**CENTRO DE POSGRADOS**

**Tema:**

# IMPLEMENTACIÓN DE UN CSIRT PARA RESPUESTAS A INCIDENTES EN LA EMPRESA MIVILSOFT

**Proyecto de investigación previo a la obtención del título de Magíster en Ciberseguridad**

**Línea de investigación:**

SEGURIDAD DE LA INFORMACIÓN

**Autor:**

Jonathan Ricardo Garcés Salazar

**Director:**

Mg. Edgar Fernando Solís Acosta

**Ambato - Ecuador**

**Abril 2025**

## DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **JONATHAN RICARDO GARCÉS SALAZAR**, con cédula de ciudadanía **1804626057**, autor del trabajo de graduación intitulado: “IMPLEMENTACIÓN DE UN CSIRT PARA RESPUESTAS A INCIDENTES EN LA EMPRESA MIVILSOFT”, previa a la obtención del título profesional de **MAGÍSTER EN CIBERSEGURIDAD**, en el centro de **POSGRADOS.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, abril 2025

Firmado electrónicamente por:
**JONATHAN RICARDO GARCES SALAZAR**

Jonathan Ricardo Garcés Salazar

CC. 1804626057

**PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR**

**SEDE AMBATO**

**APROBACIÓN DEL TRIBUNAL DE GRADO**

**Tema:**

**IMPLEMENTACIÓN DE UN CSIRT PARA RESPUESTAS A INCIDENTES EN LA EMPRESA MIVILSOFT**

**Línea de investigación:**

SEGURIDAD DE LA INFORMACIÓN

**Autor:**

Jonathan Ricardo Garcés Salazar

Edgar Fernando Solís Acosta, Ing. Mg. f._____

Firmado electrónicamente por: EDGAR FERNANDO SOLIS ACOSTA Validar únicamente con FirmaEC

CC. 1803005071

**CALIFICADOR**

Darío Javier Robayo Jácome, Ing. Mg. f._____

Firmado electrónicamente por: DARIO JAVIER ROBAYO JACOME Validar únicamente con FirmaEC

**CALIFICADOR**

José Marcelo Balseca Manzano, Ing. Mg. f._____

Firmado electrónicamente por: JOSE MARCELO BALSECA MANZANO Validar únicamente con FirmaEC

**CALIFICADOR**

Dayamy Lima Rojas, Lic. Mg. f._____

DAYAMY LIMA ROJAS Firmado digitalmente por DAYAMY LIMA ROJAS Fecha: 2025.05.05 07:33:10 -05'00'

**DIRECTORA CENTRO DE POSGRADOS**

Diego Gonzalo Coca Chanalata, Dr. f._____

DIEGO GONZALO COCA CHANALATA Firmado digitalmente por DIEGO GONZALO COCA CHANALATA Fecha: 2025.05.05 08:17:52 -05'00'

**SECRETARIO GENERAL PUCESA**

**Ambato - Ecuador**

**Abril 2025**

## DEDICATORIA

Quiero dedicar mis más sinceros agradecimientos a Dios y a mi madre, quienes siempre han sido mi fuente de apoyo, fe y luz en cada etapa de este camino. Su amor incondicional y confianza en mí han sido el motor que me ha impulsado a seguir adelante, incluso en los momentos más desafiantes.

A mi familia, gracias por estar siempre a mi lado, por su amor constante, sus palabras de aliento y por creer en mí en cada paso que he dado. Su apoyo ha sido fundamental para mantener la motivación y la perseverancia durante todo este proceso de aprendizaje y superación.

Finalmente, quiero dedicar este trabajo a todos aquellos que, de una manera u otra, contribuyeron a que este logro sea posible. Sus enseñanzas, apoyo y palabras de aliento hicieron que cada paso en este recorrido tuviera un propósito y un significado especial.

## AGRADECIMIENTO

Quiero comenzar agradeciendo a Dios por brindarme la fortaleza, la sabiduría y la guía necesaria para llegar tan lejos. A mi madre, que siempre ha sido mi pilar fundamental, que me ama sin condiciones, que nunca deja de animarme y que ha iluminado mi camino en los momentos más oscuros de mi vida.

También quiero dar las gracias a mis hermanos, quienes siempre estuvieron ahí para escucharme y darme su respaldo cuando más los necesitaba.

Finalmente, agradezco a la esta Universidad por darme la oportunidad de crecer tanto académicamente como profesionalmente. Valoro enormemente la confianza que depositaron en mi trabajo y el ambiente de aprendizaje que me brindaron a lo largo de todo este proceso.

## RESUMEN

La empresa Mivilsoft se encuentra en una posición desafiante al no contar con un CSIRT (Equipo de Respuesta ante Incidentes de Seguridad Informática), lo que la expone a ciberamenazas que podrían afectar la disponibilidad, confidencialidad e integridad de sus activos tecnológicos. En este contexto, es fundamental salvaguardar estos activos frente a las crecientes amenazas del ciberespacio y prevenir posibles ataques cibernéticos. Ante esta situación, el presente trabajo tiene como objetivo implementar un CSIRT para la protección efectiva de sus activos tecnológicos y preservar la continuidad de sus operaciones empresariales.

La investigación se desarrolla bajo un enfoque cualitativo de investigación aplicada, de tipo exploratorio y no experimental, con un diseño de corte transversal. Como marco metodológico, se emplea el “NIST Cybersecurity Framework”, que permite evaluar y fortalecer las capacidades institucionales para la respuesta ante incidentes de seguridad informática, facilitando la identificación y priorización de actividades orientadas a la reducción efectiva de riesgos en ciberseguridad.

Como resultado de la implementación del CSIRT, Mivilsoft contará de una detección temprana de amenazas, una respuesta más ágil y la adopción de medidas de seguridad eficaces. Esto contribuirá a prevenir incidentes, reducir el impacto de posibles ataques y reforzar la confianza en los procesos internos y en la relación con sus clientes.

**Palabras clave:** csirt, ciberseguridad, nist csf, respuesta ante incidentes, gestión de riesgos, protección de activos tecnológicos.

## ABSTRACT

*Mivilsoft is in the challenging position due to the absence of a CSIRT (Computer Security Incident Response Team), which exposes it to cyber threats that could affect the availability, confidentiality and integrity of its technological assets. In this context, it is essential to safeguard these assets against the growing threats in cyberspace and to prevent possible cyber-attacks. Given this situation, the present work aims to implement a CSIRT for the effective protection of their technological assets and preserve the continuity of their business operations.*

*The research is developed under a qualitative approach of applied research, exploratory and non-experimental, with a cross-sectional design. As a methodological framework, the "NIST Cybersecurity Framework" is used, which allows to evaluate and strengthen institutional capabilities for the response to computer security incidents, facilitating the identification and prioritization of activities aimed at the effective reduction of cybersecurity risks.*

*As a result of the implementation of the CSIRT, Mivilsoft will have an early detection of threats, a more agile response and the adoption of effective security measures. This will help prevent incidents, reduce the impact of potential attacks and strengthen confidence in internal processes and customer relationships.*

***Keywords:*** *csirt, cybersecurity, nist csf, incident response, risk management, technology asset protection.*

## ÍNDICE GENERAL DE CONTENIDOS

## ÍNDICE DE ILUSTRACIONES

## ÍNDICE DE TABLAS

## INTRODUCCIÓN

La ciberseguridad es esencial para proteger los sistemas de información en red frente a accidentes y amenazas deliberadas, abordando una amplia gama de cuestiones técnicas, organizativas y de gobernanza. Con la creciente digitalización de las actividades gubernamentales, comerciales y cotidianas, la ciberseguridad adquiere relevancia. Sin embargo, muchas organizaciones que digitalizan sus actividades carecen de los recursos organizativos, tecnológicos y humanos necesarios para asegurar sus sistemas, lo cual es crucial para su éxito a largo plazo (Veale & Brown, 2020).

El aumento de la conectividad a internet ha mejorado el flujo de información y ha impulsado los negocios globales en muchas industrias, pero también las ha hecho más vulnerables a los ciberataques. A medida que los sistemas se vuelven más sofisticados, la lucha contra los ataques especialmente los procedentes de cibercriminales, resulta cada vez más difícil, debido a la gran diferencia de capacidades entre las grandes y pequeñas instituciones, estas últimas suelen contar con recursos más limitados. En la actualidad, las amenazas más importantes proceden de ciberdelincuentes organizados como empresas y agentes estatales con recursos avanzados (Nish et al., 2020).

Según (Tzavara & Vassiliadis, 2024), la ciberseguridad se define como un proceso continuo destinado a proteger, preservar, resistir y defender el uso del ciberespacio contra ataques cibernéticos. Este proceso implica la organización y consolidación de recursos, procesos y estructuras para salvaguardar los sistemas habilitados para el ciberespacio y garantizar la confidencialidad, integridad y disponibilidad de los datos. La norma ISO/IEC 27032:2012 define la ciberseguridad como la protección de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. El diccionario Merriam-Webster define la ciberseguridad como los procedimientos destinados a proteger los ordenadores y los sistemas informáticos contra accesos o ataques no autorizados (Taherdoost, 2022).

El aumento global de los ciberataques, exacerbado por la mayor dependencia de los dispositivos digitales por la pandemia de COVID-19, se debe en parte al uso generalizado de sistemas antiguos y a la falta de actualizaciones de parches. Unas defensas sólidas y una capacidad eficaz de respuesta a incidentes son cruciales a la luz de esta amenaza en expansión, lo que subraya el papel vital que desempeña el CSIRT en la prevención y respuesta rápida a estos incidentes (Mohd Kassim et al., 2023).

Los CSIRT pueden reducir en gran medida la creciente cantidad de incidentes cibernéticos en todo el mundo, que empeoran por fallas del sistema y la falta de concienciación de los usuarios sobre la seguridad cibernética. Esto se vuelve aún más crucial, en industrias vitales como las universidades y las instituciones educativas, que siempre están en riesgo porque ofrecen servicios vitales a sus estudiantes (Villegas-Ch. et al., 2021).

Estos equipos contribuyen activamente a salvaguardar infraestructuras vitales, además de brindar respuestas proactivas a eventos como ataques de *ransomware*.

Con el fin de aumentar la resiliencia de la ciberseguridad y promover la cooperación internacional en la lucha contra los ciberataques, el NIS de la Unión Europea (UE) y la Unión Internacional de Telecomunicaciones (UIT) han reconocido la importancia del CSIRT y han brindado su apoyo para su desarrollo a escala global (Mohd Kassim et al., 2022). En América Latina, aunque se han implementado los CSIRT, los resultados que se esperaban aún no se han logrado. Esto se debe principalmente a la falta de conciencia e importancia sobre este problema global, lo que termina ocasionando grandes pérdidas económicas (Villegas-Ch. et al., 2021).

Actualmente, Ecuador cuenta con trece CSIRT que colaboran estrechamente con EcuCERT para manejar eventos de seguridad a escala nacional. Además de crear procedimientos oficiales para la colaboración y la respuesta a incidentes, el Ministerio de Gobierno y la Policía Nacional tienen la intención de crear un CSIRT específicamente encargado de gestionar cuestiones de seguridad relacionadas con la seguridad pública y ciudadana. La epidemia de COVID-19 impulsó el uso del

teletrabajo, la teleeducación y la telemedicina debido a la falta de conciencia y regulación sobre ciberseguridad, exponiendo a la mayoría de organizaciones e individuos a mayores amenazas de seguridad. En este caso, el riesgo cibernético está en aumento debido a que la cultura en torno a la ciberseguridad aún no está consolidada ni reconocida como una prioridad. Además, hay pocos programas educativos y organismos de certificación extranjeros, que con frecuencia son costosos y poco conocidos, y la nación carece de una política nacional para fomentar la inversión en educación en ciberseguridad, lo cual, incrementan la vulnerabilidad frente a amenazas cibernéticas (Del Pozo Barrezueta, 2021).

El aumento continuo de las ciberamenazas, tanto a nivel nacional como internacional, enfatiza lo fundamental que es proporcionar soluciones de seguridad eficientes que puedan reaccionar rápidamente ante los incidentes a tiempo. Esto amenaza seriamente la integridad de los gobiernos, las corporaciones y las comunidades, así como la seguridad nacional. La necesidad de salvaguardar los datos contra pérdidas y robos, así como de prevenir violaciones de datos, se pone de relieve por el uso cada vez mayor de la tecnología de la información y las comunicaciones. Los CSIRT son poco comunes y muy nuevos en Ecuador. Las instituciones académicas, públicas y privadas están cada vez más interesadas en establecer sus propios equipos de respuesta para salvaguardar sus activos técnicos, incluso si se creó un CSIRT nacional en 2014 (Espín, 2021).

En este sentido, Mivilsoft se encuentra en una posición desafiante porque carece de un CSIRT, lo que la deja expuesto a cualquier ciberamenaza y ataque que pueda poner en riesgo la disponibilidad, confidencialidad e integridad de sus activos tecnológicos. El problema científico radica en la necesidad de implementar un CSIRT en la empresa Mivilsoft para la protección efectiva de sus activos tecnológicos y preservar la continuidad de sus operaciones empresariales.

Desde esta perspectiva, se argumenta que la implementación de un CSIRT en la empresa Mivilsoft, contribuirá a una protección efectiva de sus activos tecnológicos y asegurará la continuidad de sus operaciones empresariales.

El propósito de este proyecto consiste en implementar un CSIRT para respuestas a incidentes en la empresa Mivilsoft, para lo cual, las tareas de investigación a desarrollar son:

- Realizar un análisis de la situación actual de la empresa Mivilsoft, a través de una evaluación de los incidentes de la seguridad informática.
- Analizar la implementación de CSIRT ya establecidos a través de un análisis documental de casos exitosos, que sirva como referencia inicial.
- Elaborar un plan detallado para el CSIRT destinado a la empresa Mivilsoft utilizando la metodología de gestión de incidentes según el marco NIST CSF, tomando en cuenta las mejores prácticas que aseguren una gestión efectiva de los incidentes de seguridad informática.
- Determinar los protocolos del CSIRT en la empresa Mivilsoft siguiendo las directrices establecidas por la institución.

Este trabajo se enmarca en un enfoque cualitativo de investigación aplicada, de tipo exploratorio y no experimental, con un diseño de corte transversal; utilizando la metodología de gestión de incidentes según el marco NIST CSF, para evaluar las capacidades de respuesta a incidentes de seguridad, se ejecutan las siguientes acciones:

Los riesgos potenciales y los activos importantes se localizan durante la fase de identificar. La fase de proteger implica la implementación de medidas preventivas. El objetivo de la fase de detectar es identificar las incidencias lo antes posible. Ante las incidencias, la fase de responder actúa de forma inmediata. La fase de recuperar concluye con énfasis en la restauración del sistema y la implementación de mejoras para detener tales eventos en el futuro.

El avance tecnológico ha intensificado la amenaza de los ataques cibernéticos tanto a nivel local como global, que incluyen incidentes en escuelas, empresas y los sectores públicos y privados. Para salvaguardar la integridad de los datos y detener el robo, daño o la interrupción del servicio en este caso, se requiere una respuesta rápida y eficiente. La falta de un equipo de respuesta ante incidentes de seguridad

Informática (CSIRT) por parte de Mivilsoft la deja abierto a potenciales ataques que podrían poner en riesgo la disponibilidad, confidencialidad e integridad de sus activos tecnológicos. Por tanto, la organización no está protegida de estas amenazas.

Por ello, este estudio se centra en la necesidad de salvaguardar los activos tecnológicos de las crecientes amenazas del ciberespacio. Para prevenir ataques, esto implica tener una detección oportuna, respuestas rápidas y medidas de seguridad efectivas. Al hacer esto, la empresa podrá identificar, abordar y prevenir posibles actividades delictivas, mejorando su reputación y confianza tanto dentro como fuera de la empresa.

# CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

Este capítulo analiza varias tecnologías importantes en el contexto de la ciberseguridad moderna, cada una de las cuales tiene una función distinta en la protección de redes, sistemas y datos confidenciales. Son esenciales para proporcionar instrumentos específicos destinados a identificar, detener y disminuir las amenazas a la ciberseguridad.

## 1.1. Activos tecnológicos en la ciberseguridad

### Sistemas de detección y prevención de intrusiones (IDS/IPS)

Los sistemas de seguridad están hechos para reconocer, detectar y reaccionar ante ataques malintencionados que pretenden poner en peligro la integridad de los sistemas informáticos, las redes o los sistemas de información en general. El software o hardware que automatiza la detección de intrusiones, vigila el tráfico de la red en busca de actividad inusual y notifica al administrador, este se conoce como Sistema de Detección de Intrusiones (IDS). Un sistema de prevención de intrusiones (IPS), por su parte, es una pieza de hardware o software que impide a los hackers acceder a una red , y mucho menos que la ataque (Azeez et al., 2020).

Estos sistemas son medidas de seguridad a nivel de red utilizadas globalmente. La principal diferencia entre IDS e IPS radica en la forma en que protegen el entorno de red en términos de detección y prevención. El IDS genera alertas cuando se produce un ataque malicioso y lo notifica al administrador de la red. Además, los administradores de red también tienen la opción de desactivar las funciones preventivas del IPS para que funcione como un IDS. En general, los papeles o funciones de IPS e IDS en la seguridad de la red son equivalentes (Thapa & Mailewa, 2020). En la Tabla 1 muestran las principales funciones de un IDS/IPS.

**Tabla 1.** Principales funciones de un IDS/IPS

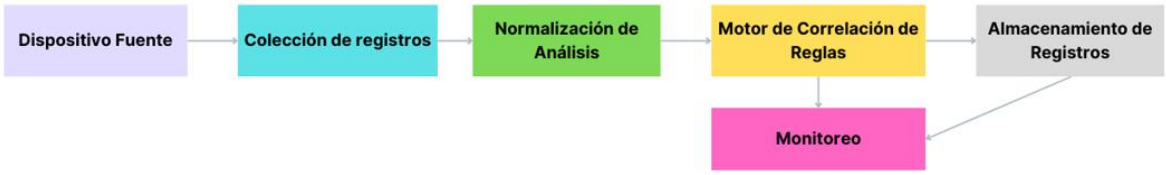
| Función | Descripción |
|---|---|
| **Recopilación de datos** | Recibe y guarda datos de entrada para su análisis. Los IDS basados en red capturan paquetes de datos, mientras que los IDS basados en host monitorizan el uso del disco y los procesos del sistema. |
| **Selección de características** | Selecciona características clave de los datos para la detección de intrusiones, como direcciones IP, tipo de protocolo, longitud y tamaño del encabezado. |
| **Análisis** | Analiza los datos utilizando métodos basados en reglas o anomalías para detectar actividades sospechosas o intrusiones. |
| **Acción** | Responde a las intrusiones notificando al administrador del sistema mediante alarmas o correos electrónicos, o tomando medidas activas como el bloqueo de paquetes o puertos. |

Fuente: modificado a partir de (Thapa & Mailewa, 2020)

## Gestión de información y eventos de seguridad (SIEM)

Según (González-Granadillo et al., 2021) el sistema de gestión de información y eventos de seguridad (SIEM), es una plataforma que ayuda a los administradores a diseñar políticas de seguridad y gestionar eventos provenientes de diversas fuentes. Los SIEM proporcionan análisis en tiempo real de eventos de seguridad generados por dispositivos de red y aplicaciones. Aunque la nueva generación de SIEMs ofrece capacidades de respuesta automatizada para seleccionar y desplegar contramedidas, los sistemas de respuesta actuales a menudo implementan medidas de seguridad sin realizar un análisis exhaustivo del impacto de los ataques y los escenarios de respuesta. Los elementos básicos de la solución SIEM estándar se presenta en la Ilustración 1.

