

INDICE

INTRODUCCIÓN	1
EMPRESA, SISTEMA DE INFORMACIÓN (SI) Y TECNOLOGÍAS DE LA INFORMACIÓN (TI)	3
INFORMACIÓN, COMPONENTES Y ESTRUCTURA DE LOS SI	9
INTERACCIONES DEL SI CON LA CADENA DE VALOR Y CON LOS DEMÁS SISTEMAS DE LA EMPRESA	16
SUBSISTEMAS TÍPICOS DE INFORMACIÓN EN LAS EMPRESAS	18
TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN	23
SOCIEDAD, EMPRESA Y NUEVAS TECNOLOGÍAS	29
LOS SISTEMAS DE GESTIÓN DE LOS SERVICIOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN (SGSTI)	41
• CONCEPTO Y CARACTERÍSTICAS	41
• COMPONENTES BÁSICOS Y MACROACTIVIDADES DEL SGSTI	43
• FASES RECOMENDADAS PARA DEFINIR EL SGSTI	44
SISTEMAS DE INFORMACIÓN Y MATRIZ DE INFORMACIÓN	47
CONSIDERACIONES SOBRE LAS TECNOLOGÍAS DE LA INFORMACIÓN COMO SOPORTE DE LOS SISTEMAS DE INFORMACIÓN	50
CONSIDERACIONES SOBRE LA INFLUENCIA DE LOS SISTEMAS DE INFORMACIÓN EN LAS ORGANIZACIONES	56
SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN	59
ENFOQUE DE LOS SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN (SGSI)	60
INTRODUCCIÓN, PLANTEAMIENTO Y ENFOQUE GENERAL DE LAS AUDITORÍAS INFORMÁTICAS	65
• INTRODUCCIÓN	65
• AUDITORÍA INFORMÁTICA DE LA EFICIENCIA	71
○ AUDITORÍA INFORMÁTICA DE LA PLANIFICACIÓN	72
○ <u>EJEMPLO</u> ILUSTRATIVO	76
○ AUDITORÍA INFORMÁTICA DE LA ORGANIZACIÓN Y ADMINISTRACIÓN	77
○ <u>EJEMPLO</u> ILUSTRATIVO	81
○ AUDITORÍA INFORMÁTICA DE LA EXPLOTACIÓN	83
○ <u>EJEMPLO</u> ILUSTRATIVO	86
○ AUDITORÍA INFORMÁTICA DEL DESARROLLO DE SISTEMAS	87
○ <u>EJEMPLO</u> ILUSTRATIVO	91
• AUDITORÍA INFORMÁTICA DE SEGURIDAD	92
○ AUDITORÍA INFORMÁTICA EN EL ENTORNO DEL HARDWARE	95
○ <u>EJEMPLO</u> ILUSTRATIVO	105
○ AUDITORÍA INFORMÁTICA EN EL ENTORNO DEL SOFTWARE	107
○ <u>EJEMPLO</u> ILUSTRATIVO	115
• PLANES DE CONTINGENCIA	118
○ Fase 1: INICIO DEL PLAN	122
○ Fase 2: DESARROLLO DE COMPONENTES CLAVE	123
▪ PROCEDIMIENTOS ORGANIZATIVOS	123
▪ PROCEDIMIENTOS ACTIVOS	134
○ Fase 3: DOCUMENTACIÓN DEL PLAN	137

○ Fase 4: PRUEBA Y MANTENIMIENTO	138
CONCEPTOS, DIRECTRICES Y CONSIDERACIONES PARA EL ESTABLECIMIENTO DE SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN DE CONFORMIDAD CON ISO/IEC 27001	139
• INTRODUCCIÓN	139
• ACTIVOS DE LA INFORMACIÓN	143
• <u>CASO PRÁCTICO RESUELTO</u>	147
• <u>RESPUESTA RECOMENDADA</u>	148
• INVENTARIO DE ACTIVOS DE INFORMACIÓN	149
• <u>EJEMPLO DE FICHA DE UN ACTIVO DE INFORMACIÓN</u>	152
• ACTUALIZACIÓN DEL INVENTARIO DE ACTIVOS Y CARACTERÍSTICAS BÁSICAS DE LA INFORMACIÓN	156
• VULNERABILIDADES, AMENAZAS, INCIDENTES, IMPACTOS Y RIESGOS	157
• <u>EJEMPLOS DE CAUSAS DE VULNERABILIDADES</u>	165
• CATÁLOGO DE AMENAZAS E INTRUSOS EN EL SISTEMA	172
• <u>EJEMPLO DE CATÁLOGO DE AMENAZAS PARA LA SEGURIDAD DE LA INFORMACIÓN</u>	174
• ANÁLISIS Y DETERMINACIÓN DE LOS RIESGOS	179
• MAPA DE RIESGOS	191
• COSTE DE LOS DAÑOS CAUSADOS POR UN ATAQUE A UN ACTIVO	192
• INVERSIÓN Y COSTE DE LA SEGURIDAD DE LA INFORMACIÓN	192
• <u>EJEMPLOS DE ACTUACIONES PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN</u>	193
• OTRAS CONSIDERACIONES DE INTERÉS SOBRE LA VALORACIÓN DE ACTIVOS Y ASIGNACIÓN DE RIESGOS	194
• <u>EJEMPLO DE VALORACIÓN DEL IMPACTO EN LOS ACTIVOS</u>	197
• RESPONSABLES DE LOS RIESGOS	197
• DECLARACIÓN DE APLICABILIDAD DE LOS CONTROLES DE SEGURIDAD	197
• POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN	198
• OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	201
PLANTEAMIENTO Y ENFOQUE DE LOS PROYECTOS DE ANÁLISIS DE RIESGOS	205
• ROLES Y FUNCIONES	205
• ACTIVIDADES PRELIMINARES	208
○ Estudio de oportunidad	208
○ Determinación del alcance del proyecto	211
○ Planificación del proyecto	214
○ Lanzamiento del proyecto	216
• CONSIDERACIONES SOBRE LA ELABORACIÓN DEL ANÁLISIS DE RIESGOS	217
○ Objetivos de las actividades del análisis de riesgos	217
○ Consideraciones sobre las fases del análisis de riesgos	218
○ Consideraciones sobre la determinación de los activos	219
○ Consideraciones sobre las vulnerabilidades	225

