RFC 2350

CSIRT

E-DEA

Glosario:

- **CISRT**: Computer Security Incident Response Team (Equipo de Respuesta a Incidentes de Seguridad Informática) es un grupo especializado de ciberseguridad que monitoriza, detecta y responde a incidentes de ciberseguridad, operando generalmente 24/7 para proteger infraestructuras críticas, empresas privadas o públicas. Además, puede ofrecer soporte técnico, gestión de vulnerabilidades y coordinación para la mitigación de amenazas para asegurar la continuidad operativa.

- **RFC:** Request for Comments (Solicitud de comentarios) es un documento numérico en el que se describen y definen protocolos, conceptos, métodos y programas de Internet. La gestión de los RFC se realiza a través de IETF.

- **IETF:** Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet). es una gran comunidad internacional de diseñadores, operadores, proveedores e investigadores de redes preocupados por la evolución de la arquitectura de internet y el funcionamiento fluido de este.

- **PGP:** Pretty Good Privacy (Privacidad bastante Buena) Programa de seguridad criptográfica diseñado por Phil Zimmermann en 1991 para proteger datos, correos electrónicos y archivos. Utiliza técnicas de criptografía simétrica y asimétrica para cifrar información y asegurar que solo el destinatario previsto acceda a ella, además de ofrecer firmas digitales para autenticar la identidad del remitente para maximizar la seguridad de las comunicaciones.

1. Información del Documento:

Este documento contiene la descripción del Equipo de Respuesta a Incidentes de Seguridad Informática (CISRT) de E-EDEA conforme al estándar RFC 2350 de IETF.

1.1. Fecha de la última actualización:

La versión vigente de este documento es la versión 0.0, publicada el 27 de marzo de 2026. Este documento tiene validez hasta ser reemplazado por una versión posterior y será notificado a través del sitio web oficial de E-dea Networks: https://www.e-dea.co

1.2. Ubicación última versión del documento:

La versión actualizada de este documento se encuentra en el sitio web oficial de E-dea Networks: https://www.e-dea.co

1.3. Autenticidad del documento:

Este documento ha sido firmado con la llave PGP de E-DEA.

1.4. Ubicación del documento:

- **Español:** https://www.e-dea.co
- **Inglés:** https://www.e-dea.co

1.5. Identificación del documento:

Título: CSIRT E-DEA RCF 2350
Versión 0.0
Fecha de publicación: 27–03-2026
Expiración: Este documento será válido hasta ser reemplazado por una versión posterior.

2. Datos de Contacto:

2.1. Nombre del equipo:

CSIRT E-DEA

2.2. Ubicación: Carrera 7 N° 156 - 10 Ofic. 1906 -1801, Centro Empresarial North Point, Torre Krystal, Bogotá D.C. – Colombia.

2.3. Zona horaria:

GMT/UTC -05:00.

2.4. Teléfono:

+57 (601) 5188433 (Ext. 1111) y al número celular 317 441 07 61.

2.5. Correo Electrónico:

Para reportar un incidente o vulnerabilidad o solicitar un servicio como: sensibilización, intercambio de información relativa a incidentes o realizar una consulta en general, deberá escribir directamente a: seguridad@e-dea.co.

2.6. Clave pública y cifrado de la información:

La clave PGP asociada al correo oficial se encuentra publicada en la URL: https://www.e-dea.co

2.7. Miembros del equipo:

No se proporciona información sobre los miembros del equipo. Se proporcionará en caso de necesidades con nuestras partes interesadas.

2.8. Horarios de atención:

- Consultas sobre servicios: horario de oficina (8.00h-18.00h)
- Reporte de incidentes y vulnerabilidades: 24x7x365

2.9. Puntos de contacto para la comunidad:

La comunicación entre el CSIRT E-DEA y las entidades tanto del nivel público, como privado y de la sociedad civil se da principalmente a través del correo electrónico oficial.

2.10. Información adicional:

Para información adicional diríjase a la página web https://www.e-dea.co.

