Taller – Creación de un CSIRT

Alumnos

Mayor Hidalgo Realpe Javier

Mayor Lagos Ascanio Leonardo Arturo

Capitán de Corbeta Moreno Rodríguez Pablo

Capitán de Corbeta Zambrano González Edgar

Aula Q

Electiva - Habilidades prácticas en el Ciberespacio

Docente

DOCTOR JAIDER OSPINA NAVAS

04 de agosto de 2024

CREACION DE UN CSIRT

1) Identificar las partes interesadas y participantes.

a. Determinar quién debe participar en cada nivel de la planificación del CSIRT, la implementación y operación.

1. Nivel Estratégico:

- Alto Mando Militar: Comandante General de las Fuerzas Militares y Comandantes de cada Fuerza “Ejercito – Armada – Fuerza Aerea” que establecen las directrices y prioridades del CSIRT.
- Ministerio de Defensa: Políticos y asesores que alinean el CSIRT con las políticas nacionales de defensa.
- Departamento de TI y Ciberseguridad del Ejército: Liderazgo técnico y estratégico en seguridad cibernética.

2. Nivel Táctico:

- Comandantes de Unidades Militares: Implementan directrices del CSIRT en sus respectivas áreas.
- Líderes de Ciberseguridad: Encargados de supervisar la implementación de políticas y procedimientos de seguridad.

3. Nivel Operacional:

- Analistas de Seguridad: Detectan y responden a incidentes en tiempo real.
- Ingenieros de Redes y Sistemas: Aseguran la infraestructura técnica y colaboran en la implementación de medidas de seguridad.
- Personal de Soporte de TI: Proporcionan apoyo técnico continuo.

b. Determinar quién se sirve o es apoyado por el CSIRT.

- Todas las Unidades Militares: Reciben apoyo directo para la protección de sus activos informáticos y para la respuesta a incidentes.
- Personal de Defensa Cibernética: Proporciona información y recursos para proteger la infraestructura cibernética militar.
- Ministerio de Defensa: Recibe informes y análisis sobre incidentes de seguridad y riesgos potenciales.

c. Identificar a las personas con quien se pueda coordinar o compartir la información, tanto dentro como fuera de la organización.

1. Internamente:

- Departamento de Inteligencia Militar: Colabora en el análisis de amenazas y la respuesta a incidentes.
- Unidades de Tecnología y Comunicaciones: Coordinan la implementación de medidas técnicas de protección.

2. Externamente:

- Organizaciones de Defensa Internacionales: Como la OTAN, para compartir información sobre amenazas globales y mejores prácticas.
- Agencias Nacionales de Ciberseguridad: Colaboran en iniciativas nacionales de ciberdefensa y compartición de inteligencia.

d. Identificar las personas que realizan la seguridad o las funciones de respuesta a incidentes y hablar con ellos.

- Especialistas en Respuesta a Incidentes: Personal militar especializado en la identificación, contención y erradicación de amenazas cibernéticas.
- Analistas de Inteligencia de Seguridad: Proporcionan información sobre nuevas amenazas y vulnerabilidades.
- Líderes de Proyectos de Ciberseguridad: Supervisan la implementación de nuevos procedimientos y tecnologías de seguridad.

e. Identificar qué organizaciones internas y externas podrían interactuar con o participar en el CSIRT.

1. Internas:

- Dirección de Operaciones Cibernéticas: Coordina las operaciones diarias y estratégicas del CSIRT.
- División de Recursos Humanos: Ayuda en la capacitación y concienciación del personal.

2. Externas:

- CERT (Computer Emergency Response Team) Nacional: Ofrece coordinación en respuesta a incidentes a nivel nacional.
- Empresas de Seguridad Cibernética: Proveen servicios de consultoría y herramientas avanzadas para la detección y respuesta a amenazas.
- Universidades y Centros de Investigación: Colaboran en proyectos de investigación y desarrollo en ciberseguridad.

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

a. Encontrar un Director Ejecutivo para Patrocinar el Proyecto

1. Identificación de Candidatos Potenciales:

- Perfil: Persona con experiencia en ciberseguridad, liderazgo en tecnología, y que tenga influencia en el ámbito militar y gubernamental.
- Ejemplos: Directores de ciberseguridad de otras agencias gubernamentales, oficiales de alto rango con experiencia en tecnología, o expertos reconocidos en ciberdefensa.

2. Rol del Director Ejecutivo:

- Actuar como enlace con ejecutivos y gerentes dentro de las Fuerzas Militares y el Estado.
- Promover y defender el proyecto en todos los niveles de la organización.
- Facilitar la comunicación entre el CSIRT y otros departamentos clave.

b. Presentar un Caso de Negocio

1. Identificación de Beneficios Clave:

- Mejora de la Seguridad: Reducción de incidentes de seguridad y mejor respuesta a amenazas.
- Protección de Activos: Salvaguardar información crítica y sistemas de las Fuerzas Militares.
- Cumplimiento Normativo: Asegurar que las operaciones cumplan con las normativas nacionales e internacionales de seguridad.

2. Presentación del Caso:

- Datos y Estadísticas: Usar ejemplos de incidentes anteriores y cómo un CSIRT podría haber mitigado los daños.
- Análisis de Costos-Beneficios: Demostrar cómo la inversión en un CSIRT puede reducir costos a largo plazo al prevenir y mitigar incidentes.

c. Obtener Apoyo para la Gestión del Proyecto

1. Reuniones de Planeación:

- Involucrar a las Partes Interesadas: Organizar reuniones con gerentes y líderes de equipo para discutir el plan y sus beneficios.
- Establecer un Comité de Apoyo: Formar un grupo de trabajo que incluya personal clave de IT, seguridad, y operaciones para guiar el proyecto.

2. Asignación de Recursos:

- Tiempo y Personal: Garantizar que se asignen suficientes recursos humanos y tiempo para la investigación y planificación.
- Presupuesto: Asegurar la disponibilidad de un presupuesto adecuado para la implementación y operación del CSIRT.

d. Explicar el Establecimiento del CSIRT

1. Educación y Concientización:

- Organizar sesiones para educar a otros gerentes sobre el CSIRT, su importancia, y beneficios.
- Distribuir folletos y presentaciones que expliquen los conceptos clave y casos de éxito de otros CSIRTs.

2. Beneficios para la Organización:
- Mejorar la capacidad de respuesta ante incidentes y reducir el tiempo de inactividad.
- Facilitar la colaboración entre diferentes unidades militares y agencias gubernamentales.

e. Solicitar el Apoyo de la Administración

1. Anuncio del Proyecto:
- Solicitar a la administración que anuncie oficialmente la formación del proyecto CSIRT.
- Pedir a las personas y departamentos que colaboren proporcionando información y recursos necesarios.

2. Monitoreo y Evaluación:
- Establecer métricas y métodos para evaluar el progreso del proyecto y ajustar estrategias según sea necesario.
- Mantener a la administración informada con informes periódicos sobre el avance del proyecto.

3) Desarrollar un plan de proyecto CSIRT.

a. Formación de un Equipo de Proyecto

Roles y Responsabilidades:

1. Jefe de Proyecto:
- Coordina todas las actividades del proyecto y sirve como punto de contacto principal para la dirección.
- Informa sobre el progreso, desafíos y logros del proyecto.

2. Analistas de Ciberseguridad:
- Realizan análisis de vulnerabilidades y evaluación de riesgos.
- Desarrollan protocolos de respuesta a incidentes.

3. Ingenieros de Redes:
- Aseguran la infraestructura de red necesaria para el funcionamiento del CSIRT.
- Implementan medidas de seguridad en las comunicaciones.

4. Especialistas en Gestión de Incidentes:
- Diseñan y prueban procedimientos de gestión de incidentes.
- Capacitan al personal en la respuesta efectiva a incidentes de seguridad.

