**CREACIÓN DE UN CSIRT PARA LAS**

**FUERZAS MILITARES DE COLOMBIA**

**MY RAMIRO ALVARADO REYES**

**MY. RAFAEL AUGUSTO GIRALDO RESTREPO**

**MY. RAFAEL ALBERTO MARTINEZ MARTINEZ**

**MY. JAIME ALBERTO PATIÑO ROMERO**

### 1. Identificar las partes interesadas y participantes

**Título:** Identificación de Partes Interesadas y Participantes en el CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Participantes Internos:**
   * **Ejército:**
     + Jefe de Seguridad: Coronel Juan Pérez
     + Personal de TI y Ciberseguridad: Mayor Luis Gómez
     + Oficial de Enlace: Capitán Daniel García
   * **Armada:**
     + Jefa de Seguridad: Capitán María Rodríguez
     + Personal de TI y Ciberseguridad: Teniente Ana Torres
     + Oficial de Enlace: Teniente Laura Sánchez
   * **Fuerza Aérea:**
     + Jefe de Seguridad: General Carlos Martínez
     + Personal de TI y Ciberseguridad: Teniente Coronel Jorge Díaz
     + Oficial de Enlace: Mayor Pedro Ramírez
2. **Participantes Externos:**
   * **Agencia de Inteligencia Nacional:** Director Álvaro Mendoza
   * **Empresas Proveedoras de Soluciones de Seguridad:**
     + Empresa A: CEO Ricardo López
     + Empresa B: CTO Sofía Méndez
   * **Ministerio de Defensa:** Secretario de Defensa, General Alejandro Suárez.
3. **Coordinación y Comunicación:**
   * **Canales de Comunicación Seguros:**
     + VPN
     + Correo electrónico cifrado
     + Reuniones semanales vía videoconferencia
   * **Puntos de Contacto:**
     + Lista de correos electrónicos y teléfonos de los participantes mencionados
   * **Tabla de Contactos:**

| **PARTICIPANTE** | **ROL** | **CONTACTO** |
| --- | --- | --- |
| Coronel Juan Pérez | Jefe de Seguridad (Ejército) | juan.perez@ejercito.mil.co |
| Mayor Luis Gómez | Personal de TI (Ejército) | luis.gomez@ejercito.mil.co |
| Capitán Daniel García | Oficial de Enlace (Ejército) | daniel.garcia@ejercito.mil.co |
| Capitán María Rodríguez | Jefa de Seguridad (Armada) | maria.rodriguez@armada.mil.co |
| Teniente Ana Torres | Personal de TI (Armada) | ana.torres@armada.mil.co |
| Teniente Laura Sánchez | Oficial de Enlace (Armada) | laura.sanchez@armada.mil.co |
| General Carlos Martínez | Jefe de Seguridad (Fuerza Aérea) | carlos.martinez@aerea.mil.co |
| Teniente Coronel Jorge Díaz | Personal de TI (Fuerza Aérea) | jorge.diaz@aerea.mil.co |
| Mayor Pedro Ramírez | Oficial de Enlace (Fuerza Aérea) | pedro.ramirez@aerea.mil.co |
| Álvaro Mendoza | Director de Agencia de Inteligencia Nacional | alvaro.mendoza@inteligencia.gov.co |
| Ricardo López | CEO de Empresa A | ricardo.lopez@empresaA.com |
| Sofía Méndez | CTO de Empresa B | sofia.mendez@empresaB.com |
| General Alejandro Suárez | Secretario de Defensa | alejandro.suarez@defensa.gov.co |