2.11. Puntos de contacto con la comunidad:

El CSIRT E-DEA prefiere recibir los informes de incidentes por correo electrónico a seguridad@e-dea.co. Por favor, utilice nuestra clave criptográfica para garantizar la integridad y la confidencialidad. En caso de emergencia, utilice la etiqueta [URGENTE] en el asunto de su correo electrónico.

3. Constitución:

3.1. Misión:

El CSIRT E-DEA tiene como misión mejorar la identificación, mitigación y respuesta ante ciberataques en el sector público y privado. Usamos metodologías coordinadas para reducir tiempos de reacción e impacto de incidentes, afinando nuestras capacidades tecnológicas y humanas para una gestión eficaz de la ciberseguridad.

3.2. Circunscripción (Jurisdicción) comunidad a la que brinda servicios:

El CSIRT E-DEA es el equipo de respuesta de apoyo a la respuesta de incidentes del sector tecnológico de organizaciones públicas y privadas que fomenta la colaboración de sus miembros y el intercambio de información para afrontar de manera efectiva las amenazas cibernéticas.

3.3. Afiliación:

El CSIRT E-DEA está ubicado dentro del Proceso de Operaciones de E-DEA.

3.4. Autoridad:

El CSIRT E-DEA opera, dentro del Proceso de Operaciones, bajo la autoridad del Responsable de la Seguridad de la Información y de la Dirección de Operaciones de E-EDEA.

4. Políticas

4.1. Tipos de incidentes y nivel de apoyo

El CSIRT E-DEA es el punto de contacto central para incidentes informáticos relacionados con la seguridad en organizaciones públicas y privadas clientes de E-DEA.

El nivel de asistencia que ofrece varía según el tipo y la gravedad del incidente o problema, el tipo de usuario, la importancia del impacto en infraestructuras o servicios críticos o esenciales, y los recursos disponibles del CSIRT E-DEA en ese momento.

Los servicios de E-DEA incluyen servicios reactivos y proactivos:

- Alertas y avisos;
- Análisis forense de incidentes;
- Asistencia y soporte en respuesta a incidentes;
- Respuesta y remediación de incidentes (también in situ);
- Análisis de vulnerabilidades y malware;
- Respuesta ante vulnerabilidades;
- Análisis e intercambio de inteligencia sobre amenazas.

4.2. Cooperación, interacción y distribución de información

La información relacionada con incidentes, como nombres y detalles técnicos, no se publica sin el consentimiento de las partes interesadas. Salvo acuerdo contrario, la información proporcionada se mantiene confidencial. El CSIRT E-DEA nunca cederá información a terceros a menos que lo exija la ley.

El CSIRT E-DEA dentro del funcionamiento normal de sus actividades interactúa con diversos interesados, entre los que se cuentan clientes, organizaciones de seguridad a nivel Colombia e internacional, como grupos de CSIRTS y fuentes de

inteligencia, proveedores, fabricantes y medios de comunicación, de acuerdo con las relaciones que se tenga con cada una de ellas, así mismo se puede establecer comunicaciones con diferentes roles con encargados de seguridad de la información, ingenieros, encargados de recursos humanos, usuarios finales y/o periodistas.

De igual forma se considera de vital importancia establecer contacto con otros equipos de repuesta a incidentes como el COLCERT, CSIRT-PONAL, COCIB como parte del proceso de intercambio de mejores prácticas de respuestas de incidentes y endurecimiento del entorno.

Para la distribución de información se utilizará el etiquetado de documentos y comunicaciones como se describe a continuación:

Confidencial: Información disponible solo para los procesos autorizados de la compañía y que en caso de ser conocida por entidades no autorizadas puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.

La información se clasifica como confidencial en los siguientes casos:
a) Acceso restringido a la alta dirección.
b) Información de los clientes.
c) Contiene información confidencial de las partes interesadas (tener en cuenta documentación como, pólizas, acuerdos de confidencialidad (NDA), informes con detalles técnicos privados del cliente, contratos).
d) Contiene información personal de cualquiera de sus categorías a excepción de la pública.