○ Consideraciones sobre las amenazas	225
○ Consideraciones sobre los impactos potenciales	227
○ Consideraciones para la determinación del riesgo potencial	229
○ Consideraciones sobre las salvaguardas	230
○ Consideraciones sobre el impacto residual	235
○ Consideraciones sobre el riesgo residual	236
• COMUNICACIÓN DE RESULTADOS	236
• DOCUMENTACIÓN RESULTANTE	237
• RECOMENDACIONES SOBRE LAS SESIONES DE TRABAJO EN LOS PROYECTOS DE ANÁLISIS DE RIESGOS	238
○ Entrevistas	238
○ Reuniones	241
○ Presentaciones	242
• <u>EJEMPLOS RESUMIDOS DE ACTIVIDADES CONCRETAS DE LOS PROYECTOS DE ANÁLISIS DE RIESGOS</u>	245
PROCESO GENERAL DE GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	253
RECORDATORIO	262
RESEÑA SOBRE LA NORMA <u>UNE-EN ISO/IEC 27001</u> PARA LA CERTIFICACIÓN DE SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN	265
• ANTECEDENTES HISTÓRICOS DE LA NORMA	265
• SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN EN EL MARCO UNE-EN ISO/IEC 27001	266
• CONSIDERACIONES GENERALES SOBRE UNE-EN ISO/IEC 27001	268
AUDITORÍA DE LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	272
• INTRODUCCIÓN	272
• CONCEPTO Y CARACTERÍSTICAS	273
• <u>EJEMPLOS</u> DE CAUSAS DESENCADENANTES DE UNA AUDITORIA DE UN SGSI	277
• CRITERIOS DE AUDITORÍA	278
• PRINCIPIOS GENERALES DE LAS AUDITORÍAS DE LOS SGSI	279
• BENEFICIOS DE LAS AUDITORIAS DE LOS SGSI	281
• PREVENCIÓN DE ERRORES EN LAS AUDITORIAS DE LOS SGSI	283
• DEFINICIONES IMPORTANTES	284
• ELEMENTOS A CONSIDERAR EN LAS AUDITORÍAS DE LOS SGSI	288
• DIRECTRICES PARA LA GESTIÓN DE PROGRAMAS Y PLANES DE AUDITORÍAS PARA LOS SGSI	288
• <u>EJEMPLOS</u> DE TIPOS DE AUDITORIAS DE UN SGSI	300
• PERSONAS QUE PUEDEN INTERVENIR EN LAS AUDITORÍAS DE LOS SGSI	306
• COMPETENCIAS, FUNCIONES Y RESPONSABILIDADES DE LOS AUDITORES DE LOS SGSI	308
• DECÁLOGO DE REFERENCIA PARA AUDITORES DE SGSIs	325
• COSTES SIGNIFICATIVOS DE UNA AUDITORIA DE UN SGSI	327

