COMANDO DE INFORMÁTICA Y TÉCNOLOGÍA

CSIRT

“CSIRT”

ALUMNO:

TTE. DE INF. MORALES BATZ

INSTRUCTOR:

TTE. DE INTENDECIA CASTRO ROLDAN

GUATEMALA, 28 SEPTIEMBRE DE 2023

CSIRT PARA EL SECTOR MILITAR

A. ASOCIACIONES CLAVE

Ministerio de Defensa: Como entidad principal responsable de la defensa nacional, el Ministerio de Defensa es una asociación fundamental. Debe haber un memorando de entendimiento (MOU) que formalice la colaboración y defina roles y responsabilidades.

Otras Ramas Militares: Colaboración con todas las ramas militares (ejército, marina, fuerza aérea, etc.) para garantizar una respuesta unificada a las amenazas cibernéticas.

Unidades de Inteligencia Militar: Colaboración con unidades de inteligencia militar para el intercambio de información sobre amenazas cibernéticas y actividades de ciberespionaje.

Agencias de Seguridad Nacional: Establecer acuerdos de intercambio de información para compartir datos sobre amenazas cibernéticas y actividades maliciosas a nivel nacional.

Aliados Internacionales: Mantener relaciones con CSIRT militares de países aliados para el intercambio de información de inteligencia cibernética y la colaboración en la lucha contra amenazas cibernéticas globales.

Empresas de Defensa y Tecnología: Establecer alianzas estratégicas con proveedores de tecnología de defensa para garantizar la seguridad de los sistemas y equipos militares.

Organizaciones de la Industria de Defensa: Colaboración con asociaciones de la industria de defensa para obtener apoyo técnico y recursos relacionados con la ciberseguridad.

Organismos Gubernamentales de Regulación: Mantener una comunicación cercana con las autoridades reguladoras encargadas de la seguridad cibernética y cumplir con las normativas aplicables.

Redes de Inteligencia: Colaboración con redes de inteligencia y sistemas de alerta temprana para detectar amenazas cibernéticas en tiempo real.

B. ACTIVIDADES CLAVE Y RECURSOS CLAVE

Actividades Clave:

Detección de Amenazas Cibernéticas: Monitoreo constante de la red militar para identificar patrones de actividad sospechosa y amenazas emergentes.

Análisis de Incidentes: Investigación en profundidad de incidentes de seguridad cibernética para comprender la naturaleza de la amenaza y su impacto potencial.

Respuesta a Incidentes: Implementación de planes de respuesta para mitigar los incidentes y restaurar la operatividad normal de los sistemas.

Coordinación de Respuesta: Colaboración con asociados clave para garantizar una respuesta unificada y eficiente a incidentes cibernéticos.

Inteligencia Cibernética: Recopilación, análisis y diseminación de inteligencia cibernética para anticipar amenazas y tomar decisiones informadas.

Educación y Sensibilización: Desarrollo y ejecución de programas de capacitación en seguridad cibernética para el personal militar y civil.

Desarrollo de Políticas y Procedimientos: Establecimiento y revisión de políticas y procedimientos de seguridad cibernética para guiar las operaciones.

Cooperación Internacional: Colaboración con CSIRT militares extranjeros para compartir información sobre amenazas cibernéticas a nivel global.

Recursos Clave:

Personal Especializado: Contratación y retención de expertos en seguridad cibernética, incluyendo analistas, ingenieros y expertos forenses.

Herramientas de Seguridad Cibernética: Adquisición y mantenimiento de software y hardware especializado para monitorear, detectar y responder a amenazas.

Infraestructura de Red Segura: Mantenimiento de una infraestructura de red resistente y segura para garantizar la confidencialidad y la integridad de los datos.

Centro de Operaciones de Seguridad (SOC): Establecimiento de un SOC para el monitoreo constante y la respuesta en tiempo real a incidentes.

Laboratorio Forense Digital: Mantenimiento de un laboratorio especializado para el análisis forense de incidentes cibernéticos.

Comunicaciones Seguras: Establecimiento de canales seguros para compartir información clasificada y sensible con asociados clave.

Recursos de Capacitación: Desarrollo de materiales y programas de formación en seguridad cibernética para el personal.

Presupuesto: Asignación de recursos financieros para operaciones y adquisiciones de seguridad cibernética.

Alianzas Estratégicas: Mantenimiento de relaciones sólidas con asociaciones clave y colaboradores estratégicos para apoyo y recursos adicionales.

Políticas y Normativas: Desarrollo y actualización constante de políticas y normativas de seguridad cibernética para guiar y respaldar las operaciones del CSIRT.

