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.

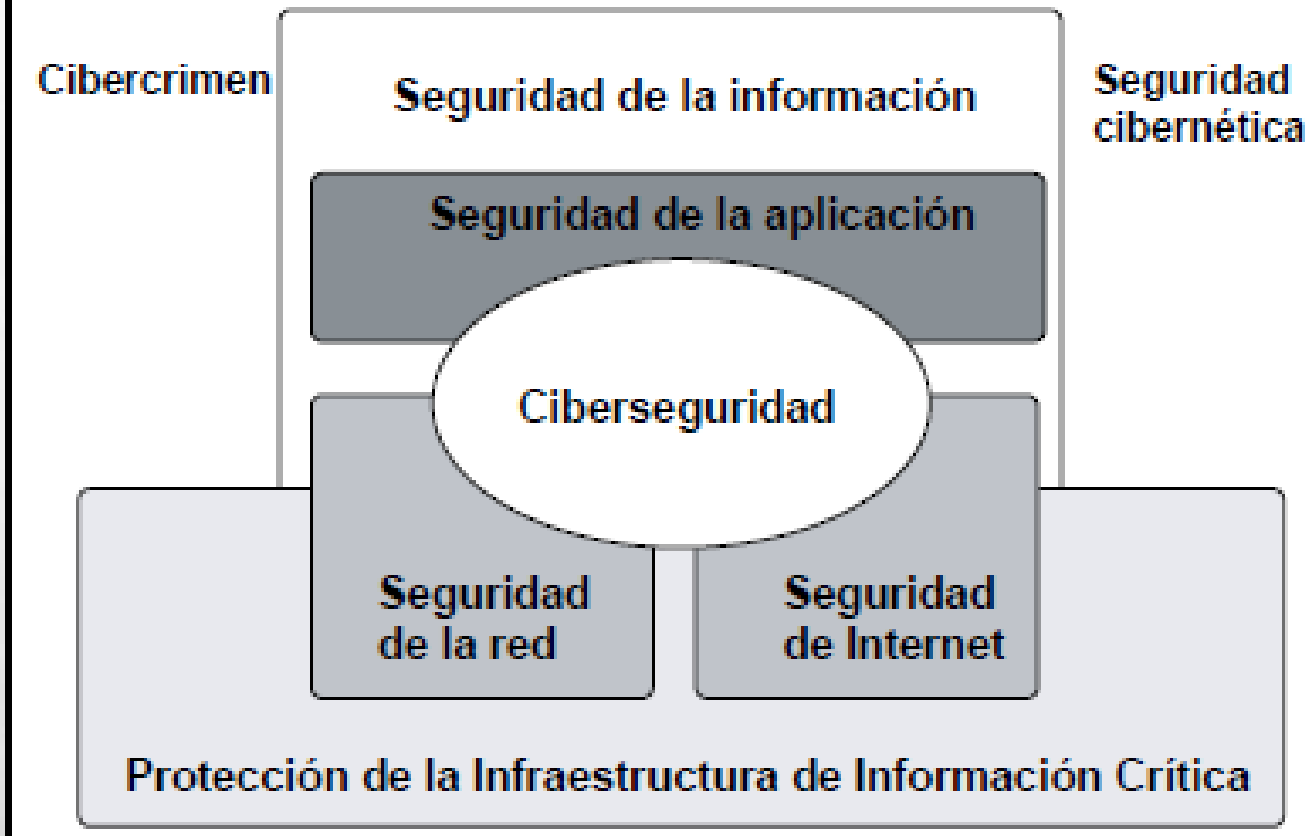
1. INTRODUCCIÓN A LA CIBERSEGURIDAD

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

GOBIERNO Y GESTIÓN DE LAS TIC'S

ISACA APOYA LOS CONOCIMIENTOS Y LAS HABILIDADES PARA AYUDAR A LOS PROFESIONALES EN EL ALCANCE DE OBJETIVOS ESTRATÉGICOS Y OBTENER LOS BENEFICIOS DEL NEGOCIO. MEDIANTE EL USO EFECTIVO E INNOVADOR DE LA TECNOLOGÍA.