• FASES DE UNA AUDITORIA DE UN SGSI	328
• FASE DE INICIACION DE LA AUDITORÍA	330
• FASE DE PREPARACION DE LA AUDITORÍA	336
• FASE DE EJECUCION DE LA AUDITORÍA	340
• FASE DEL INFORME DE LA AUDITORÍA	347
• FASE DE CIERRE DE LA AUDITORÍA	353
• ACCIONES CORRECTIVAS Y DE MEJORA	354
• CALIDAD DE LAS AUDITORÍAS DE LOS SGSI	355
• CUESTIONARIO DE ASIMILACIÓN (preguntas)	356
• CUESTIONARIO DE ASIMILACIÓN (respuestas recomendadas)	361
• DIRECTRICES ESPECÍFICAS PARA LA AUDITORÍA DEL TRATAMIENTO DE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	394
• RECORDATORIO Y OTRAS CONSIDERACIONES DE INTERÉS	414
GUÍA PARA LA PRÁCTICA PROFESIONAL DE LA CONSULTORÍA DE SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN (SGSI)	428
• MÁXIMO CONOCIMIENTO DE LA SEGURIDAD DEL SISTEMA DE INFORMACIÓN DE LA EMPRESA	428
• NECESIDAD DE TRABAJAR BAJO PROYECTO	432
• REQUERIMIENTOS Y PAUTAS A SEGUIR ANTES DE COMENZAR A DESARROLLAR EL PROYECTO	432
• REQUERIMIENTOS Y PAUTAS A SEGUIR DURANTE EL DESARROLLO DEL PROYECTO	438
• REQUERIMIENTOS Y PAUTAS A SEGUIR AL FINALIZAR EL PROYECTO	440
• PUNTOS DE ESPECIAL ATENCIÓN EN LA CONSULTORÍA DE SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN	441
• OTROS ASPECTOS BÁSICOS A TENER PRESENTES EN LOS PROYECTOS DE CONSULTORÍA SOBRE LOS SGSI	444
CIBERSEGURIDAD	
CONCEPTO	451
CARACTERÍSTICAS SIGNIFICATIVAS Y OTRAS CONSIDERACIONES	457
<u>EJEMPLOS</u> DE TIPOS DE ATAQUE CONTRA LOS QUE INTENTA DEFENDER LA CIBERSEGURIDAD	478
CONSIDERACIONES Y RECOMENDACIONES PARA LA PROTECCIÓN DE LOS USUARIOS FINALES	482
FUNCIONAMIENTO, TIPOS, BENEFICIOS Y ESTRATEGIA DE LA CIBERSEGURIDAD	486
<u>EJEMPLOS</u> DE FALSOS MITOS SOBRE CIBERSEGURIDAD	490
<u>EJEMPLOS</u> DE TECNOLOGÍAS DESTACADAS DE CIBERSEGURIDAD Y DE BUENAS PRÁCTICAS	491
CARACTERÍSTICAS Y CONSIDERACIONES SOBRE LA RESILIENCIA CONTRA LOS CIBERATAQUES	493
CIBERSEGURIDAD Y VENTAJA COMPETITIVA	496
<u>EJEMPLO</u> DE INDICADORES PARA MEJORAR LA CIBERRESILIENCIA	499
MODELO IMC DE EVALUACIÓN DEL NIVEL DE CIBERRESILIENCIA DE LOS SERVICIOS ESENCIALES	522

RECORDATORIO FINAL	525
TÉRMINOS DE INTERÉS DE CIBERSEGURIDAD	538
INFRAESTRUTURAS CRÍTICAS	
CONCEPTO	591
CATACTERÍSTICAS GENERALES	596
INFRAESTRUTURAS CRÍTICAS DIGITALES	601
SINOPSIS DE CONCEPTOS BÁSICOS	606
ESTRATEGIA DE LA SEGURIDAD NACIONAL PARA LAS INFRAESTRUTURAS CRÍTICAS	609
RESPONSABLES MÁS SIGNIFICATIVOS DE LA PROTECCIÓN DE LAS INFRAESTRUTURAS CRÍTICAS	610
PRINCIPALES FUNCIONES DE LOS OPERADORES CRÍTICOS EN MATERIA DE SEGURIDAD	612
<u>EJEMPLOS DE AMENAZAS Y VULNERABILIDADES DE LAS INFRAESTRUTURAS CRÍTICAS</u>	612
PLAN DE SEGURIDAD DEL OPERADOR (PSO)	615
PLAN DE PROTECCIÓN ESPECÍFICO (PPE)	616
ACTUALIZACIÓN DEL PSO Y DEL PPE	617
RECOMENDACIÓN PRÁCTICA SOBRE LOS PLANES PSO Y PPE	617
<u>EJEMPLOS DE GUÍAS DE BUENAS PRÁCTICAS</u>	619
FORMACIÓN Y CONCIENCIACIÓN DEL PERSONAL EN EL ÁMBITO DE LA SEGURIDAD	620
MEDIDAS DE SEGURIDAD	625
• Seguridad en la red	626
• Aseguramiento de los equipos	628
• Control de accesos y autenticación	636
• Protección frente al malware	651
• Seguridad en el ciclo de vida de los sistemas	660
• Auditorías de seguridad	669
• Gestión de los registros	673
ANÁLISIS DE RIESGOS	675
• INTRODUCCIÓN	675
• FASE I: IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS ACTIVOS	679
• FASE II: VALORACIÓN DE LOS ACTIVOS IDENTIFICADOS	683
• FASE III: IDENTIFICACIÓN Y CARACTERIZACIÓN DE LAS AMENAZAS	690
• FASE IV: IDENTIFICACIÓN DE LOS IMPACTOS DE LAS AMENAZAS	694
• FASE V: VALORACIÓN DE LOS RIESGOS	696
OBJETIVOS Y ASPECTOS RELEVANTES DE LOS PLANES DE SEGURIDAD	700
SEGURIDAD DE LA INFORMACIÓN ANTE EL ACCESO DE TERCEROS	705
GESTIÓN DE INCIDENTES	709
PLANES DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO	720
RECORDATORIO Y OTRAS CONSIDERACIONES Y RECOMENDACIONES	726