5. Expertos en Cumplimiento y Regulación:
- Garantizan que el CSIRT cumpla con las leyes y regulaciones colombianas.

- Supervisan la alineación con estándares internacionales de ciberseguridad.

6. Personal de Apoyo Administrativo:
- Asisten en tareas administrativas, logística y documentación del proyecto.

Selección del Equipo:

- Internos:
- Personal de las fuerzas militares con experiencia en ciberseguridad y tecnología.
- Oficiales con conocimiento en operaciones y logística.

- Externos:
- Consultores de ciberseguridad con experiencia en la creación de CSIRTs.
- Especialistas en gestión de proyectos.

b. Nombramiento del Jefe de Proyecto

Criterios de Selección:

- Experiencia previa en gestión de proyectos de tecnología y seguridad.
- Conocimiento profundo de la estructura y operaciones de las fuerzas militares de Colombia.
- Habilidades de liderazgo y comunicación efectiva.

Recomendación:

Nombrar a un oficial superior con experiencia en ciberseguridad y gestión de proyectos, quien pueda establecer una comunicación efectiva entre el equipo de proyecto y la dirección de las fuerzas militares.

c. Aplicación de los Conceptos de Gestión de Proyectos

Fases del Proyecto:

1. Inicio:
- Definición de objetivos y alcance del CSIRT.
- Análisis de factibilidad y establecimiento de requerimientos.

2. Planificación:
- Desarrollo de un plan de proyecto detallado, incluyendo cronograma, presupuesto y recursos necesarios.
- Identificación de riesgos y desarrollo de estrategias de mitigación.

3. Ejecución:
- Implementación de la infraestructura técnica necesaria.
- Contratación y capacitación del personal del CSIRT.

4. Monitoreo y Control:
- Seguimiento del progreso del proyecto respecto al cronograma y presupuesto.
- Ajustes necesarios en respuesta a incidentes y cambios en el entorno.

5. Cierre:
- Evaluación del desempeño del CSIRT y cumplimiento de objetivos.
- Documentación de lecciones aprendidas y recomendaciones para mejoras futuras.

Herramientas de Gestión:
- Software de gestión de proyectos: Para seguimiento de tareas y colaboración en equipo.
- Tableros de control (dashboards): Para el monitoreo de métricas clave y reportes a la dirección.
- Análisis FODA: Para evaluar fortalezas, oportunidades, debilidades y amenazas del proyecto.

Consideraciones Finales
El éxito del proyecto dependerá de la colaboración efectiva entre los diferentes departamentos de las fuerzas militares y la adaptación continua a los cambios en el panorama de ciberseguridad. La integración del CSIRT en la estructura existente debe asegurar una respuesta rápida y eficiente a incidentes, fortaleciendo la postura de seguridad nacional.

4) Reunir información.

a. Conversaciones con Partes Interesadas

1. Determinación de Necesidades y Requerimientos:
   Partes Interesadas:
- Comando General de las Fuerzas Militares.
- Ministerios relacionados (Defensa, Tecnologías de la Información y Comunicaciones).
- Agencias de inteligencia nacionales.
- Organizaciones académicas y de investigación en ciberseguridad.
- Socios internacionales en ciberdefensa.

   Requerimientos:
- Protección de infraestructuras críticas.
- Capacidades de respuesta rápida ante ciberataques.
- Integración con sistemas de inteligencia y seguridad nacional.

2. Recoger Información sobre Incidentes:
- Revisar reportes de incidentes pasados y presentes.
- Evaluar tipos de amenazas predominantes (e.g., ataques APT, ransomware, phishing).
- Identificar brechas en la respuesta actual a incidentes.
3. Gestión de Incidencias Existentes:
- Evaluar los procesos y protocolos de respuesta actuales.
- Identificar áreas de mejora en coordinación y comunicación interdepartamental.

4. Cuestiones Jurídicas, Políticas y Culturales:
- Normativas de privacidad y protección de datos (Ley 1581 de 2012).
- Políticas de ciberseguridad nacional.
- Cultura organizacional y disposición al cambio.

5. Propiedad de Datos y PI:
- Definir derechos y responsabilidades sobre la información gestionada por el CSIRT.
- Establecer acuerdos de confidencialidad y protección de la propiedad intelectual.

b. Definir Políticas y Cumplimiento Normativo

1. Políticas y Normas:
- Desarrollo de una política de seguridad cibernética específica para el CSIRT.
- Cumplimiento con normas nacionales e internacionales (ISO 27001, NIST).
- Establecimiento de procedimientos para la gestión de incidentes y respuesta.

2. Sectores Por Considerar:
- Público: Cumplimiento con las regulaciones nacionales.
- Privado: Colaboración con empresas proveedoras de tecnología y servicios.
- Académico: Investigación y desarrollo en ciberseguridad.
- Gubernamental y Militar: Integración con políticas de defensa nacional.

c. Entender la Historia Anterior

1. Intentos Anteriores de Crear un CSIRT:
- Investigación sobre iniciativas previas y sus resultados.
- Identificación de desafíos enfrentados y lecciones aprendidas.

2. Expectativas de la Organización:
- Clarificación de roles y responsabilidades del CSIRT.
- Definición de indicadores de éxito y métricas de desempeño.

3. Disponibilidad de Nombre de Dominio:
- Verificación de disponibilidad de un nombre de dominio específico para el CSIRT.
- Registro y aseguramiento del dominio lo antes posible para evitar conflictos futuros.

Recomendaciones Adicionales

1. Capacitación y Concienciación:
- Desarrollar programas de formación continua para el personal.
- Fomentar una cultura de ciberseguridad dentro de las fuerzas militares.

2. Infraestructura y Tecnología:
- Implementar tecnologías avanzadas para la detección y respuesta a incidentes.
- Garantizar la interoperabilidad con sistemas existentes de las fuerzas militares.

3. Colaboración Internacional:
- Establecer lazos con CSIRTs de otros países para compartir información y mejores prácticas.
- Participar en ejercicios de ciberdefensa internacionales.

La creación de un CSIRT efectivo requiere un enfoque multifacético que integre aspectos técnicos, organizacionales y legales. Este plan debe ser adaptable y considerar las dinámicas cambiantes del ciberespacio y las necesidades de seguridad del país.

5) Identificar la circunscripción CSIRT.

a. Determinar el Grupo Inicial de Personas u Organizaciones

1. Fuerzas Militares de Colombia: Este sería el grupo principal al que se le proporcionaría servicio, incluyendo el Ejército, la Armada y la Fuerza Aérea.
2. Ministerio de Defensa Nacional: Como organismo rector, el ministerio debe estar directamente involucrado.
3. Agencias de Inteligencia Nacional: Colaborar con entidades como la Dirección Nacional de Inteligencia para asegurar una coordinación efectiva.
4. Infraestructura Crítica: Organizaciones encargadas de la infraestructura crítica relacionada con la defensa, como proveedores de telecomunicaciones y tecnologías militares.

b. Identificar Tipos de Servicios de CSIRT

1. Para las Fuerzas Militares:

- Implementación de sistemas para el monitoreo continuo de redes y sistemas militares.
- Proporcionar asistencia inmediata en caso de incidentes cibernéticos.
- Servicios de análisis post-incidente para determinar la causa raíz y el impacto.
- Entrenamiento en ciberseguridad para personal militar.

2. Para Infraestructura Crítica:
- Identificar y mitigar vulnerabilidades en sistemas críticos.
- Ayuda en la formulación de políticas de ciberseguridad.

3. Para el Público General:
- Campañas de sensibilización sobre ciberseguridad.

c. Identificar y Establecer Socios Estratégicos

1. Entidades Gubernamentales:
- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC): Para coordinación en políticas nacionales de ciberseguridad.
- Policía Nacional: Colaboración en cibercrimen.

