MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LA FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO”

MY. BETANCOURT RUIZ DIEGO
MY. BUITRAGO LOZANO DIEGO
MY. CERQUERA PASTRANA LIBARDO
MY. CABEZAS CABEZAS MANUEL

DOCENTE
DR. JAIDER OSPINA NAVAS

ASIGNATURA
HABILIDADES PRÁCTICAS EN EL CIBERESPACIO

BOGOTÁ D.C
2024

Propuesta para la Creación de un CSIRT en el Ejército de Colombia
Introducción

La creciente sofisticación y frecuencia de las ciberamenazas a nivel global plantean un desafío significativo para la seguridad nacional. El Ejército de Colombia, como institución fundamental en la defensa del país, no es ajeno a estos riesgos. La protección de la información sensible, los sistemas críticos y la infraestructura digital es esencial para garantizar la integridad de las operaciones militares y la confianza de la ciudadanía. En este contexto, la creación de un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) se presenta como una necesidad estratégica para el Ejército. El CSIRT actuará como un centro especializado en la prevención, detección, respuesta y recuperación ante incidentes de seguridad cibernética, fortaleciendo la capacidad de la institución para enfrentar las amenazas en el ciberespacio.

Justificación

La creación del CSIRT para el Ejército Nacional cobra gran relevancia en el momento que se ha determinado el ciberespacio como un dominio más para la nación y la responsabilidad de las fuerzas militares es innegable, en ese contexto la imperatividad de acción y gobernanza en este aspecto se convierte en una necesidad.

“La creación del CSIRT requiere de un proceso de formalización que, normalmente, depende de un mandato derivado de una instancia de gobierno. En Latinoamérica y el Caribe los mandatos se han promovido, entre otros, por medio de: Decreto Presidencial, Plan Nacional de Desarrollo, Estrategia Nacional de Ciberseguridad, Iniciativa Legislativa, Resolución Exenta, Acuerdo Ministerial.” Guia-CSIRT 2023.

Como estrategia nacional se ve la necesidad de iniciar las gestiones para adquirir capacidades en el entorno del ciberespacio y por ende la ciberseguridad y

ciberdefensa, en tal motivo los aspectos que se buscarían fortalecer con la creación del CSIRT serian la protección a la información crítica, continuidad de las operaciones, fortalecimiento de la ciberdefensa, cumplimiento normativo, generación de confianza, teniendo en cuenta que la principal motivación el la responsabilidad de seguridad y defensa que tiene el Ejercito Nacional frente a estas nuevas amenazas.

Partes interesadas y participantes

Las partes interesadas de la creación del CSIRT del Ejercito Nacional involucra directamente a la institución al Ministerio de Defensa Nacional y a la sociedad en conjunto al momento de defender los intereses de la nación, para implementación del CSIRT se plantea de la siguiente manera:

1. Fase de Planificación:

- **Alto Mando:**
  - Comandante del Ejército: Define la visión estratégica y la importancia del CSIRT para la seguridad nacional y las operaciones militares.
  - Estado Mayor Conjunto: Asegura la alineación con la estrategia de ciberseguridad nacional y la coordinación con otros CSIRT militares y gubernamentales.
  - Jefe de Inteligencia: Evalúa los riesgos y amenazas cibernéticas relevantes para las operaciones militares.
- **Nivel Táctico:**
  - Oficial de Ciberdefensa: Lidera la planificación técnica y operativa del CSIRT.
  - Representantes de las Fuerzas: Aportan conocimiento sobre las necesidades específicas de ciberseguridad de cada rama del Ejército.
  - Asesores Jurídicos: Garantizan el cumplimiento de leyes y regulaciones nacionales e internacionales relacionadas con la ciberseguridad.

2. Fase de Implementación:

- **Alto Mando:**
    - Comandante del Ejército: Emite directrices a los comandos funcionales de personal y presupuesto para asegura la asignación de personal, presupuesto y tecnología necesarios para el funcionamiento del CSIRT.