### 2. Obtener el apoyo de la gestión y patrocinio

**Título:** Estrategia de Apoyo y Patrocinio para el CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Patrocinador Ejecutivo:**
   * **General Alejandro Suárez, Secretario de Defensa**
2. **Caso de Negocio:**
   * **Beneficios del CSIRT:**
     + **Reducción del tiempo de respuesta a incidentes cibernéticos en un 50%**: Mediante la creación de procedimientos estandarizados y un equipo dedicado.
     + **Mejora de la protección de la infraestructura crítica militar**: Implementación de medidas proactivas y reactivas para mitigar ataques cibernéticos.
     + **Prevención de pérdidas de datos sensibles**: Uso de tecnologías avanzadas de cifrado y monitoreo continuo.
   * **Ejemplos de incidentes pasados:**
     + **Ataque DDoS a sistemas de comunicación en 2022**: Impacto en la coordinación de operaciones durante 48 horas.
     + **Infiltración de malware en sistemas de control de armas en 2023**: Riesgo de acceso no autorizado a información clasificada.
3. **Comunicación con la Gestión:**
   * **Reuniones Mensuales con la Alta Dirección:**
     + **Objetivo:** Presentar avances y necesidades del CSIRT.
     + **Agenda:** Actualización de incidentes, estado de implementación, requerimientos de recursos.
   * **Solicitud de Recursos:**
     + **Presupuesto Anual:** $500.000 USD
     + **Contratación:** 5 especialistas en ciberseguridad
     + **Adquisición de Herramientas:** Sistemas de detección y análisis de amenazas

**Gráfico de Beneficios:**

### 3. Desarrollar un plan de proyecto CSIRT

**Título:** Plan de Proyecto para la Creación del CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Equipo de Proyecto:**
   * **Jefe de Proyecto:** Mayor Luis Gómez (Ejército)
   * **Equipo:**
     + Teniente Ana Torres (Armada)
     + Teniente Coronel Jorge Díaz (Fuerza Aérea)
     + Capitán Daniel García (Ejército)
     + Teniente Laura Sánchez (Armada)
     + Mayor Pedro Ramírez (Fuerza Aérea)
2. **Gestión del Proyecto:**
   * **Hitos del Proyecto:**
     + **Formación del equipo:** 1 mes
     + **Recolección de información:** 2 meses
     + **Desarrollo de políticas y procedimientos:** 3 meses
     + **Implementación inicial:** 6 meses
     + **Evaluación y ajustes:** 1 mes

**Cronograma del Proyecto:**

Hito | Duración | Fecha de Inicio | Fecha de Fin

--------------------------------------------------|----------|-----------------|--------------

Formación del equipo | 1 mes | 1/9/2024 | 30/9/2024

Recolección de información | 2 meses | 1/10/2024 | 30/11/2024

Desarrollo de políticas y procedimientos | 3 meses | 1/12/2024 | 28/2/2025

Implementación inicial | 6 meses | 1/3/2025 | 31/8/2025

Evaluación y ajustes | 1 mes | 1/9/2025 | 30/9/2025

**Herramientas de Gestión:**

* **Microsoft Project:** Para seguimiento de tareas e hitos
* **Trello:** Para la gestión de tareas diarias y colaboración del equipo

### 4. Reunir información

**Título:** Recolección de Información para el CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Necesidades y Requerimientos:**
   * **Encuestas a Unidades Militares:**
     + **Objetivo:** Identificar los incidentes de seguridad más comunes y evaluar la infraestructura actual.
     + **Metodología:** Encuestas en línea y entrevistas con personal clave.

**Ejemplo de Encuesta:**

**Encuesta sobre Incidentes de Seguridad**

1. ¿Cuáles son los incidentes de seguridad más frecuentes en su unidad?

- [ ] Phishing

- [ ] Malware

- [ ] Ataques DDoS

- [ ] Acceso no autorizado

- [ ] Otros: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. ¿Con qué frecuencia ocurren estos incidentes?

- [ ] Diario

- [ ] Semanal

- [ ] Mensual

- [ ] Ocasionalmente

3. ¿Qué medidas de seguridad están implementadas actualmente en su unidad?

- [ ] Antivirus/Antimalware

- [ ] Firewalls

- [ ] Sistemas de detección de intrusos

- [ ] Otros: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. ¿Considera que las medidas actuales son suficientes?

- [ ] Sí

- [ ] No

- [ ] No estoy seguro

5. ¿Qué mejoras recomendaría para aumentar la seguridad en su unidad?

- \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + **Reuniones con Personal de TI:**
    - **Objetivo:** Identificar vulnerabilidades actuales y capacidades existentes.
    - **Metodología:** Talleres y sesiones de brainstorming.