TERMINOS CLAVES DE ISACA

EMPRESA: UN GRUPO DE PERSONAS QUE TRABAJAN JUNTAS PARA ALCANZAR **UN PROPÓSITO COMÚN**, NORMALMENTE EN EL CONTEXTO DE UNA ORGANIZACIÓN COMO UNA CORPORACIÓN, AGENCIA PÚBLICA, CARIDAD O FIDEICOMISO.

ES UNA ESTRUCTURA DE COMPONENTES RELACIONADOS ENTRE SI, DEFINIDA POR UN **OBJETIVO Ó ALCANCE PARTICULAR**. (CONTINUACION)

GOBIERNO: ASEGURA QUE LAS NECESIDADES, CONDICIONES Y OPCIONES DE LAS PARTES INTERESADAS SE EVALÚAN PARA DETERMINAR LOS OBJETIVOS EMPRESARIALES EQUILIBRADOS Y ACORDADOS QUE DEBEN LOGRARSE; ESTABLECER UNA DIRECCIÓN A TRAVÉS DE LA PRIORIZACIÓN Y TOMA DE DECISIONES; Y MONITOREAR EL DESEMPEÑO Y CUMPLIMIENTO DE LA DIRECCIÓN Y LOS OBJETIVOS ACORDADOS.

GESTIÓN: PLANIFICA, CONSTRUYE, EJECUTA Y MONITOREA ACTIVIDADES, ALINEADAS CON LA DIRECCIÓN ESTABLECIDA POR EL ÓRGANO DE GOBIERNO PARA ALCANZAR LOS OBJETIVOS DE LA EMPRESA.

"LAS INTRUSIONES CIBERNÉTICAS REPETIDAS EN LA INFRAESTRUCTURA CRÍTICA DEMUESTRAN LA NECESIDAD DE UNA CIBERSEGURIDAD MEJORADA. LA AMENAZA CIBERNÉTICA CONTRA LA INFRAESTRUCTURA CRÍTICA NO PARA DE CRECER Y REPRESENTA UNO DE LOS MÁS GRAVES RETOS DE SEGURIDAD NACIONAL QUE DEBEMOS AFRONTAR." ORDEN EJECUTIVA EE. UU. 13636.

COBIT: *CREA UN VALOR AGREGADO ÓPTIMO DE LAS TI ASEGURANDO EL EQUILIBRIO ENTRE LA OBTENCIÓN DE BENEFICIOS Y LA OPTIMIZACIÓN DE LOS NIVELES DE RIESGO Y EL USO DE RECURSOS. PERMITE QUE LAS TIC'S SEAN GOBERNADAS Y GESTIONADAS DE MANERA HOLÍSTICA EN TODA LA EMPRESA, TOMANDO PLENA RESPONSABILIDAD DE LAS ÁREAS FUNCIONALES DEL NEGOCIO Y SUS PARTES INTERESADAS INTERNAS Y EXTERNAS.*

1.3 OBJETIVOS DE CIBERSEGURIDAD

CONCEPTOS CLAVES DE S.I.

Confidencialidad
La protección de la información contra el acceso y la divulgación no autorizada

Integridad
La protección de la información contra la modificación no autorizada.

Disponibilidad
La capacidad de acceder a la información y recursos requeridos por el proceso de negocio en forma oportuna y confiable

CONSECUENCIAS DE PÉRDIDA Y MÉTODOS DE PRESERVACIÓN

CONFIDENCIALIDAD

LA PROTECCIÓN DE INFORMACIÓN DESDE DIVULGACIÓN NO AUTORIZADA

Consecuencias de perdida incluidas

divulgación de información protegida por leyes de privacidad

Pérdida de confianza del público

Pérdida de ventaja competitiva

Acción legal contra la empresa

Interferencia con la seguridad nacional

pérdida de cumplimiento

métodos de preservación incluidos

control de acceso

permisos de archivo

Cifrada (Encriptada)

INTEGRIDAD

LA PRECISIÓN Y LA INTEGRIDAD DE LA INFORMACIÓN DE ACUERDO CON LOS VALORES Y EXPECTATIVAS DEL NEGOCIO

Consecuencias de perdida incluidas

Inexactitud

Decisiones erróneas

Fraude

Falla de hardware

Pérdida de cumplimiento

Métodos de preservación incluidos

control de acceso

Inicio sesión

firmas digitales

Hashes

Copias de seguridad

Cifrada

DISPONIBILIDAD

LA CAPACIDAD DE ACCEDER A INFORMACIÓN Y RECURSOS REQUERIDOS POR EL PROCESO DE NEGOCIO.