**Ilustración 1.** Componentes básicos SIEM




Fuente: modificado a partir de (González-Granadillo et al., 2021)

## Gestión de identidad y acceso (IAM)

El concepto de Gestión de Identidad y Acceso (IAM) engloba tanto la gestión de identidades como la gestión de accesos e incluye tanto la administración de identidades como los procesos de autenticación y autorización en las organizaciones. Las identidades pueden ser reclamadas tanto por actores humanos como no humanos. En un contexto empresarial, los actores humanos incluyen empleados, proveedores, socios y clientes, mientras que los actores no humanos incluyen organizaciones, máquinas y aplicaciones de software (Glöckler et al., 2023).

Debido a que cubre elementos esenciales como la gestión de usuarios, la autenticación y la autorización de acceso, la IAM es esencial para garantizar la seguridad y el cumplimiento de las regulaciones en las organizaciones. Por ello, facilita la modificación de soluciones convencionales y es esencial para la gestión eficiente de la conectividad en las redes de información modernas. Además, mejora la autenticación de los usuarios al integrarse con tecnologías de inteligencia artificial (IA), lo que garantiza un alto nivel de confiabilidad y seguridad en los sistemas (Singh et al., 2023).

## Firewalls

Un firewall, según (Ahmed & HamaAmin, 2022), es un dispositivo de red que utiliza reglas para representar y mantener las políticas de seguridad de una organización, filtrando paquetes de datos entrantes y salientes. De igual manera, examina cada paquete que pasa por la red y decide si aceptarlo o rechazarlo. Por su parte, los firewalls basados en host, que regulan el tráfico entre los dispositivos finales y la red, y los firewalls basados en red, que protegen las conexiones entre redes y dispositivos, son los dos tipos principales de estos dispositivos, resultando fundamentales para la seguridad de cualquier organización. En la Tabla 2 se muestran los tipos de Firewall que operan en diferentes capas del modelo TCP/IP.

**Tabla 2.** Tipos de Firewall

| Tipo de Firewall | Concepto |
|---|---|
| **Filtrado de paquetes** | Filtra paquetes según reglas preestablecidas, como IP de origen/destino y número de puerto. |
| **Puerta de enlace a nivel de circuito** | Utiliza el protocolo TCP *handshake* para permitir o denegar tráfico. |
| **Inspección de paquetes con estado** | Combina filtrado de paquetes y TCP *handshake;* usa una tabla de sesiones para mantener el estado de las conexiones. |
| **Firewall proxy** | Filtra el tráfico en el borde de la red al nivel de la capa de aplicación; inspecciona el contenido de los paquetes. |
| **Firewall de próxima generación** | Combina múltiples capas de protección como IPS, Antivirus y filtrado de URL con firewalls tradicionales. |
| **Firewall en la nube** | Protege centros de datos en la nube usando asignación dinámica de recursos y detección de eventos; ideal para entornos SDN. |

Fuente: modificado a partir de (Ahmed & HamaAmin, 2022)

## 1.2. CSIRT en la seguridad informática

### ¿Qué es un CSIRT?

Un Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT) es un equipo especializado en la prevención, identificación, gestión y respuesta eficaz ante incidentes de seguridad informática dentro de una organización o grupo de usuarios. Estos equipos siguen procedimientos rigurosos alineados frecuentemente con las fases de respuesta a incidentes delineadas por el Instituto Nacional de Estándares y Tecnología (NIST), que comprenden la preparación, identificación, contención, erradicación y recuperación de incidentes (Hauptman et al., 2023).

El CSIRT no solo maneja incidentes de seguridad, sino que también puede incluir responsabilidades adicionales como la gestión de vulnerabilidades, monitoreo de seguridad, concienciación situacional y transferencia de conocimientos en ciberseguridad. Su rol ha evolucionado para coordinar y comunicar con diferentes partes interesadas, países y sectores específicos (ENISA, 2020).

Actualmente, existen diversos términos o abreviaturas para describir a un equipo de respuesta a incidentes, como se muestra en la Tabla 3.

**Tabla 3.** Abreviaturas y términos de equipos de respuesta a incidentes

| Siglas | Significado |
|---|---|
| **CSIRT** | Equipo de Respuesta a Incidentes de Seguridad Informática |
| **CIRT** | Equipo de Respuesta a Incidentes Informáticos |
| **CIRC** | Centro (o Capacidad) de Respuesta a Incidentes Informáticos |
| **CSIRC** | Centro (o Capacidad) de Respuesta a Incidentes de Seguridad Informática |
| **SOC** | Centro de Operaciones de Seguridad |
| **CSOC** | Centro de Operaciones de Ciberseguridad |
| **CERT** | Equipo de Respuesta a Emergencias Informáticas |

Fuente: modificado a partir de (Knerler et al., 2022)

Existen variaciones comunes en los nombres de estos equipos de ciberseguridad, que pueden incluir términos como "red", "computadora", "seguridad", "ciber", "emergencia", "incidente", "operaciones" o "empresa". No hay un término universalmente aceptado para estos especialistas en ciberseguridad, la preferencia por los términos ha cambiado con el tiempo, puede variar según el país y a menudo está relacionada con el alcance de la misión del equipo (Knerler et al., 2022).

## Ventajas de un CSIRT

Los CSIRTs están encargados de prevenir, gestionar y responder a problemas de ciberseguridad, ofreciendo servicios especializados a sectores como la comunidad académica, bancario, comercial, gubernamental, militar, energético, financiero y organizaciones internas. La presencia de un equipo especializado en seguridad de TI permite a las organizaciones reducir y prevenir incidentes críticos, asegurando la protección de sus activos (Saraiva & Mateus-Coelho, 2022). En la Tabla 4 presenta las principales ventajas de contar con un CSIRT.

**Tabla 4.** Ventajas de un CSIRT

| Ventaja | Descripción |
|---|---|
| **Diversidad de Audiencias y Sectores** | Sirve a una amplia gama de sectores como academia, bancos, comercio, gobierno, militar, energético y financiero. |
| **Funciones Clave** | Prevención, gestión y respuesta a problemas de ciberseguridad, además de proporcionar servicios especializados a su jurisdicción. |
| **Principios Fundamentales** | Mantenimiento de recursos actualizados, generación de confianza con empresas y usuarios, reacción rápida ante amenazas y colaboración efectiva con partes interesadas nacionales y otros CSIRTs/CERTs. |

Fuente: modificado a partir de (Saraiva & Mateus-Coelho, 2022)

## Tipos de CSIRT

Actualmente, los roles y responsabilidades de los CSIRT varían significativamente según su financiamiento y experiencia. Es crucial que cada CSIRT tenga una comunidad objetivo claramente definida. Esto implica comunicar cualquier superposición con otros equipos para que los miembros de la comunidad objetivo comprendan qué servicios deben solicitar a cada equipo. Este enfoque ayuda al CSIRT a identificar las necesidades específicas de la comunidad, determinar qué activos proteger y establecer cómo será la interacción con ellos. Instituciones como ENISA han categorizado a los CSIRTs en diversos tipos según los servicios que ofrecen o los sectores a los que están orientados (Van der Heide, 2020).

### a) CSIRT nacionales

Actúan como el principal punto de contacto a nivel nacional para las partes involucradas en la respuesta a incidentes dentro del país, así como para otros CSIRTs nacionales en todo el mundo.

### b) CSIRT sectoriales

Están dedicados a sectores específicos de la sociedad o la economía, como el sector bancario o educativo.

### c) CSIRT organizacionales

Su función principal es vigilar y responder a incidentes que ocurran en las redes internas de la organización a la que pertenecen. Estos equipos están presentes tanto en empresas privadas como en organizaciones gubernamentales e instituciones académicas.

En el contexto de esta investigación, se utilizará este modelo como base para la implementación y evaluación de estrategias de respuesta a incidentes de seguridad dentro de la empresa Mivilsoft.

**d) CSIRT de proveedores**

Estos son grupos dentro de empresas tecnológicas que crean productos como sistemas operativos comerciales que son utilizados tanto por individuos como por empresas. Su objetivo principal es ayudar a sus usuarios y clientes ofreciéndoles soporte operativo y servicio al cliente.

**e) CSIRT comerciales**

Ofrecen servicios de gestión de incidentes a otras organizaciones. Los equipos comerciales venden servicios de respuesta a incidentes, mientras que los equipos sin fines de lucro cuentan con honorarios, donaciones y alianzas con empresas.

**f) CSIRT regionales**

Ayudan en la colaboración entre los CSIRT nacionales y promueven el intercambio de información a nivel regional.

**Servicios de un CSIRT**

Un equipo CSIRT ofrece diversos servicios categorizados como "reactivos", "proactivos" y "de gestión de calidad de seguridad". Es fundamental que un CSIRT incluya el servicio de gestión de incidentes para cumplir con los estándares reconocidos. Este servicio, parte de los "servicios reactivos", permite al CSIRT ofrecer una perspectiva diferente a la de los departamentos tradicionales que gestionan funciones similares (Kalonji, 2022).

Es crucial que estos servicios sean realistas y se adapten a los recursos financieros, laborales y técnicos disponibles en cada país. Además de servir como el principal punto de contacto para reportar incidentes de seguridad cibernética y estar fácilmente disponibles para sus usuarios, un CSIRT debe cumplir tres roles esenciales (Saraiva & Mateus-Coelho, 2022):

- Estar estratégicamente ubicados geográficamente para maximizar sus recursos.
- Participar activamente en la educación sobre seguridad informática.
- Desempeñar un papel crucial en la respuesta a incidentes de seguridad informática.

En la Tabla 5 se presenta una lista analítica de los servicios proporcionados de los CSIRT.

**Tabla 5.** Servicios proporcionados por los CSIRT

| **Servicios Reactivos** | **Servicios Proactivos** | **Manejo de Artefactos** | **Gestión de la Calidad de Seguridad** |
|---|---|---|---|
| Manejo de vulnerabilidades | Investigación Tecnológica | Análisis de artefactos | Análisis de riesgo |
| Análisis de vulnerabilidad | Auditorías de seguridad | Respuesta de artefacto | Continuidad del negocio |
| Respuesta a la vulnerabilidad | Mantenimiento de la seguridad | Coordinación de artefactos | Recuperación de desastres |
| Soporte de respuesta a incidentes | Desarrollo de Herramientas de Seguridad | | Educación |
| Análisis de incidentes Alarmista | Difusión de la concienciación sobre la seguridad | | |

Fuente: modificado a partir de (Saraiva & Mateus-Coelho, 2022)

## Plan de procesos de un CSIRT

Para implementar y apoyar los servicios acordados de un CSIRT, es necesario establecer procesos específicos. Cada tipo de entrega de servicios se implementa generalmente utilizando al menos un proceso. En algunos casos, puede ser necesario más de un proceso para proporcionar un servicio, especialmente si la provisión del servicio requiere la participación de varios grupos de trabajo o el logro de objetivos intermedios específicos (ENISA, 2020).

Cada proceso incluye uno o más flujos de trabajo, representados por diagramas de flujo que detallan cada paso desde el inicio hasta la fase final de la actividad.

La Ilustración 2 presenta un diagrama de flujo de trabajo para el manejo de incidentes de seguridad.

**Ilustración 2.** Ejemplo de flujo de trabajo de manejo de incidentes


Fuente: tomado a partir de (ENISA, 2020)

## 1.3. Casos de éxito de la implementación de un CSIRT

### Implementación del CSIRT.CZ en República Checa

El equipo CSIRT.CZ fue creado bajo una subvención dirigida a abordar las amenazas cibernéticas y los intereses de seguridad de la República Checa, con el propósito de establecer una práctica modelo de CSIRT y evaluar la capacidad de los proveedores de red y servicios para gestionar incidentes de seguridad. La tarea fue asignada a la asociación CESNET, responsable de formar el primer equipo oficial CSIRT del país. En 2007, CSIRT.CZ fue reconocido por la comunidad global. En 2010, un memorando con el Ministerio del Interior estableció a CSIRT.CZ como el CSIRT Nacional de la República Checa, y en 2012, un nuevo acuerdo con la Autoridad de Seguridad Nacional ajustó la gestión del equipo (CSIRT.CZ, 2024a). Los objetivos principales de CSIRT.CZ son (CSIRT.CZ, 2024a):

- Mantener relaciones internacionales con la comunidad global de equipos CERT/CSIRT y organizaciones de apoyo.

- Cooperar con diversas entidades en la República Checa, incluyendo ISPs, proveedores de contenido, bancos, organismos de seguridad, instituciones académicas y autoridades públicas.
- Proporcionar servicios de seguridad como la gestión y coordinación de incidentes de seguridad, ofrecer educación y tutoría, y brindar servicios proactivos en el área de seguridad.

La Ilustración 3 muestra las estadísticas de los incidentes gestionados por el CSIRT.CZ de los últimos 4 años.

**Ilustración 3.** Incidentes informáticos gestionados por CSIRT.CZ

| | 2020 | 2021 | 2022 | 2023 | 2024 | Total |
|---|---|---|---|---|---|---|
| **Sensor Network*** | 16217 | 10284 | 8815 | 8903 | 5720 | 49939 |
| **Phishing** | 738 | 1297 | 1485 | 2064 | 754 | 6338 |
| **Spam** | 216 | 163 | 220 | 352 | 137 | 1088 |
| **Malware** | 111 | 153 | 228 | 163 | 44 | 699 |
| **Information gathering** | 97 | 74 | 71 | 105 | 50 | 397 |
| **Other** | 86 | 26 | 24 | 35 | 28 | 199 |
| **Intrusions** | 3 | 1 | 39 | 21 | 38 | 102 |
| **DOS** | 16 | 11 | | 12 | 1 | 40 |
| **Total** | 1267 | 1725 | 2067 | 2752 | 1052 | 8863 |

Fuente: tomado a partir de (CSIRT.CZ, 2024b)

### Implementación del CERT.br en Brazil

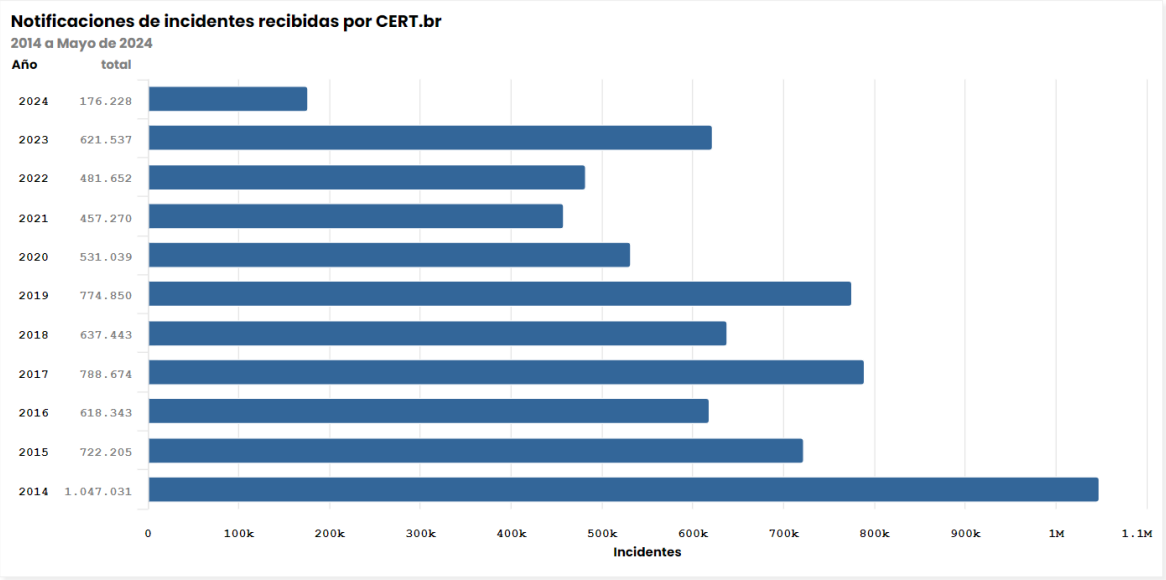
El CERT.br, creado en 1997 por el Comité Gestor de Internet en Brasil (CGI.br), sigue recomendaciones para mejorar la seguridad de las redes en Brasil. Documentado como un ejemplo de buenas prácticas en el guía "*Getting started with a National CSIRT*", el CERT.br contribuye a establecer directrices estratégicas y estándares técnicos para la seguridad de Internet, representando a Brasil en foros internacionales. Además, ofrece servicios gratuitos de seguridad a redes que

utilizan recursos administrados por NIC.br, financiados por el registro de dominios bajo el ccTLD .br (CERT.br, 2024a).

Su función inicial era actuar como una organización neutral, siendo el punto focal para los incidentes de seguridad en Brasil y facilitando el intercambio de información y la gestión de incidentes. En la actualidad, su labor se centra en atender los requisitos de seguridad y emergencias en Internet brasileña, colaborando estrechamente con entidades y organismos responsables (CERT.br, 2024a).

La Ilustración 4 muestra las estadísticas de los incidentes gestionados por el CERT.br a lo largo de los últimos 10 años.

**Ilustración 4.** Incidentes informáticos gestionados por el CERT.br




Fuente: tomado a partir de (CERT.br, 2024b)

## Implementación del EcuCERT en Ecuador

El EcuCERT, establecido en julio de 2014 por la resolución ST-2014-0247, es el Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones, cuya finalidad es *"Brindar a su Comunidad Objetivo el apoyo en la prevención y resolución de incidentes de seguridad*

*informática, a través de la coordinación, capacitación y soporte técnico."* (EcuCERT, 2024).

Desde su creación en julio de 2014, EcuCERT es reconocido como un CIRT nacional oficial y miembro certificado de FIRST. Su comunidad objetivo incluye el sector de telecomunicaciones y las instituciones públicas y privadas que requieran sus servicios. Las funciones del EcuCERT están reguladas por la Ley Orgánica de Telecomunicaciones. En 2018, ARCOTEL emitió una norma técnica para gestionar incidentes y vulnerabilidades, que establece un catálogo de vulnerabilidades, tiempos de respuesta y protocolos de seguridad para los proveedores de servicios de telecomunicaciones (Del Pozo Barrezueta, 2021).

Según (EcuCERT, 2024), los servicios que ofrecen son:

- Reactivos:
    - Catálogo de incidentes y vulnerabilidades.
    - Coordinación de la respuesta de Gestión de incidentes.
    - Coordinación de la respuesta de Gestión de vulnerabilidades.
    - Alertas y advertencias.
- Proactivos:
    - Comunicados.
    - Estadísticas.
    - Evaluaciones de auditorías de seguridad ejecutadas a los PST.
- De valor agregado
    - Guías y consejos.
    - Charlas de sensibilización.

En la Ilustración 5, se observan las estadísticas de los diferentes tipos de incidentes gestionados por el EcuCERT, notificadas durante el año 2023.