C. PROPUESTA DE VALOR

El CSIRT Militar se compromete a salvaguardar la seguridad cibernética del sector militar y la nación mediante:

Seguridad Integral: Proporcionamos una seguridad cibernética completa, desde la detección de amenazas hasta la respuesta efectiva.

Respuesta Ágil: Estamos disponibles las 24/7 para abordar amenazas cibernéticas en tiempo real.

Colaboración Global: Mantenemos alianzas estratégicas con CSIRT militares internacionales y compartimos información para fortalecer la seguridad global.

Expertos en Ciberseguridad: Contamos con un equipo altamente capacitado en seguridad cibernética.

Infraestructura Segura: Garantizamos la seguridad de los sistemas y comunicaciones críticas.

Educación y Cultura de Seguridad: Promovemos la formación en seguridad cibernética para el personal militar.

Cumplimiento Normativo: Operamos según las políticas y normativas de seguridad cibernética.

Soporte a la Misión Militar: Contribuimos al éxito de las misiones militares protegiendo sistemas y comunicaciones.

Confidencialidad y Seguridad: Mantenemos altos estándares de confidencialidad y seguridad en la gestión de información sensible.

Coordinación Efectiva: Trabajamos en estrecha colaboración con el Ministerio de Defensa y otras entidades para una respuesta unificada.

D. RELACIONES Y CANALES

Relaciones

Junta Directiva del CSIRT: La junta directiva del CSIRT debe establecer un comité de seguridad cibernética que incluya representantes de alto nivel de las diversas ramas militares y unidades de inteligencia.

Equipo de Respuesta a Incidentes: Establecer relaciones cercanas con el equipo de respuesta a incidentes interno para garantizar una comunicación fluida y una colaboración eficiente durante los incidentes cibernéticos.

Unidades de Inteligencia Militar: Mantener una relación estrecha con las unidades de inteligencia militar para compartir información sobre amenazas cibernéticas y actividades de ciberespionaje.

Relaciones Externas:

CSIRT de Aliados Internacionales: Establecer acuerdos de colaboración con CSIRT militares de países aliados para compartir información de inteligencia cibernética y coordinar respuestas a amenazas globales.

Agencias de Seguridad Nacional: Mantener relaciones con agencias de seguridad nacional y organismos gubernamentales encargados de la ciberseguridad para el intercambio de información y recursos.

Empresas de Defensa y Tecnología: Establecer alianzas estratégicas con proveedores de tecnología de defensa para garantizar la seguridad de los sistemas y equipos militares.

Organizaciones de la Industria de Defensa: Colaborar con asociaciones de la industria de defensa para obtener apoyo técnico y recursos relacionados con la ciberseguridad.

Canales de Comunicación:

Centro de Operaciones de Seguridad (SOC): Establecer un SOC para el monitoreo constante de la red militar y la comunicación interna en tiempo real durante incidentes cibernéticos.

Redes de Inteligencia Cibernética: Utilizar redes de inteligencia cibernética para compartir información de inteligencia sobre amenazas cibernéticas en tiempo real.

Sistema de Alerta Temprana: Implementar un sistema de alerta temprana que permita la notificación rápida de amenazas cibernéticas a las partes interesadas clave.

Plataforma de Colaboración Segura: Utilizar una plataforma segura de colaboración en línea para compartir información clasificada y sensible con aliados internacionales y agencias gubernamentales.

Comunicaciones Codificadas: Establecer comunicaciones codificadas para garantizar la confidencialidad de la información compartida.

Relaciones de Confianza:

Establecer Acuerdos Formales: Formalizar relaciones mediante acuerdos y MOUs que definan claramente roles, responsabilidades y expectativas.

Participación en Ejercicios Conjuntos: Colaborar en ejercicios conjuntos de ciberseguridad con asociados clave para fortalecer la capacidad de respuesta.

Compartir Información Sensible: Fomentar la confianza al compartir información relevante y sensible de manera segura y oportuna.

Participación en Comités de Ciberseguridad: Ser miembro activo en comités de ciberseguridad gubernamentales y de la industria para estar al tanto de las últimas amenazas y tendencias.

E. COMUNIDAD

1. Participación en Foros y Grupos de Discusión:

   Foros de Seguridad Cibernética: El CSIRT Militar debe participar activamente en foros de seguridad cibernética nacionales e internacionales, donde se discuten tendencias, amenazas y soluciones. La contribución a estos foros con información relevante es fundamental.

   Grupos de Trabajo: Unirse a grupos de trabajo dedicados a la seguridad cibernética, tanto en el ámbito militar como civil, para colaborar en proyectos conjuntos y compartir mejores prácticas.

2. Colaboración con la Industria:

   Asociaciones de Ciberseguridad: Mantener relaciones sólidas con asociaciones de ciberseguridad de la industria para acceder a la experiencia de la comunidad empresarial en la protección contra amenazas cibernéticas.