Restringido: Información disponible para todos los procesos de la compañía y que en caso de ser conocida por entidades sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la compañía o de terceros y puede ser utilizada por todos los colaboradores de la compañía para realizar labores propias de los procesos, pero no puede ser conocida por entidades sin autorización del propietario. Podrá ser compartida con terceros con los cuales se tengan relaciones comerciales, aplica para documentos que son de uso interno de la compañía, como procedimientos, actas de reunión, formatos administrativos, etc.

Público: Información que puede ser conocida o publicada sin restricciones a cualquier persona dentro y fuera de la compañía, sin que esto implique daños a terceros, ni a las actividades y procesos de la entidad, sin generar impacto negativo de índole legal, operativa, de pérdida de imagen o económica.

Dentro de CSIRT E-EDEA, la información se transmitirá según su clasificación y

el principio de necesidad de conocer, por lo que solo se transmiten los extractos anonimizados y específicamente relevantes.

Cuando CSIRT E-EDEa reciba información que aplica el Protocolo de Semáforo (TLP), respetará la política de intercambio de información definida por FIRST en: https://www.first.org/tlp/.

4.3. Comunicación y autenticación

El método de comunicación preferido es el correo electrónico. Para el intercambio de información confidencial y comunicaciones autenticadas, el CSIRT E-EDA utiliza PGP para cifrar y/o firmar mensajes. Toda comunicación confidencial dirigida al CSIRT E-DEA debe cifrarse con nuestra clave pública PGP.

La cuenta de correo y la clave pública PGP son las que se indican a continuación:

seguridad@e-dea.co Huella digital:
A3C5489FF3D878E79837D1300C31E08B1D43C54B

Clave pública PGP:
mQINBGnf6ikBEAC9glqGwkj4qjp5fZgz6kW9MxpiWcbyU6kMtOS33zJl0XzaMByV
4aZZF6G4KjqQB/7xVaaWVRDWtRfuhx9DcvEUYdDfQWVCoXuq52tiZ5xUlZQBvp
HwuGUVSNfFKjsrtmkrWRVnC50gP/zRLuEM7jVv0ulZU1HjXtXBGfRlMWDcyClaS8
Vnj0BtPt9+3xmzB35cdArwYO5wo+jLoWZ/f/ioLvcPumCdQpLSCefl7afAU62SOu
Z24s++9HFmhm5kBW50e1L+TdjMqm0dDQsa5JXYIm0Y56np+ZkpcAzGYD/xqd
FZ5WozTHd8SdVlHZhXJ+ha+YTZnMNBt01W3cZaAi2Tf9mD4bpMnVdDtlvymzN
U8Z84rh3GdzfI0C3uqxUVJdASoEzMBtBIr0lHFDMcP4KhRh0caMwf7HaiLsnNHk
SbW0+ucUjz0NQzqRgbvaKTDpd6PSlYsYh5YfMrXw0LIkw0ggj6re38P8AX28Tip
pZVIKnoLyvL/Eiuve7lJx61lEbbu2XBpma6Xsskt2FI2kXHBcZm5b1cuY0+Eu0n8i
WzBWS1onTyEmueh/4JYPKQDDTEhXmNMJgpQgO8fm2qG3KMU6J6X/e4jPjtyL
uqdpMG7jSLwkXhqm0Wjwgs16hR6EzHIkTZHH5Mj18u9g0A1u/ItnDTpgfDhN0HI
uqSNl+23QARAQABtCBDU0lSVCBFLURFQSA8c2VndXJpZGFkQGUtZGVhLmNvP
okCcwQTAQgAXRYhBKPFSJ/z2HjnmDfRMAwx4IsdQ8VLBQJp3+opGxSAAAAA
AAQADm1hbnUyLDIuNSsxLjEyLDIsMQIbgQUJBaTF5wULCQgHAgIiAgYVCgkICwI
EFgIDAQIeBwIXgAAKCRAMMeCLHUPFSyvsD/4kTw+NRbVGmJfvvaR8WPnmDA
WvILI0Em05q/YSd4xjUVARcmV0Fh0i4QfLVTCw3ykKVgyGTSs65Y6SpTvuiSFV
PWWoxpxfmfGkzFW/18GUUf7w0RdanG3Z7ZQQTSqLvhEM7NU7HF/3S/Lf3TyQQ
t3RLdBeHHuNvajxiwqZ++tqyfC7KIqbAY2o0rBPSkPAVImdnFXA7hdHStwHEGtS
8HeoE1Ak/03gL+7BiIXDUFhstpRGf7h3BJKgq8s5dtxyjJHTHR0JP3W+nmrD+Ib
PEo1QqqV3AazqJJHEcw/yMvFO735XnDy5+JexipyYAtZSdwmaBq/2KzFxYVGV
H7p8s6wScwoact7RMY0wxGICfbawTNVjGwz560n27JLv4vkzIADi0mqvZm7AE
Wh8IrcALIBduYeen1ScdG/2aNGa7H7mYrzynKLDCm2x8MgJyS4S9BBTI4J46wH
CjN0z6EbN7zHQhYc/ELX0oBPZgc1ylEJ0aIbFV/hv3+NMDg6RjmUCI/z0TMghUc
0AS91pNzhSoekRYFS2vcVQ0xxJ/Jli0DfnOnAX0mH/yUt++RoBBQDuC0jHRMhp
dpsrh0kD0XQ3kf7Gipy/2d4mwivWdZt0b12Al1flqbTzsFUZG3LhmTHk2XH0//LsZ