- **Nivel Táctico:**

  En el nivel táctico la recomendación es implementar el CSIRT a través de un Batallón de ciberseguridad con el fin de alinear esta organización a la estructura del ejército nacional, esto permitirá obtener la dinámica que lleva el Ejército, traslados de personal especializado, pensar en la escalabilidad en cuanto a la adaptación que tendría en caso de seguir creciendo, capacidad operativa y proyección de la fuerza.

  La organización para la implementación del CSIRT en este caso iniciaría con:

    - Oficial de Ciberdefensa del comando del Ejercito: Supervisa la implementación técnica, la selección de herramientas y la capacitación del personal.
    - Equipo Técnico del CSIRT: Configura la infraestructura, establece los procesos de respuesta a incidentes y prueba la operatividad del CSIRT.
    - Representantes de Comunicaciones: Integran el CSIRT con los sistemas de comunicación existentes del Ejército.

  En cuanto al Batallón donde se implementaría el CSIRT estaría organizado de la siguiente manera:

El Batallón de Ciberseguridad podría estar compuesto por:

- **Compañías Especializadas:**
    - Detección y Análisis de Amenazas
    - Respuesta a Incidentes
    - Ingeniería y Desarrollo de Herramientas
    - Investigación y Análisis Forense
    - Capacitación y Concientización

- **Pelotones de Apoyo:**
    - Inteligencia Cibernética
    - Asuntos Legales
    - Relaciones Públicas
    -

Consideraciones Adicionales:

- El Batallón podría estar ubicado en un cantón militar con capacidad de brindar todas las herramientas tecnológicas para el fortalecimiento de las capacidades del CSIRT, con acceso a infraestructura tecnológica y comunicaciones seguras.

- El Batallón debería establecer mecanismos de cooperación con otros CSIRT militares, gubernamentales e internacionales, así como con el sector privado y la academia.

- El Batallón necesitará contar con herramientas y tecnologías de vanguardia para la detección, análisis y respuesta a incidentes cibernéticos.

3. Fase de Operación:

En la fase de operación es donde mas se requiere tener adelantada la parte legal de la organización del CSIRT, así como también el desarrollo doctrinal para la puesta en marcha de las operaciones en ese sentido se plantea contar con los siguientes equipos:

- Equipo de expertos: Analistas, investigadores, expertos en respuesta a incidentes, y personal de soporte técnico, personal militar experto en doctrina y operaciones militares.

- Visitas estratégicas a otros CSIRT: Coordinan la respuesta a incidentes que afecten a las operaciones militares, implementando convenios interinstitucionales que involucren la ciber diplomacia.

- Equipo de CSIRT externos: Colaboran en la detección y respuesta a amenazas a nivel nacional e internacional.

Obtener el apoyo de la gestión y el patrocinio

En cuanto al apoyo y patrocinio en la creación del CSIRT es importante tener cuenta generar confianza en las organizaciones que forman parte de los beneficiados por la creación del CSIRT; las instituciones a las cuales se les aporta seguridad y defensa en pro de mitigar la amenaza no deben sentir temor al reportar un incidente o solicitar apoyo, sobre todo en momentos de crisis, ya que un CSIRT es un organismo que, principalmente, provee apoyo, recomendaciones y mentoría, pero no impone, juzga o regula, en este sentido, con esta premisa es que debemos mostrar la importancia de nuestro proyecto y así mismo hacer ver que somos una institución encargada de la ciberseguridad y ciberdefensa del país.

Estos patrocinadores o socios serian:

- Ministerio de Defensa Nacional: Principal patrocinador y responsable de la seguridad nacional. Aportaría recursos financieros, infraestructura y apoyo político.
- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC): Colaboraría en la definición de políticas de ciberseguridad, capacitación y desarrollo de capacidades técnicas.
- Departamento Administrativo de Ciencia, Tecnología e Innovación (Colciencias): Podría financiar proyectos de investigación y desarrollo relacionados con la ciberseguridad militar.
- Comando General de las Fuerzas Militares: Aportaría recursos humanos, conocimiento especializado y apoyo logístico.