**Ilustración 5.** Número de IPs notificadas durante el año 2023


Fuente: tomado a partir de (EcuCERT, 2024)

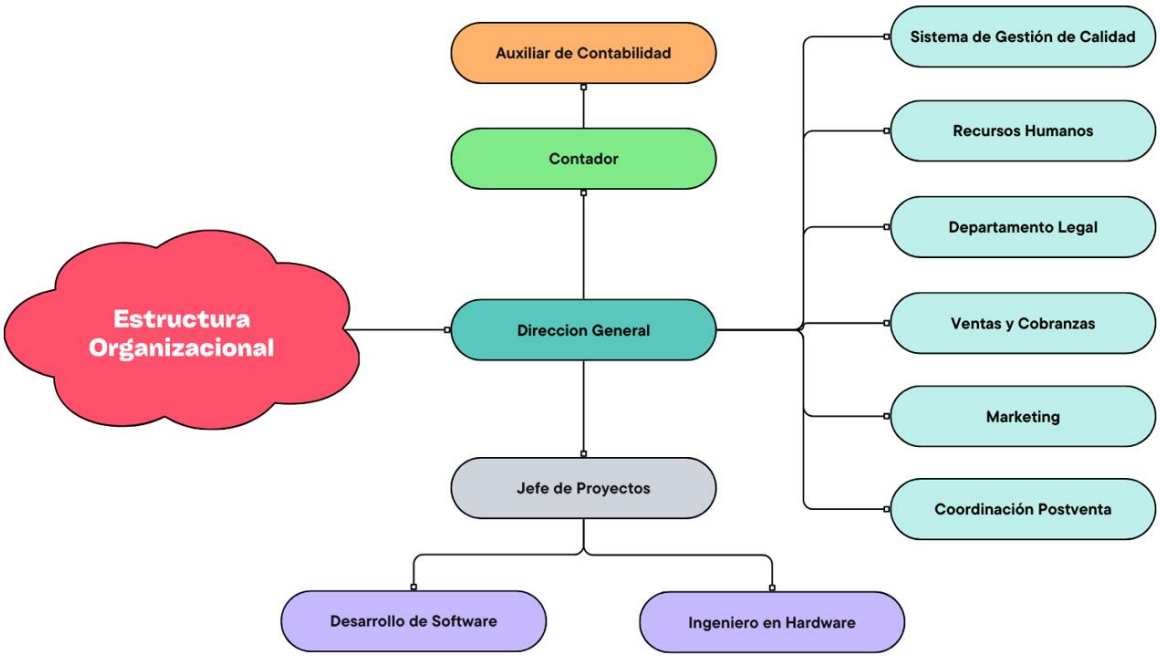
# CAPÍTULO II. DISEÑO METODOLÓGICO

## 2.1. Caracterización de la institución

Mivilsoft se ha convertido en uno de los principales proveedores de soluciones de software avanzadas en Ecuador desde su establecimiento en el año 2018. La empresa ofrece soluciones y servicios técnicos a la industria del transporte, como sistemas de gestión de flotas, videovigilancia, consultoría de desarrollo de software y productos que incluyen unidades GPS y *routers* de conectividad.

Como se muestra en la Ilustración 6, la estructura organizacional de la empresa busca reforzar la colaboración y la eficacia entre los diferentes grupos funcionales. La creación y el mantenimiento de sistemas y aplicaciones que faciliten las operaciones y servicios de la empresa es responsabilidad exclusiva del departamento de desarrollo de software.

**Ilustración 6.** Estructura Organizacional de Mivilsoft




Fuente: elaboración propia

Para proteger los sistemas y datos vitales de la empresa, se implementará un CSIRT en el departamento de Software de Mivilsoft. Esto ayudará a detectar y

eliminar posibles riesgos de seguridad de la información asociados a los activos tecnológicos de la organización.

## 2.2. Metodología de investigación

Este trabajo se enmarca en un enfoque cualitativo de investigación aplicada, de tipo exploratorio y no experimental, con un diseño de corte transversal.

Según (Torres-Chavez, 2021), el método cualitativo es una metodología exhaustiva, participativa e inductiva que tiene como objetivo generar teorías al comprender el significado de las acciones, eventos y circunstancias de los participantes. Su enfoque principal está en el análisis e interpretación del contexto, que incluyen ideas, variables, conexiones, símbolos, teorías y creencias de personas o grupos.

Según (Idammi, 2022), la investigación aplicada es una investigación científica dirigida a abordar problemas prácticos urgentes que enfrenta una sociedad o una organización.

Según (Halim et al., 2023), la investigación exploratoria evalúa la viabilidad de una estrategia utilizando la literatura y la evidencia actualmente accesible. Revisiones de literatura, conversaciones informales, observaciones metódicas, pruebas experimentales y estudios de casos son algunos de los métodos que emplea. Su objetivo es adquirir un conocimiento profundo del tema para resolver problemas de investigación y orientar estudios posteriores.

Según (Sidharth, 2023), los estudios no experimentales utilizan métodos observacionales y frecuentemente incluyen subdiseños como pre y postest de un solo grupo, series temporales interrumpidas y diseños correlacionales, tanto longitudinales como transversales. El investigador tiene una capacidad limitada para controlar factores externos, por lo que es fundamental manejarlos con precaución para minimizar posibles sesgos en el estudio.

Según (Zuleika & Siswo, 2022), afirma que un estudio transversal es un tipo de investigación observacional donde se miden variables en un punto concreto en el tiempo. Cada sujeto recibe una única observación y las mediciones se realizan sin más seguimiento. Se pueden recopilar datos confiables utilizando este método, lo que facilita sacar conclusiones y probar la premisa del estudio.

Los procedimientos fundamentales se conocen como técnicas de recopilación de datos y ayudan a los investigadores a obtener la información que necesitan para responder sus preguntas de investigación. Para investigaciones mixtas, cuantitativas o cualitativas, se pueden utilizar herramientas como encuestas, entrevistas, análisis de contenido y observaciones sistemáticas. Para garantizar la autenticidad de los resultados generados, estas herramientas deben ser imparciales, válidas y confiables (Mendoza & Avila, 2020).

Se utilizan diversas herramientas que maximizan la gestión y recolección de información que ayudan al desarrollo del presente proyecto. Entre ellas se encuentran plantillas de Excel para definir el estado actual y deseado de la implementación del CSIRT, entrevistas estructuradas y semiestructuradas para recopilar datos cualitativos, Zotero para gestionar las referencias bibliográficas. Los datos también se analizan mediante Power BI, lo que permite visualizar de forma eficaz el proceso de implementación del CSIRT.

### 2.3. Metodología de desarrollo

El presente proyecto propone la implementación de un CSIRT en la empresa Mivilsoft para la protección efectiva de sus activos tecnológicos. Para lograr esto, se utilizará la metodología de gestión de incidentes basado en el marco de trabajo NIST CSF, para evaluar y mejorar la capacidad de responder a incidentes cibernéticos.

Según (Frayssinet Delgado et al., 2021), la metodología de gestión de incidentes del marco de trabajo NIST CSF ofrece un vocabulario consistente para comprender, gestionar y comunicar los riesgos de ciberseguridad a las partes interesadas

internas y externas. Este marco se puede aplicar a toda la organización o concentrarse en la prestación de servicios esenciales dentro de un área particular de la misma, y facilita la identificación y priorización de actividades para reducir los riesgos de ciberseguridad.

Según (Perwej et al., 2021), el marco de ciberseguridad NIST es una conjunto de directrices y mejores prácticas destinadas a ayudar a las empresas a gestionar y reducir los riesgos de ciberseguridad. Al utilizar una metodología estructurada de cinco fases que cubre la identificación, protección, detección, respuesta y recuperación, se busca fortalecer la seguridad de las infraestructuras y sistemas de información vitales ante las amenazas cibernéticas.

Las cinco funciones centrales, concurrentes y continuas que se muestran en la Tabla 6, proporcionan una visión estratégica de alto nivel del ciclo de vida de una organización, lo que a su vez facilita la toma de decisiones en la gestión de riesgos.

**Tabla 6.** Categorías de metodología del marco NIST

| Identificador de Función | Función | Identificador de Categoría | Categoría |
|---|---|---|---|
| **ID** | Identificar | ID.AM | Gestión de Activos |
| | | ID.BE | Entorno Empresarial |
| | | ID.GV | Gobernanza |
| | | ID.RA | Evaluación de Riesgos |
| | | ID.RM | Estrategia de Gestión de Riesgos |
| | | ID.SC | Gestión de Riesgos de la Cadena de Suministro |
| **PR** | Proteger | PR.AC | Gestión de Identidad y Control de Acceso |
| | | PR.AT | Conciencia y Capacitación |
| | | PR.DS | Seguridad de los Datos |
| | | PR.IP | Procesos y Procedimientos de Protección de la Información |
| | | PR.MA | Mantenimiento |
| | | PR.PT | Tecnología Protectora |
| **DE** | Detectar | DE.AE | Anomalías y Eventos |
| | | DE.CM | Monitoreo Continuo de la Seguridad |
| | | DE.DP | Procesos de Detección |
| **RS** | Responder | RS.RP | Planificación de Respuesta |
| | | RS.CO | Comunicaciones |
| | | RS.AN | Análisis |
| | | RS.MI | Mitigación |
| | | RS.IM | Mejoras |
| **RC** | Recuperar | RC.RP | Planificación de Recuperación |
| | | RC.IM | Mejoras |
| | | RC.CO | Comunicaciones |

Fuente: tomado a partir de (Frayssinet Delgado et al., 2021)

## Identificar

Esta etapa se enfoca en identificar procesos y recursos críticos importantes, documentar los flujos de información, mantener un inventario de hardware y software, crear políticas de ciberseguridad con roles y responsabilidades claramente definidos e identificar riesgos, vulnerabilidades y amenazas que impactan los activos de la organización (NIST, 2023).

### Gestión de activos (ID.AM)

La Tabla 7 presenta los activos de la organización que protegerá el CSIRT, siguiendo la norma ISO 27001. A continuación, se listan dichos activos:

- **Código:** Código único del activo asignado por la institución.
- **Nombre:** Nombre específico del activo.
- **Descripción:** Breve descripción del activo para identificar su función principal.
- **Tipo de activo:** Categoría del activo que posee la organización.
- **Tipo de ubicación:** Ubicación física o lógica de un activo.
- **Valoración (C, I, D):** El nivel de importancia del activo se evalúa en función de su confidencialidad, integridad y disponibilidad (alto, medio, bajo).
- **Nivel de confidencialidad:** Nivel de sensibilidad de la información del activo.

**Tabla 7.** Inventario de activos críticos de Mivilsoft

| Código | Nombre | Descripción | Tipo de activo | Tipo de ubicación | Valoración (C, I, D) | Nivel de tasación |
|---|---|---|---|---|---|---|
| **S-009** | Django Server | Servidor web para sistema SIU | Software | Lógica | 2 | Medio |
| **S-010** | Kibana Server | Servidor para la gestión de incidentes informáticos | Software | Lógica | 3 | Alto |
| **S-015** | OdooUI | Servidor web para sistema SAE | Software | Lógica | 3 | Alto |
| **S-016** | OdooDB | Servidor de base de datos para sistema SAE | Software | Lógica | 3 | Alto |
| **S-017** | TraccarDB | Servidor de base de datos para sistema GPS | Software | Lógica | 3 | Alto |
| **S-018** | TraccarUI | Servidor web para sistema GPS | Software | Lógica | 3 | Alto |
| **S-022** | Miral Odoo 13 | Servidor web de la empresa Miral | Software | Lógica | 3 | Alto |

Fuente: elaboración propia

## Entorno empresarial (ID.BE)

Para garantizar el cumplimiento de la norma ISO 27001, se han establecido los roles y responsabilidades para la toma de decisiones de seguridad en función de la misión, los objetivos y los procedimientos de la organización.

Se seleccionó el modelo organizacional CSIRT, Mivilsoft es una pequeña empresa. Los servicios básicos del CSIRT, como la distribución de avisos de seguridad y la coordinación de incidentes, serán manejados por tres empleados durante el horario de oficina.

El departamento de desarrollo de software ha acordado proporcionar apoyo al CSIRT cuando sea necesario, cuenta con un personal altamente capacitado. Cuatro profesionales en el área a tiempo completo formarán el núcleo principal del CSIRT.

Se han definido roles específicos utilizando este estándar como referencia, tal como se muestra en la Tabla 8.

**Tabla 8.** Roles y responsabilidades del CSIRT en Mivilsoft

| Rol | Responsabilidades |
|---|---|
| **Jefe de proyectos (Coordinador del CSIRT)** | Liderar y gestionar todas las actividades del CSIRT para garantizar la protección de los activos y la continuidad de las operaciones. |
| **Desarrollador de Software (Gestor de incidentes)** | Implementar prácticas de codificación segura. Manejar y supervisar los incidentes de seguridad. |
| **DevOps (Gestor de Infraestructuras Digitales)** | Responsable de la seguridad de los servidores en la nube, incluyendo la definición de las reglas de seguridad a nivel del sistema operativo y las aplicaciones. |
| **Project Manager (Oficial de Seguridad y Confianza Digital)** | Asegurar que los proyectos de desarrollo de software cumplan con las políticas y procedimientos de seguridad. |

Fuente: elaboración propia

El CSIRT de Mivilsoft proporcionará información y asistencia para proteger los activos críticos de la empresa, reduciendo el riesgo de incidentes de seguridad informática y respondiendo de manera eficaz cuando ocurran. En la Ilustración 7 se muestran los servicios básicos que ofrecerá el CSIRT.

**Ilustración 7.** Servicios ofertados por el CSIRT de Mivilsoft


Fuente: elaboración propia

**Gobernanza (ID.GV)**

Para gestionar eficazmente los requisitos regulatorios y garantizar la seguridad de la información, se establecen políticas y procesos. Tras revisar las políticas actuales de la organización, se determina que se debe fortalecer el cumplimiento y especificar las políticas fundamentales más relevantes, tales como:

- Definir y aplicar políticas integrales para la seguridad cibernética en toda la organización para definir las responsabilidades y expectativas de CSRIT en la protección de activos, cumpliendo con las regulaciones de la norma ISO 27001.
- Establecer los roles y responsabilidades del equipo de seguridad cibernética utilizando las mejores prácticas de gobernanza. Esto comprende la participación activa de la alta dirección en el seguimiento y apoyo continuo del CSIRT, así como el nombramiento de un coordinador del CSIRT con el poder y los recursos necesarios para encabezar las medidas de seguridad.
- Disponer de un marco de gobernanza para garantizar una supervisión eficiente de las operaciones de ciberseguridad, que incluye la realización de auditorías para verificar la eficacia y el cumplimiento de las medidas de seguridad del CSIRT, así como evaluaciones frecuentes de políticas y procedimientos.

**Evaluación de riesgos (ID.RA)**

El marco de trabajo NIST establece que la gestión de riesgos debe incluir todos los activos y actividades de una organización, incluida su reputación e imagen. Esta gobernanza brindará especial consideración a los activos críticos de la organización. Se llevará a cabo una política de gestión de riesgos con énfasis en seguridad de la información basada en normativas, procedimientos y evidencias. Este plan incluirá identificación de amenazas, retroalimentación de vulnerabilidades y priorización de respuestas utilizando controles apropiados de acuerdo con la norma ISO 27001.

## Estrategia de gestión de riesgos (ID.RM)

Se definen las prioridades y restricciones necesarias para gestionar de manera efectiva los riesgos operacionales de la organización. Estos riesgos se determinan en función de los activos identificados en la Tabla 7 y se clasifican según su nivel de importancia, como se detalla en la Tabla 9.

**Tabla 9.** Valoración de la probabilidad

| Valoración | Estimación de la amenaza | Estimación de la vulnerabilidad |
|---|---|---|
| **Alto (3)** | La ocurrencia es muy probable (probabilidad > 50%). | No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza. |
| **Medio (2)** | La ocurrencia es probable (probabilidad = 50%). | Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable. |
| **Bajo (1)** | La ocurrencia es menos probable (probabilidad > 0 y < 50%). | La medida de seguridad es adecuada. |

Fuente: elaboración propia

El CSIRT debe implementar un plan de mitigación para reducir el impacto de posibles ataques, ante los recursos tecnológicos de la empresa. Las prioridades de gestión de riesgos son:

- **Proteger datos confidenciales y sensibles:** Determinar y priorizar la protección de los datos confidenciales y sensibles que se encuentran dentro de los activos tecnológicos, asegurándose de que cualquier efecto negativo sobre estos datos se mantenga al mínimo.
- **Proteger el software contra ataques:** Implementar medidas de seguridad para mantener la seguridad y la integridad de los datos críticos en un entorno de nube.
- **Reducir la interrupción de los recursos informáticos:** Aunque mantener los sistemas tecnológicos en funcionamiento es esencial, minimizar las interrupciones para evitar problemas mayores en el futuro.

El Coordinador del CSIRT es responsable de llevar a cabo la gestión detallada de riesgos, asegurando que se identifiquen, evalúen y gestionen los riesgos de seguridad de manera efectiva en toda la organización.

### Gestión del riesgo de la cadena de suministro (ID.SC)

Inicialmente, la gestión de riesgos de la cadena de suministro carecía de una metodología sistemática. No obstante, se ha implementado un procedimiento que cumple con NIST para manejar este aspecto crucial de la seguridad empresarial. Con tal efecto, se han tomado las siguientes medidas:

- Establecer procedimientos para manejar las interacciones con proveedores y socios externos para garantizar que sigan las pautas de seguridad establecidas y que sus operaciones cumplan con los requisitos del CSIRT.
- Identificar vulnerabilidades y riesgos potenciales, analizando la fortaleza de sus procedimientos de seguridad de la información y su capacidad para salvaguardar datos y actividades críticas compartidas con Mivilsoft.
- Implementar sistemas para verificar periódicamente la seguridad y el cumplimiento de los socios y proveedores externos, garantizando un nivel adecuado de protección durante toda la relación comercial.

## Proteger

Esta fase se encarga de controlar el acceso a la información mediante el uso de cuentas distintas y autenticación, salvaguardar la información privada con cifrado, realizar copias de seguridad frecuentes, actualizar y proteger los dispositivos con firewalls y capacitar a los usuarios en procedimientos de ciberseguridad (NIST, 2023).

### Gestión de identidad, autenticación y control de acceso (PR.AC)

Se utilizan una serie de procedimientos estrictos y bien coordinados para asegurar el acceso a los recursos tecnológicos de la empresa. Con esa finalidad, se debe utilizar una dirección IP pública registrada con nuestro proveedor de servicios en la nube, para poder acceder a estos recursos. Esta restricción geográfica garantiza que solo los usuarios dentro de la red aprobada puedan conectarse, adicionando una capa de seguridad adicional contra el acceso remoto no autorizado.

Sólo los empleados autorizados del CSIRT pueden acceder a los recursos tecnológicos a través de un protocolo de acceso seguro, que requiere un nombre de usuario y una contraseña, asegurando que solo el personal autorizado pueda acceder a los sistemas críticos.

El panel de control de los recursos tecnológicos tiene una autenticación de dos factores incorporada. El jefe del departamento es la única persona autorizada a obtener un código necesario para este acceso. Este enfoque protege aún más los activos tecnológicos de la organización al garantizar que solo los empleados con un grado adecuado de autorización puedan realizar cambios representativos dentro de los sistemas relacionados con el CSIRT.