BzBIPImvivwmaIBnGI8soI0sUB0WEhLCIuQxbkCDQRp3+opARAAtcfkv0Bv4pK0
T1Xrc9f0CoRQU8kITajjeg9I8vvdI9oS4m81pPx5kjViwB9PPmGA9/0rgYPiavj0e5/
5/K0HeGIdUEUrZbIe7fu4LvFMJcX9zDsJHCA+S3KmF05bM9ae3bX4XlYjXSeMN
emJAGvTlXab6XYzWSxtRj0h5402yr0awQytihhIcaj37EDQ7tikgapY/9Jh3rCZeYv
zT17xfwqEV5B53jSbQLNSi3BRUiAPAIW1g3vTZt7aPIW+eTSNM2wTE7N4Fuk0RCj
6wAVEWoSh0hzugakgF0UGwS4VFgkV3a52RP5fBMW22Bk6qpp0kHRQR3bcy/z
vMP+VarI2PB++7LrU/vvTHGcXDoVN6pb/jYzIRkbQh8bkTHsH7NfuegJFxIvbP00
qx+Zx+29ARZmNUJYy0YSsShUqo8Savj36ahHHSSatudUk9LjShISRAdFZqYc10
eKms6IKWqeIcBS95b8yNafazPL00K1vh4Fbe2nzpI0mDJ+fFgFwLPfeKW52sNJ/
koqZNwfbTzuY3/A5W7kRbsiurZLwEQ0VgNRvA70B09n7uLUd/1up2mFn0UBGft
FGSD4YQ09MainZunM/pGClMpRmrm+kUSNDQ8q5u9WsnZeru1CZBwZow00TjY
cNoK1P3wZHq7S+0VBy/kISm64nTI9QZN92Cg2seP0AEQEAAYkCWAQYAQgAQh
YhBKPFSJ/z2HjnmDfRMAwx4IsdQ8VLBQJp3+opGxSAAAAAAAQADm1hbnUyL
DIuNSsxLjEyLDIsMQIbDAUJBaTF5wAKCRAMMeCLHUPFSw3GEACTw/2DzB8GX
NW2ZFVty6N0wZW4wAtrV1xK9KaDw0Qs8CT3bsMXC9gyhZNDnxGK8/ZcLsgyb
85/fAL4RuhbFxCXiT0at21mrkn0dzTCRtNFX9Dr7H6XgZs2ItzHdHNf0JtrFcND42
sW+mLBbvDCJCzyEvtDRJx0dArXNkwt5XTgEerQTr5iFUUn1EfkCKPIBg7Z4Nc6P
NqIcwV+fNdrsIfAY4dIKxA4+E6UB8frSXZEhch7p7fPoYfbr01iw3qYviEWSrAX/48
0C4NfsYajrJIZ0d3DuKF2uj0qPdI68ID4RzLhfqUfgV84BwcAYXq+3bQNrEoGKUV
b/DjBTKnGeBI638I5SJDwBbGZVYkSC3Y2cq9aBZNQsm9/ITWAM+glrxWf3z8X8
GjNI1ohlwZl6oCgdCM/NxqsOolZl5uhn17DzmUswpPPhMJWjRtZ0B5Z/FSG4745g
cHahX5vwixi66J9rJjTwTH2bW2Wufg/KS3d1n7tLYLAOr+FhP8MCie/guHmLX2A
0EJEj0NSp6HvA3Gg69SFE6cThudm0GIf8Xvt4MQVyvta40eE8HazBAQx6AFaY
akPMtzcn5WkEaQQfixY53IovjUb7L8Fs0d7uaWjW9U9ffKYus3amZ1g45RvhJcKF
TyAI8Iq60Kr2k5PzDKwThJwe8ayBrezRbiGpzvE57kCDQRp3+pDARAAn8z0DLgc
GYTQkDDKr+IXMjIBfxwAswRXxxNI8i/Zv+dbRDe216X/xuX/2hk6SMvWIntWk57+1
46LsJo0HLuRiHeouME5R5pENDimsQAW7us8nw7fnZzntM0t2mIzpuKKUiq+TX6
0QQTF6er0IDap1WrxQTaQnDYKqti9yWf2dmXaB9eZLZ8hcr0uoQSnFVYQ6zKGzz
NTWweEsAFH46p3n3bnzf/k8CLpY82vBMNi0/pZi145jmDastAG4ILKIx69dbwbn
R0UipWVTAZgbKqE+vMeGfeJQcDb/cr8dfR0PztX1Y5wIvZvRSsXggCgEWjtijdGC
zHPVxBTw0/IVV0DWxKWx4zr0ls1Lgkf9CeFdBl1QaLZudwQYgsc6wUo3dWRMu5
E6MCNAdo52NaRo4cedkQdC3ejxyKZlNjUtGtr5Yq6/2xU8mIv5hZNsIwZrA1xQZY
tCr+UYmlltfueYxS4wx9qXw5mHWvKZ4GOOxP3dWW1ElMbLLnjNSQDpP/DJ3f0j
GAn9RTE/6LEToR6wQKhf+GLyAPdMantw05Z0YNS57ESxkumkaVzMdPFxtC5Q
6xhyMfCmLoJNSEgPmpXN6a4pSQLb9qxN7sBzYpiDOXxLj5vT2OENzDdoCIhwY
D42Ir5qU4KgVyR5tRrs70eJL3m3qq1tUQq7vCITmR5Drifj8sAEQEAAYkEiAQYAQ
gAPBYhBKPFSJ/z2HjnmDfRMAwx4IsdQ8VLBQJp3+pDGxSAAAAAAAQADm1hb
nUyLDIuNSsxLjEyLDIsMQIbAgJACRAMMeCLHUPFS8F0IAQZAQgAHRYhBPQQVg
P6l1gafYtg7PycTP7zYKasBQJp3+pDAAoJEPycTP7zYKasrPcQAJFsd7L23A1K8qi
Cr4pyKst5VqcoahbULn+OO0UkcHNzhTzkLQ1D2jGQkdilXnXcYaZsWLc5aWU70u
+gKKSpxdCHi+IJBI5W7ffH6iatsPkywZQDKHRqJbjlxCxNSye78xzELhnvw93e88G
S/pbdS3kpVWGVw3dNHtzF2LcdWxda9+6Z49D5ob2TavXCvWW63dI/pv0MjBko
JjF4+RMjrvcTrjytuVAKFq+W9sTLkTnAKRLUliSRK8ne+ExZkUXMf07xaUDoq9NU
TZfrBQ0NM2pV6a0cqFezgtoZm1WydGjJHgTwTVf1Ps60G7A09khfymaTQJBT7O
ynA5QRgi53HLN8EVUPoMOy0YggRlicQhuQIWmXII/JCe78rKlq0dfgq5mH7KFiZd