- **Sector Privado quienes se involucración como socios a través de convenios que estarían suscritos por el Comando del Ejército así:**

  - Empresas de tecnología y ciberseguridad: Podrían aportar soluciones tecnológicas, servicios de consultoría y capacitación especializada.
  - Bancos y entidades financieras: Podrían apoyar en la protección de sistemas financieros y en la prevención de fraudes cibernéticos.
  - Operadores de infraestructuras críticas: Podrían colaborar en la protección de sectores estratégicos como energía, telecomunicaciones y transporte.

- **Organismos Internacionales:**

  - Organización del Tratado del Atlántico Norte (OTAN): Podría ofrecer programas de cooperación en ciberdefensa, capacitación y ejercicios conjuntos.
  - Centro de Cooperación Hemisférica para la Ciberseguridad (OEA): Podría brindar asistencia técnica, intercambio de información y buenas prácticas en ciberseguridad.

- Comando Sur de los Estados Unidos: Podría colaborar en la capacitación, desarrollo de capacidades y ejercicios conjuntos.

Los dineros con los que se buscaría iniciar el proyecto vendrían de:

- Presupuesto Nacional: Asignación de recursos específicos en el presupuesto de defensa para la creación y operación del CSIRT.

- Cooperación Internacional: Búsqueda de fondos y programas de cooperación con organismos internacionales y países aliados.

- Alianzas público privadas: Establecimiento de acuerdos con empresas del sector privado para el desarrollo conjunto de soluciones y servicios de ciberseguridad.

Reunir información

El Csirt del ejército está orientado al seguimiento de la información que se encuentra circulando en el ciberespacio y sobre todo estudia y se prepararse para contrarrestar las posibles amenazas en cuanto a ciberseguridad y ciberdefensa que se pueda presentar contra el país y la infraestructura critica, estatal y privada, por ende se reconoce la necesidad de recolectar información de los siguientes aspectos para desarrollar las capacidades de este así:

Ataques dirigidos:

- APT (Amenazas Persistentes Avanzadas): Grupos de hackers patrocinados por estados u organizaciones criminales que buscan acceso a largo plazo a información clasificada o sistemas críticos. Ejemplos:
  - Operación Aurora: Ataque dirigido a empresas tecnológicas y de defensa en 2009.

    - Stuxnet: Gusano informático diseñado para sabotear sistemas industriales, utilizado contra Irán en 2010.

- Ataques de ransomware: Cifrado de datos y extorsión para su liberación. Ejemplos:
    - WannaCry: Ataque global en 2017 que afectó a hospitales, empresas y gobiernos.
    - Ryuk: Ransomware dirigido a grandes empresas y organizaciones.

- Campañas de phishing: Correos electrónicos fraudulentos diseñados para robar credenciales o instalar malware.

Ataques oportunistas:

- Malware: Software malicioso que infecta sistemas para robar datos, espiar o causar daño. Ejemplos:
-
    - Virus, gusanos, troyanos: Diversos tipos de malware con diferentes objetivos.
    - Botnets: Redes de dispositivos infectados controladas por atacantes.

- Ataques de denegación de servicio (DoS/DDoS): Sobrecarga de sistemas para interrumpir su funcionamiento.

- Vulnerabilidades de software: Fallos de seguridad en software que pueden ser explotados por atacantes.

Preparación del personal en la cultura de la ciberseguridad, es un aspecto fundamental en la preparación de las personas que integran las instituciones interesadas con el fin de evitar aspectos tales como:

- Errores humanos: Configuración incorrecta de sistemas, pérdida de dispositivos, apertura de archivos adjuntos maliciosos.

- Fugas de información: Divulgación accidental o intencional de información confidencial.

- Uso indebido de recursos: Utilización de sistemas y redes para actividades no autorizadas.

En cuanto a la seguridad y defensa del país se busca vincular a todas las instituciones que son esenciales para el funcionamiento del país y las instituciones que lo integran publicas y privadas tales como:

- Ataques a proveedores: Ataques a proveedores de servicios del Ejército que pueden afectar indirectamente a sus sistemas.

- Vulnerabilidades en la cadena de suministro: Fallos de seguridad en software o hardware de terceros que pueden ser explotados para atacar al Ejército.

