Seminario de Seguridad Informática con énfasis en hacking ético.

joseroberto.rivas@itservicesin.com

503-78876717

07/Febrero/2021

INGENIERO JOSE ROBERTO RIVAS MAGAÑA. MBA. M.SC.

DOCENTE MINED NIVEL I, GERENTE DE PROYECTOS Y AUDITOR LIDER INTEGRADO.

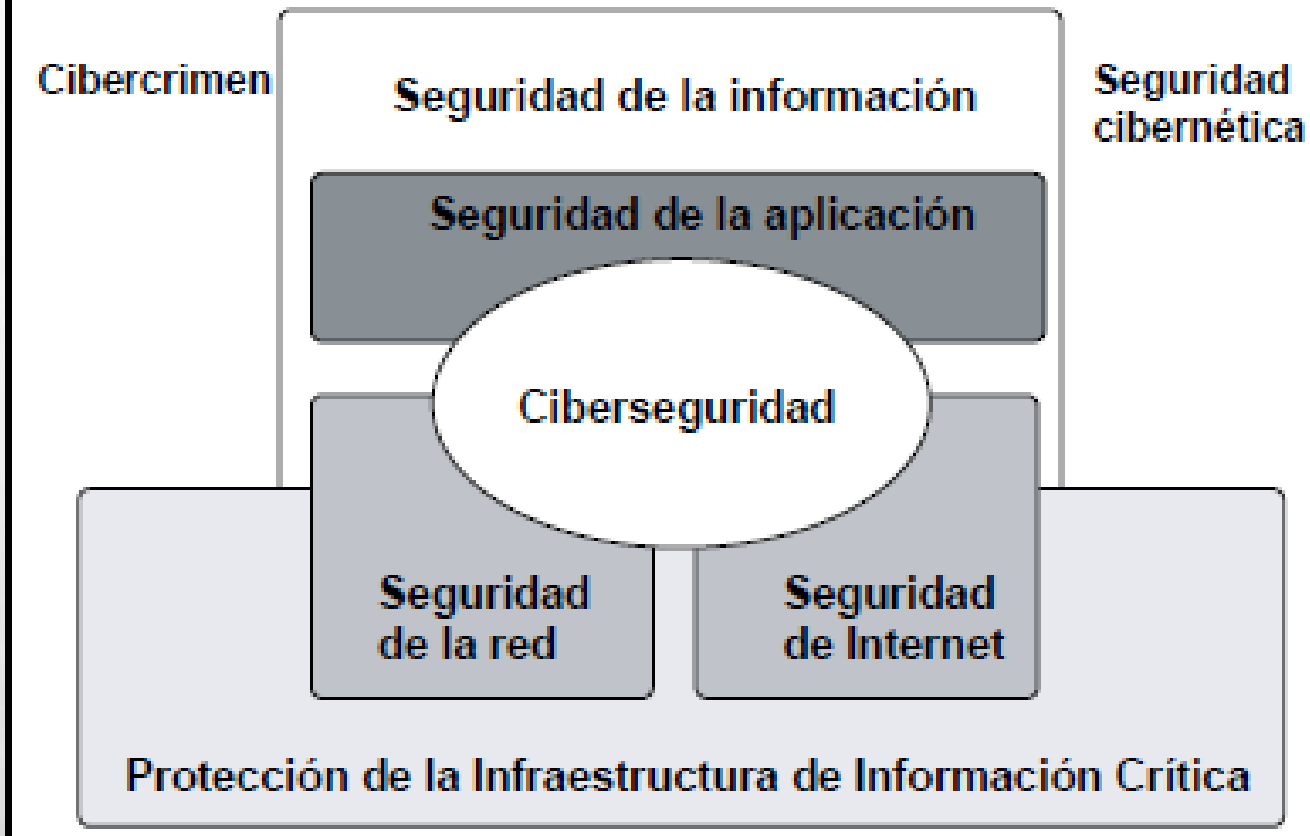
1. INTRODUCCIÓN A LA CIBERSEGURIDAD

1.1 INTRODUCCION A CIBERSEGURIDAD

¿QUE ES CIBERSEGURIDAD?

- LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN Y SE REALIZA ABORDANDO LAS AMENAZAS A LA INFORMACIÓN PROCESADA ALMACENADA Y TRANSPORTADA POR LOS SISTEMAS DE INFORMACIÓN INTERCONECTADOS.

Figura 1.2—Relación entre la ciberseguridad y otros dominios de la seguridad



Fuente: Organización internacional de normalización, *ISO/IEC 27032:2012: Information technology—Security techniques—Guidelines for cybersecurity*, Suiza, 2012

CONCIENCIA SITUACIONAL

Comprensión del entorno organizacional

Conocimiento de amenazas de información

Profesionales en Ciberseguridad

FACTORES TECNOLÓGICOS QUE AFECTAN LA SEGURIDAD

- NIVEL DE COMPLEJIDAD DE IT
- CONECTIVIDAD DE RED INTERNA, TERCERO, PUBLICO
- DISPOSITIVOS ESPECIALIZADOS DE LA INDUSTRIA INSTRUMENTACIÓN
- PLATAFORMAS, APLICACIONES Y HERRAMIENTAS
- EN INSTALACIONES EN LA NUBE O SISTEMAS HIBRIDOS
- SOPORTE OPERATIVO PARA SEGURIDAD
- COMUNIDAD DE USUARIOS Y CAPACIDADES
- HERRAMIENTAS DE SEGURIDAD NUEVAS O EMERGENTES