uNvcY6BjVXRx7Gj9SZqLrT9uCYwr1fUEAMv0xQqm7kfxoF9MVXvCGcbeg5BEiBB
HpU5vEAERJ3kTmNozmBHxVq9rHsnJv99pZFYDEpZYQ8LQ+TVtf9ZXd9iHOAzt
KBTEbRlj4SGHuTZeurNgmF8v5hqxEQhLzK04EMMljrEUoUhS0/0gHwIES3Ksb8A
MtsbPhnOsZBGZMeeXcEEsPv3KXuTYLnH67r021YJXY+xfnbA/ge5uOuEfPIBh83
O8LTRgNyAZKKv26aXyjfXwV30qfK90LgdILuWT6FaQsQAJvQKMi/PwLLYcoIbw9
FYQvkRoUciEx0j6oUx74H9cifYYXGUKEU6H8vpYcoU1s0qZ83nkB5rxysyd90Ua
U8clJcfCG9cTOcYVAcBt2XE4uEJMK5hdqZtNrYc6HtKnf0aNXdjuIl5EadY8VDby
HOzHbm2m9WMcsr14vgigKJT9zYqhOcqfNGdIT2Ju3tayNKyLtDNr1JoOIo39wdE
b5IbQa6/JNpCDy1LYZJ1LI7LXc0/ex143a3q07jjdfAtAurFiV72O9511tjxQGbUoT2g
RXQlUF7nnvCce9maV9m9nbdfspIS+sSnenu21uaWaLahhlqRxG3qevFs4ix1pZw
WqXSdB7ao3jWVN38hpBGaHnPHQgEeQG4m8YWFrka5TleY5X3J5/hQpyX0p0y
RqxaKLAyUUKw7MHwD+KnrIxTTdyeZlxq7TW8ex4vNjCd+5xmpDvb2x2U67qHyR
MW7IYBuoZ1oFEpIv1TFgZyVJ+kx0+iNeoiMxKZbDnpC5tQlxWwriPlPJdQywuOIvrl
lOuUBNfCoEW3UPgSPmHtaDKL2Y/bdvsfcZi344EK6evJ2wIIMLp5x9FU4qF7y+
wwa7IUa86GI+pu9boH9vyDKkx4kWvyIQznQUAfB3ZGw1QE/SUKiiU7Im6sEFNNR
ULis13oS263sKKq+h/Z0vKiFnnRL78o
=2iO6