Los permisos de acceso basadas en el Control de Acceso Basado en Roles (RBAC) del CSIRT se muestran en la Tabla 10. Cada rol recibe autorizaciones específicas, lo que garantiza que cada miembro del CSIRT tenga acceso a los sistemas y datos necesarios para llevar a cabo sus responsabilidades.

**Tabla 10.** Permisos de acceso a los sistemas del CSRIT

| Rol | Permisos de Acceso | Sistemas |
|---|---|---|
| **Coordinador del CSIRT** | Acceso total a todos los sistemas y datos del CSIRT. | Sistemas de gestión de incidentes, informes, herramientas de coordinación. |
| **Gestor de incidentes** | Acceso a los sistemas de gestión de incidentes y datos relacionados. | Sistemas de gestión de incidentes, base de datos de incidentes, sistemas software de la organización |
| **Gestor de Infraestructuras Digitales** | Acceso a sistemas de infraestructura, configuración de red, y servidores. | Herramientas de administración de servidores, configuración de red. |
| **Oficial de Seguridad y Confianza Digital** | Acceso a sistemas de seguridad y herramientas de auditoría. | Sistemas de monitoreo de seguridad, herramientas de auditoría, políticas de seguridad. |

Fuente: elaboración propia

Los datos críticos y el acceso a los recursos tecnológicos se monitorean continuamente para identificar y responder ante cualquier actividad sospechosa. A fin de, que los registros de los sistemas se examinan periódicamente para buscar patrones extraños que puedan indicar una violación de la seguridad. Para facilitar una reacción rápida y bien coordinada, se generan notificaciones en tiempo real

sobre intentos de acceso no autorizados y otros eventos cruciales utilizando herramientas como Wazuh.

**Concienciación y capacitación (PR.AT)**

La ausencia de un programa integral de concientización y capacitación en ciberseguridad en este momento indica una grave debilidad en las defensas de la organización contra los ataques cibernéticos. Sin un programa formal, es posible que los empleados no estén completamente informados sobre las políticas internas, las mejores prácticas de seguridad y los procedimientos para responder los incidentes de seguridad.

El CSIRT de la organización debe utilizarse junto con un programa de concientización y capacitación que esté alineado con el marco NIST CSF para reducir los riesgos. Por ende, todos los empleados deben recibir capacitaciones frecuentes, con énfasis en temas importantes que incluyen la detección de correos electrónicos falsos (phishing), el valor de crear contraseñas seguras y la protección de datos privados, entre otros.

Se debe incluir en la capacitación el uso adecuado de las herramientas y sistemas de seguridad de la empresa, así como la función del CSIRT en la gestión de incidentes. Todos los miembros del personal también deben estar familiarizados con los protocolos de respuesta y notificación de incidentes, así como la función del CSIRT en la coordinación y mitigación de estos eventos.

**Seguridad de los datos (PR.DS)**

Con la ayuda de una variedad de tácticas y procedimientos, la empresa otorga una alta prioridad a la protección de la información. Las tecnologías de seguridad en la comunicación como HTTPS y SSL se utilizan para cifrar todos los datos enviados a través del navegador web, salvaguardando la confidencialidad e integridad de la información. Por tal razón, esta medida permite que cualquier intercambio de datos sea seguro y protegido contra posibles interceptaciones.

Las aplicaciones que manejan información sensible utilizan direcciones IP internas para conectarse. Este enfoque asegura que la transmisión de datos dentro del entorno de red de la empresa esté protegida, manteniendo la confidencialidad de la información crítica.

Cada seis meses, el CSRIT realiza copias de seguridad de sus bases de datos, que son necesarias para garantizar la disponibilidad de los sistemas en caso de incidentes graves que puedan poner en peligro la integridad de la información, aunque en este momento no existe una política formal de recuperación ante desastres.

El jefe del departamento se encarga de supervisar la aprobación de cualquier nuevo desarrollo. Por ende, este procedimiento garantiza que todas las modificaciones sean examinadas y aceptadas antes de ser puestas en producción. Antes de que las actualizaciones estén disponibles para los usuarios finales, el jefe del departamento las revisa para asegurarse de que cumplan con los criterios de calidad y seguridad establecidos.

**Procesos y procedimientos de protección de la información (PR.IP)**

Se utiliza una política de seguridad de la información para controlar el ciclo de vida de los activos. Para gestionar los activos del sistema sin afectar su estado actual, se implementa un plan de acción documentado para realizar actualizaciones o escalabilidad en los sistemas. De tal manera, que garantiza una implementación efectiva y reduce el impacto de las operaciones en curso, al mismo tiempo se cumplen las políticas establecidas para preservar la disponibilidad e integridad del sistema.

**Mantenimiento (PR.MA)**

Se establece un plan de mantenimiento integral de los activos, que incorpora la programación regular de actualizaciones de software, parches de seguridad y mantenimientos preventivos. Estas medidas tienen como objetivo reducir los

riesgos de fallos y reducir el deterioro de los sistemas. También garantizan el cumplimiento de estándares y regulaciones de la industria, mejorando la resistencia a los ciberataques.

**Tecnología de protección (PR.PT)**

Todas las operaciones pertinentes, incluidos los accesos, modificaciones y eliminación de datos de las bases de datos importantes, están minuciosamente documentadas por el sistema de registro. En cada registro se incluyen detalles precisos sobre la identidad del usuario, la fecha y hora de la acción y los datos o configuraciones involucradas. Para proporcionar trazabilidad y control de todas las modificaciones, también se registran las transacciones importantes y cambios en la configuración del sistema.

El análisis de registros se lleva a cabo con frecuencia para encontrar patrones inusuales o comportamientos sospechosos que puedan indicar posibles amenazas o fallas de seguridad, así pues, se evalúa la eficiencia de las políticas de seguridad y la integridad de los datos, mediante auditorías internas y externas. Asimismo, el CSIRT cuenta con un sistema de alerta para notificar los eventos o anomalías detectadas durante el proceso de auditoría, permitiendo respuestas rápidas y adecuadas.

**Detectar**

Esta fase consiste en desarrollar y probar procesos para detectar entidades y acciones no autorizadas, mantener y supervisar registros de actividad, conocer los flujos de datos esperados y comprender el impacto de los eventos relacionados con la ciberseguridad (NIST, 2023).

**Anomalías y eventos (DE.AE)**

Con la ayuda de tecnologías como Wazuh, se monitorea continuamente la seguridad de todas las máquinas críticas de la empresa. Por tal razón, estas

configuraciones detectan automáticamente comportamientos inusuales como accesos no autorizados o actividades sospechosas, utilizando reglas y listas de vulnerabilidades más recientes.

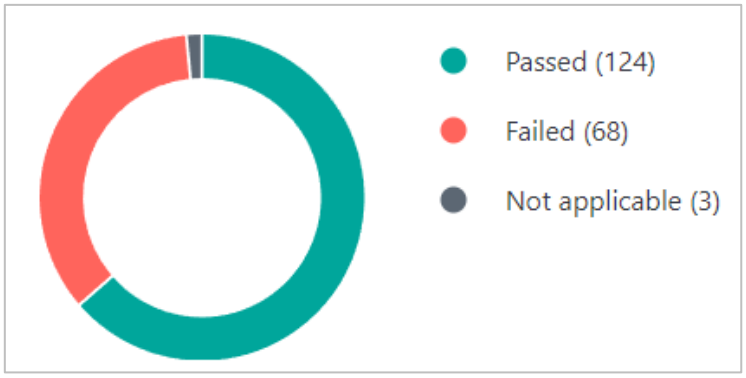
Se realizan evaluaciones periódicas de las políticas de seguridad utilizando las especificaciones de SCAP (*Security Content Automation Protocol*), para asegurar la seguridad y el cumplimiento de los sistemas internos de la empresa. Por consiguiente, se ha establecido una política predeterminada denominada CIS Ubuntu Linux 20.04 LTS Benchmark v1.1.0, que es ampliamente reconocida y que actualmente está aplicada en los activos clave de la empresa.

A continuación, se muestra la disposición de los componentes del proceso de evaluación del cumplimiento de seguridad:

- **Escáner SCAP:** Wazuh utiliza el escáner OpenSCAP certificado por NIST para evaluar el cumplimiento de la política de seguridad.
- **Políticas de seguridad (SCAP Content):** El Centro para la Seguridad de Internet (CIS) ha establecido una colección de pautas y definiciones de seguridad.
- **Perfiles:** Dentro de la política elegida se establecen perfiles particulares que agrupan un subconjunto de reglas.
- **Evaluación (*Scan*):** Se utiliza OpenSCAP para realizar escaneos automatizados con el objetivo de evaluar el cumplimiento de las políticas de seguridad.

En la Ilustración 8 se presentan los resultados de la aplicación de esta política en un activo tecnológico de Mivilsoft. Esta configuración se ha implementado en todos los activos críticos de la organización para garantizar la uniformidad y el cumplimiento de los estándares de seguridad.

**Ilustración 8.** Aplicación de CIS Ubuntu Linux 20.04 LTS Benchmark




Fuente: elaboración propia

## Monitoreo Continuo de la Seguridad (DE.CM)

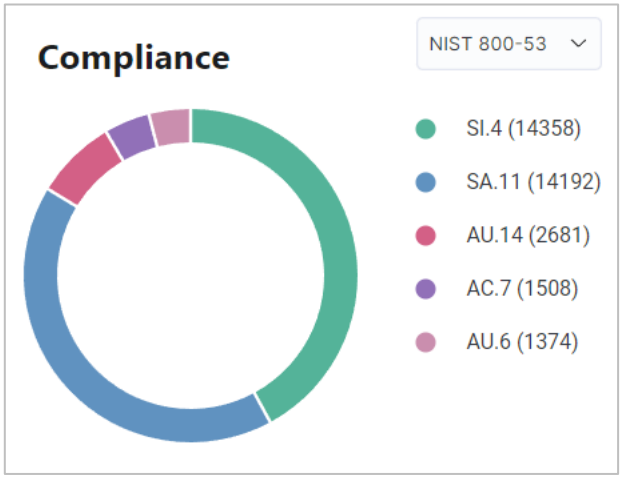
Se lleva a cabo una evaluación continua de la integridad de archivos y configuraciones de los sistemas en cada instancia virtual mediante la herramienta Wazuh, para esto, se configuran vulnerabilidades conocidas y desconocidas en tiempo real para monitorear continuamente la postura de seguridad de los activos tecnológicos, lo que ayuda a la detección temprana de amenazas potenciales.

Se implementan los siguientes procedimientos aprovechando las capacidades de Wazuh, para cumplir con los controles establecidos por NIST 800-53:

- Las herramientas de análisis de registros de Wazuh se utilizan para encontrar violaciones de políticas, mal funcionamiento del sistema e incidentes de seguridad.
- Para preservar los activos tecnológicos, se identifican cambios no autorizados y se verifica la integridad de los datos críticos. Con esa finalidad, se mantiene activo el módulo de monitoreo de integridad de archivos que proporciona Wazuh.
- Las funciones de detección de amenazas de Wazuh se emplean para identificar comportamientos sospechosos y conductas malévolas en los activos tecnológicos.

En la Ilustración 9 se muestran los controles del NIST 800-53 implementados en todos los activos críticos de Mivilsoft.

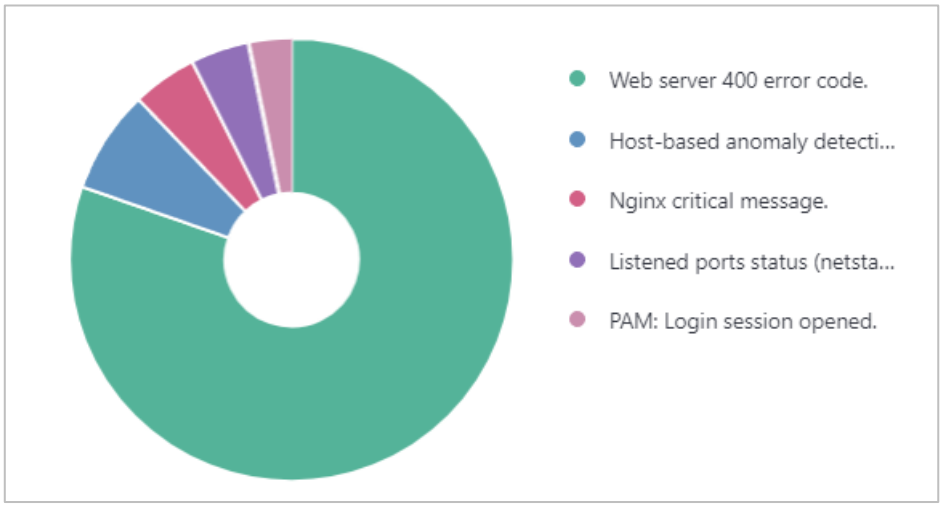
**Ilustración 9.** Implementación de controles NIST 800-53




Fuente: elaboración propia

Además, la Ilustración 10 presenta las cinco alertas de seguridad más frecuentes detectadas por Wazuh en los activos tecnológicos. Las alertas se muestran como un gráfico circular y cada sección representa un tipo diferente de alerta. En conjunto, estos datos resaltan las áreas clave de preocupación en términos de seguridad, siendo el “Web server 400 error code” el incidente más frecuente.

**Ilustración 10.** Top 5 alertas de seguridad más frecuentes detectadas en Mivilsoft




Fuente: elaboración propia

**Procesos de Detección (DE.DP)**

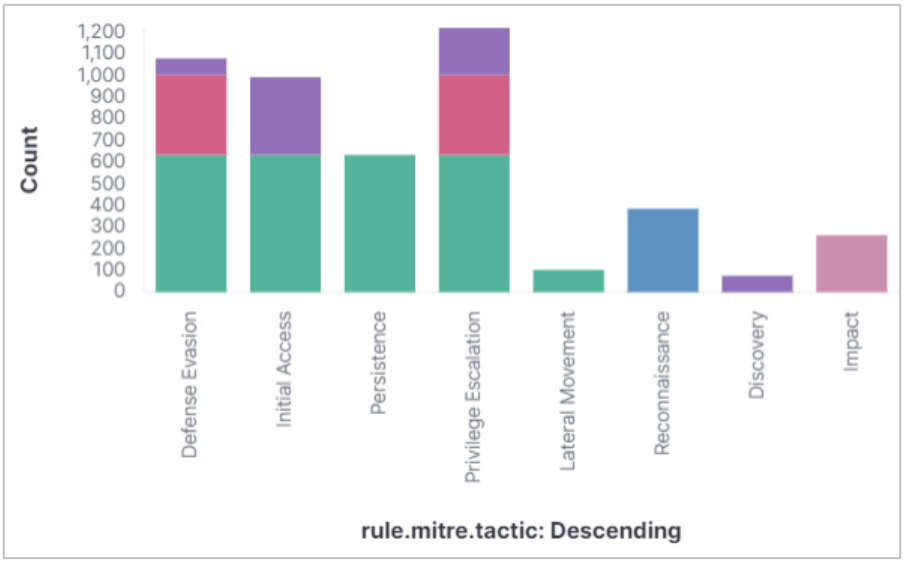
Los procedimientos de detección de Wazuh se han mejorado mediante la adición de nuevas reglas creadas especialmente para identificar comportamientos sospechosos y actividades maliciosas en los activos críticos de Mivilsoft. A medida que se descubren nuevos riesgos y patrones de ataque, estas regulaciones se modifican constantemente para mantener al CSRIT actualizado y preparado frente a las últimas amenazas cibernéticas

El marco MITRE ATT&CK se emplea para desarrollar y optimizar reglas en la detección de comportamientos sospechosos y actividades maliciosas utilizando estrategias y enfoques establecidos. Dado que, incluye 14 estrategias y otras herramientas que ayudan a identificar y analizar ataques en curso, ofreciendo una colección globalmente accesible de acciones y comportamientos observados de amenazas reales. Por lo tanto, este marco contribuye a:

- Proporcionar una referencia integral para identificar y comprender las tácticas del adversario, lo que fortalece la capacidad de detectar conductas maliciosas que puedan comprometer los activos tecnológicos.
- Facilitar la vinculación de los incidentes de seguridad con las estrategias y tácticas establecidas para que sea posible una reacción más centrada y eficaz.
- Permitir ajustar las políticas y procesos de seguridad a los nuevos métodos de ataque, proporcionando información sobre los peligros emergentes.

La implementación del marco MITRE ATT&CK en los sistemas de Mivilsoft, permitió identificar y categorizar los incidentes de seguridad encontrados en los últimos 3 meses. Estos sucesos se clasifican por tácticas como se muestra en la Ilustración 11, lo que revela que los atacantes priorizan la evasión de defensas, obtención de acceso inicial y escalamiento de privilegios. Con el fin de fortalecer las defensas en los puntos más vulnerables y comprender mejor las estrategias empleadas por los adversarios, este proceso de detección resulta fundamental.

**Ilustración 11.** Tácticas comunes del framework MITRE ATT&CK en Mivilsoft



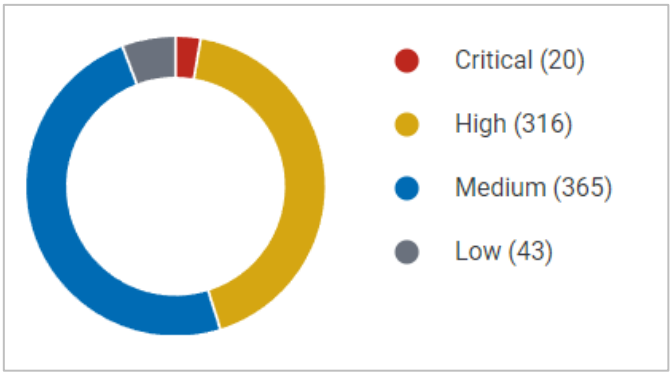

Fuente: elaboración propia

La incorporación del módulo de detección de vulnerabilidades a los recursos tecnológicos de Mivilsoft es un componente esencial de la estrategia proactiva de ciberseguridad del CSIRT. El inventario de software y la documentación de vulnerabilidades, especialmente los registros CVE, pueden correlacionarse más fácilmente gracias a este módulo. Por ello, se utiliza el formato JSON CVE 5 para organizar y estandarizar estos documentos, los cuales provienen de la plataforma de Inteligencia de Amenazas Cibernéticas (CTI).

Este proceso de detección identifica paquetes vulnerables en las bases de datos de inventario y registra los hallazgos en un inventario de vulnerabilidades por cada activo. Esto permite al CSIRT responder de manera rápida y efectiva al ofrecer información sobre el estado actual de los activos y las vulnerabilidades no resueltas.

El estado de seguridad de un activo específico se muestra en la Ilustración 12. Por tal razón, es el único en Mivilsoft con un número significativamente alto de vulnerabilidades, incluidas varias fallas de alta gravedad. De acuerdo con las directrices y procedimientos del CSIRT, este análisis es fundamental para establecer prioridades para las medidas correctivas y la mitigación de riesgos.

**Ilustración 12.** Vulnerabilidades detectadas en un agente específico de Mivilsoft




Fuente: elaboración propia

## Responder

Esta fase consiste en probar y actualizar los planes de respuesta, asegurando que todos los involucrados comprendan claramente sus responsabilidades y mejorando la efectividad del proceso mediante la incorporación de lecciones aprendidas (NIST, 2023).