1. **Cuestiones Legales y Políticas:**
   * **Consultas con el Departamento Legal del Ministerio de Defensa:**
     + **Objetivo:** Entender las normativas de ciberseguridad aplicables y requisitos de cumplimiento.
     + **Metodología:** Revisión de documentos legales y reuniones con asesores legales.
   * **Documentación de Políticas Internas:**
     + **Objetivo:** Compilar y revisar todas las políticas relacionadas con la gestión de incidentes y ciberseguridad.
     + **Metodología:** Análisis de documentos y entrevistas con responsables de política.

**Tabla de Necesidades y Requerimientos:**

| **Unidad** | **Incidentes Comunes** | **Medidas Actuales** | **Mejoras Recomendadas** |
| --- | --- | --- | --- |
| Unidad de Operaciones | Phishing, Malware | Antivirus, Firewalls | Actualización de software, capacitación |
| Centro de Mando y Control | DDoS, Acceso no autorizado | IDS, Firewalls | Mejora de firewalls, sistemas de monitoreo avanzados |
| Departamento de Logística | Malware, Phishing | Antivirus, IDS | Integración de sistemas, entrenamiento especializado |

### 5. Identificar la circunscripción del CSIRT

**Título:** Definición de la Circunscripción del CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Grupo de Servicio:**
   * **Unidades de Operaciones Especiales:** Proteger la información y operaciones críticas.
   * **Centros de Mando y Control:** Asegurar la continuidad y seguridad de las comunicaciones.
   * **Departamentos de Logística:** Proteger la integridad y disponibilidad de los sistemas de logística.
2. **Socios Estratégicos:**
   * **Centro Nacional de Inteligencia (CNI):**
     + **Objetivo:** Intercambio de información y coordinación en la respuesta a incidentes.
     + **Metodología:** Acuerdos de colaboración y reuniones periódicas.
   * **Agencia de Seguridad Nacional (ASN):**
     + **Objetivo:** Apoyo en la identificación y mitigación de amenazas cibernéticas.
     + **Metodología:** Compartir inteligencia de amenazas y realizar ejercicios conjuntos.

### 6. Definir la misión del CSIRT

**Título:** Misión y Objetivos del CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Misión:**
   * Proveer una respuesta coordinada y efectiva a incidentes de seguridad informática, protegiendo la infraestructura crítica y la información sensible de las Fuerzas Militares de Colombia.
2. **Objetivos:**
   * **Reducir el impacto de incidentes cibernéticos:** Implementar medidas proactivas y reactivas para mitigar los efectos de los incidentes.
   * **Fortalecer las capacidades de defensa cibernética:** Capacitación continua y uso de tecnologías avanzadas.
   * **Promover la adopción de mejores prácticas de seguridad:** Difusión de guías y formación en ciberseguridad.

### 7. Asegurar el financiamiento para las operaciones del CSIRT

**Título:** Plan de Financiamiento para el CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Recursos Iniciales:**
   * **Personal:**
     + Contratación de 5 especialistas en ciberseguridad
   * **Infraestructura:**
     + 10 servidores dedicados
     + Sistemas de detección de intrusos
     + Software de análisis de amenazas
   * **Capacitación:**
     + Cursos avanzados en ciberseguridad y análisis forense
2. **Modelo de Financiamiento:**
   * **Presupuesto Específico del Ministerio de Defensa:** Asignación anual de fondos.
   * **Apoyo de Programas de Cooperación Internacional:** Fondos adicionales y recursos técnicos.

**Tabla de Financiamiento:**

| **Recurso** | **Cantidad** | **Costo Estimado USD** |
| --- | --- | --- |
| Especialistas en Ciberseguridad | 5 | $250,000 |
| Servidores Dedicados | 10 | $100,000 |
| Sistemas de Detección | 5 | $50,000 |
| Software de Análisis | 5 | $50,000 |
| Capacitación | Variada | $50,000 |
| **Total** |  | **$500,000** |

### 8. Decidir sobre la amplitud y el nivel de servicios del CSIRT

**Título:** Servicios del CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Servicios Iniciales:**
   * **Monitoreo y Detección de Incidentes:** Vigilancia continua de la red para identificar actividades sospechosas.
   * **Respuesta y Recuperación:** Implementación de medidas para contener y resolver incidentes.
   * **Análisis Forense:** Investigación de incidentes para determinar el origen y alcance.
2. **Expansión de Servicios:**
   * **Inteligencia de Amenazas:** Recolección y análisis de datos sobre amenazas emergentes.
   * **Simulaciones de Ataques y Ejercicios de Respuesta:** Realización de pruebas periódicas para mejorar la preparación del equipo.

