36K/BgOrUUTTyeHLopkHgOjaVxMKJh8alT1UI9U4rxyuYiuWP0iz8a0

Pl6iyI2ApqXNVNoQCUfQnU9PIx6L74V8gSlgM/7NADBXy2191LDgkMAFQx5RnEvF

hliT+dmpglPX+guUyOZbR04Pr2Ge8ZjkMalK+gCpdmQgPM+eehQxp2k5HgdghkeV

ShW/p564/qJNHwj/Rh55zGjUojY8ATv8tJgllrlnMbzxcMEQao4nyDKYYDWvW+pc

a7bXpgPqP0FbEkWZdr6UcV4XmPBCOmIMVG0hpCVARoEc6l1TcKqIypeJHLku8epY

++jMuFAFSucptaOX/guqcQMbDM+lMTg50etVr4LwJdWx9Nl9N3V5/9tOPb52WkAO

10jHnine4qlWG8/4KgTzasd9h6eZPfPpoXJnrduS60C/exgSZzZ3fO5YE//D7bVO

gULLvbChKbUK9IUaCVl+zBVyT2u8dFdjoHSzkGVczMIm8i63IWhqRTSYoOmFb9bX

uCdz4aA2Y371Rpiotd8S

=9wJP

-----END PGP PUBLIC KEY BLOCK-----

El CSIRT puede emitir **alertas preventivas y comunicados de seguridad**, asegurando la anonimización de la información sensible.

4.4 Política de competencias, capacitación y resiliencia del personal

El **CSIRT DICOFRA** garantiza su operación continua mediante la *Política de Resiliencia del Personal* y la *Política de Competencias, Capacitación y Desarrollo*.
El equipo mantiene personal disponible **24×7**, respaldado por el **CSOC DICOFRA**, con mecanismos de sustitución temporal ante ausencias y planes de continuidad operativa.
Todos los miembros del CSIRT participan en programas de **capacitación técnica, ética y de liderazgo**, que incluyen certificaciones reconocidas (CHFI, GCIH, CEH, OSCP, CCISO, entre otras) y entrenamientos internos en comunicación y manejo de crisis.
Las competencias se evalúan anualmente para mantener la excelencia operativa y cumplimiento normativo.

4.5 Política de escalamiento y gobernanza

El **Proceso de Escalamiento del CSIRT** establece los niveles de comunicación y autoridad durante incidentes de alto impacto.

Los incidentes críticos se escalan de inmediato al **Líder SOC**, al **Gerente de Seguridad Ofensiva y Defensiva** y al **Director de Operaciones**, conforme a su severidad y alcance.
El proceso define rutas de contacto seguras y responsables designados 24×7 para temas de gobernanza, comunicación, prensa y asesoría legal, asegurando una respuesta rápida, controlada y trazable.

4.6 Código de conducta y ética del CSIRT

Todos los integrantes del **CSIRT DICOFRA** deben cumplir con el *Código de Conducta y Ética del CSIRT*, el cual establece principios de **confidencialidad, integridad profesional, responsabilidad, respeto y uso adecuado de los recursos institucionales**.
Cada miembro firma una **Declaración de Aceptación** al incorporarse al equipo y la renueva anualmente.

El incumplimiento de este código puede derivar en sanciones internas o consecuencias legales conforme a la gravedad de la falta.

4.7 Resumen del proceso de gestión de incidentes

El **CSIRT DICOFRA** ejecuta el *Procedimiento de Gestión de Eventos e Incidentes de Seguridad*, alineado con **ISO/IEC 27035** y **NIST SP 800**.

El proceso abarca las siguientes fases:

1. **Detección y registro:** Identificación de alertas en consolas (SIEM, EDR, WAF, DLP, etc.).

2. **Análisis inicial (Tier 1):** Validación, clasificación y escalamiento según los criterios definidos.
3. **Notificación:** Registro en ITSM y aviso a los responsables internos y al cliente.
4. **Análisis avanzado (Tier 2 / CSIRT):** Investigación técnica y coordinación entre verticales (Blue / Red Team).
5. **Contención y mitigación:** Ejecución de *playbooks* y aplicación de contramedidas aprobadas.
6. **Comunicación y escalamiento:** Activación de los procesos de comunicación y gobernanza.
7. **Interacción con terceros:** Coordinación con proveedores o fabricantes.
8. **Cierre y RCA:** Elaboración del análisis de causa raíz y validación por el cliente.
9. **Lecciones aprendidas:** Actualización de reglas, controles y automatizaciones.

Los tiempos de atención se rigen por los **SLA definidos en el Anexo 10 del mismo proceso.**

El proceso es dirigido por el **Gerente de Seguridad Ofensiva y Defensiva**, con apoyo del **Líder de SOC**, **Líderes de Vertical T2**, **Blue Team**, **Red Team** y **CSIRT**, garantizando trazabilidad y calidad de respuesta.

4.8 Confidencialidad y autenticidad documental

Toda la información entregada al **CSIRT DICOFRA** se trata como confidencial salvo indicación contraria del remitente.

El equipo mantiene la integridad, autenticidad y reserva de los datos conforme a sus políticas internas y acuerdos contractuales.

5. Servicios

5.1 Respuesta a incidentes: Análisis, contención, erradicación y recuperación.
5.2 Detección y caza de amenazas: Monitoreo continuo e investigación de amenazas emergentes.
5.3 Gestión de vulnerabilidades: Evaluación, priorización y seguimiento de remediaciones.
5.4 Análisis forense digital: Recolección y análisis de evidencia bajo prácticas de cadena de custodia.
5.5 Alertas y concientización: Publicación de boletines y guías para partes interesadas internas y externas.

6. Reporte de Incidentes

Los incidentes deben reportarse al correo csirt@dicofra.com.mx con la siguiente información:

- Nombre y organización del contacto
- Fecha y hora de la observación
- Sistemas o servicios afectados
- Descripción breve del incidente
- Evidencia relevante (logs, encabezados, capturas, etc.)
- Formulario estándar disponible en: https://www.dicofra.com/servicios-csirt

7. Descargo de responsabilidad

El CSIRT DICOFRA toma todas las precauciones para garantizar la exactitud de la información contenida en sus avisos y comunicaciones; sin embargo, no asume responsabilidad por errores u omisiones, ni por los daños derivados del uso de esta información.