El desarrollo de operaciones militares del CSIRT estarían orientadas a los diferentes incidentes que se han presentado en la historia, esto como punto inicial del desarrollo de la doctrina de las operaciones en ciberdefensa y ciberseguridad así:

- Guerra electrónica: Interferencia en comunicaciones y sistemas electrónicos militares.

- Ataques a sistemas de mando y control: Intentos de interrumpir o manipular las operaciones militares.

- Espionaje cibernético: Robo de información militar clasificada.

Antecedentes históricos CSIRT Ejercito:

El gobierno nacional ha tratado de fortalecer las capacidades cibernéticas del país, y en el año 2016 lanza la política de defensa y seguridad cibernética, Actualmente, el Ejército Nacional de Colombia se encuentra en proceso de fortalecer sus capacidades de ciberdefensa, incluyendo la formación de personal especializado, la adquisición de tecnología y la implementación de medidas de protección de sus sistemas de información.

Aunque aún no existe un CSIRT específico para el Ejército, los avances mencionados anteriormente sientan las bases para su futura creación. La experiencia adquirida en la implementación del Centro Cibernético del Comando Conjunto pueden ser aprovechados para el desarrollo de un CSIRT del ejército nacional.

Jurisdicción del CSIRT Ejército:

El ámbito de aplicación del CSIRT el Ejercito tiene como finalidad defender la infraestructura del estado y los hombres que la integran, así mismo garantizar la obediencia debida que tiene como responsabilidad el gobierno nacional para evitar el uso indebido de nuestro ciberespacio por cualquier agente interno o externo, así mismo se mantendrá la articulación con el sector privado con el fin de garantizar la capacidad de reacción ante cualquier amenaza cibernética, para lo que tendríamos que iniciar con:

- Sistemas y redes de información del Ejército Nacional: El CSIRT tendrá jurisdicción sobre todos los sistemas, redes, dispositivos y datos que sean propiedad o estén bajo el control del Ejército Nacional.

- Personal militar: El CSIRT tendrá jurisdicción sobre el personal militar en lo que respecta a incidentes de ciberseguridad que ocurran en el ámbito de sus funciones y responsabilidades.

- Operaciones militares: El CSIRT tendrá jurisdicción sobre la detección, análisis y respuesta a incidentes cibernéticos que puedan afectar las operaciones militares, tanto en tiempo de paz como en situaciones de conflicto.

- Sistemas y redes de otras entidades: El CSIRT no tendrá jurisdicción sobre sistemas y redes de información que pertenezcan a otras entidades gubernamentales o al sector privado, a menos que exista un acuerdo de cooperación específico.

- Delitos comunes: El CSIRT no tendrá jurisdicción sobre delitos comunes que no estén relacionados con la ciberseguridad o que no afecten directamente a los sistemas operaciones del Ejército. Estos casos serán competencia de las autoridades judiciales correspondientes.

- Asuntos de inteligencia: El CSIRT no tendrá jurisdicción sobre actividades de inteligencia cibernética, las cuales serán responsabilidad de las unidades de inteligencia del Ejército.

Misión de CSIRT Ejercito

El CSIRT del Ejército Nacional de Colombia protege la integridad, confidencialidad y disponibilidad de los sistemas, redes y datos del Ejército, desarrolla operaciones de ciberseguridad y ciberdefensa enmarcadas dentro de la reglamentación legal, generando un ambiente seguro mediante la detección temprana, análisis y respuesta efectiva a incidentes de ciberseguridad, como la recuperación de los sistemas afectados, garantizando la continuidad de las operaciones militares y la seguridad nacional.

Objetivos del CSIRT

- Prevenir: Implementar medidas de seguridad proactivas para reducir el riesgo de incidentes cibernéticos y fortalecer la resiliencia de los sistemas del Ejército.

- Detectar: Monitorear y analizar continuamente los sistemas y redes del Ejército para identificar amenazas y vulnerabilidades, así como detectar incidentes de ciberseguridad en etapas tempranas.