2. Organizaciones Internacionales:
- CERTs Regionales e Internacionales: Participación en el intercambio de información y mejores prácticas.
- Organizaciones de Defensa Internacionales: Cooperación con socios como la OTAN para estándares y formación.

3. Sector Privado:
- Empresas Tecnológicas: Colaboración para el desarrollo de capacidades tecnológicas avanzadas.

d. Identificar Cómo los Miembros de la Circunscripción Obtendrán los Servicios del CSIRT

1. Portal Web Seguro: Plataforma en línea para reportar incidentes y obtener soporte.

2. Línea de Emergencia 24/7: Línea telefónica para la atención inmediata de incidentes.

3. Oficinas Regionales: Presencia física en bases y comandos para acceso directo a los servicios.

e. Identificar Componentes para el Soporte a Largo Plazo

1. Inteligencia Artificial y Machine Learning: Desarrollo de capacidades para automatizar la detección de amenazas y la respuesta.

2. Big Data y Análisis Avanzado: Utilización de análisis avanzado para prever amenazas emergentes.

3. Integración con Sistemas Internacionales: Participación en redes internacionales de ciberseguridad para mejorar la capacidad de respuesta.

6) Definir la misión del CSIRT.

a. Misión del CSIRT

El CSIRT de las Fuerzas Militares de Colombia tiene como misión proporcionar una defensa cibernética robusta y efectiva para proteger los activos de información críticos del país. Este equipo será responsable de la detección, análisis, respuesta y mitigación de incidentes de seguridad cibernética, asegurando la continuidad operativa de las infraestructuras tecnológicas militares y contribuyendo a la seguridad nacional. El CSIRT trabajará en colaboración con otras agencias gubernamentales, el sector privado y aliados internacionales para fortalecer la resiliencia cibernética y promover un entorno digital seguro.

b. Metas y Objetivos Principales

1. Detección y Respuesta a Incidentes:

- Implementar sistemas avanzados de monitoreo y alerta temprana para identificar amenazas cibernéticas en tiempo real.
- Desarrollar procedimientos de respuesta rápidos y efectivos para mitigar el impacto de los incidentes cibernéticos.

2. Fortalecimiento de Capacidades:

- Capacitar a personal militar en prácticas de ciberseguridad y defensa cibernética.
- Fomentar la investigación y el desarrollo en tecnologías de seguridad cibernética dentro de las fuerzas militares.

3. Colaboración y Coordinación:

- Establecer alianzas estratégicas con otras agencias gubernamentales y organizaciones internacionales para compartir información y recursos.
- Participar en ejercicios de ciberseguridad nacionales e internacionales para mejorar la preparación y respuesta ante incidentes.

4. Gestión de Riesgos:
- Realizar evaluaciones continuas de riesgos cibernéticos para identificar vulnerabilidades y priorizar acciones de mitigación.
- Desarrollar planes de contingencia y recuperación ante desastres para asegurar la continuidad operativa de sistemas críticos.

5. Concienciación y Educación:
- Promover una cultura de ciberseguridad dentro de las fuerzas militares mediante programas de concienciación y entrenamiento regular.
- Facilitar campañas de educación en ciberseguridad para aumentar la resiliencia individual y organizacional.

c. Obtención de Acuerdo sobre la Misión

Para garantizar el éxito del CSIRT, es crucial obtener el consenso de todas las partes interesadas. A continuación, se describen pasos para asegurar que todos los actores entiendan y apoyen la misión del CSIRT:

1. Consulta y Participación:
- Organizar talleres y reuniones con representantes de las fuerzas militares, la gestión electoral, colaboradores y otros actores relevantes para discutir y refinar la misión del CSIRT.

2. Comunicación Clara:
- Desarrollar materiales de comunicación claros y concisos que expliquen la misión, metas y beneficios del CSIRT a todos los niveles de la organización.

3. Feedback y Revisión:
- Recoger feedback de las partes interesadas sobre la declaración de misión propuesta y realizar ajustes según sea necesario para reflejar sus preocupaciones y expectativas.

4. Compromiso de Liderazgo:
- Asegurar el apoyo y compromiso del liderazgo de las fuerzas militares y del gobierno para proporcionar los recursos y la autoridad necesarios para implementar la misión del CSIRT.

7) Asegurar el financiamiento para las operaciones de CSIRT.

a. Estrategia de Financiación

- Financiación Inicial y a Corto Plazo

1. Plantilla Inicial y Desarrollo Profesional:

- Solicitar fondos iniciales a través de subvenciones gubernamentales específicas para la ciberseguridad y defensa nacional.
- Buscar apoyo de organizaciones internacionales como la OTAN, la OEA, o el Banco Mundial, que tienen programas para fortalecer la ciberseguridad en países en desarrollo.
- Colaborar con universidades y centros de investigación para obtener financiamiento y apoyo en la capacitación y desarrollo profesional del personal.

2. Equipos, Herramientas e Infraestructura:
- Proponer una línea de presupuesto específica dentro del Ministerio de Defensa para cubrir la adquisición de equipos y herramientas esenciales.
- Establecer asociaciones con empresas tecnológicas para obtener descuentos o donaciones de software y hardware necesarios.

3. Instalaciones y Seguridad de Datos:
- Asegurar fondos específicos del presupuesto nacional para la construcción y mantenimiento de instalaciones seguras.
- Utilizar un modelo de financiamiento de arrendamiento para infraestructura crítica, minimizando la necesidad de grandes desembolsos de capital inicial.

- Financiación a Largo Plazo

1. Desarrollo Profesional Continuo:
- Implementar programas de desarrollo profesional financiados por el gobierno para mantener al personal actualizado en las últimas tendencias de ciberseguridad.

2. Mantenimiento y Actualización de Equipos:
- Integrar el mantenimiento y la actualización de equipos en el presupuesto operativo anual del Ministerio de Defensa.
- Asegurar contratos a largo plazo con proveedores para la actualización continua de software y hardware.

b. Modelo de Financiación Sostenible

1. Apoyo del Gobierno
- Establecer una línea presupuestaria dedicada dentro del presupuesto del Ministerio de Defensa para el financiamiento continuo del CSIRT.

2. Pago por Servicio
- Ofrecer servicios de ciberseguridad a otras entidades gubernamentales bajo un modelo de pago por servicio para generar ingresos adicionales.

3. Cuotas de Miembros
- Implementar un sistema de cuotas para organizaciones o departamentos que requieran servicios especializados del CSIRT.

4. Asociaciones Estratégicas
- Colaborar con empresas privadas para recibir apoyo financiero a cambio de servicios de ciberseguridad o acceso a investigaciones y desarrollo en el área de ciberdefensa.

8) Decidir sobre la amplitud y el nivel de los servicios del CSIRT ofrecerá.

a. Comenzar con algo pequeño y crecer

1. Evaluación de Capacidades Actuales:
- Realizar un inventario de las capacidades de ciberseguridad existentes en las fuerzas militares, incluyendo personal, tecnología y procesos.
- Identificar las brechas en términos de habilidades, infraestructura y procesos que se deben abordar en el corto plazo.

2. Establecimiento de Metas Iniciales:
- Definir objetivos claros y alcanzables para el CSIRT en sus etapas iniciales. Esto podría incluir la gestión de incidentes menores, la concienciación sobre ciberseguridad, y el monitoreo básico de amenazas.

3. Selección de Personal:
- Iniciar con un equipo pequeño y altamente capacitado, compuesto por personal con experiencia en ciberseguridad y manejo de incidentes.

4. Desarrollo de Capacidades:
- Implementar un programa de capacitación continua para el personal del CSIRT, asegurando que estén actualizados con las últimas amenazas y tecnologías.

b. Determinar los servicios del CSIRT y el electorado

1. Servicios Iniciales del CSIRT:
- Establecer capacidades para identificar y responder a incidentes de seguridad en tiempo real.
- Investigar y analizar incidentes para comprender su origen y mitigar su impacto.
- Proveer asistencia técnica a las unidades militares afectadas por incidentes de seguridad.