### Planificación de la Respuesta (RS.RP):

Aunque no se cuenta con un plan formalizado de respuesta a incidentes de seguridad cibernética, se han implementado medidas siguiendo las mejores prácticas. Estas medidas incluyen actualizar y configurar los sistemas de forma segura, identificando y analizando amenazas con tecnologías sofisticadas como SIEM y adherirse al ciclo de gestión y respuesta que se muestra en la Ilustración 13.

**Ilustración 13.** Procesos de gestión de incidentes de seguridad


Fuente: elaboración propia

Los incidentes significativos se informan al CSRIT de Mivilsoft, la evidencia del incidente se conserva para un análisis detallado y todas las partes involucradas están en constante comunicación.

El CSIRT trabaja en estrecha colaboración con los miembros responsables del equipo para planificar y coordinar la respuesta en caso de un incidente. La asignación de funciones entre los distintos roles durante la gestión de incidentes se detalla en la Tabla 11.

**Tabla 11.** Roles y responsabilidades del CSIRT en la respuesta a incidentes

| Actividad | Coordinador del CSIRT | Gestor de Incidentes | Gestor de Infraestructuras Digitales | Oficial de Seguridad y Confianza Digital |
|---|---|---|---|---|
| **Reunión del Equipo** | Implementa | Aconseja | Ninguno | Ninguno |
| **Evaluación Inicial** | Aconseja | Dueño | Aconseja | Ninguno |
| **Respuesta Inicial** | Aconseja | Dueño | Implementa | Actualiza |
| **Recoger Pruebas Forenses** | Aconseja | Implementa | Aconseja | Dueño |
| **Implementar un Arreglo Temporal** | Aconseja | Dueño | Implementa | Aconseja |
| **Enviar la Comunicación** | Implementa | Aconseja | Aconseja | Aconseja |
| **Implementar un Arreglo Permanente** | Aconseja | Dueño | Implementa | Actualiza |
| **Determinar el Impacto Financiero en los Negocios** | Aconseja | Actualiza | Actualiza | Dueño |

Fuente: elaboración propia

Se establece un tiempo máximo de respuesta en la gestión de incidentes de seguridad, teniendo en cuenta la criticidad e impacto y sus posibles repercusiones. Las restricciones de tiempo enumeradas en la Tabla 12, representan la cantidad máxima de tiempo necesaria para manejar cada evento; no representan el tiempo necesario para resolver completamente cada uno de ellos, el cual puede diferir según las particularidades de cada caso.

**Tabla 12.** Tiempos máximos de atención de incidentes

| Nivel de Incidente | Tiempo de Respuesta |
|---|---|
| **Bajo** | 5 horas |
| **Moderado** | 2 horas |
| **Alto** | 30 minutos |
| **Crítico** | 15 minutos |

Fuente: elaboración propia

Además, de garantizar que los problemas se resuelvan con prontitud y eficacia, los tiempos de respuesta definidos ofrecen un método organizado para gestionar y clasificar los incidentes según su gravedad. Con esta estrategia, el CSIRT puede actuar rápidamente para disminuir los efectos y la resolución final del incidente puede personalizarse para adaptarse a los recursos y la complejidad que sean necesarios.

**Comunicaciones (RS.CO):**

Se comunican las medidas de mitigación y la documentación necesarias en caso de un ciberataque. Todos los empleados pertinentes de Mivilsoft están comprometidos a ejecutar medidas de prevención y respuesta. El desarrollador de software (Gestor de Incidentes) está a cargo de las tareas de mitigación más complejas. Como se indica en la Tabla 13, se ha desarrollado una política de niveles de respuesta a incidentes alineadas con las mejores prácticas del NIST SP 800-61.

**Tabla 13.** Niveles de incidentes cibernéticos

| Nivel de Incidente | Descripción |
|---|---|
| **Bajo** | El incidente es menor y no compromete significativamente las operaciones. |
| **Moderado** | El incidente afecta moderadamente las operaciones, pero no causa una interrupción significativa. |
| **Alto** | El incidente causa una interrupción significativa de las operaciones y puede comprometer la seguridad de la infraestructura crítica. |
| **Crítico** | El incidente compromete gravemente la seguridad y funcionalidad de los activos tecnológicos, causando una interrupción mayor. |

Fuente: elaboración propia

Cualquier sospecha de un incidente de seguridad, ya sean internos o externos al CSIRT, deberán notificarse inmediatamente a través de correo electrónico u otro canal adecuado. Para garantizar una coordinación efectiva y reducir el impacto, el Coordinador del CSIRT formará un equipo y decidirá a quién se debe contactar

además del CSIRT principal. Inicialmente, sólo se notificará a las personas directamente involucradas en la respuesta al incidente. Después de eso, el Coordinador del CSIRT determinará qué otras personas deben ser informadas.

Además, cualquier suceso que afecte la seguridad de Mivilsoft deberá ser reportado por los proveedores de servicios críticos de Mivilsoft, y viceversa. Para este comunicado se utilizará un correo electrónico o un documento escrito que describa las posibles fuentes de alerta. Se seguirá el plan de respuesta establecido a la hora de tomar medidas correctivas.

**Análisis (RS.AN):**

Para determinar el origen y tipo de vulnerabilidades, se examinan las alertas generadas de Wazuh. Este análisis permite al CSIRT responder con prontitud y eficacia implementando medidas como el aislamiento de los dispositivos o áreas afectadas hasta que se solucione la vulnerabilidad.

En función del valor o importancia del sistema dentro de la organización y el proceso que soporta determina la prioridad del incidente. Este aspecto es fundamental para determinar cómo el CSRIT manejará los eventos. Los niveles de criticidad de los sistemas en cuestión se enumeran en la Tabla 14.

**Tabla 14.** Niveles de criticidad de impacto

| Nivel de Criticidad | Valor | Definición |
|---|---|---|
| **Baja** | 1 | Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no esenciales. |
| **Moderada** | 2 | Sistemas que apoyan a una sola dependencia o proceso no crítico de la entidad. |
| **Alta** | 3 | Sistemas que apoyan a múltiples dependencias o procesos importantes dentro de la entidad. |
| **Crítica** | 4 | Sistemas críticos, fundamentales para la operación de la entidad, cuya interrupción puede causar graves daños. |

Fuente: elaboración propia

El impacto de los incidentes encontrados se evalúa mediante registros detallados y análisis exhaustivos, que ayudan a determinar con precisión el impacto de un incidente, se lleva a cabo una evaluación de riesgos de los activos y servicios

involucrados. Esto permite implementar acciones correctivas adecuadas para reducir cualquier efecto adverso. Por esta razón, se utiliza una escala de valores para cuantificar estos impactos, teniendo en cuenta tanto el daño inmediato producido, como el impacto futuro que podría surgir si el problema no se contiene adecuadamente. La clasificación de la Tabla 15, sirve como base para la evaluación de estos niveles.

**Tabla 15.** Niveles de impacto actual y futuro

| Nivel de Impacto | Valor | Definición |
|---|---|---|
| **Bajo** | 1 | Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo. |
| **Moderado** | 2 | Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo. |
| **Alto** | 3 | Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo. |
| **Crítico** | 4 | Impacto severo en uno o más componentes de uno o más sistemas de información, con potencial para causar interrupciones significativas. |

Fuente: elaboración propia

## Mitigación (RS.MI):

La plataforma de monitoreo Wazuh gestiona y mitiga incidentes de manera eficiente de acuerdo con las mejores prácticas de seguridad. Tan pronto como se descubre un incidente, se toman medidas inmediatas para minimizar su impacto en los activos. El incidente se clasifica utilizando la siguiente fórmula: Nivel de Prioridad = (Impacto Actual * 2,5) + (Impacto Futuro * 2,5) + (Criticidad del Sistema * 5)

Para conocer la prioridad de atención del incidente, los resultados de esta fórmula se contrastan con la Tabla 16:

**Tabla 16.** Niveles de prioridad del incidente

| Nivel de Prioridad | Valor |
|---|---|
| **Bajo** | 10.0 - 19.99 |
| **Moderado** | 20.0 - 29.99 |
| **Alto** | 30.0 - 39.99 |
| **Crítico** | 40.0 - 50.0+ |

Fuente: elaboración propia

El CSIRT puede priorizar las acciones necesarias para contener y erradicar la amenaza utilizando la Tabla 16, clave en el proceso de triage. Entre las medidas a considerar están la restauración de la integridad de los sistemas afectados, la aplicación de parches de seguridad y la rápida actuación para evitar la propagación del incidente.

Eliminar cualquier evidencia del incidente, incluido el código malicioso, es un paso crucial en el enfoque de mitigación. Esto garantiza que el sistema esté seguro y libre de riesgos persistentes que puedan causar más daño o facilitar futuros ataques.

**Mejoras (RS.IM):**

Para encontrar oportunidades de mejora, se realiza un análisis exhaustivo de los protocolos de recuperación tras cada ciberataque. Las lecciones aprendidas se registran como parte de este proceso de retroalimentación continua y los planes de recuperación se actualizan en consecuencia.

Los siguientes pasos están incluidos en el proceso de adquisición de experiencia:

- **Documentación Detallada:** Registrar todo lo que sucedió, cuándo sucedió y cómo se manejó el incidente.
- **Revisión de Procedimientos:** Evaluar los procesos registrados para ver si se siguieron adecuadamente o si se requirieron ajustes.
- **Análisis de Medidas:** Evaluar si se realizaron las acciones necesarias y si pudieron contribuir a una recuperación más efectiva.
- **Gestión del Personal:** Evaluar la gestión del personal durante el evento y planificar mejoras para el futuro.
- **Acciones Correctivas:** Implementar medidas correctivas para detener futuros incidentes similares.

- **Herramientas y Recursos:** Identificar herramientas y recursos adicionales necesarios para mejorar la detección, análisis y mitigación de futuros incidentes.

Este proceso permite identificar fallos o imprecisiones en los procedimientos y sirve como punto de partida para realizar los cambios necesarios. Dado que la tecnología de la información y el personal están en constante cambio, el CSRIT debe revisar y actualizar regularmente toda la documentación y los procedimientos para el manejo de incidentes.

**Recuperar**

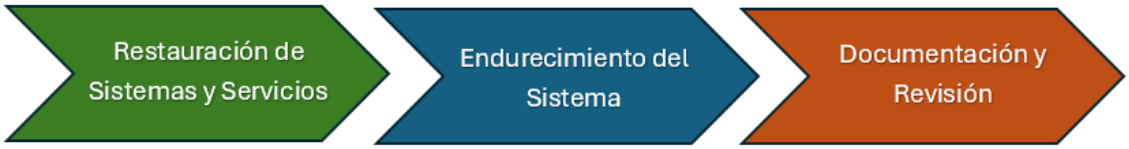
Esta fase consiste en desarrollar e implementar actividades adecuadas para mantener los planes de resiliencia, asegurando la restauración de cualquier capacidad o servicio que haya sido afectado (NIST, 2023).

**Planificación de la recuperación (RC.RP):**

De conformidad con el marco NIST 800-184, los procedimientos de recuperación se registran para garantizar una pronta restauración del servicio afectados por eventos cibernéticos. Para minimizar los errores, esto implica desarrollar un plan de recuperación con distintas fases, procedimientos técnicos y criterios de salida para cada fase, así como automatizar procesos cruciales. También se encontraron alternativas estratégicas para garantizar la resiliencia operativa y se evaluaron requisitos de continuidad.

La Ilustración 14, muestra las acciones clave del plan de recuperación del CSIRT, incluida la restauración del sistema y los servicios, el fortalecimiento del sistema para prevenir futuros incidentes y la documentación y revisión después del incidente para evaluar y mejorar el proceso.

**Ilustración 14.** Acciones principales del plan de recuperación




Fuente: elaboración propia

Además, los miembros del CSIRT son capacitados para evaluar los riesgos afectados de los incidentes. La restauración de los sistemas a partir de copias de seguridad limpias y la recuperación de sistemas son ejemplos de operaciones técnicas, mientras que las acciones no técnicas se ocupan de cambios esenciales en los procesos comerciales.

**Mejoras (RC.IM):**

En la fase de recuperación, una de las partes más importantes del proceso es la integración de las lecciones aprendidas. Este componente es esencial para garantizar que el CSIRT evolucione y se adapte a nuevas amenazas, avances tecnológicos y experiencias previas. Por tal razón, es importante enfocarse en puntos clave, tales como:

- Implementar procedimientos y tecnologías automatizadas para acelerar y simplificar la recuperación de los sistemas y servicios afectados.
- Realizar una verificación exhaustiva de vulnerabilidades posterior al incidente para encontrar y corregir vulnerabilidades en los sistemas afectados.
- Evaluar el incidente y la respuesta para encontrar áreas donde se podrían fortalecer los procedimientos de recuperación.
- Para garantizar la disponibilidad e integridad de la copia de seguridad, pruebe la recuperación de la copia de seguridad periódicamente.

Implementar estas mejoras basadas en las lecciones aprendidas garantiza que el CSIRT de Mivilsoft pueda enfrentar futuros incidentes con mayor eficacia, minimizando su impacto y fortaleciendo la resiliencia organizacional. La evolución

continua del equipo y la actualización de los procedimientos son fundamentales para mantener una postura de seguridad robusta y adaptable.

**Comunicaciones (RC.CO):**

Para garantizar que toda la información pertinente se transmita a todas las partes involucradas (incluidos los miembros del personal, clientes y socios) de manera oportuna y precisa, existen estándares de comunicación claros. Por ende, estos protocolos implican la preparación de mensajes preestablecidos para diferentes casos, el uso de múltiples canales de comunicación y la designación de un equipo de comunicación de incidentes.

Una comunicación clara y transparente promueve la confianza y facilita la planificación de una respuesta exitosa. Fundamentalmente, existen estrategias de recuperación para minimizar el tiempo de inactividad y las pérdidas económicas en caso de una interrupción del servicio.

# CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

## 3.1. Validación de la propuesta

El marco NIST es la base del CSIRT de Mivilsoft y proporciona una guía estructurada para gestionar la ciberseguridad. Los siete pasos se describen a continuación.

### Priorización y alcance

Mivilsoft, es una empresa de soluciones integradas centrada en ciudades y transporte, maneja varios sistemas informáticos vitales que prestan servicios a los empleados y clientes ecuatorianos. Estos sistemas son cruciales para la continuidad del negocio y la ejecución de las tareas diarias, por lo que es primordial que estén siempre operativos.

El desarrollo del perfil inicial en Mivilsoft incluye la identificación de los objetivos de negocio y proporciona el contexto necesario para identificar las actividades de mitigación de riesgos. La Tabla 17 muestra el alcance de las actividades de la organización.

**Tabla 17.** Priorización y Alcance

| Actividades que desarrolla la organización | Descripción de los límites de esta actividad |
|---|---|
| **Gestión Comercial** | Incluye todas las actividades de generación de relaciones comerciales con el cliente y su satisfacción |
| **Diseño y Desarrollo** | Incluye todas las actividades de diseño y desarrollo de software en la organización |
| **Gestión de Operaciones** | Incluye las actividades de control, trazabilidad y liberación de los productos y servicios |
| **Servicio Postventa** | Incluye las actividades de seguimiento, actualizaciones, mantenimiento y garantías al cliente luego de la venta del producto |

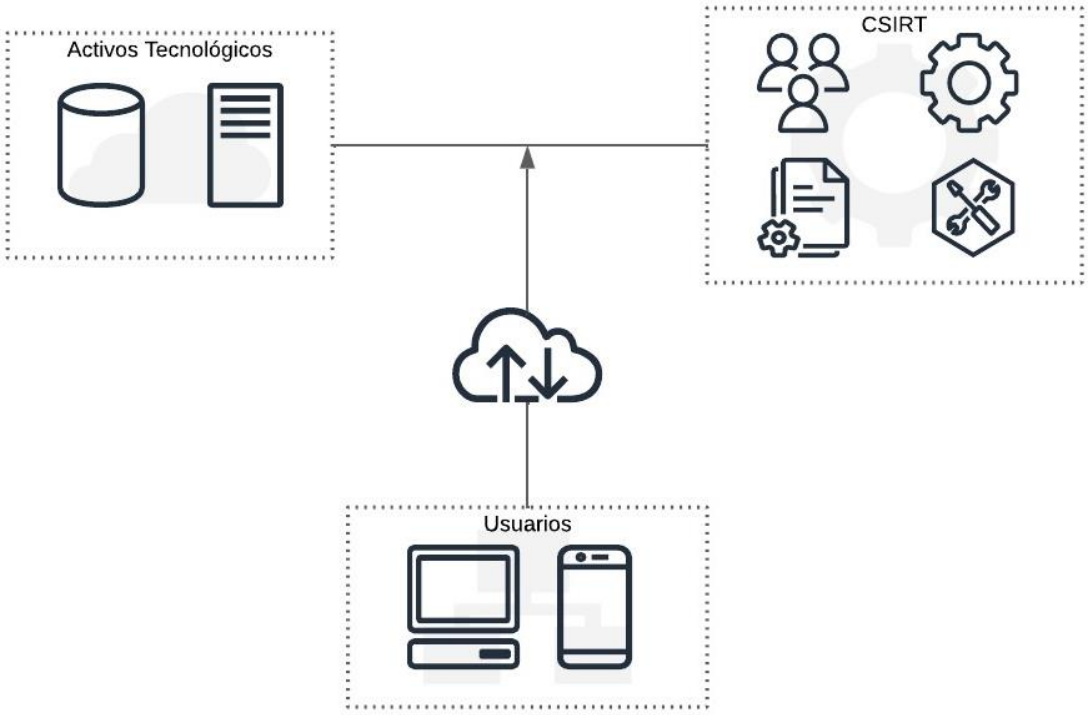
Fuente: elaboración propia

Por lo tanto, en conjunto con el gerente administrativo, se ha definido que el alcance de la implementación del CSRIT se centrará en las actividades de diseño y desarrollo, priorizando los activos informáticos relacionados.

## Orientar

Para garantizar una adecuada gestión de los riesgos de ciberseguridad en Mivilsoft, el CSIRT implementa un enfoque sistemático basado en las directrices del marco de trabajo del NIST. Este enfoque se enfoca en la identificación de los sistemas y activos críticos, como se presenta en la Tabla 7. Además, la Ilustración 15 presenta la infraestructura tecnológica que respalda el funcionamiento del CSIRT en Mivilsoft.

**Ilustración 15.** Infraestructura Tecnológica del CSIRT de Mivilsoft




Fuente: elaboración propia

## Perfil Actual

Para la creación del perfil actual de la empresa de Mivilsoft, se parte de los niveles de implementación establecidos por el marco de trabajo NIST, como se muestra en la Ilustración 16. Estos niveles permiten a la organización, y específicamente al CSIRT, catalogarse en un umbral predefinido, teniendo en cuenta sus prácticas

actuales de gestión de riesgos, el entorno de amenazas, y los requerimientos legales y regulatorios.

**Ilustración 16.** Niveles de implementación del NIST CSF


Fuente: elaboración propia

Además, se considera la estructura del marco de trabajo NIST, que se organiza en categorías y se desglosa en subcategorías, tal como se presenta en la Ilustración 16.

Para calcular el estado actual, se emplea la valoración establecida por el marco de trabajo NIST, como se muestra en la yabla 18. Los valores están organizados de la siguiente manera:

- **Nivel:** El marco NIST se despliega en cuatro niveles distintos, como se muestra en la Figura 16.