### 9. Determinar la estructura de información del CSIRT, la autoridad y el modelo organizativo

**Título:** Estructura Organizativa del CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Estructura:**
   * **Organigrama:**
     + Jefe de CSIRT -> Coordinador de Respuesta -> Analistas de Incidentes -> Soporte Técnico
2. **Autoridad:**
   * **Reporte Directo:** Reporte directo al Secretario de Defensa

### 10. Identificar los recursos necesarios

**Título:** Recursos Necesarios para el CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Infraestructura:**
   * **Servidores Dedicados:** 10 servidores dedicados para análisis y almacenamiento de datos.
   * **Sistemas de Detección de Intrusos:** Herramientas para monitoreo continuo.
   * **Software de Análisis de Amenazas:** Herramientas para identificación y mitigación de amenazas.
2. **Personal:**
   * **Especialistas en Ciberseguridad:** 5 especialistas con conocimientos en análisis forense, monitoreo de redes y respuesta a incidentes.
   * **Analistas Forenses:** Personal dedicado a la investigación y análisis de incidentes.
   * **Técnicos de Soporte:** Personal de soporte técnico para mantener la infraestructura del CSIRT.

**Tabla de Recursos:**

| **Recurso** | **Cantidad** | **Costo Estimado** |
| --- | --- | --- |
| Especialistas en Ciberseguridad | 5 | $250,000 |
| Servidores Dedicados | 10 | $100,000 |
| Sistemas de Detección | 5 | $50,000 |
| Software de Análisis | 5 | $50,000 |
| Capacitación | Variada | $50,000 |
| **Total** |  | **$500,000** |

### 11. Definir las interacciones e interfaces

**Título:** Interacciones e Interfaces del CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Interacciones:**
   * **Comunicación con Otras Agencias de Seguridad:** Coordinación con el CNI y la ASN para intercambio de información.
   * **Proveedores de Servicios de Internet (ISP):** Colaboración para la mitigación de amenazas.
   * **Otros CSIRT:** Establecer relaciones con otros CSIRT para compartir experiencias y mejores prácticas.
2. **Protocolos de Comunicación:**
   * **Canales Seguros:** VPN, correo electrónico cifrado, reuniones regulares vía videoconferencia.
   * **Métodos de Colaboración:**
     + Definición de procedimientos para el intercambio de información.
     + Protocolos de respuesta conjunta a incidentes.

### 12. Definir las funciones, responsabilidades y la autoridad correspondiente

**Título:** Funciones y Responsabilidades del CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Funciones:**
   * **Monitoreo y Detección:** Vigilancia continua de las redes y sistemas para identificar posibles amenazas.
   * **Análisis de Incidentes:** Investigación de los incidentes de seguridad para determinar su causa y alcance.
   * **Respuesta y Recuperación:** Implementación de medidas para contener y resolver los incidentes de seguridad.
   * **Capacitación y Concientización:** Proveer formación continua y difundir mejores prácticas de seguridad.
2. **Autoridad:**
   * **Límites de Autoridad y Responsabilidades:**
     + Definir claramente los roles y responsabilidades de cada miembro del CSIRT.
     + Establecer una jerarquía clara para la toma de decisiones durante los incidentes.

**Tabla de Funciones y Responsabilidades:**

| **Rol** | **Funciones** | **Responsabilidades** |
| --- | --- | --- |
| Jefe de CSIRT | Supervisión general, toma de decisiones | Coordinación de todos los esfuerzos del CSIRT |
| Coordinador de Respuesta | Gestión de incidentes, coordinación de equipos | Supervisión de la respuesta a incidentes |
| Analistas de Incidentes | Detección y análisis de incidentes | Identificación y mitigación de amenazas |
| Soporte Técnico | Mantenimiento de la infraestructura | Garantizar el correcto funcionamiento de los sistemas del CSIRT |

### 13. Documentar el flujo de trabajo

**Título:** Flujos de Trabajo del CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Diagramas:**
   * **Diagrama de Flujo de Trabajo para Detección y Respuesta a Incidentes:**
2. **Garantía de Calidad:**
   * **Medidas de Calidad en los Procesos Documentados:**
     + Establecer procedimientos estandarizados para la detección y respuesta a incidentes.
     + Implementar revisiones periódicas y auditorías internas para asegurar el cumplimiento de los procedimientos.