- Desarrollar programas de concienciación y capacitación en ciberseguridad para todo el personal militar.

2. Electorado Objetivo:
- Los servicios del CSIRT se ofrecerán inicialmente a las unidades militares de Colombia, con un enfoque particular en las áreas más críticas o vulnerables.
- A medida que el CSIRT crezca, se puede expandir el alcance para incluir otras entidades gubernamentales relacionadas con la defensa.

c. Definir el proceso de prestación de servicios

1. Horas de Operación:
- El CSIRT debe estar operativo 24/7 para responder rápidamente a cualquier incidente.

2. Métodos de Contacto:
- Establecer múltiples canales de comunicación para reportar incidentes, incluyendo teléfono, correo electrónico seguro, y un portal web.

3. Difusión de Información:
- Implementar un sistema para la difusión de alertas y actualizaciones de seguridad a las unidades militares. Esto puede incluir boletines regulares y actualizaciones en tiempo real.

4. Procesos Relacionados:
- Definir procesos claros para la gestión de incidentes, incluyendo la identificación, contención, erradicación y recuperación.
- Desarrollar procedimientos para la coordinación con otras entidades de ciberseguridad nacionales e internacionales.

d. Decidir cómo el CSIRT mercadea su servicio

1. Concienciación Interna:
- Realizar campañas de concienciación dentro de las fuerzas militares para informar sobre la existencia y los servicios del CSIRT.
- Organizar seminarios y talleres para demostrar las capacidades del CSIRT y su importancia en la defensa cibernética.

2. Colaboración Interinstitucional:
- Establecer alianzas con otras agencias gubernamentales y organizaciones de ciberseguridad para fortalecer la cooperación y el intercambio de información.

3. Participación en Eventos:
- Participar en conferencias y eventos de ciberseguridad para promover las capacidades del CSIRT y atraer talento y colaboración.

4. Informes de Actividad:
- Publicar informes periódicos sobre las actividades del CSIRT, destacando los logros y lecciones aprendidas, para aumentar la visibilidad y credibilidad del equipo.

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

a. Ubicación del CSIRT en la Estructura Organizativa

1. Nivel de Operación:
- Nacional: Un CSIRT a nivel nacional podría integrarse dentro del Ministerio de Defensa, ya que esto permitiría un enfoque centralizado para la coordinación de ciberseguridad entre las distintas ramas de las Fuerzas Militares.
- Independiente: Alternativamente, podría establecerse como una entidad independiente bajo la jurisdicción del gobierno, lo que facilitaría la colaboración con otras agencias de ciberseguridad del estado colombiano.

2. Percepciones y Funcionamiento:
- Integración en el Ministerio de Defensa: Esta opción podría percibirse como una extensión natural de la defensa nacional, con lo cual el electorado podría ver el CSIRT como un componente esencial para la seguridad del país.
- Independencia Operativa: Esto podría dar lugar a una percepción de mayor especialización y enfoque, aunque podría haber desafíos en términos de integración y comunicación con otras agencias gubernamentales.

b. Creación y Mantenimiento de un Organigrama

1. Estructura Propuesta:
- Director del CSIRT: Responsable de la supervisión general, reportando directamente al Ministro de Defensa o un delegado militar de alto rango.
- Equipo de Análisis y Respuesta: Encargado de identificar, analizar y mitigar incidentes de seguridad.
- Equipo de Inteligencia de Amenazas: Dedicado a la vigilancia proactiva de amenazas cibernéticas.
- Equipo de Comunicación y Coordinación: Responsable de la comunicación con otras agencias gubernamentales y el público en caso de incidentes importantes.

2. Mantenimiento del Organigrama:
- Actualizaciones regulares para reflejar cambios en el personal o la estructura.
- Inclusión de roles y responsabilidades claras para cada miembro del equipo.

c. Relación Jerárquica y Reportes

1. Relación con Otras Entidades:
- El CSIRT debe tener un enlace claro con el Comando Conjunto de Ciberdefensa, asegurando que las operaciones estén alineadas con los objetivos estratégicos militares.
- Debe informar a un consejo asesor interinstitucional compuesto por representantes de diferentes ramas militares y agencias de seguridad nacional.

2. Modelo de Reporte:
- Informar directamente al Ministro de Defensa o al alto mando militar sobre incidentes críticos y tendencias en ciberseguridad.
- Colaboración estrecha con el Centro Cibernético Policial para compartir información y recursos.

d. Educación y Comunicación

1. Capacitación del Personal:
- Programas de formación continua para los miembros del CSIRT sobre las últimas tendencias en ciberseguridad y técnicas de respuesta a incidentes.
- Talleres y seminarios para educar a las Fuerzas Militares sobre el papel y las capacidades del CSIRT.

2. Gestión de Solicitudes:
- Desarrollo de un protocolo estándar para manejar y priorizar solicitudes de trabajo.
- Capacitación en habilidades de comunicación para rechazar diplomáticamente solicitudes que no se alineen con la misión del CSIRT, ofreciendo alternativas o recomendaciones.

3. Difusión del Trabajo del CSIRT:
- Elaboración de informes periódicos sobre el estado de la ciberseguridad y las actividades del CSIRT.
- Utilización de plataformas digitales y medios de comunicación interna para mantener a todas las partes interesadas informadas sobre las operaciones del CSIRT.

10) Identificar los recursos necesarios, tales como personal, equipo e infraestructura.

a. Infraestructura Protegida, Segura y Controlada

1. Protección Física de las Instalaciones:

- Establecer el CSIRT en una ubicación con acceso controlado y medidas de seguridad física, como vigilancia 24/7, control de accesos con tarjetas electrónicas y sistemas de videovigilancia.
- Implementar medidas para proteger contra desastres naturales y fallos eléctricos, como generadores de respaldo y sistemas de protección contra incendios.

2. Seguridad de Repositorios de Datos:

- Todos los datos deben estar encriptados tanto en reposo como en tránsito.
- Implementar políticas de control de acceso estricto basadas en roles (RBAC) para asegurar que solo el personal autorizado tenga acceso a la información crítica.
- Establecer auditorías regulares y un sistema de monitoreo continuo para detectar y responder a accesos no autorizados o anomalías en el sistema.

b. Procesos de Recolección, Registro, Seguimiento y Archivo de Información

1. Recolección de Información:

- Utilizar herramientas de monitoreo y detección de amenazas para recopilar datos de eventos de seguridad en tiempo real.

2. Registro y Seguimiento:

- Implementar un Sistema de Gestión de Eventos de Seguridad (SIEM) para centralizar y gestionar logs y eventos de seguridad.
- Desarrollar un proceso de gestión de incidentes que permita la identificación, categorización, análisis y seguimiento de los incidentes de seguridad.

3. Archivo de Información:

- Establecer políticas de retención de datos que definan el tiempo de almacenamiento y el método de eliminación segura de la información archivada.
- Utilizar soluciones de almacenamiento seguro para mantener registros históricos de incidentes y acciones correctivas.

c. Descripciones de Funciones y Conocimientos Requeridos (KSA)

1. Analista de Seguridad Cibernética:

- Conocimientos: Protocolos de red, herramientas de monitoreo de seguridad (e.g., IDS/IPS, SIEM), análisis de malware.

- Destrezas: Análisis forense digital, gestión de incidentes, identificación de amenazas.
- Habilidades: Pensamiento crítico, capacidad de resolución de problemas, habilidades de comunicación.

2. Especialista en Respuesta a Incidentes:
- Conocimientos: Tácticas, técnicas y procedimientos de amenazas (TTPs), estándares de ciberseguridad (e.g., ISO 27001, NIST).
- Destrezas: Manejo de crisis, coordinación de respuesta a incidentes, recuperación de sistemas.
- Habilidades: Trabajo en equipo, capacidad de toma de decisiones bajo presión, habilidades interpersonales.