- **Logro:** Cada nivel se clasifica según el grado de cumplimiento: Parcial, Riesgo Informado, Repetible, o Adaptado.

- **Descripción:** Evalúa la efectividad en la implementación del marco en cada uno de estos niveles.

- **Valor:** Se asigna una valoración que oscila entre el 25% y el 100%, según el nivel alcanzado.

**Tabla 18.** Determinación de porcentaje de cumplimiento

| Nivel | Logro | Descripción | Valor |
|---|---|---|---|
| **1** | Parcial | Procesos inexistentes o no formalizados. | 25% |
| **2** | Riesgo Informado | Procesos aprobados, pero podrían no ser establecidos como políticas de toda la organización. | 50% |
| **3** | Repetible | Procesos aprobados y se expresan como políticas. | 75% |
| **4** | Adaptado | Mejor continua que incluye lecciones aprendidas e indicadores predictivos. | 100% |

Fuente: elaboración propia

A continuación, se presentan los porcentajes obtenidos para cada categoría evaluada, los cuales fueron utilizados por el CSIRT de Mivilsoft para determinar el perfil actual de la empresa, como se muestra en la Tabla 19. Estos resultados se derivan de los porcentajes de cumplimiento detallados en la Tabla18. Los valores se desglosan de la siguiente manera:

- **Función:** Se describe cada una de las categorías del marco de trabajo de NIST.

- **Categoría:** Corresponde al código asignado según el checkList de NIST, como se observa en la **¡Error! No se encuentra el origen de la referencia.**.

- **%Logro:** Se calcula el porcentaje obtenido conforme a la Tabla 18, sumando los valores y dividiéndolos por el máximo logro alcanzado.

**Tabla 19.** Resultados de la primera implementación del Checklist de NIST

| Función | Categoría | %Logro |
|---|---|---|
| **IDENTIFICAR (ID)** | ID.AM | 50.00% |
| | ID.BE | 35.00% |
| | ID.GV | 25.00% |
| | ID.RA | 33.33% |
| | ID.RM | 41.67% |
| | ID.SC | 30.00% |
| **Función ID** | | **35.83%** |
| **PROTEGER (PR)** | PR.AC | 25.00% |
| | PR.AT | 25.00% |
| | PR.DS | 25.00% |
| | PR.IP | 25.00% |
| | PR.MA | 37.50% |

| | | |
|---|---|---|
| | PR.PT | 25.00% |
| **Función PR** | | **27.08%** |
| **DETECTAR (DE)** | DE.AE | 35.00% |
| | DE.CM | 37.50% |
| | DE.DP | 25.00% |
| **Función DE** | | **32.50%** |
| **RESPONDER (RS)** | RS.RP | 25.00% |
| | RS.CO | 25.00% |
| | RS.AN | 25.00% |
| | RS.MI | 25.00% |
| | RS.IM | 25.00% |
| **Función RS** | | **25.00%** |
| **RECUPERAR (RC)** | RC.RP | 25.00% |
| | RC.IM | 25.00% |
| | RC.CO | 25.00% |
| **Función RC** | | **25.00%** |

Fuente: elaboración propia

## Evaluación de riesgos

Según la NIST 800-60, se clasifica los activos de información en función del impacto potencial de las amenazas de seguridad, determinado por los criterios de Disponibilidad, Integridad y Confidencialidad.

- **Confidencialidad:** La información está protegida contra divulgaciones no autorizadas.
- **Integridad:** La información se preserva sin modificaciones no autorizadas.
- **Disponibilidad:** La información y los sistemas están disponibles y accesibles cuando se necesitan.

La aplicación de la Tabla 9 permite evaluar la criticidad de cada activo, facilitando la identificación de aquellos que requieren atención prioritaria. La Tabla 7 presenta la clasificación de activos según su nivel de criticidad, lo que permite al CSIRT de Mivilsoft enfocar los recursos y esfuerzos en las áreas más críticas para abordar las brechas identificadas y desarrollar un plan de acción efectivo.

Con los datos obtenidos sobre la identificación de amenazas, se clasifica el nivel de riesgo de cada activo para definir su perfil actual. La Tabla 20 proporciona una

visión detallada de las amenazas encontradas, ayudando al CSIRT a priorizar las medidas de protección y respuesta de manera más eficiente. Los valores se presentan de la siguiente manera:

- **Código:** Código único del activo asignado por la institución.
- **Nombre:** Nombre específico del activo.
- **Criticidad:** Calificación asignada al activo, determinada según la valoración en la Tabla 9.

**Tabla 20.** Identificación de amenazas de los activos de Mivilsoft

| Código | Nombre | Amenaza | Probabilidad | Impacto | Nivel de Riesgo |
|---|---|---|---|---|---|
| S-009 | Django Server | Las APIs del servidor web son públicas | Los atacantes pueden explotar APIs expuestas, comprometiendo la seguridad del servidor web | Cualquier usuario, incluido un atacante, podría interactuar con ellas | 12 - Alto |
| S-010 | Kibana Server | La ausencia de un certificado SSL en el servidor web | El atacante puede interceptar los de datos en tránsito | Interceptación de datos sensibles por parte de los atacantes | 18 - Alto |
| S-015 | OdooUI | El puerto predeterminado del servidor web está abierto | Un atacante podría explotar los puertos abiertos para lanzar un ataque | Un atacante podría identificar y explotar vulnerabilidades | 18 - Alto |
| S-016 | OdooDB | El puerto por defecto del servidor de base de datos está expuesto | Un atacante puede acceder al servidor de base de datos | Expone el servidor de base de datos a accesos no autorizados y posibles ataques | 18 - Alto |
| S-017 | TraccarDB | El puerto por defecto del servidor de base de datos está expuesto | Un atacante puede acceder al servidor de base de datos | Expone el servidor de base de datos a accesos no autorizados y posibles ataques | 18 - Alto |
| S-018 | TraccarUI | El puerto predeterminado del servidor web está abierto | Un atacante podría explotar los puertos abiertos para lanzar un ataque | Un atacante podría identificar y explotar | 18 - Alto |

| | | | | | |
|---|---|---|---|---|---|
| | | | | vulnerabilidades | |
| S-022 | Miral Odoo 13 | La configuración del servidor tiene configuraciones desactualizadas | La falta de medidas de seguridad adecuadas puede facilitar la explotación de vulnerabilidades | Los atacantes pueden explotar vulnerabilidades y obtener acceso no autorizado a los sistemas | 18 - Alto |

Fuente: elaboración propia

Esta evaluación de riesgos permitirá al CSIRT de Mivilsoft priorizar de manera efectiva sus esfuerzos y recursos en las áreas de mayor riesgo, facilitando así la comunicación y la toma de decisiones informadas con la alta dirección de la empresa.

**Creación del Perfil Deseado**

Para la implementación del CSIRT en Mivilsoft, el perfil deseado se establece mediante una comparación entre el perfil actual del CSIRT y el perfil objetivo que se busca alcanzar. Esta evaluación determina si se cumplen los requisitos dentro del plazo establecido y si las capacidades del CSIRT están alineadas con los objetivos de seguridad de la organización.

Los detalles obtenidos del *checklist* se reflejan en la Tabla 21. Los valores se desglosan de la siguiente manera:

- **Función:** Se describe cada una de las categorías del marco de trabajo de NIST.

- **Categoría:** Corresponde al código asignado según el checkList de NIST, como se observa en la Figura 16.

- **%Objetivo:** El porcentaje obtenido se calcula sumando los valores de la Tabla 18 y dividiéndolos por el máximo logro alcanzado.

**Tabla 21.** Perfil Objetivo del Checklist de NIST

| Función | Categoría | %Objetivo |
|---|---|---|
| **IDENTIFICAR (ID** | ID.AM | 62.50% |
| | ID.BE | 55.00% |
| | ID.GV | 50.00% |
| | ID.RA | 66.67% |
| | ID.RM | 50.00% |
| | ID.SC | 50.00% |
| **Función ID** | | **55.69%** |
| **PROTEGER (PR** | PR.AC | 57.14% |
| | PR.AT | 65.00% |
| | PR.DS | 59.38% |
| | PR.IP | 54.17% |
| | PR.MA | 62.50% |
| | PR.PT | 50.00% |
| **Función PR** | | **58.03%** |
| **DETECTAR (DE)** | DE.AE | 60.00% |
| | DE.CM | 59.38% |
| | DE.DP | 60.00% |
| **Función DE** | | **59.79%** |
| **RESPONDER (RS)** | RS.RP | 75.00% |
| | RS.CO | 50.00% |
| | RS.AN | 65.00% |
| | RS.MI | 66.67% |
| | RS.IM | 62.50% |
| **Función RS** | | **63.83%** |
| **RECUPERAR (RC)** | RC.RP | 50.00% |
| | RC.IM | 62.50% |
| | RC.CO | 50.00% |
| **Función RC** | | **54.17%** |

Fuente: elaboración propia

## Determinar, analizar y priorizar brechas

Con el apoyo de los *checklists* realizados y la comparación entre el perfil actual y el perfil deseado, se han identificado las brechas que permitirán al CSIRT de Mivilsoft establecer las prioridades estratégicas dentro del plan de acción de la organización.

Este enfoque basado en perfiles proporciona al CSIRT la capacidad de tomar decisiones fundamentadas sobre las actividades de seguridad, respaldar la gestión de riesgos y llevar a cabo mejoras específicas y costo-efectivas en las prácticas de ciberseguridad.

**Función Identificar (ID):** Es la primera función en el núcleo del marco NIST, se compone de 6 categorías, cada una de las cuales incluye sus propias subcategorías. El análisis de los resultados se presenta en la Tabla 22.

- **Gestión de activos (ID.AM):** Administra activos clave según su importancia para la organización.
- **Entorno empresarial (ID.BE):** Prioriza la misión y objetivos para guiar decisiones de riesgo.
- **Gobernanza (ID.GV):** Monitorea políticas y requisitos para gestionar riesgos.
- **Evaluación de riesgos (ID.RA):** Comprende los riesgos cibernéticos para la organización.
- **Estrategia de gestión de riesgos (ID.RM):** Define prioridades y tolerancias de riesgo.
- **Gestión del riesgo de la cadena de suministro (ID.SC):** Gestiona riesgos en la cadena de suministro.

**Tabla 22.** Brechas de la Función Identificar

| **Gestión de activos (ID.AM)** | | | | | | |
|---|---|---|---|---|---|---|
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **ID.AM-1** | Riesgo Informado | 2 | Repetible | 3 | 1 | Baja |
| **ID.AM-2** | Riesgo Informado | 2 | Repetible | 3 | 1 | Baja |
| **ID.AM-3** | Riesgo Informado | 2 | Riesgo Informado | 2 | 0 | Objetivo alcanzado |
| **ID.AM-4** | Riesgo Informado | 2 | Riesgo Informado | 2 | 0 | Objetivo alcanzado |
| **ID.AM-5** | Riesgo Informado | 2 | Riesgo Informado | 2 | 0 | Objetivo alcanzado |
| **ID.AM-6** | Riesgo Informado | 2 | Repetible | 3 | 1 | Baja |
| **Entorno empresarial (ID.BE)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **ID.BE-1** | Riesgo Informado | 2 | Riesgo Informado | 2 | 0 | Objetivo alcanzado |
| **ID.BE-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **ID.BE-3** | Riesgo Informado | 2 | Riesgo Informado | 2 | 0 | Objetivo alcanzado a |

| | | | | | | |
|---|---|---|---|---|---|---|
| **ID.BE-4** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **ID.BE-5** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **Gobernanza (ID.GV)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **ID.GV-1** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **ID.GV-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **ID.GV-3** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **ID.GV-4** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **Evaluación de riesgos (ID.RA)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **ID.RA-1** | Riesgo Informado | 2 | Repetible | 3 | 1 | Baja |
| **ID.RA-2** | Parcial | 1 | Adaptable | 4 | 3 | Alta |
| **ID.RA-3** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **ID.RA-4** | Riesgo Informado | 2 | Riesgo Informado | 2 | 0 | Objetivo alcanzado |
| **ID.RA-5** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **ID.RA-6** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **Estrategia de gestión de riesgos (ID.RM)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **ID.RM-1** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **ID.RM-2** | Riesgo Informado | 2 | Riesgo Informado | 2 | 0 | Objetivo alcanzado |
| **ID.RM-3** | Riesgo Informado | 2 | Riesgo Informado | 2 | 0 | Objetivo alcanzado |
| **Gestión del riesgo de la cadena de suministro (ID.SC)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **ID.SC-1** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **ID.SC-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **ID.SC-3** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **ID.SC-4** | Riesgo Informado | 2 | Riesgo Informado | 2 | 0 | Objetivo alcanzado |
| **ID.SC-5** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |

Fuente: elaboración propia

**Función Proteger (PR):** Es la segunda función en el núcleo del marco NIST, se compone de 6 categorías, cada una de las cuales incluye sus propias subcategorías. El análisis de los resultados se presenta en la Tabla 23.

- **Gestión de identidad, autenticación y control de acceso (PR.AC):** Limita y administra el acceso a activos según el riesgo de acceso no autorizado.
- **Concienciación y capacitación (PR.AT):** Educa y capacita al personal y socios en seguridad cibernética conforme a las políticas.
- **Seguridad de los datos (PR.DS):** Protege la confidencialidad, integridad y disponibilidad de la información según la estrategia de riesgo.
- **Procesos y procedimientos de protección de la información (PR.IP):** Mantiene políticas y procedimientos para proteger sistemas y activos.
- **Mantenimiento (PR.MA):** Realiza mantenimiento y reparación de sistemas conforme a políticas y procedimientos.
- **Tecnología de protección (PR.PT):** Gestiona soluciones técnicas para asegurar la seguridad y recuperación de sistemas y activos.

**Tabla 23.** Brechas de la Función Proteger

| **Gestión de identidad, autenticación y control de acceso (PR.AC)** | | | | | | |
|---|---|---|---|---|---|---|
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **PR.AC-1** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.AC-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.AC-3** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **PR.AC-4** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **PR.AC-5** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.AC-6** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.AC-7** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **Concienciación y capacitación (PR.AT)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **PR.AT-1** | Parcial | 1 | Adaptable | 4 | 3 | Alta |
| **PR.AT-2** | Parcial | 1 | Repetible | 3 | 2 | Baja |
| **PR.AT-3** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.AT-4** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |

| | | | | | | |
|---|---|---|---|---|---|---|
| **PR.AT-5** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **Seguridad de los datos (PR.DS)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **PR.DS-1** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.DS-2** | Parcial | 1 | Adaptable | 4 | 2 | Alta |
| **PR.DS-3** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.DS-4** | Parcial | 1 | Repetible | 3 | 0 | Media |
| **PR.DS-5** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.DS-6** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.DS-7** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.DS-8** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **Procesos y procedimientos de protección de la información (PR.IP)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **PR.IP-1** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.IP-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.IP-3** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.IP-4** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.IP-5** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.IP-6** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.IP-7** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **PR.IP-8** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.IP-9** | Parcial | 1 | Repetible | 3 | 1 | Media |
| **PR.IP-10** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.IP-11** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.IP-12** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **Mantenimiento (PR.MA)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **PR.MA-1** | Riesgo Informado | 2 | Repetible | 3 | 1 | Baja |
| **PR.MA-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **Tecnología de protección (PR.PT)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **PR.PT-1** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.PT-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.PT-3** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.PT-4** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **PR.PT-5** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |

Fuente: elaboración propia

**Función Detectar (DE):** Es la tercera función en el núcleo del marco NIST, se compone de 3 categorías, cada una de las cuales incluye sus propias subcategorías. El análisis de los resultados se presenta en la Tabla 24.

- **Anomalías y Eventos (DE.AE):** Detecta actividad inusual y evalúa su impacto potencial.
- **Monitoreo Continuo de la Seguridad (DE.CM):** Monitorea sistemas y activos para identificar eventos de seguridad y verificar la eficacia de las medidas de protección.
- **Procesos de Detección (DE.DP):** Mantiene procesos aprobados para asegurar la detección de eventos anómalos.

**Tabla 24.** Brechas de la Función Detectar

| **Anomalías y Eventos (DE.AE)** | | | | | | |
|---|---|---|---|---|---|---|
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **DE.AE-1** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **DE.AE-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **DE.AE-3** | Repetible | 3 | Repetible | 3 | 0 | Objetivo alcanzado |
| **DE.AE-4** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **DE.AE-5** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **Monitoreo Continuo de la Seguridad (DE.CM)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **DE.CM-1** | Repetible | 3 | Repetible | 3 | 0 | Objetivo alcanzado |
| **DE.CM-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **DE.CM-3** | Parcial | 1 | Repetible | 3 | 2 | Media |

| | | | | | | |
|---|---|---|---|---|---|---|
| **DE.CM-4** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **DE.CM-5** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **DE.CM-6** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **DE.CM-7** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **DE.CM-8** | Repetible | 3 | Repetible | 3 | 0 | Objetivo alcanzado |
| **Procesos de Detección (DE.DP)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **DE.DP-1** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **DE.DP-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **DE.DP-3** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **DE.DP-4** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **DE.DP-5** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |

Fuente: elaboración propia

**Función Responder (RS):** Es la cuarta función en el núcleo del marco NIST, se compone de 5 categorías, cada una de las cuales incluye sus propias subcategorías. El análisis de los resultados se presenta en la Tabla 25.

- **Planificación de la Respuesta (RS.RP):** Ejecuta y mantiene procesos para responder a incidentes de ciberseguridad.
- **Comunicaciones (RS.CO):** Coordina las actividades de respuesta con partes interesadas internas y externas.
- **Análisis (RS.AN):** Realiza análisis para asegurar una respuesta eficaz y apoyar la recuperación.
- **Mitigación (RS.MI):** Implementa acciones para contener, mitigar, y resolver el incidente.
- **Mejoras (RS.IM):** Mejora la respuesta incorporando lecciones aprendidas de incidentes pasados.

**Tabla 25.** Brechas de la Función Responder

| Planificación de la Respuesta (RS.RP) | | | | | | |
|---|---|---|---|---|---|---|
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **RS.RP-1** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **Comunicaciones (RS.CO)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **RS.CO-1** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **RS.CO-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **RS.CO-3** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **RS.CO-4** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **RS.CO-5** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **Análisis (RS.AN)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **RS.AN-1** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **RS.AN-2** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **RS.AN-3** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **RS.AN-4** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **RS.AN-5** | Parcial | 1 | Repetible | 3 | 3 | Media |
| **Mitigación (RS.MI)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **RS.MI-1** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **RS.MI-2** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **RS.MI-3** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **Mejoras (RS.IM)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **RS.IM-1** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **RS.IM-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |

Fuente: elaboración propia

**Función Recuperar (RC):** Es la última función en el núcleo del marco NIST, se compone de 3 categorías, cada una de las cuales incluye sus propias subcategorías. El análisis de los resultados se presenta en la Tabla 26.

- **Planificación de la Recuperación (RC.RP):** Ejecuta y mantiene procesos para restaurar sistemas o activos tras incidentes de ciberseguridad.
- **Mejoras (RC.IM):** Incorpora lecciones aprendidas para mejorar la planificación y los procesos de recuperación.
- **Comunicaciones (RC.CO):** Coordina las actividades de restauración con partes internas y externas.