5. Servicios

5.1. Servicios Proactivos

Los servicios proactivos son un conjunto de acciones y estrategias implementadas para identificar, prevenir y mitigar posibles amenazas y vulnerabilidades en los sistemas informáticos antes de que ocurran incidentes de seguridad. Los servicios proactivos buscan anticiparse a las amenazas. Estos servicios permiten a las organizaciones fortalecer su postura de seguridad, reducir el riesgo de ataques y minimizar el impacto de posibles incidentes.

Alertas y advertencias.

Este servicio proporciona notificaciones tempranas sobre amenazas, vulnerabilidades y actividades sospechosas en el entorno digital de una organización.

Análisis de vulnerabilidades.

El análisis de vulnerabilidad es un servicio que identifica, evalúa y prioriza las debilidades en sistemas, redes o aplicaciones para prevenir posibles ataques y fortalecer la seguridad informática.

Comunicados y anuncios.

Divulgar de manera clara y oportuna información sobre amenazas, vulnerabilidades, actualizaciones y buenas prácticas para proteger a las

organizaciones y usuarios frente a ciberataques, fortaleciendo la conciencia y la seguridad digital.

Evaluaciones o auditorias de la seguridad.

Procesos sistemáticos que analizan y verifican las políticas, controles y sistemas de una organización para identificar vulnerabilidades, asegurar el cumplimiento normativo y mejorar la protección contra amenazas digitales.
Monitorización de redes.