FACTORES RELACIONADOS CON EL NEGOCIO QUE AFECTAN LA SEGURIDAD

- NATURALEZA DEL NEGOCIO
- TOLERANCIA AL RIESGO Y APETITO
- MISIÓN DE SEGURIDAD, VISIÓN Y ESTRATEGIA
- ALINEACIÓN DE LA INDUSTRIA Y TENDENCIAS DE SEGURIDAD
- REQUISITOS Y REGULACIONES DE CUMPLIMIENTO
- FUSIONES, ADQUISICIONES Y ASOCIACIONES
- OUTSOURCING DE SERVICIOS O PROVEDORES

1.2 DIFERENCIA ENTRE SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD

SEGURIDAD DE INFORMACIÓN VS CIBERSEGURIDAD

Seguridad de información

- ATENCIÓN, PROTECCIÓN DE IN FORMACIÓN, INDEPENDIENTEMENTE DE FORMATO, INCLUYENDO
- DOCUMENTOS DE PAPEL
- PROPIEDAD DIGITAL E INTELECTUAL
- COMUNICACIONES VERBALES O VISUALES

ciberseguridad

- ATENCIÓN, PROTECCIÓN DE RECURSOS DIGITALES, INCLUYENDO
- HARDWARE DE RED
- SOFTWARE
- INFORMACIÓN PROCESADA Y ALMACENADA EN SISTEMAS AISLADOS O EN RED

PROTECCIÓN DE ACTIVOS DIGITALES

National Institute of Standards and Technology
U.S. Department of Commerce

Identificar

- Utilizar la comprensión organizacional para minimizar el riesgo para los sistemas, activos, datos y capacidades.

Proteger

- Diseñar salvaguardas para limitar el impacto de eventos potenciales en los servicios e infraestructura críticos

Detectar

- implementar actividades para identificar la ocurrencia de un evento de ciberseguridad.

Responder

tomar las medidas apropiadas después de enterarse de un evento de seguridad

Recuperar

planificar para tener la resiliencia y la recuperación oportuna de capacidades y servicios comprometidos

Figura 1: Implementación del MCS: Público Objetivo y Beneficios

Rol del Marco	Rol/Función	Beneficio de/Razón para Aplicar el Marco
Ejecutivo	Consejo y Dirección Ejecutiva	• Comprensión de sus responsabilidades y roles en ciberseguridad dentro de la organización. • Mejor comprensión de la postura de ciberseguridad actual. • Mejor comprensión del riesgo de ciberseguridad para la organización. • Mejor comprensión del estado objetivo de ciberseguridad. • Comprensión de las acciones requeridas para cerrar las brechas de seguridad entre la postura de ciberseguridad actual y el estado objetivo.
Negocio/Proceso	Gerencia de TI	• Concienciación de los impactos en el negocio. • Comprensión de la relación de los sistemas de negocio con el apetito de riesgo asociado.
Negocio/Proceso	Gestión de Procesos de TI	• Comprensión de los requerimientos del negocio y los objetivos de la misión y sus prioridades.
Negocio/Proceso	Gestión de Riesgos	• Visión mejorada del entorno operacional para discernir la probabilidad de un evento de ciberseguridad.
Negocio/Proceso	Expertos Legales	• Comprensión de las amenazas cibernéticas a las unidades de negocio y sus objetivos de la misión. • Comprensión de todos los requerimientos de cumplimiento para cada unidad de negocio.
Implementación/Operador	Equipo de Implementación	• Comprensión de los controles de seguridad y su importancia en la gestión de riesgos de seguridad operacional. • Comprensión detallada de las acciones requeridas para cerrar las brechas en los requerimientos de ciberseguridad.
Implementación/Operador	Empleados	• Comprensión de los requerimientos de ciberseguridad para los sistemas de negocio asociados.

Figura 12: Identificadores y Categorías del Marco Básico

Categoría Único Identificador	Funciones	Función Único Identificador	Categorías
ID	Identificar	AM	Gestión de Activos
		BE	Entorno de Negocio
		GV	Gobierno
		RA	Evaluación del riesgo
		RM	Estrategia de Gestión de Riesgos
PR	Proteger	AC	Control de Acceso
		AT	Concienciación y Capacitación
		DS	Seguridad de los Datos
		IP	Procesos e Información de Protección de Información
		PT	Tecnología de Protección
DE	Detectar	AE	Anomalías y Eventos
		CM	Monitoreo Continuo de Seguridad
		DP	Procesos de Detección
RS	Responder	CO	Comunicaciones
		AN	Análisis
		MI	Mitigación
		IM	Mejoras
RC	Recuperar	RP	Planificación de Recuperación
		IM	Mejoras
		CO	Comunicaciones

Fuente: *Marco para Mejorar la Ciberseguridad de la Infraestructura Crítica*, NIST, EE. UU., 2014, tabla 1