3. Administrador de Sistemas de Seguridad:
- Conocimientos: Administración de sistemas operativos (e.g., Windows, Linux), herramientas de seguridad (e.g., firewalls, VPNs).
- Destrezas: Configuración y mantenimiento de infraestructuras seguras, gestión de vulnerabilidades.
- Habilidades: Meticuloso, orientado a los detalles, capacidad de adaptación a nuevas tecnologías.

d. Plan de Orientación y Capacitación

1. Programa de Capacitación Inicial:
- Introducción a la misión, visión y objetivos del CSIRT.
- Cursos intensivos sobre ciberseguridad, manejo de herramientas y protocolos específicos de la organización.
2. Capacitación Continua:
- Realizar ejercicios regulares para evaluar la capacidad de respuesta del equipo.
- Talleres y seminarios sobre nuevas amenazas y tecnologías emergentes.
3. Desarrollo Profesional:
- Incentivar la obtención de certificaciones reconocidas en ciberseguridad (e.g., CISSP, CEH).
- Establecer programas de mentoría para el desarrollo de habilidades y conocimientos especializados.

e. Requisitos de Verificación de Antecedentes y Certificaciones

1. Verificación de Antecedentes:
- Realizar evaluaciones de antecedentes detalladas para asegurar la integridad y confiabilidad del personal.
- Determinar el nivel de autorización necesario para cada posición y gestionar los procesos de obtención de estas.

2. Certificaciones Requeridas:
- Fomentar la obtención de certificaciones como CompTIA Security+, Certified Information Systems Security Professional (CISSP), y Certified Ethical Hacker (CEH).
- Considerar certificaciones específicas para la gestión de incidentes y respuesta a amenazas (e.g., GIAC Certified Incident Handler - GCIH).

11) Definir las interacciones e interfaces.

a. Interacciones e Interfaces con Partes Clave

1. Circunscripción Interna:
- Comando General de las Fuerzas Militares: Coordinación directa para la aprobación de políticas y estrategias.
- Ejército, Armada y Fuerza Aérea: Interacción con sus departamentos de ciberseguridad para reportes y acciones conjuntas.

2. Partes Interesadas Externas:
- Ministerio de Defensa: Colaboración para alinear las políticas de ciberdefensa con las estrategias nacionales.
- Presidencia de la República: Interacción en casos de incidentes de gran impacto nacional.

3. Socios y Colaboradores:
- Colciencias y Universidades: Investigación y desarrollo conjunto en ciberseguridad.
- Empresas Tecnológicas: Colaboración para soluciones tecnológicas y entrenamiento.

b. Coordinación con Otras Entidades

- ENTIC: Para la coordinación en incidentes que afecten infraestructuras críticas.
- Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC): Para la regulación y normativas en el ámbito cibernético.
- CSIRTs Nacionales e Internacionales: Para el intercambio de información sobre amenazas y mejores prácticas.

c. Flujo de Información

- Uso de plataformas seguras de comunicación interna (por ejemplo, sistemas cifrados y VPNs) para el intercambio de información entre las fuerzas militares y otras entidades.
- Establecimiento de procedimientos estandarizados para la notificación y gestión de incidentes.

d. Interfaces y Métodos de Colaboración

- Creación de un protocolo conjunto para la investigación y respuesta a incidentes cibernéticos.
- Acuerdos de colaboración para garantizar la respuesta rápida y efectiva a vulnerabilidades en los productos.
- Establecimiento de memorandos de entendimiento para la protección conjunta de infraestructuras críticas.
- Participación en redes internacionales de CSIRT para el intercambio de inteligencia de amenazas.

e. Métodos de Comunicación Interna

- Implementación de aplicaciones de mensajería cifrada para la comunicación entre el personal del CSIRT.
- Realización de reuniones semanales para la revisión de incidentes y actualizaciones de seguridad.

f. Gestión de Datos

- Datos de Incidentes: Propiedad del CSIRT, bajo la supervisión del Comando General.
- Compartida con las entidades colaboradoras bajo acuerdos de confidencialidad.
- Jefe del CSIRT: Responsable de la integridad y seguridad de los datos manejados.
- Uso de sistemas de gestión de seguridad de la información (ISMS) para controlar el acceso y almacenamiento de datos.

g. Difusión de Información

- Elaboración de informes periódicos para el alto mando y las partes interesadas.
- Envío de notificaciones inmediatas a las unidades afectadas y socios en caso de incidentes.

h. Documentos Estándar para Difusión

- Resúmenes mensuales de amenazas y vulnerabilidades emergentes.
- Documentos detallados sobre cada incidente, incluyendo análisis de impacto y medidas de mitigación.
- Publicaciones para educar y prevenir incidentes cibernéticos.

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

a. Funciones y Responsabilidades del CSIRT

- Supervisar continuamente la infraestructura de TI para detectar actividades inusuales o sospechosas.
- Utilizar herramientas de análisis de tráfico de red y detección de intrusiones.
- Evaluar la gravedad y el impacto de los incidentes de seguridad.
- Coordinar acciones inmediatas para contener y mitigar los efectos de un incidente.
- Documentar incidentes y acciones tomadas para futuras referencias y lecciones aprendidas.
- Realizar investigaciones forenses digitales para determinar la causa y el origen de los incidentes.
- Preservar evidencias digitales siguiendo procedimientos legales y de seguridad adecuados.
- Identificar y evaluar vulnerabilidades en los sistemas de TI.
- Coordinar con los equipos de TI para aplicar parches y actualizaciones de seguridad.
- Desarrollar programas de capacitación para mejorar la concienciación sobre seguridad cibernética entre el personal militar.
- Realizar simulacros y ejercicios de respuesta a incidentes para preparar al personal.
- Crear y mantener políticas de seguridad cibernética acordes a las necesidades de las Fuerzas Militares.
- Definir procedimientos estandarizados para la gestión de incidentes.

b. Interfaces entre el CSIRT y Funciones Externas

- Establecer relaciones de cooperación con otros CSIRTs a nivel nacional e internacional.
- Participar en redes de intercambio de información sobre amenazas cibernéticas.
- Trabajar con el Ministerio de Defensa y otras agencias gubernamentales para alinear las estrategias de ciberseguridad.
- Reportar incidentes críticos y coordinar respuestas con el Centro Cibernético Policial de Colombia.
- Colaborar con proveedores de soluciones de seguridad para implementar tecnologías efectivas.
- Evaluar nuevas tecnologías y herramientas de seguridad para su adopción.
- Establecer canales de comunicación claros para reportar incidentes y vulnerabilidades.
- Proveer informes periódicos sobre el estado de la seguridad cibernética.

c. Identificación de Áreas de Autoridad Ambigua o Superpuesta

1. <u>Autoridad en la Respuesta a Incidentes:</u>

- Problema: Posible superposición de autoridad entre el CSIRT y los departamentos de TI locales.

- Solución: Establecer un protocolo de escalamiento claro donde el CSIRT tenga autoridad centralizada en la gestión de incidentes críticos.

2. Gestión de Vulnerabilidades:
- Problema: Ambigüedad en la responsabilidad de aplicar parches de seguridad.
- Solución: Definir claramente que el CSIRT es responsable de la identificación y priorización de vulnerabilidades, mientras que los equipos de TI locales ejecutan la implementación de soluciones.

3. Colaboración Interinstitucional:
- Problema: Superposición en la coordinación con agencias de inteligencia y otros CSIRTs.
- Solución: Designar roles específicos para la comunicación externa, asegurando que el CSIRT actúe como el punto de contacto principal para todas las colaboraciones interinstitucionales.

4. Desarrollo de Políticas:
- Problema: Inconsistencias en la aplicación de políticas de seguridad entre diferentes unidades militares.
- Solución: Centralizar la creación de políticas de seguridad dentro del CSIRT y asegurar la adopción uniforme en todas las unidades.