**Tabla 26.** Brechas de la Función Recuperar

| **Planificación de la recuperación (RC.RP)** | | | | | | |
|---|---|---|---|---|---|---|
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **RC.RP-1** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **Mejoras (RC.IM)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **RC.IM-1** | Parcial | 1 | Repetible | 3 | 2 | Media |
| **RC.IM-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **Comunicaciones (RC.CO)** | | | | | | |
| **Subcategoría** | **Estado actual** | | **Objetivo deseado** | | **Prioridad** | |
| | **Logro** | **Nivel** | **Logro** | **Nivel** | **Brecha** | **Prioridad** |
| **RC.CO-1** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **RC.CO-2** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |
| **RC.CO-3** | Parcial | 1 | Riesgo Informado | 2 | 1 | Baja |

Fuente: elaboración propia

La Tabla 27 refleja los detalles obtenidos del checklist al comparar el perfil actual con el perfil objetivo, mostrando las brechas identificadas y los valores correspondientes para el CSIRT de Mivilsoft. Los valores se desglosan de la siguiente manera:

- **Función:** Descripción de cada categoría dentro del marco de trabajo NIST.
- **Categoría:** Corresponde a las distintas categorías asociadas a cada función del marco de trabajo NIST.
- **%Logro:** Porcentaje alcanzado según la situación actual de la organización.

- **%Objetivo:** Porcentaje de cumplimiento esperado tras el establecimiento de metas.
- **%Brecha:** Diferencias identificadas entre el logro actual y el objetivo para cada categoría del marco de trabajo NIST.

**Tabla 27.** Comparativa del Logro vs Objetivo en la Implementación del CSIRT

| Función | Categoría | %Logro | %Objetivo | %Brecha |
|---|---|---|---|---|
| **IDENTIFICAR (ID)** | ID.AM | 50.00% | 62.50% | 12.50% |
| | ID.BE | 35.00% | 55.00% | 20.00% |
| | ID.GV | 25.00% | 50.00% | 25.00% |
| | ID.RA | 33.33% | 66.67% | 33.33% |
| | ID.RM | 41.67% | 50.00% | 8.33% |
| | ID.SC | 30.00% | 50.00% | 20.00% |
| **Función ID** | | **35.83%** | **55.69%** | **19.86%** |
| **PROTEGER (PR)** | PR.AC | 25.00% | 57.14% | 32.14% |
| | PR.AT | 25.00% | 65.00% | 40.00% |
| | PR.DS | 25.00% | 59.38% | 34.38% |
| | PR.IP | 25.00% | 54.17% | 29.17% |
| | PR.MA | 37.50% | 62.50% | 25.00% |
| | PR.PT | 25.00% | 50.00% | 25.00% |
| **Función PR** | | **27.08%** | **58.03%** | **30.95%** |
| **DETECTAR (DE)** | DE.AE | 35.00% | 60.00% | 25.00% |
| | DE.CM | 37.50% | 59.38% | 21.88% |
| | DE.DP | 25.00% | 60.00% | 35.00% |
| **Función DE** | | **32.50%** | **59.79%** | **27.29%** |
| **RESPONDER (RS)** | RS.RP | 25.00% | 75.00% | 50.00% |
| | RS.CO | 25.00% | 50.00% | 25.00% |
| | RS.AN | 25.00% | 65.00% | 40.00% |
| | RS.MI | 25.00% | 66.67% | 41.67% |
| | RS.IM | 25.00% | 62.50% | 37.50% |
| **Función RS** | | **25.00%** | **63.83%** | **38.83%** |
| **RECUPERAR (RC)** | RC.RP | 25.00% | 50.00% | 25.00% |
| | RC.IM | 25.00% | 62.50% | 37.50% |
| | RC.CO | 25.00% | 50.00% | 25.00% |
| **Función RC** | | **25.00%** | **54.17%** | **29.17%** |

Fuente: elaboración propia

## Implementar un plan de acción

Para abordar las brechas identificadas, se implementará un plan de acción diseñado para gestionar los riesgos de manera efectiva y satisfacer las necesidades

inmediatas del CSIRT de Mivilsoft, con un enfoque que se llevará a cabo desde 2024 hasta 2028, tal como se detalla en el anexo 2.

### 3.2. Importancia de la implementación del CSIRT

La implementación del CSIRT en Mivilsoft es parte fundamental de su estrategia integral de ciberseguridad. Por tal razón, esta estructura permite responder de manera eficiente ante incidentes y mejorar la protección continua de los activos críticos a través de un enfoque integral en materia de seguridad.

La detección y respuesta tempranas son posibles gracias al CSIRT, que es crucial tanto para prevenir posibles daños como para preservar la continuidad de la empresa en momentos críticos. Además de contar con un protocolo sólido y estructurado de detección y clasificación de incidentes, según lo recomendado por NIST SP 800-61, aumenta la resiliencia de la organización, permitiéndole construir una defensa eficiente contra nuevas amenazas cibernéticas.

Por otra parte, al alinear el CSIRT con los estándares internacionales y las mejores prácticas de la industria, Mivilsoft aumentará su resiliencia, garantizará el cumplimiento de normativas clave, reducirá los riesgos legales y fortalecerá sus defensas frente a amenazas, protegiendo así su reputación.

Además, al evaluar y revisar continuamente las políticas y procedimientos de seguridad, el CSIRT de Mivilsoft promueve un enfoque de mejora continua. Para desarrollar una cultura de ciberseguridad que no solo se ajuste a un entorno dinámico de amenazas globales, sino que también anticipe y mitigue los riesgos, la organización puede utilizar las lecciones aprendidas para modificar sus tácticas y procedimientos en respuesta a las amenazas emergentes.

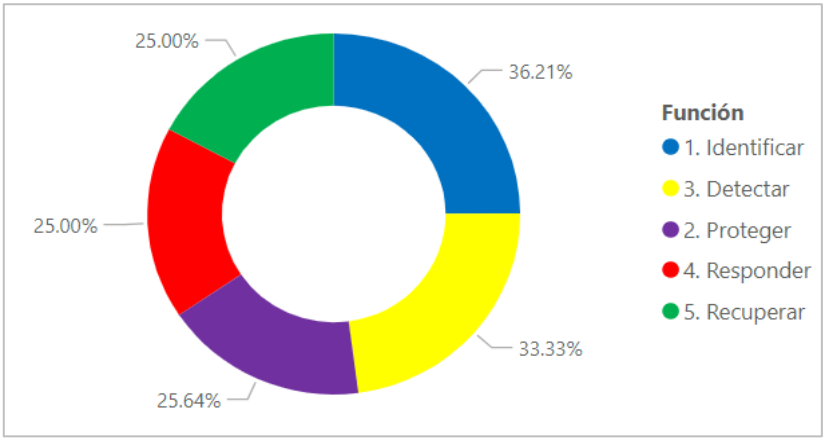
En última instancia, la implementación del CSIRT por parte de Mivilsoft no sólo representa avances en la gestión de incidentes, sino que también fortalece una cultura de seguridad que permite el progreso continuo en la protección de la organización.

## 3.3. Cuadro de mando

La implementación del CSIRT en Mivilsoft es un proceso progresivo que comenzó en 2024 con una evaluación de la situación actual y se prolongará hasta 2028 para alcanzar un nivel óptimo de eficacia y madurez. De acuerdo con la estructura del marco de trabajo NIST, cada año se enfocará en lograr objetivos particulares dentro de cada fase del CSIRT, asegurando que todos los aspectos sean cubiertos de manera exhaustiva para alcanzar el estado deseado.

El estado de implementación inicial de CSIRT de Mivilsoft para 2024 se presenta en la Ilustración 17, donde la empresa ha adoptado el marco de trabajo NIST, alcanzando un progreso promedio del 29,63%.

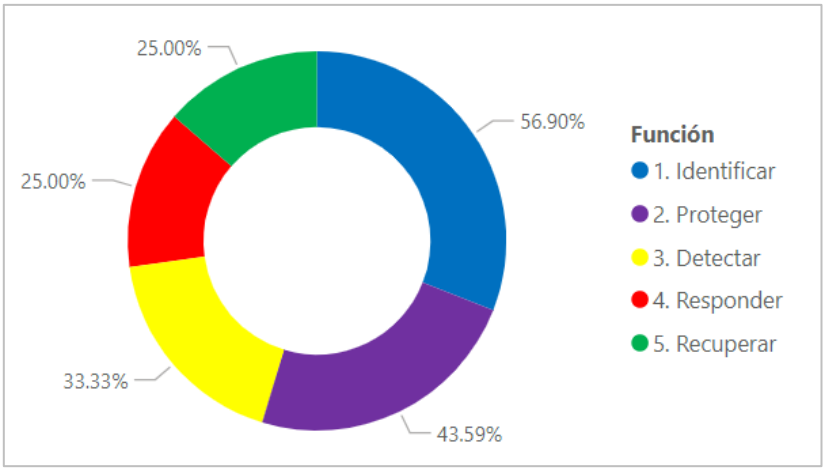
**Ilustración 17.** Implementación del CSIRT de Mivilsoft en 2024




Fuente: elaboración propia

En la Ilustración 18, se muestra el progreso de la implementación del CSIRT en Mivilsoft para 2025, abarcando toda la fase de Identificar y parte de la fase de Proteger. El avance alcanzado es del 41.67%, basado en el estado objetivo que se busca lograr según el marco de trabajo NIST.

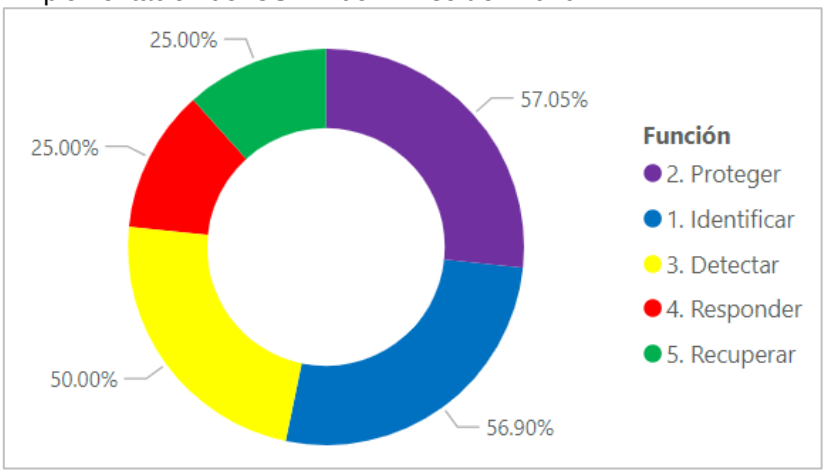
**Ilustración 18.** Implementación del CSIRT de Mivilsoft en 2025




Fuente: elaboración propia

En la Ilustración 19, se muestra el progreso de la implementación del CSIRT en Mivilsoft para 2026, abarcando toda la fase de Proteger y parte de la fase de Detectar. El avance alcanzado es del 49.31%, basado en el estado objetivo que se busca lograr según el marco de trabajo NIST.

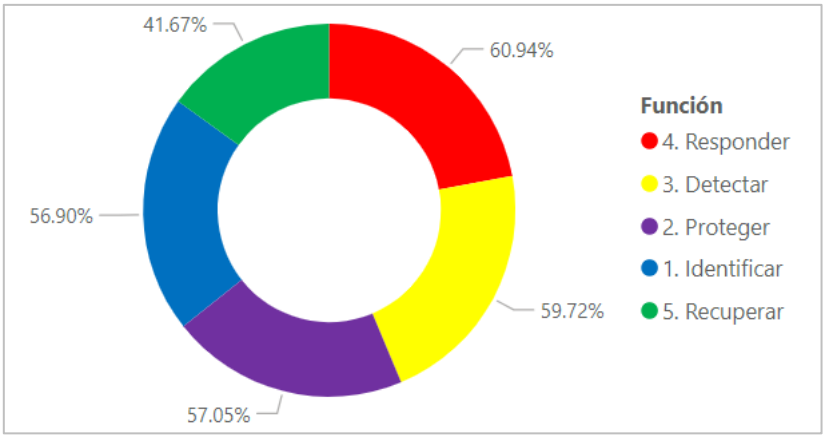
**Ilustración 19.** Implementación del CSIRT de Mivilsoft en 2026




Fuente: elaboración propia

En la Ilustración 20, se muestra el progreso de la implementación del CSIRT en Mivilsoft para 2027, abarcando toda la fase de Detectar y parte de la fase de Recuperar. El avance alcanzado es del 57.18%, basado en el estado objetivo que se busca lograr según el marco de trabajo NIST.

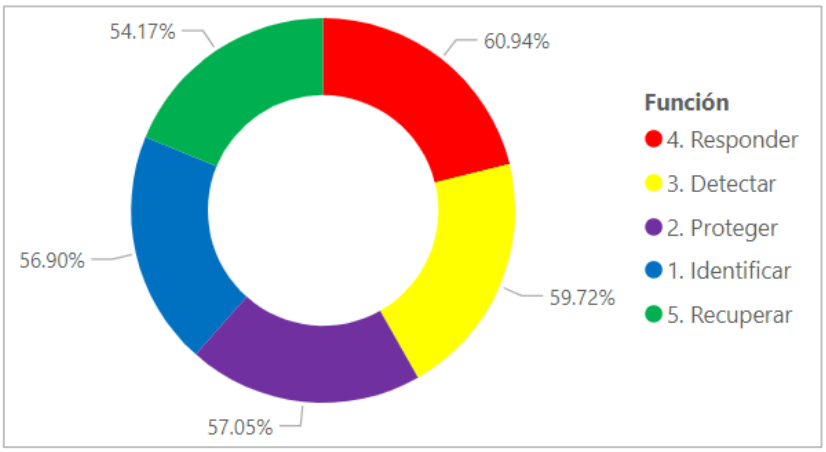
**Ilustración 20.** Implementación del CSIRT de Mivilsoft en 2027




Fuente: elaboración propia

En la Ilustración 21, se muestra el progreso de la implementación del CSIRT en Mivilsoft para 2028, abarcando toda la fase Recuperar. El avance alcanzado es del 57.87%, basado en el estado objetivo que se busca lograr según el marco de trabajo NIST.

**Ilustración 21.** Implementación del CSIRT de Mivilsoft en 2028

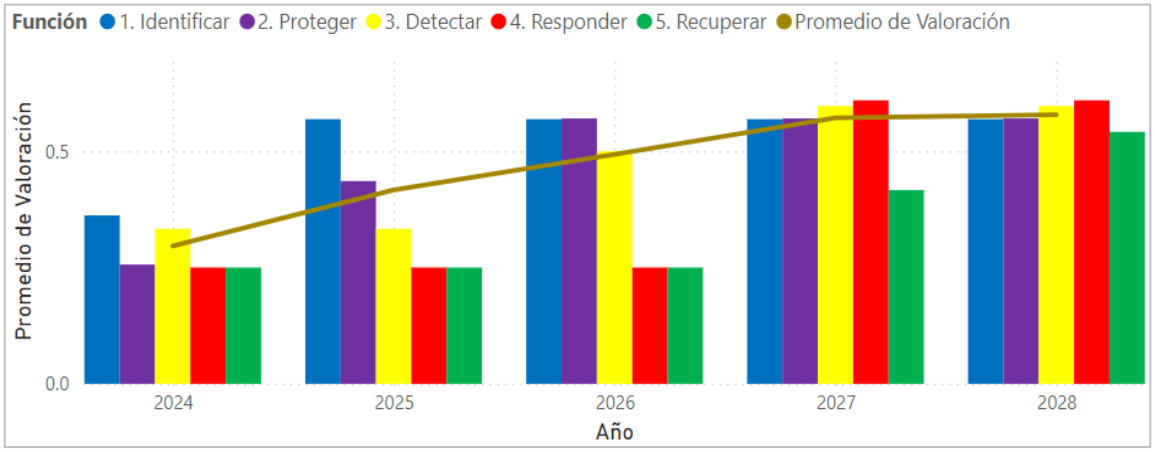



Fuente: elaboración propia

En la Ilustración 22, muestra la evolución acumulada de la implementación del CSIRT en Mivilsoft, abarcando todas las fases identificadas por colores desde 2024 hasta 2028. Refleja el progreso general hacia el objetivo de madurez, destacando las áreas que han recibido mayor atención y los logros alcanzados hasta el momento, con el propósito de alcanzar el objetivo deseado, conforme al marco de trabajo NIST.

A partir del análisis gráfico realizado, se concluyó que el principal objetivo a alcanzar de forma global para todas las fases es un progreso del 57.87%, necesario para cumplir con los requerimientos establecidos por la organización.

**Ilustración 22.** Evolución de la Implementación del CSIRT en Mivilsoft




Fuente: elaboración propia

## CONCLUSIONES

- La implementación del CSIRT en Mivilsoft, siguiendo el marco de trabajo NIST, ha fortalecido la capacidad de la empresa para identificar, gestionar y mitigar los riesgos de ciberseguridad, demostrando avances significativos en la formalización de los procedimientos de seguridad comparando el perfil actual y deseado.

- El análisis de casos exitosos de CSIRT en Latinoamérica ha resaltado la importancia de la concienciación y la formación de las comunidades para prevenir y abordar incidentes de ciberseguridad. De igual manera, ha ofrecido un modelo de mejores prácticas que enfatiza la utilidad de metodologías estructuradas, como el marco NIST, para mejorar la respuesta ante incidentes y gestionar los riesgos de manera más efectiva.

- La elaboración de un plan de implementación del CSIRT en Mivilsoft, basado en el marco de trabajo NIST, ha establecido directrices claras para una gestión eficaz de los incidentes, alineando el CSIRT con las mejores prácticas internacionales y con los objetivos estratégicos de seguridad de la empresa.

- La definición de protocolos internos para el CSIRT de Mivilsoft, alineados con sus directrices, ha sido un paso crucial para fortalecer la capacidad de respuesta ante incidentes de seguridad. Al establecer una base sólida en la gestión de incidentes, Mivilsoft refuerza su resiliencia frente a ciberamenazas, lo que le permite actuar de manera coherente y efectiva ante cualquier tipo de amenaza, asegurando la protección continua de sus activos tecnológicos.

- Los resultados del proyecto han evidenciado que el CSIRT es flexible y puede ajustarse a las futuras necesidades de Mivilsoft, permitiendo la expansión de sus capacidades de gestión de incidentes y protección de activos a medida que la empresa evoluciona. Este enfoque asegura que el

modelo implementado sea sostenible a largo plazo y pueda adaptarse para enfrentar las nuevas amenazas de ciberseguridad que puedan surgir en el futuro.

## RECOMENDACIONES

- Se recomienda que Mivilsoft establezca y ponga en marcha procesos claros para identificar, analizar y responder a incidentes, con el objetivo de reforzar la estructura y funcionamiento del CSIRT. Esto incluye documentar de manera detallada todos los procedimientos y llevar a cabo pruebas periódicas para asegurarse de que sean efectivos.

- Se recomienda crear un programa de capacitación constante para el equipo del CSIRT y otros empleados clave, con el fin de mejorar sus habilidades para prevenir, detectar y responder de manera eficiente cualquier amenaza cibernética.

- Se recomienda definir métricas claras y concretas para medir la efectividad de las respuestas a incidentes y el desempeño del CSIRT. Contar con estos indicadores facilitará un mejor análisis del impacto de las acciones de la organización en materia de ciberseguridad, actualmente la falta de datos medibles complica esta evaluación.