**Tabla de Flujo de Trabajo:**

| **Paso** | **Descripción** | **Responsable** |
| --- | --- | --- |
| Detección de Incidente | Identificación de actividad sospechosa | Analistas de Incidentes |
| Notificación | Informar a los responsables de seguridad | Coordinador de Respuesta |
| Análisis Inicial | Evaluación preliminar del incidente | Analistas de Incidentes |
| Contención | Implementar medidas para contener el incidente | Coordinador de Respuesta |
| Erradicación | Eliminar la amenaza de los sistemas afectados | Soporte Técnico |
| Recuperación | Restaurar los sistemas a su estado normal | Soporte Técnico |
| Análisis Forense | Investigación detallada del incidente | Analistas Forenses |
| Informe Final | Documentación del incidente y lecciones aprendidas | Jefe de CSIRT |

### 14. Desarrollar políticas y procedimientos correspondientes

**Título:** Políticas y Procedimientos del CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Definiciones:**
   * **Establecer Definiciones Claras:**
     + **Evento de Seguridad Informática:** Cualquier evento que comprometa la seguridad de la información.
     + **Incidente de Seguridad Informática:** Un evento que resulta en un acceso no autorizado, uso, divulgación, modificación o destrucción de información.
2. **Procedimientos:**
   * **Documentar Procedimientos Iniciales Necesarios para la Operación del CSIRT:**
     + **Notificación de Incidentes:** Proceso para reportar incidentes de seguridad.
     + **Respuesta a Incidentes:** Pasos a seguir para contener y resolver un incidente.
     + **Análisis Forense:** Procedimientos para investigar y analizar un incidente.

**Tabla de Procedimientos:**

| **Procedimiento** | **Descripción** | **Responsable** |
| --- | --- | --- |
| Notificación de Incidentes | Proceso para reportar y registrar incidentes de seguridad | Coordinador de Respuesta |
| Respuesta a Incidentes | Pasos para contener y resolver incidentes | Analistas de Incidentes |
| Análisis Forense | Investigación detallada y análisis de incidentes | Analistas Forenses |
| Documentación y Reportes | Registro y documentación de incidentes y lecciones aprendidas | Jefe de CSIRT |

### 15. Crear un plan de implementación y solicitar comentarios

**Título:** Plan de Implementación del CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Retroalimentación:**
   * **Solicitar Comentarios de las Partes Interesadas y Ajustar el Plan Según Sea Necesario:**
     + **Encuestas y Reuniones:** Reuniones con representantes de las diferentes ramas de las Fuerzas Militares y encuestas para recoger opiniones y sugerencias sobre el plan de implementación.

**Ejemplo de Encuesta para Retroalimentación:**

**Encuesta de Retroalimentación sobre el Plan de Implementación del CSIRT**

1. ¿Considera que el plan de implementación propuesto es viable?

- [ ] Sí

- [ ] No

- [ ] No estoy seguro

2. ¿Qué aspectos del plan considera que necesitan mejoras?

- [ ] Estructura organizativa

- [ ] Procedimientos de respuesta

- [ ] Recursos necesarios

- [ ] Otros: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. ¿Tiene alguna sugerencia para mejorar el plan de implementación?

- \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Apoyo:**
   * **Asegurar el Apoyo de la Gestión y los Interesados para la Implementación del CSIRT:**
     + **Presentaciones a la Alta Dirección:** Presentaciones para explicar los beneficios y la necesidad del CSIRT y solicitar recursos adicionales si es necesario.