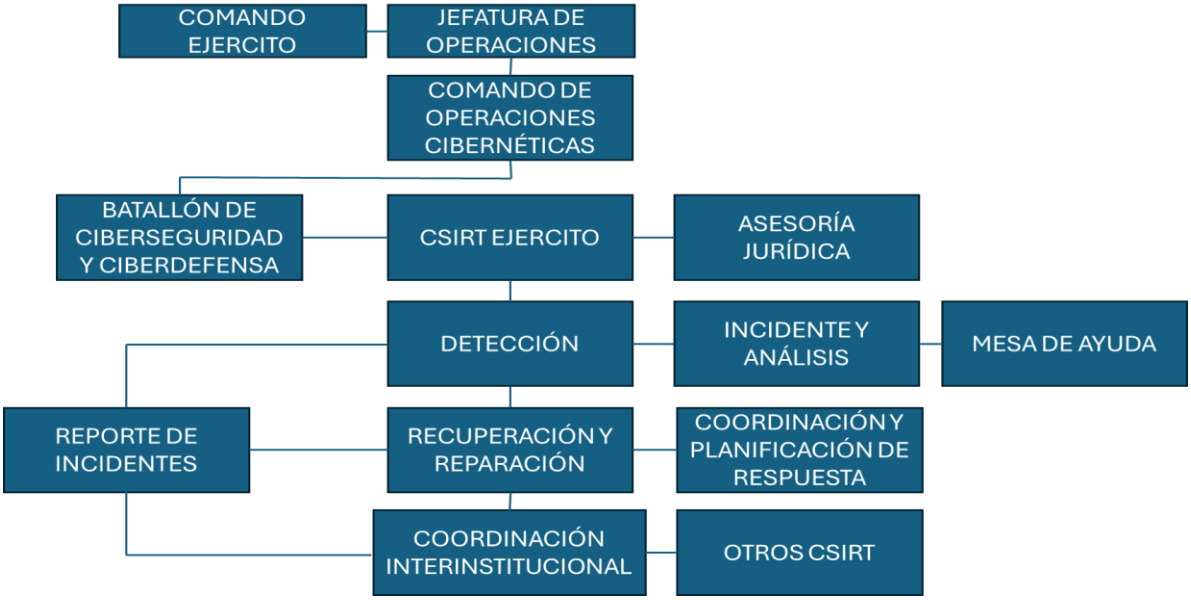
- Responder: Coordinar y ejecutar acciones de respuesta rápida y efectiva ante incidentes de ciberseguridad, minimizando el impacto en las operaciones militares y la seguridad nacional.
- Recuperar: Restaurar los sistemas y servicios afectados por incidentes de ciberseguridad, garantizando la continuidad de las operaciones militares y la disponibilidad de la información crítica.

- Concientizar: Promover una cultura de ciberseguridad en el Ejército Nacional, capacitando al personal militar sobre las amenazas y mejores prácticas de seguridad.

- Colaborar: Establecer alianzas y mecanismos de cooperación con otros CSIRT nacionales e internacionales, así como con el sector privado y la academia, para fortalecer la ciberdefensa del país.

- Investigar: Realizar investigaciones forenses de incidentes de ciberseguridad para identificar a los responsables y determinar las causas raíz, con el fin de mejorar las medidas de prevención y respuesta.

Organización del CSIRT Ejercito:



Elaboración Propia

BIBLIOGRAFÍA

- "Computer Security Incident Response Teams (CSIRTs): A Comprehensive Guide to Managing and Responding to Cyber Attacks" por Brian King, James J. Stapleton, y Kevin Mandia. Este libro proporciona una guía completa sobre la creación y gestión de CSIRT, incluyendo aspectos técnicos, operativos y legales.

- "Cybersecurity Framework" (NIST): Este marco proporciona un conjunto de estándares, directrices y prácticas recomendadas para la gestión del riesgo cibernético.
- Política de Defensa y Seguridad Cibernética (Ministerio de Defensa Nacional, 2016): Establece las directrices para la protección de la infraestructura crítica y los sistemas de información del sector defensa en Colombia.
- Estrategia Nacional de Ciberseguridad (2022): Define los objetivos y acciones para fortalecer la ciberseguridad en todos los sectores del país.
- GUÍA PRÁCTICA PARA CSIRTs Un modelo de negocio sustentable, Volumen 2, 2023