   Participación en Conferencias y Eventos: Asistir a conferencias y eventos de ciberseguridad para establecer contactos con líderes de la industria y estar al tanto de las últimas tecnologías y amenazas.

3. Capacitación y Concienciación Pública:

   Programas de Sensibilización: Desarrollar programas de sensibilización en seguridad cibernética para educar al público en general y fomentar prácticas seguras en línea.

   Participación en Campañas de Ciberseguridad: Colaborar con campañas de concienciación en ciberseguridad gubernamentales y de la industria para difundir información sobre amenazas y buenas prácticas.

4. Colaboración con Academia:

   Asociación con Instituciones Educativas: Establecer alianzas con instituciones educativas y universidades que ofrezcan programas de ciberseguridad para fomentar la investigación y el desarrollo de talento en seguridad cibernética.

   Programas de Pasantías y Becas: Ofrecer programas de pasantías y becas para estudiantes de seguridad cibernética con el objetivo de atraer talento joven al campo.

5. Compartir Información con Comunidades Militares y de Defensa:

Colaboración con Organizaciones de Defensa: Mantener relaciones con otras organizaciones militares de defensa y compartir información sobre amenazas cibernéticas y tácticas utilizadas por actores adversarios.

Participación en Ejercicios Conjuntos: Colaborar en ejercicios de seguridad cibernética conjuntos con otras ramas militares y fuerzas de seguridad.

6. Colaboración Internacional:

Participación en Redes Internacionales: Ser parte de redes internacionales de CSIRT militares para compartir información y colaborar en la protección contra amenazas globales.

Intercambio de Expertos: Facilitar intercambios de expertos en seguridad cibernética con aliados internacionales para el enriquecimiento mutuo de conocimientos.

7. Portal de Recursos para la Comunidad:

Desarrollo de un Portal de Recursos: Establecer un portal en línea que brinde acceso a recursos de seguridad cibernética, informes de amenazas y herramientas útiles para la comunidad.

F. FUENTES DE INGRESOS

Personal Especializado: Los costos de personal representan una parte significativa del presupuesto. Esto incluye salarios, beneficios, capacitación y desarrollo continuo del equipo de seguridad cibernética.

Infraestructura Tecnológica: Inversiones en hardware y software especializado, servidores, sistemas de monitoreo, herramientas de seguridad cibernética y licencias de software.

Operaciones del Centro de Operaciones de Seguridad (SOC): Mantenimiento y operación del SOC, incluyendo monitores, consolas, energía, conectividad y sistemas de gestión de incidentes.

Capacitación y Sensibilización: Recursos para desarrollar y ejecutar programas de capacitación en seguridad cibernética para el personal militar y otros usuarios.

Investigación y Desarrollo: Fondos destinados a investigaciones en seguridad cibernética, desarrollo de herramientas de seguridad y tecnologías de próxima generación.

Gastos Generales: Costos administrativos, alquiler de instalaciones, servicios públicos, suministros de oficina y otros gastos generales relacionados con la operación diaria.

Equipamiento de Laboratorio Forense: Mantenimiento y actualización de equipos y herramientas forenses utilizados en la investigación de incidentes cibernéticos.

Comunicaciones Seguras: Mantenimiento de sistemas de comunicación segura para la coordinación con partes interesadas clave.

Adquisición de Inteligencia Cibernética: Compra de datos y servicios de inteligencia cibernética para enriquecer la comprensión de las amenazas.

Seguridad Física y Controles de Acceso: Implementación y mantenimiento de medidas de seguridad física para proteger las instalaciones y los activos del CSIRT.

Marketing y Promoción: Si se ofrecen servicios de consultoría o capacitación, es necesario incluir gastos relacionados con la promoción y el marketing.

Gastos de Cumplimiento y Regulación: Costos asociados con el cumplimiento de las regulaciones de seguridad cibernética y la auditoría.

Respaldo Financiero para Respuesta a Incidentes: Un fondo dedicado para cubrir los costos inmediatos relacionados con la respuesta a incidentes cibernéticos.

Apoyo a Comunidades de Ciberseguridad: Si el CSIRT participa en programas de concienciación y colaboración, se deben asignar recursos para estos esfuerzos.

Seguro de Ciberseguridad: La inversión en pólizas de seguro de ciberseguridad para mitigar los riesgos financieros en caso de incidentes graves.

Inversión en Innovación: Fomentar la innovación en seguridad cibernética mediante la asignación de fondos para investigar y adoptar tecnologías emergentes.

Reservas de Emergencia: Mantener una reserva financiera para hacer frente a crisis imprevistas o incidentes cibernéticos graves.