13) Documento del flujo de trabajo.

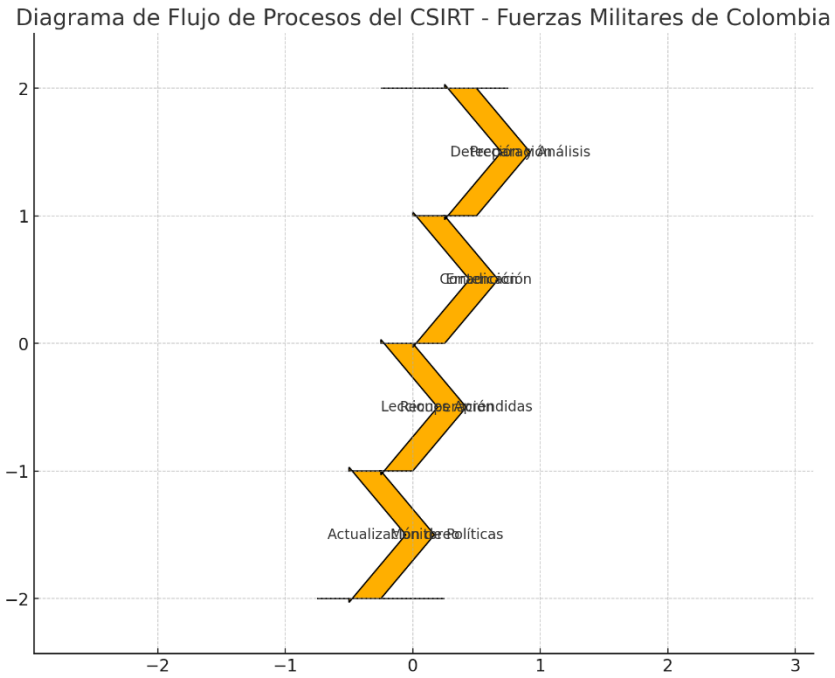
a. Diagrama de Flujo (Gráfico de Carril)

Para la creación del diagrama de flujo, es importante identificar las fases principales en un proceso típico de respuesta a incidentes, como la preparación, detección, contención, erradicación, recuperación y lecciones aprendidas. A continuación, se describe cada etapa y sus interacciones clave:

- Preparación:
- Desarrollo de políticas y procedimientos de seguridad.
- Capacitación del personal y establecimiento de herramientas de monitoreo.
- Interacción con otras entidades para la coordinación inicial.
- Detección y Análisis:
- Monitoreo continuo de la red para identificar posibles incidentes.
- Análisis de alertas y validación de incidentes.
- Notificación inicial a las partes interesadas.
- Contención, Erradicación y Recuperación:
- Implementación de medidas para contener el incidente y evitar su propagación.
- Eliminación de la causa raíz del incidente.

- Restauración de los sistemas afectados y retorno a operaciones normales.
- <u>Lecciones Aprendidas:</u>
- Revisión post-incidente para identificar mejoras en los procesos.
- Actualización de procedimientos y políticas basadas en las lecciones aprendidas.

Diagrama de flujo (gráfico de carril) para ilustrar estos procesos.
Diagrama de Flujo de Procesos del CSIRT - Fuerzas Militares de Colombia



El diagrama de flujo presentado muestra un gráfico de carril que ilustra los procesos y fases clave del CSIRT dentro de las fuerzas militares de Colombia. A continuación, detallo las interacciones y las medidas de garantía de calidad correspondientes para cada etapa.

b. Medidas de Garantía de Calidad

<u>Preparación</u>

- Políticas y Procedimientos: Desarrollar y actualizar continuamente políticas claras de ciberseguridad y respuesta a incidentes.
- Capacitación: Implementar programas regulares de capacitación y simulacros para el personal.
- Coordinación: Establecer canales de comunicación claros con otras agencias de seguridad y organismos estatales.

<u>Detección y Análisis</u>

- Monitoreo Continuo: Utilizar herramientas avanzadas para la detección temprana de amenazas y asegurar la cobertura 24/7.
- Validación de Incidentes: Implementar un sistema de clasificación para priorizar incidentes basados en su impacto potencial.
- Notificación Efectiva: Establecer procedimientos para notificaciones rápidas y claras a todas las partes relevantes.

Contención, Erradicación y Recuperación

- Contención Inmediata: Aplicar medidas de contención tan pronto como se confirme un incidente para limitar su alcance.
- Erradicación Eficaz: Implementar técnicas comprobadas para eliminar completamente las amenazas.
- Recuperación Rápida: Restaurar sistemas y servicios de manera segura y en el menor tiempo posible.

Lecciones Aprendidas

- Revisión Post-Incidente: Conducir análisis detallados después de cada incidente para identificar puntos de mejora.
- Documentación: Mantener registros detallados de incidentes y acciones tomadas.
- Mejora Continua: Actualizar políticas y procedimientos basándose en las lecciones aprendidas.

Integración con la Estructura de las Fuerzas Militares

El CSIRT debe integrarse dentro de la estructura actual de las fuerzas militares, manteniendo una comunicación fluida con el comando central y otros departamentos relevantes, como la inteligencia militar y la seguridad de las comunicaciones.

Estas medidas de garantía de calidad y el flujo de trabajo del CSIRT están diseñados para asegurar una respuesta eficiente y coordinada ante incidentes de ciberseguridad, protegiendo así la infraestructura crítica y los datos sensibles de las fuerzas militares de Colombia.

14) Desarrollar políticas y procedimientos correspondientes.

a. Establecer las definiciones de la terminología

1. Evento de Seguridad Informática: Cualquier observación de un sistema que pueda tener implicaciones de seguridad. Esto puede incluir anomalías en el comportamiento del sistema, detección de malware, o accesos no autorizados, entre otros.
2. Incidente de Seguridad Informática: Un evento que compromete la confidencialidad, integridad o disponibilidad de los datos o sistemas de

información. Los incidentes pueden incluir ataques de denegación de servicio, violaciones de datos, y compromisos de cuentas, entre otros.

3. Términos Exclusivos de la Organización:

- CSIRT: Equipo de Respuesta a Incidentes de Seguridad Informática, encargado de gestionar y mitigar incidentes de seguridad dentro de las fuerzas militares.
- Zona de Operaciones Críticas: Áreas dentro de la infraestructura de TI donde un incidente podría tener un impacto severo en las operaciones militares.
- Respuesta Rápida: Protocolo de acción inmediata para contener y mitigar un incidente de alta prioridad.

b. Determinar las categorías correspondientes a los incidentes, las prioridades y criterios de progresividad

1. Categorías de Incidentes:

- Categoría 1: Incidentes Críticos: Compromisos de sistemas críticos, violaciones de datos sensibles, o interrupciones mayores en operaciones militares.
- Categoría 2: Incidentes Severos: Ataques de malware propagados, accesos no autorizados a sistemas internos, o intentos de exfiltración de datos.
- Categoría 3: Incidentes Moderados: Amenazas de seguridad potenciales, como intentos de phishing o exploraciones de vulnerabilidades.
- Categoría 4: Incidentes Menores: Anomalías menores que no comprometen directamente la seguridad del sistema pero que deben ser monitoreadas.

2. Prioridades:

- Alta: Respuesta inmediata requerida (Categoría 1).
- Media: Respuesta dentro de 24 horas (Categoría 2).
- Baja: Respuesta dentro de 72 horas (Categoría 3 y 4).

3. Criterios de Progresividad:

- Escalamiento: Procedimientos para elevar la prioridad de un incidente basado en su evolución.
- Desescalamiento: Procedimientos para reducir la prioridad una vez que el incidente esté bajo control.

c. Identificar las políticas y procedimientos iniciales

1. Políticas y Procedimientos Iniciales (antes de la operación):

- Política de Notificación: Establecer quién debe ser notificado en caso de un incidente y los canales de comunicación a utilizar.
- Procedimientos de Respuesta Inicial: Protocolos para la contención y análisis inicial de los incidentes.
- Formación y Capacitación: Programas para asegurar que todo el personal entienda las políticas de seguridad y sus responsabilidades.