**Tabla de Retroalimentación:**

| **Aspecto Evaluado** | **Comentarios y Sugerencias** | **Ajustes Realizados** |
| --- | --- | --- |
| Estructura Organizativa | Necesita mayor claridad en roles y responsabilidades | Se ajustó el organigrama y se definieron roles específicos |
| Procedimientos de Respuesta | Se requieren más detalles en los pasos a seguir | Se detallaron los procedimientos y se añadieron ejemplos |
| Recursos Necesarios | Falta de recursos para capacitación continua | Se incluyó un presupuesto adicional para capacitación |

### 16. Anunciar el CSIRT cuando entre en funcionamiento

**Título:** Anuncio del CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Comunicación:**
   * **Planificar un Anuncio Formal y Difundir Material Informativo sobre el CSIRT:**
     + **Comunicado de Prensa Oficial del Ministerio de Defensa:**
       - Anuncio de la creación del CSIRT y su misión.
       - Resaltar la importancia del CSIRT para la seguridad nacional.
   * **Material de Marketing:**
     + Folletos informativos sobre el CSIRT y sus servicios.
     + Presentaciones para sesiones informativas y seminarios.
     + Cursos de formación y concientización sobre ciberseguridad.

**Ejemplo de Comunicado de Prensa:**

**Comunicado de Prensa**

**Ministerio de Defensa de Colombia**

Fecha: 01/09/2025

**Anuncio de la Creación del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) de las Fuerzas Militares de Colombia**

El Ministerio de Defensa se complace en anunciar la creación del CSIRT de las Fuerzas Militares de Colombia. Este equipo tiene la misión de proporcionar una respuesta coordinada y efectiva a incidentes de seguridad informática, protegiendo la infraestructura crítica y la información sensible de nuestras fuerzas armadas.

La creación del CSIRT es un paso fundamental para fortalecer nuestras capacidades de defensa cibernética y asegurar la continuidad de nuestras operaciones en el ciberespacio. Invitamos a todas las unidades y personal a colaborar con el CSIRT y participar en los programas de formación y concientización que estaremos ofreciendo.

Para más información, por favor, contacte a:

Departamento de Comunicaciones del Ministerio de Defensa

Email: comunicaciones@defensa.gov.co

Tel: +57 1 2345678

### 17. Definir los métodos para evaluar el desempeño del CSIRT

**Título:** Evaluación del Desempeño del CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Criterios de Medición:**
   * **Establecer Métricas de Rendimiento y Procedimientos de Evaluación:**
     + **Tiempo de Respuesta a Incidentes:** Medir el tiempo desde la detección hasta la resolución de un incidente.
     + **Número de Incidentes Detectados y Resueltos:** Registrar la cantidad de incidentes gestionados.
     + **Impacto de los Incidentes en las Operaciones Militares:** Evaluar cómo los incidentes afectaron las operaciones.
2. **Métodos de Evaluación:**
   * **Encuestas de Satisfacción:** Encuestas periódicas a las unidades atendidas por el CSIRT para evaluar su satisfacción con los servicios.
   * **Análisis de Informes:** Revisión de informes de incidentes y análisis forenses para identificar áreas de mejora.
   * **Auditorías Internas:** Auditorías periódicas para asegurar el cumplimiento de los procedimientos y políticas establecidos.

**Ejemplo de Encuesta de Satisfacción:**

**Encuesta de Satisfacción del CSIRT**

1. ¿Qué tan satisfecho está con el tiempo de respuesta del CSIRT a los incidentes reportados?

- [ ] Muy satisfecho

- [ ] Satisfecho

- [ ] Neutral

- [ ] Insatisfecho

- [ ] Muy insatisfecho

2. ¿Considera que el CSIRT resolvió adecuadamente los incidentes reportados?

- [ ] Sí

- [ ] No

- [ ] Parcialmente

3. ¿Qué aspectos del servicio del CSIRT cree que pueden mejorarse?

- \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. ¿Alguna otra sugerencia o comentario?