Monitoreo de IOC e IOA.

El servicio de monitoreo de los (indicadores de compromiso) IOC permiten identificar evidencia específica de una amenaza, como archivos, direcciones IP o hashes, mientras que los (indicadores de ataque) IOA muestran cómo estas amenazas están afectando o comprometiendo la integridad de los sistemas, permitiendo una respuesta rápida y efectiva ante incidentes de seguridad.

5.2. Servicios Reactivos

Servicios que consisten en responder y gestionar incidentes de seguridad, como ataques o brechas, para detectar, contener y remediar rápidamente las amenazas y minimizar su impacto en la organización.

Análisis de incidentes.

Consiste en identificar, evaluar y responder a eventos o amenazas que comprometen la seguridad de los sistemas y datos, con el objetivo de mitigar daños, prevenir futuras ocurrencias y fortalecer la protección de la infraestructura digital.

Respuesta a incidentes.

Consiste en la detección, análisis y mitigación de ataques o brechas de seguridad en los sistemas informáticos, con el objetivo de minimizar el impacto y restaurar la seguridad de la organización de manera efectiva y rápida.

Coordinación de la respuesta a incidentes.

Actividades que buscan ejecutar un proceso organizado que involucra a diferentes equipos y entidades para detectar, contener, mitigar y recuperar de manera efectiva ante amenazas y ataques cibernéticos, garantizando la protección de los activos digitales y la continuidad de las operaciones**.**

Asistencia remota a vulnerabilidades e incidentes.

La asistencia remota a vulnerabilidades e incidentes consiste en brindar soporte técnico a distancia para identificar, analizar y resolver problemas de seguridad informática, como vulnerabilidades, ataques o incidentes, mediante conexiones remotas seguras

5.3. Gestión de la Seguridad

Consiste en planificar, implementar y mantener políticas, procedimientos y controles para proteger los activos digitales, prevenir amenazas y responder eficazmente a incidentes, garantizando la confidencialidad, integridad y disponibilidad de la información.

Consultoría de seguridad.

Servicio especializado que ayuda a las organizaciones a identificar, evaluar y mitigar riesgos digitales, garantizando la protección de sus sistemas, datos y activos frente a amenazas cibernéticas de en procesos o áreas.

Sensibilización.

Actividades que buscan concienciar a los usuarios sobre buenas prácticas digitales, promoviendo el uso responsable y seguro de la tecnología para prevenir amenazas como malware, phishing y fraudes en línea.

Transferencias de conocimiento.

Consisten en compartir y difundir información, habilidades técnicas y mejores prácticas entre individuos, organizaciones y comunidades para mejorar la protección de sistemas, datos y redes frente a amenazas digitales.

Análisis de riesgos.

Consiste en identificar, evaluar y priorizar las amenazas y vulnerabilidades que pueden afectar los activos digitales de una organización, con el fin de implementar medidas preventivas y correctivas, con el fin de proteger la información y sistemas críticos.

6. Formulario de comunicación de incidentes

No se necesitan formularios especiales para informar sobre incidentes de seguridad de terceros.

Cuando un cliente detecta un evento o incidente de seguridad, podrá reportarlo al CSIRT E-DEA a través del correo **seguridad@e-dea.co**. En el intercambio de esta información se utilizarán las medidas de protección, mediante el uso de claves PGP. Estas medidas tendrán en cuenta tanto la clasificación de la información, como los acuerdos que se hayan establecido con cada cliente al inicio de la prestación del servicio.

7. Descarga de responsabilidades

Si bien se tomarán todas las precauciones necesarias en la preparación de la información, notificaciones y las alertas, el CSIRT E-DEA no asume ninguna responsabilidad por errores u omisiones, ni por los daños que resulten del uso de la información contenida en ellas.

Versión	Fecha	Descripción del cambio
00	27/03/2026	Creación del documento

Elaborador por:	Revisado por:	Aprobado por:
German Serrato	Maure Muñoz Luna	Juan Fernández
Chief Information Security Officer (CISO)	Security and Information Compliance Officer	Chief Technology Officer (CTO)