2. Políticas y Procedimientos Posteriores (después de la operación del CSIRT):
- Revisión y Mejora Continua: Evaluaciones periódicas de los procedimientos para identificar mejoras.
- Gestión de Conocimiento: Bases de datos de incidentes pasados y lecciones aprendidas.
- Colaboración Interinstitucional: Procedimientos para colaborar con otros organismos nacionales e internacionales.

d. Elaborar directrices de notificación de incidentes

1. Directrices de Notificación:
- Interna: Notificar inmediatamente al líder del CSIRT y al personal de TI relevante.
- Externa: Notificaciones a entidades gubernamentales y, si es necesario, a socios internacionales.

2. Formas de Publicidad:
- Comunicados Internos: A través de boletines y reuniones para informar al personal sobre incidentes relevantes.
- Informes Anuales: Resúmenes de incidentes y respuestas publicadas en informes de seguridad interna.

e. Definir y documentar los criterios para la prestación de servicios del CSIRT

1. Criterios para la Prestación de Servicios:
- Coherencia: Desarrollo de protocolos estándar para todos los tipos de incidentes.
- Fiabilidad: Asegurar que los sistemas de detección y respuesta sean precisos y estén bien mantenidos.
- Procesos Repetibles: Documentación detallada de cada paso en la gestión de incidentes para asegurar que se pueda replicar de manera efectiva.

2. Documentación:
- Manual del CSIRT: Incluir procedimientos, definiciones, y guías para el personal.
- Evaluación de Rendimiento: Herramientas y métricas para evaluar la eficacia de la respuesta a incidentes.

15) Crear un plan de aplicación y solicitar comentarios.

Plan de Aplicación para la Creación de un CSIRT en las Fuerzas Militares de Colombia

1. Introducción

- Objetivo: Establecer un CSIRT para fortalecer la capacidad de respuesta a incidentes de seguridad cibernética dentro de las fuerzas militares de Colombia.
- Alcance: Definir el ámbito de actuación del CSIRT dentro de la estructura actual de las fuerzas militares y su integración con el estado colombiano.

2. Análisis de Situación
- Analizar el estado actual de la ciberseguridad en las fuerzas militares.
- Identificar las principales amenazas cibernéticas que enfrentan las fuerzas militares.
- Evaluar las capacidades actuales de respuesta a incidentes y recursos disponibles.

3. Estructura del CSIRT
- Definir la misión y visión del CSIRT alineadas con los objetivos de las fuerzas militares.
- Establecer roles claros para el personal del CSIRT y sus responsabilidades.
- Detallar cómo el CSIRT se integrará con otras entidades del estado y actores internacionales.

4. Componentes Clave del CSIRT
- Especificar los requisitos técnicos para la operación del CSIRT (herramientas, software, hardware).
- Definir los procedimientos estándar para la gestión de incidentes, comunicación y reporte.
- Planificar programas de formación continua para el personal del CSIRT.

5. Plan de Implementación
- Detallar las fases del proyecto desde el diseño hasta la operación completa.
- Establecer un cronograma detallado para cada fase del proyecto.
- Identificar los recursos humanos, técnicos y financieros requeridos.

6. Revisión y Retroalimentación
- Presentar el plan a expertos en ciberseguridad y ciberdefensa para obtener su opinión.
- Ajustar el plan basado en la retroalimentación recibida para asegurar que cumpla con la misión.

7. Gestión y Apoyo Constituyente
- Obtener el respaldo de la alta dirección de las fuerzas militares y otras partes interesadas.
- Resaltar los beneficios del CSIRT para la seguridad nacional y la protección de activos críticos.

8. Conclusión

- Describir el impacto positivo esperado de la implementación del CSIRT en la ciberseguridad de las fuerzas militares.
- Asegurar la sostenibilidad del CSIRT mediante planes de mantenimiento y actualización continua.

Pasos para la Solicitud de Comentarios y Gestión de Apoyo

- Seleccionar a expertos en CSIRT y ciberseguridad que puedan proporcionar comentarios valiosos.
- Compartir el plan con estos expertos mediante reuniones, talleres o envíos de documentos.
- Tomar nota de todas las sugerencias y críticas constructivas.
- Incorporar los comentarios pertinentes para mejorar el plan.
- Presentar el plan revisado a los líderes de las fuerzas militares para su aprobación.
- Preparar materiales y mensajes clave para comunicar el plan a todas las partes interesadas.

16) Anunciar que el CSIRT cuando entre en funcionamiento.

a. Solicitar a la administración para hacer un anuncio formal

1. Propuesta formal a la administración:

- Preparar un documento detallado que explique los objetivos, beneficios y funciones del CSIRT.
- Destacar cómo el CSIRT mejorará la ciberseguridad y ciberdefensa de las fuerzas militares, integrándose en la estructura actual.

2. Reunión de alto nivel:

- Organizar una reunión con los líderes militares y funcionarios del gobierno para presentar la propuesta y obtener su apoyo.
- Utilizar presentaciones visuales y datos que demuestren la necesidad y el impacto positivo del CSIRT.

3. Anuncio oficial:

- Solicitar que la administración emita un comunicado oficial, mediante un evento o conferencia de prensa, para anunciar la creación del CSIRT.
- Incluir declaraciones de líderes clave que refuercen la importancia de esta iniciativa.

b. Proporcionar material de marketing y las directrices de notificación de incidentes

1. Material de marketing:

- Crear folletos, infografías y videos explicativos sobre el CSIRT, sus servicios y su importancia.
- Desarrollar un logo y una identidad visual para el CSIRT que sea reconocible y profesional.

2. Directrices de notificación de incidentes:

- Elaborar un documento claro que describa los procedimientos para reportar incidentes de seguridad informática.
- Incluir ejemplos de incidentes comunes y las respuestas esperadas.
- Asegurarse de que las directrices sean accesibles en formato digital e impreso.

c. Incorporar la formación sobre los servicios del CSIRT en los programas de orientación personal

1. Desarrollo del programa de formación:

- Diseñar módulos de formación específicos que expliquen los servicios del CSIRT y cómo interactuar con él.
- Incluir ejercicios prácticos y estudios de caso para mejorar la comprensión.

2. Integración en la orientación personal:

- Incorporar la formación sobre el CSIRT en el programa de orientación para nuevos reclutas y personal.
- Asegurarse de que todos los miembros del personal actualicen sus conocimientos regularmente.

3. Evaluación continua:

- Implementar evaluaciones para medir la efectividad del programa de formación y realizar mejoras según sea necesario.

d. Difundir información sobre los servicios del CSIRT

1. Plataformas internas:

- Utilizar la intranet de las fuerzas militares y otros portales internos para difundir información sobre el CSIRT.
- Publicar actualizaciones regulares y casos de estudio relevantes para mantener el interés y la conciencia.

2. Sitios web y medios digitales:

- Crear una sección dedicada al CSIRT en el sitio web oficial de las fuerzas militares.
- Utilizar redes sociales, newsletters y correos electrónicos para llegar a un público más amplio.

3. Materiales impresos y eventos:

- Distribuir folletos y carteles en instalaciones militares y centros de formación.

- Organizar seminarios, talleres y cursos de formación abiertos al personal para fomentar la participación y el entendimiento.

4. Colaboración y alianzas:
- Establecer relaciones con otras organizaciones y CSIRTs para compartir mejores prácticas y aprendizajes.
- Participar en conferencias y eventos de ciberseguridad para posicionar al CSIRT como un referente en la región.