- Se recomienda que el CSIRT de Mivilsoft siga de cerca el plan de acción establecido y avance paso a paso en cada una de las fases del marco de trabajo NIST. De esta manera, se podrá alcanzar el objetivo deseado y fortalecer gradualmente la seguridad cibernética en toda la organización.

## BIBLIOGRAFÍA

Ahmed, D., & HamaAmin, R. (2022). Multi-layered firewall to mitigate the impact of Distributed Denial of Service on a network. *Passer Journal of Basic and Applied Sciences*, *4*(Special issue), 51-62. https://doi.org/10.24271/psr.2022.160803

Azeez, N. A., Bada, T. M., Misra, S., Adewumi, A., Van der Vyver, C., & Ahuja, R. (2020). Intrusion Detection and Prevention Systems: An Updated Review. En N. Sharma, A. Chakrabarti, & V. E. Balas (Eds.), *Data Management, Analytics and Innovation* (pp. 685-696). Springer. https://doi.org/10.1007/978-981-32-9949-8_48

CERT.br. (2024a). *CERT.br—Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil*. https://www.cert.br/

CERT.br, S. (2024b). *CERT.br—Estatísticas*. CERT.br - Estatísticas. https://stats.cert.br/

CSIRT.CZ. (2024a). *CSIRT.CZ - About us*. https://csirt.cz/en/about-us/

CSIRT.CZ, S. (2024b). *CSIRT.CZ - Statistics*. https://csirt.cz/en/about-us/statistics/

Del Pozo Barrezueta, H. (2021). *Política Nacional de Ciberseguridad* (Registro Oficial - Quinto Suplemento Nº 479 479). MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN. http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoicm8iLCJ1dWlkIjoiMGY0ZGMxYWEtODI3Ni00MTljLTg3MmQtMmM4NTEwMzE4YTM3LnBkZiJ9

EcuCERT. (2024). *EcuCERT de Arcotel – Centro de Respuesta a Incidentes Informáticos de la ARCOTEL*. https://www.ecucert.gob.ec/

ENISA. (2020, diciembre 10). *How to set up CSIRT and SOC* [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

Espín, F. V. (2021). Guidelines and Their Challenges in Implementing CSIRT in Ecuador. En M. Botto-Tobar, O. S. Gómez, R. Rosero Miranda, & A. Díaz Cadena (Eds.), *Advances in Emerging Trends and Technologies* (pp. 239-251). Springer International Publishing. https://doi.org/10.1007/978-3-030-63665-4_19

Frayssinet Delgado, M., Esenarro, D., Juárez Regalado, F. F., & Díaz Reátegui, M. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. *3 c TIC: Cuadernos de Desarrollo Aplicados a Las TIC*, *10*(2), 123-141.

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. *Business & Information Systems Engineering*. https://doi.org/10.1007/s12599-023-00830-x

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, *21*(14), 4759. https://doi.org/10.3390/s21144759

Halim, Y., ElDeeb, M., Abbas, Z., Vlachos, P., & Journal, M.-M. (2023). THE IMPACT OF POLITICAL CORRECTNESS ON BRAND IMAGE AND PURCHASE INTENTIONS: AN EXPLORATORY CASE STUDY OF BIRELL, EGYPT. *MSA-Management Sciences Journal*, *2*, 1-37.

Hauptman, A. I., Schelble, B. G., McNeese, N. J., & Madathil, K. C. (2023). Adapt and overcome: Perceptions of adaptive autonomous agents for human-AI teaming. *Computers in Human Behavior*, *138*, 107451. https://doi.org/10.1016/j.chb.2022.107451

Idammi, Y. (2022). *Research Methodology: An Introduction for Undergraduates - FLASH UIZ (2022–23)*. https://www.academia.edu/91592650/Research_Methodology_An_Introduction_for_Undergraduates_FLASH_UIZ_2022_23_

Kalonji, K. (2022). *Capabilities and Use of Cortex as part of the DYNAMO project* [fi=AMK-opinnäytetyö|sv=YH-examensarbete|en=Bachelor's thesis|]. http://www.theseus.fi/handle/10024/751207

Knerler, K., Parker, I., & Zimmerman, C. (2022). 11 Strategies of a World-Class Cybersecurity Operations Center. *Produced in Conjunction with MITRE Strategic Communications*, 452.

Mendoza, S. H., & Avila, D. D. (2020). Técnicas e instrumentos de recolección de datos. *Boletín Científico de las Ciencias Económico Administrativas del ICEA*, *9*(17), Article 17. https://doi.org/10.29057/icea.v9i17.6019

Mohd Kassim, S. R. B., Li, S., & Arief, B. (2022). Incident Response Practices Across National CSIRTs: Results from an Online Survey. *OIC-CERT Journal of Cyber Security*, *4*(1), Article 1.

Mohd Kassim, S. R. B., Li, S., & Arief, B. (2023). Understanding How National CSIRTs Evaluate Cyber Incident Response Tools and Data: Findings from Focus Group Discussions. *Digital Threats: Research and Practice*, *4*(3), 1-24. https://doi.org/10.1145/3609230

Nish, A., Naumaan, S., & Muir, J. (2020). *Enduring Cyber Threats and Emerging Challenges to the Financial Sector* (Enduring Cyber Threats and Emerging Challenges to the Financial Sector). Carnegie Endowment for International Peace. https://www.jstor.org/stable/resrep27701.1

NIST, C. (2023). CSF 1.1 Quick Start Guide. *NIST*. https://www.nist.gov/cyberframework/csf-11-quick-start-guide

Perwej, Dr. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, Dr. N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, *9*(12), 669-710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Saraiva, M., & Mateus-Coelho, N. (2022). CyberSoc Framework a Systematic Review of the State-of-Art. *Procedia Computer Science*, *204*, 961-972. https://doi.org/10.1016/j.procs.2022.08.117

Sidharth, G. (2023). *Research Designs for Contemporary Social Science Research: An Overview*.

Singh, C., Thakkar, R., & Warraich, J. (2023). IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. *European Journal of Engineering and Technology Research*, *8*(4), Article 4. https://doi.org/10.24018/ejeng.2023.8.4.3074

Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, *215*, 483-487. https://doi.org/10.1016/j.procs.2022.12.050

Thapa, S., & Mailewa, A. (2020, abril 3). *The role of intrusion detection/prevention systems in modern computer networks: A review*.

Torres-Chavez, L. J. (2021). Metodología cualitativa como herramienta en la investigación de la calidad de vida. *Journal de Ciencias Sociales*, 171-175. https://doi.org/10.18682/jcs.vi16.4601

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security*, *23*(3), 1695-1719. https://doi.org/10.1007/s10207-023-00811-x

Van der Heide, M. (2020). *Establishing a CSIRT*. Tailand Computer Emergency Respose Team. https://socsirt.cedia.edu.ec/docs/Establishing-a-CSIRT-v1.3-es_EC.pdf

Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, *9*(4), 1-22. https://doi.org/10.14763/2020.4.1533

Villegas-Ch., W., Ortiz-Garces, I., & Sánchez-Viteri, S. (2021). Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus. *Computers*, *10*(8), Article 8. https://doi.org/10.3390/computers10080102

Zuleika, P., & Siswo, L. (2022). Cross-Sectional Study as Research Design in Medicine. *Archives of The Medicine and Case Reports*, *3*, 256-259. https://doi.org/10.37275/amcr.v3i2.193

# ANEXOS

### Anexo 1. Encuesta sobre la situación actual de la ciberseguridad en Mivilsoft

**Instrucciones:** Por favor, responda las siguientes preguntas de acuerdo con su criterio. Su participación es importante para evaluar la preparación y la situación actual de Mivilsoft en relación con la gestión de incidentes de seguridad y la futura implementación del CSIRT. Agradecemos su tiempo y colaboración.

**Introducción:** La implementación de un CSIRT en Mivilsoft es esencial para mejorar la gestión de la ciberseguridad y la respuesta a incidentes. Esta encuesta tiene como objetivo recopilar información sobre la percepción y el conocimiento del personal respecto a la ciberseguridad dentro de la organización. Sus respuestas ayudarán a identificar las áreas que necesitan atención y a definir mejor las estrategias a implementar.

**Objetivo:** Evaluar la situación actual de la conciencia y gestión de incidentes de seguridad en Mivilsoft antes de la implementación completa del CSIRT.

¿Conoce usted la función y los objetivos del CSIRT que se está implementando en Mivilsoft?

- Sí
- No
- No estoy seguro

¿Ha recibido capacitación sobre la gestión de incidentes de seguridad?

- Sí
- No
- Si la respuesta es sí, ¿cuándo fue la última capacitación?

¿Considera que la infraestructura actual de ciberseguridad en Mivilsoft es adecuada para gestionar incidentes de seguridad?

- Muy adecuada
- Adecuada
- Poco adecuada
- No adecuada

¿Cómo calificaría la comunicación sobre ciberseguridad en Mivilsoft?

- Muy efectiva
- Efectiva
- Poco efectiva
- No efectiva

¿Está familiarizado con los procedimientos de respuesta a incidentes que se están desarrollando?

- Sí
- No
- No estoy seguro

¿Cuáles cree que son las principales amenazas a la ciberseguridad que enfrenta Mivilsoft?

¿Se siente preparado para actuar en caso de un incidente de seguridad?

- Muy preparado
- Preparado
- Poco preparado
- No preparado

¿Cuál es su nivel de confianza en el equipo de IT para manejar incidentes de seguridad?

- Muy confiado
- Confiado

- Poco confiado
- No confiado

¿Considera que se necesita más capacitación en ciberseguridad para el personal?

- Sí
- No
- No estoy seguro

¿Está dispuesto a colaborar y participar en el proceso de implementación del CSIRT?

- Sí
- No
- Tal vez

¡Gracias por su participación! Su opinión es fundamental para ayudarnos a entender la situación actual de la ciberseguridad en Mivilsoft.

**Anexo 2. Plan de Acción del CSRIT de Mivilsoft**

| PLAN DE ACCIÓN DEL CSIRT DE MIVILSOFT (2024 - 2028) | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Objetivo estratégico** | Fortalecer la postura de ciberseguridad de Mivilsoft | | | | | | |
| **Estrategia** | Estructurar y formalizar políticas de ciberseguridad para proteger los activos críticos de Mivilsoft | | | | | | |
| **Tipo de plan** | Plan de Mejora | | | | | | |
| **Nombre del plan** | Plan de mejora continua basado en las brechas identificadas durante la implementación del CSIRT de Mivilsoft conforme al marco de trabajo NIST | | | | | | |
| **Objetivo del plan** | Implementar los mejores estándares internacionales en ciberseguridad para fortalecer los controles del CSIRT de Mivilsoft y alcanzar un nivel de madurez óptimo, abordando las brechas según su criticidad | | | | | | |
| **Insumo que sustenta la elaboración del plan** | Marco de trabajo NIST y resultados del análisis de brechas del CSIRT de Mivilsoft | | | | | | |
| **Indicador de medición del plan de acción** | Cumplimiento de objetivos de ciberseguridad y reducción de brechas identificadas | | | | | | |
| **Líder del plan de acción** | Coordinador del CSIRT | | | | | | |
| **Unidad responsable** | Departamento de Desarrollo de Software | | | | | | |
| **Nº** | **Actividad** | **Descripción** | **Plazo** | **Responsable** | **Recursos** | **Resultado Esperado** | **Evidencia** |
| **1** | Gestión de activos | Identificar y administrar los activos de la organización (datos, personal, dispositivos, sistemas e instalaciones) de forma coherente con su importancia relativa para los objetivos y estrategia de riesgos | 15 días | Coordinador del CSIRT | Consultores externos en seguridad | Mejora en la identificación y gestión de activos críticos | ID.AM |
| **2** | Entorno empresarial | Realizar un análisis de la misión, objetivos, partes interesadas y actividades de la organización para informar las decisiones de gestión de | 25 días | Coordinador del CSIRT | Consultores externos en estrategia empresarial | Priorización efectiva de los objetivos y actividades organizacionales para la gestión de ciberseguridad | ID.BE |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | riesgos de seguridad cibernética. | | | | | |
| **3** | Gobernanza | Establecer políticas y procedimientos claros para administrar los requisitos regulatorios, legales, de riesgo y operativos de la organización | 28 días | Gestor de Seguridad y Confianza Digital | Asesoría legal y consultores en gestión de riesgos | Creación de un marco de gobernanza para la seguridad cibernética | ID.GV |
| **4** | Evaluación de riesgos | Realizar una evaluación integral de los riesgos de seguridad cibernética para las operaciones, activos y reputación de la organización | 52 días | Gestor de Incidentes | Herramientas de evaluación de riesgos | Identificación y comprensión detallada de los riesgos cibernéticos | ID.RA |
| **5** | Estrategia de gestión de riesgos | Definir y establecer las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización para respaldar las decisiones operacionales | 20 días | Coordinador del CSIRT | Asesoría en gestión de riesgos operacionales | Plan de gestión de riesgos estructurado y alineado con la estrategia organizacional | ID.RM |
| **6** | Gestión del riesgo de la cadena de suministro | Establecer procesos para identificar, evaluar y gestionar los riesgos asociados con la cadena de suministro, asegurando la resiliencia ante amenazas externas | 50 días | Gestor de Infraestructuras Digitales | Consultores en ciberseguridad y cadena de suministro | Implementación de un proceso formal para la gestión de riesgos de la cadena de suministro | ID.SC |
| **7** | Gestión de identidad, autenticación y control de acceso | Implementar un sistema de gestión de acceso para asegurar que solo los usuarios, procesos y dispositivos autorizados tengan acceso a los activos físicos y lógicos, según el riesgo evaluado | 122 días | Gestor de Infraestructuras Digitales | Consultores en gestión de acceso y herramientas de autenticación | Reducción del acceso no autorizado y mejora en el control de acceso | PR.AC |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **8** | Concienciación y capacitación | Desarrollar y ejecutar un programa continuo de capacitación en ciberseguridad para el personal y socios, alineado con las políticas y procedimientos establecidos | 19 días | Coordinador del CSIRT | Consultores en ciberseguridad y capacitación | Mejorar el nivel de conciencia y habilidades de seguridad cibernética del personal | PR.AT |
| **9** | Seguridad de los datos | Implementar políticas y procedimientos para gestionar la protección de la confidencialidad, integridad y disponibilidad de los datos según la estrategia de riesgo de la organización | 74 días | Gestor de Seguridad y Confianza Digital | Consultores en protección de datos | Garantizar la protección y gestión adecuada de los datos críticos | PR.DS |
| **10** | Procesos y procedimientos de protección de la información | Crear y mantener políticas de seguridad, procesos y procedimientos para gestionar la protección de los sistemas de información y los activos críticos de la organización | 99 días | Coordinador del CSIRT | Asesoría en políticas de seguridad y procesos de protección | Definir y estructurar procesos operacionales efectivos en protección de la información | PR.IP |
| **11** | Mantenimiento | Establecer y ejecutar procedimientos de mantenimiento regular de los sistemas y componentes críticos de la infraestructura de TI, conforme a las políticas de seguridad | 15 días | Gestor de Infraestructuras Digitales | Herramientas de gestión de mantenimiento | Mantenimiento efectivo y proactivo de los componentes del sistema | PR.MA |
| **12** | Tecnología de protección | Gestionar e implementar soluciones técnicas de seguridad para asegurar la protección continua y capacidad de recuperación de los sistemas y activos clave | 39 días | Gestor de Infraestructuras Digitales | Consultores en soluciones de protección tecnológica | Refuerzo de la protección técnica y capacidad de respuesta ante incidentes | PR.PT |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **13** | Anomalías y Eventos | Desarrollar un sistema para detectar actividad anómala y evaluar el impacto potencial de los eventos de ciberseguridad | 46 días | Coordinador del CSIRT | Consultores en análisis de eventos y software de monitoreo | Detección temprana de eventos anómalos y evaluación precisa del impacto | DE.AE |
| **14** | Monitoreo Continuo de la Seguridad | Implementar un sistema de monitoreo continuo para identificar eventos de seguridad y verificar la efectividad de las medidas de protección | 70 días | Gestor de Infraestructuras Digitales | Herramientas de monitoreo en tiempo real y consultores en ciberseguridad | Mejora en la visibilidad y efectividad de la protección cibernética | DE.CM |
| **15** | Procesos de Detección | Establecer procesos y procedimientos para la detección de eventos anómalos y garantizar que todos los eventos sean conocidos y gestionados | 56 días | Coordinador del CSIRT | Asesoría en procesos de detección y tecnologías de seguridad | Mejorar los tiempos de respuesta ante eventos anómalos | DE.DP |
| **16** | Planificación de la Respuesta | Desarrollar y mantener procedimientos de respuesta para garantizar la reacción rápida y efectiva a incidentes de ciberseguridad | 20 días | Gestor de Seguridad y Confianza Digital | Consultores en gestión de incidentes y procedimientos de respuesta | Asegurar una respuesta eficiente ante incidentes | RS.RP |
| **17** | Comunicaciones | Coordinar las actividades de respuesta con partes interesadas internas y externas, incluyendo organismos encargados de hacer cumplir la ley | 31 días | Coordinador del CSIRT | Herramientas de comunicación y consultores en gestión de crisis | Mejora en la coordinación y respuesta ante incidentes | RS.CO |
| **18** | Análisis | Implementar procesos para el análisis de incidentes, apoyando la toma de decisiones en la respuesta y recuperación | 76 días | Gestor de Infraestructuras Digitales | Software de análisis forense y expertos en ciberseguridad | Respuestas más efectivas y fundamentadas ante incidentes | RS.AN |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **19** | Mitigación | Desarrollar estrategias para evitar la expansión de incidentes y mitigar sus efectos, asegurando la rápida resolución del evento | 55 días | Coordinador del CSIRT | Consultores en mitigación y protocolos de respuesta rápida | Reducción del impacto de los incidentes y su propagación | RS.MI |
| **20** | Mejoras | Mejorar continuamente las actividades de respuesta incorporando lecciones aprendidas de eventos pasados y actuales | 40 días | Coordinador del CSIRT | Herramientas para gestión de lecciones aprendidas y análisis de incidentes previos | Incremento en la eficacia de las respuestas y prevención | RS.IM |
| **21** | Planificación de la recuperación | Establecer y mantener procedimientos para la recuperación de los sistemas y activos afectados por incidentes de ciberseguridad | 20 días | Gestor de Infraestructuras Digitales | Herramientas de recuperación y expertos en gestión de desastres | Restablecimiento rápido de sistemas y activos afectados | RC.RP |
| **22** | Mejoras | Incorporar lecciones aprendidas en los procedimientos de recuperación para optimizar la respuesta ante futuros incidentes | 20 días | Coordinador del CSIRT | Consultores en mejora continua y análisis post-incidente | Mejoras en los procesos de recuperación a largo plazo | RC.IM |
| **23** | Comunicaciones | Coordinar las actividades de restauración con partes internas y externas, incluyendo proveedores, CSIRT, y otras organizaciones relevantes | 15 días | Gestor de Infraestructuras Digitales | Herramientas de comunicación y coordinación con equipos externos | Coordinación fluida durante la restauración y recuperación | RC.CO |

Fuente: elaboración propia