- \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Tabla de Evaluación del Desempeño:**

| **Métrica** | **Descripción** | **Método de Evaluación** |
| --- | --- | --- |
| Tiempo de Respuesta | Tiempo desde la detección hasta la resolución | Análisis de tiempos de respuesta |
| Número de Incidentes | Cantidad de incidentes gestionados | Registro de incidentes |
| Impacto en Operaciones | Evaluación del impacto en operaciones militares | Informes de impacto |

### 18. Tener un plan de copia de seguridad para cada elemento del CSIRT

**Título:** Plan de Recuperación y Continuidad del CSIRT de las Fuerzas Militares de Colombia

**Contenido Extendido:**

1. **Recuperación:**
   * **Diseñar Planes de Recuperación ante Desastres y Continuidad del Negocio:**
     + **Procedimientos para Restaurar Sistemas Críticos:** Pasos a seguir para restaurar sistemas críticos en caso de un incidente mayor.
     + **Planes de Contingencia:** Planes para asegurar la continuidad de las operaciones.
2. **Simulacros:**
   * **Realizar Ejercicios de Simulacro para Probar la Capacidad de Respuesta:**
     + **Ejercicios Periódicos:** Realización de ejercicios periódicos para evaluar la preparación del equipo.
     + **Simulaciones de Ataques:** Realización de simulaciones de ataques y respuesta a incidentes.

**Ejemplo de Plan de Recuperación:**

**Plan de Recuperación ante Desastres del CSIRT**

1. **Objetivo:** Asegurar la continuidad de las operaciones del CSIRT en caso de un desastre.

**2. Procedimientos:**

**- Activación del Plan de Recuperación:**

- Notificar a todos los miembros del CSIRT y al personal clave.

- Activar los sistemas de respaldo y recuperación de datos.

**- Restauración de Sistemas Críticos:**

- Identificar y priorizar los sistemas críticos a ser restaurados.

- Seguir los procedimientos documentados para la restauración.

**- Verificación y Pruebas:**

- Verificar la integridad de los sistemas restaurados.

- Realizar pruebas para asegurar que todos los sistemas funcionan correctamente.

**3. Planes de Contingencia:**

- **Personal de Respaldo:** Listado de personal de respaldo que puede asumir funciones críticas.

- **Infraestructura Alterna:** Ubicaciones alternas para operar en caso de que las instalaciones principales estén inoperativas.

**4. Simulacros:**

- **Frecuencia:** Ejercicios de simulacro cada 6 meses.

- **Escenarios:** Simulaciones de ataques DDoS, infecciones de malware, y fallas de infraestructura.

**Tabla de Recuperación:**

| **Elemento** | **Procedimiento de Recuperación** | **Plan de Contingencia** |
| --- | --- | --- |
| Servidores Críticos | Restauración desde respaldos | Uso de servidores alternos |
| Sistemas de Detección | Reinicio y verificación de integridad | Sistemas de detección redundantes |
| Personal Crítico | Contacto inmediato y asignación de tareas | Personal de respaldo entrenado |
| Comunicaciones | Activación de canales de emergencia | Uso de comunicaciones alternativas |