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

a. Definir líneas de base para la notificación de incidentes y manejo dentro de la organización

1. Identificación de Activos Críticos:
- Catalogar todos los activos de información críticos para las operaciones militares.
- Determinar el nivel de sensibilidad y criticidad de cada activo.

2. Establecimiento de Tipos de Incidentes:
- Definir una taxonomía de incidentes basada en estándares internacionales como NIST o ISO/IEC 27035.
- Clasificar los incidentes por su severidad e impacto potencial en las operaciones.

3. Protocolos de Notificación:
- Desarrollar protocolos de notificación que incluyan tiempos de respuesta inicial, canales de comunicación y partes responsables.
- Establecer procedimientos para la escalada de incidentes críticos.

4. Capacitación y Concienciación:
- Implementar programas de formación continua para el personal sobre la importancia de la notificación oportuna y precisa de incidentes.

b. Definir los criterios de medición y los parámetros de control de calidad

1. Criterios de Medición:
- Medir el tiempo desde la detección hasta la respuesta inicial y la resolución completa.
- Evaluar la cantidad de incidentes detectados respecto a los esperados.
- Analizar la exactitud en la clasificación de incidentes según su severidad.

2. Parámetros de Control de Calidad:
- Controlar la cantidad de incidentes mal clasificados o ignorados.

- Verificar la adherencia a los procedimientos establecidos para la gestión de incidentes.
- Recabar feedback de las unidades militares sobre la eficacia del CSIRT.

c. Definir los métodos para la obtención de información electoral

Este punto parece estar fuera del ámbito tradicional de un CSIRT militar. Sin embargo, si se refiere a la protección de procesos internos relacionados con decisiones estratégicas o procesos de votación interna, se pueden implementar los siguientes métodos:

1. Monitoreo y Protección de Comunicaciones:
- Utilizar tecnologías de encriptación para proteger la información sensible durante su transmisión.
- Implementar sistemas de monitoreo para detectar accesos no autorizados o intentos de manipulación de datos.
-
2. Auditorías de Seguridad:
- Realizar auditorías regulares de los sistemas que almacenan y procesan información sensible.
- Asegurar que los sistemas de votación internos cumplan con estándares de seguridad robustos.

3. Análisis de Vulnerabilidades:
- Implementar escaneos periódicos de vulnerabilidades en los sistemas y aplicaciones involucrados.
- Realizar pruebas de penetración para evaluar la robustez de las defensas actuales.

d. Implementar procedimientos de informes y auditoría

1. Informes de Incidentes:
- Establecer un formato estándar para la documentación de incidentes que incluya detalles como el tipo, impacto, tiempo de resolución y lecciones aprendidas.
- Proveer informes regulares a los líderes militares sobre el estado de la ciberseguridad y los incidentes manejados.

2. Auditorías Internas:
- Implementar auditorías trimestrales del CSIRT para evaluar la adherencia a los procedimientos y la eficacia en el manejo de incidentes.
- Utilizar métricas definidas para medir el rendimiento del equipo y realizar mejoras continuas.

3. Acuerdos de Nivel de Servicio (SLA) e Indicadores de Desempeño (KPI):

- Definir SLA claros que especifiquen los tiempos de respuesta y resolución para diferentes tipos de incidentes.
- Establecer KPIs para medir el rendimiento del CSIRT en áreas clave como la eficiencia operativa y la satisfacción del cliente interno.

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

a. Identificar las funciones clave del CSIRT y crítica, servicios y equipos
Funciones Clave del CSIRT:

- Supervisar las redes y sistemas para identificar incidentes de seguridad.
- Coordinar y ejecutar acciones para mitigar y resolver incidentes de seguridad.
- Investigar incidentes para determinar la causa raíz y el impacto.
- Identificar y mitigar vulnerabilidades en sistemas y redes.
- Formar al personal sobre prácticas de seguridad y protocolos de respuesta.
- Mantener la comunicación con otras unidades y organizaciones de seguridad.

Servicios Críticos:

- Sistemas de Alerta Temprana
- Bases de Datos de Incidentes
- Plataformas de Gestión de Incidentes
- Sistemas de Comunicación Segura

Equipos Clave:

- Servidores de Alta Disponibilidad
- Dispositivos de Seguridad de Red (firewalls, IDS/IPS)
- Herramientas de Análisis Forense
- Software de Gestión de Incidentes y Vulnerabilidades

b. Diseñar un plan de recuperación ante desastres y continuidad del negocio

Plan de Recuperación Ante Desastres (DRP):

- Identificar posibles amenazas y vulnerabilidades que puedan afectar los servicios del CSIRT.
- Implementar servidores y sistemas de almacenamiento redundantes en ubicaciones separadas geográficamente.
- Realizar respaldos regulares de datos críticos y configuraciones de sistemas, almacenados en ubicaciones seguras.
- Desarrollar procedimientos para restaurar rápidamente servicios críticos desde copias de seguridad.

Plan de Continuidad del Negocio (BCP):

- Identificar funciones críticas y su impacto en la organización.
- Establecer procedimientos para mantener operaciones críticas durante interrupciones.
- Asegurar que los planes del CSIRT se alineen con los planes de continuidad de la organización militar en su conjunto.

c. Plan de contingencia para roles y recursos

- Definir sustitutos para roles críticos en caso de que el personal clave no esté disponible.
- Identificar ubicaciones alternativas desde donde el CSIRT pueda operar si la instalación principal no está disponible.
- Mantener un inventario actualizado de equipos y recursos críticos, con opciones de reemplazo en caso de fallos.

d. Implementar simulacros y pruebas

- Realizar simulacros regulares para probar la capacidad del CSIRT para manejar incidentes y operar bajo presión.
- Analizar los resultados de los simulacros para identificar áreas de mejora.
- Revisar y actualizar los planes de DRP y BCP basados en los resultados de los simulacros y cambios en el entorno de amenaza.

Implementación y Evaluación

- Implementar una fase piloto para probar la efectividad de los planes y ajustar según sea necesario.
- Establecer un proceso de revisión regular para asegurar que los planes sigan siendo relevantes y efectivos.

19) Sea flexible.

- Definir claramente las tareas críticas para evitar sobrecargar al equipo. Establecer procesos para evaluar y priorizar nuevas oportunidades que surjan.
- Diseñar un marco para evaluar nuevas oportunidades, considerando recursos disponibles y potencial impacto en los servicios existentes.
- Implementar sistemas avanzados de monitoreo que evolucionen con el tiempo.
- Fomentar un entorno de aprendizaje constante, ofreciendo cursos de actualización en nuevas tecnologías y amenazas emergentes.
- Realizar revisiones periódicas de las tecnologías empleadas para asegurarse de que las estrategias de respuesta sean efectivas ante nuevas amenazas.
- Establecer un subgrupo dentro del CSIRT dedicado a la investigación de nuevas amenazas y el desarrollo de estrategias de mitigación innovadoras.
- Fomentar una cultura de trabajo en equipo dentro del CSIRT, promoviendo la comunicación abierta y el intercambio de conocimientos entre miembros.

- Establecer alianzas con otros CSIRTs, organizaciones de seguridad y entidades gubernamentales para compartir información sobre amenazas y mejores prácticas.
- Implementar un ciclo de retroalimentación para evaluar y mejorar continuamente los procedimientos y estrategias del CSIRT.
- Crear informes regulares sobre el rendimiento del CSIRT y usar estos datos para ajustar tácticas y estrategias.
- Desarrollar y mantener protocolos detallados para la respuesta a incidentes, asegurando la rápida identificación, contención y recuperación.
- Realizar ejercicios regulares para probar la efectividad de los protocolos y mejorar la preparación del equipo.
- Implementar herramientas de automatización para la detección y respuesta a incidentes, reduciendo el tiempo de reacción y mejorando la eficiencia.
- Utilizar análisis de datos avanzados para identificar patrones de amenazas y predecir posibles ataques.