Consecuencia de perdida incluidas

pérdida de funcionalidad y operación efectiva

pérdida de tiempo productivo

multas de reguladores o una demanda

interferencia con los objetivos de la empresa

pérdida de cumplimiento

Métodos de perseverancia incluidos

redundancia de red, sistema, datos

arquitecturas de sistemas altamente disponibles

copias de seguridad

controles de acceso

Un buen diseño de recuperación ante desastres

plan o plan de continuidad comercial

NO REPUDIO

- EL NO REPUDIO SE REFIERE AL CONCEPTO DE ASEGURAR QUE UN MENSAJE U OTRA INFORMACIÓN SEA GENUINA
- EN CIBERSEGURIDAD, LA INFORMACIÓN RECIBIDA DEBE VERIFICARSE COMO PROVENIENTE DE LA FUENTE DE ENVÍO REAL INDICADA
- TAMBIÉN ES IMPORTANTE QUE NI EL REMITENTE NI EL RECEPTOR PUEDAN NEGAR MÁS TARDE QUE ENVIARON O RECIBIERON LA INFORMACIÓN
- LAS NO REPUDIACIONES SE IMPLEMENTAN MEDIANTE FIRMAS DIGITALES Y REGISTROS TRANSACCIONALES

1.4 GOBIERNO DE LA CIBERSEGURIDAD

GOBIERNO, GESTION DE RIESGOS Y CUMPLIMIENTO

GESTIÓN DEL RIESGO

El proceso de la organización para manejar el riesgo en niveles aceptables

GOBIERNO

- Asegura que los objetivos sean alcanzados
- Garantiza que el clima de riesgo sea manejado apropiadamente
- Verifica que los recursos se usen adecuadamente

CUMPLIMIENTO

El acto de alinearse y la capacidad de demostrar adherencia a los requerimientos definidos por leyes y regulaciones

ROLES DE CIBERSEGURIDAD

- **JUNTA DIRECTIVA**

IDENTIFICA ACTIVOS CLAVE Y VERIFICA QUE LOS NIVELES Y PRIORIDADES DE PROTECCIÓN SON APROPIADOS

- **COMITÉ EJECUTIVO**

ESTABLECE EL TONO PARA LA GESTIÓN DE LA SEGURIDAD CIBERNÉTICA Y GARANTIZA QUE LAS FUNCIONES NECESARIAS, LOS RECURSOS Y LA INFRAESTRUCTURA ESTÉN DISPONIBLES Y SE UTILICEN ADECUADAMENTE

- **GERENTE DE SEGURIDAD DE LA INFORMACION**

DESARROLLA ESTRATEGIAS DE SEGURIDAD Y MITIGACIÓN DE RIESGOS, IMPLEMENTA PROGRAMAS DE SEGURIDAD Y GESTIONA INCIDENTES Y REMEDIACIÓN

- **PROFESIONALES DE LA CIBERSEGURIDAD**

DISEÑAR, IMPLEMENTAR Y GESTIONAR PROCESOS Y CONTROLES TÉCNICOS Y RESPONDER A EVENTOS E INCIDENTES

1.5 DOMINIOS DE LA CIBERSEGURIDAD

DOMINIOS DE CIBERSEGURIDAD

- Conceptos de ciberseguridad
- principios de arquitectura de seguridad
- Seguridad de red ,sistemas, aplicación y datos
- Respuesta a incidentes
- implicaciones de seguridad y adopción de tecnología en evolución

Evaluación de conocimientos adquiridos.