### 19. Ser flexible

**Título:** Flexibilidad y Adaptabilidad del CSIRT de las Fuerzas Militares de Colombia

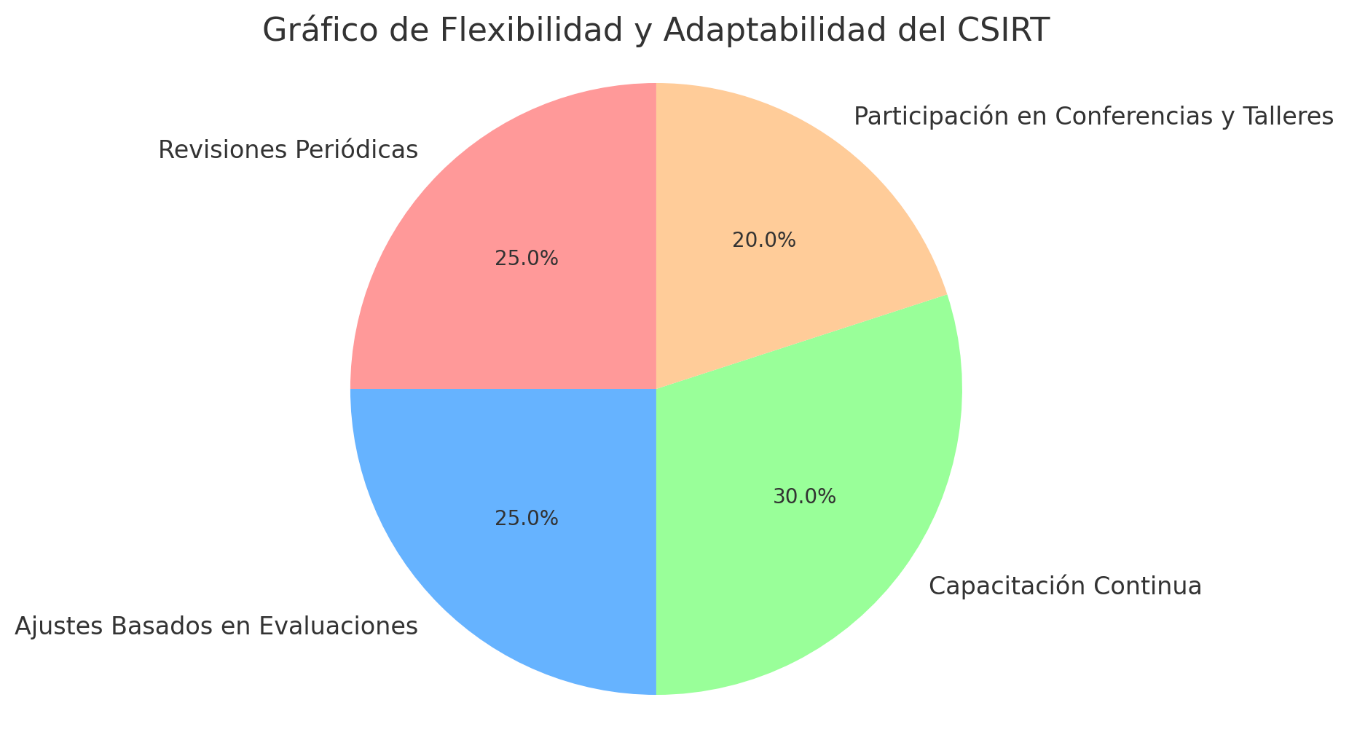
**Contenido Extendido:**

1. **Adaptación:**
   * **Estar Preparados para Ajustar y Mejorar los Servicios del CSIRT Según Sea Necesario:**
     + **Revisiones Periódicas:** Realizar revisiones periódicas de los procedimientos y políticas.
     + **Ajustes Basados en Evaluaciones:** Ajustar los servicios y procedimientos basados en los resultados de las evaluaciones y feedback de los usuarios.
2. **Capacitación Continua:**
   * **Fomentar la Formación Continua y la Actualización de Conocimientos:**
     + **Programas de Capacitación Continua:** Desarrollar y ejecutar programas de capacitación continua para el personal del CSIRT.
     + **Participación en Conferencias y Talleres:** Fomentar la participación en conferencias y talleres sobre ciberseguridad.

**Tabla de Capacitación Continua:**

| **Programa de Capacitación** | **Descripción** | **Frecuencia** |
| --- | --- | --- |
| Curso Avanzado en Ciberseguridad | Capacitación en técnicas avanzadas de ciberseguridad | Semestral |
| Talleres de Análisis Forense | Formación en técnicas de análisis forense digital | Trimestral |
| Seminarios de Actualización | Seminarios sobre nuevas amenazas y tecnologías | Mensual |
| Participación en Conferencias | Asistencia a conferencias y eventos de ciberseguridad | Anual |

**Gráfico de Flexibilidad y Adaptabilidad:**



**Distribución de los esfuerzos en las distintas áreas clave:**

Revisiones Periódicas: 25%

Ajustes Basados en Evaluaciones: 25%

Capacitación Continua: 30%

**BIBLIOGRAFÍA**

Carnegie Mellon University. (2011). *The CERT Guide to Coordinated Vulnerability Disclosure. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=453662.*

CERT Coordination Center. (2003)*. Handbook for Computer Security Incident Response Teams (CSIRTs). Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=59863.*

ENISA (European Union Agency for Cybersecurity). (2021).CSIRT Maturity Framework. Retrieved from https://www.enisa.europa.eu/publications/csirt-maturity-framework

Kossakowski, K.-P., Allen, J. H., Alberts, C. J., & Stikvoort, D. (1999)*. Incident Management Capabilities. In Handbook for Computer Security Incident Response Teams (CSIRTs). Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=60021*

National Institute of Standards and Technology (NIST). (2012). *Computer Security Incident Handling Guide (SP 800-61 Rev. 2). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*