IFCT0109. SEGURIDAD INFORMÁTICA

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

UD03

ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. **INTRODUCCIÓN**
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

1. INTRODUCCIÓN

LOS SISTEMAS DE INFORMACIÓN DE LAS ORGANIZACIONES TIENEN MULTITUD DE **RECURSOS VULNERABLES** ANTE ATAQUES DE SEGURIDAD.

POR ELLO, ES NECESARIO QUE DESARROLLEN **ESTRATEGIAS Y HERRAMIENTAS** QUE SEAN CAPACES DE IDENTIFICAR Y VALORAR ESTOS RECURSOS Y QUE, A SU VEZ, PUEDAN DAR INFORMACIÓN SOBRE LOS ATAQUES Y DAÑOS QUE PUEDEN AFECTARLES.

1. INTRODUCCIÓN

LAS HERRAMIENTAS DE GESTIÓN DE RIESGOS AYUDAN A **IDENTIFICAR LOS RECURSOS** IMPORTANTES EN LA ORGANIZACIÓN, **LOS RIESGOS** A LOS QUE ESTÁN SOMETIDOS **Y EL DAÑO** QUE PUEDEN SUFRIR EN CASO DE PRODUCIRSE UNA AMENAZA DE CUALQUIER TIPO.

SE DESCRIBEN LAS **HERRAMIENTAS FUNDAMENTALES DE GESTIÓN DE RIESGO**, SE FACILITAN **GUÍAS DE APOYO** PARA PODER IDENTIFICAR TODOS LOS FACTORES QUE FORMAN PARTE DE ESTA Y SE COMENTAN **VARIAS TÉCNICAS** QUE PERMITAN A LAS ORGANIZACIONES COMBATIR LOS RIESGOS Y AUMENTAR LA SEGURIDAD DE SUS SISTEMAS DE INFORMACIÓN.

CONTENIDOS

1. INTRODUCCIÓN
2. **INTRODUCCIÓN AL ANÁLISIS DE RIESGOS**
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

UN **RIESGO** ES ***UN EVENTO O CONJUNTO DE EVENTOS QUE PUEDE PONER EN PELIGRO UN PROYECTO DE LA ORGANIZACIÓN O QUE PUEDE IMPEDIR SU ÉXITO***.

LAS **CARACTERÍSTICAS** COMUNES QUE DEBE TENER TODO **RIESGO INFORMÁTICO** SON:

INCERTIDUMBRE

EL EVENTO QUE CARACTERIZA AL RIESGO PUEDE OCURRIR O NO OCURRIR, NO HAY CERTEZA SOBRE SU OCURRENCIA.

PÉRDIDA

EN CASO DE MATERIALIZARSE EL RIESGO, HABRÍA VARIAS CONSECUENCIAS NEGATIVAS PARA LA ORGANIZACIÓN. SI NO HAY EFECTOS NEGATIVOS, NO HAY RIESGO EN SÍ.

UNIDAD 03. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

ES BASTANTE COMÚN LA CONFUSIÓN ENTRE LAS **DEFINICIONES DE PROBLEMA, PREOCUPACIÓN Y RIESGO**, SIENDO NECESARIO CONOCER SUS DIFERENCIAS:

UNA PREOCUPACIÓN

ES UNA **SITUACIÓN SOBRE LA QUE HAY DUDAS Y QUE DEBERÁ SER EVALUADA COMO UN POSIBLE RIESGO**. NO OBSTANTE, ANALIZADA LA PREOCUPACIÓN ES POSIBLE QUE SE DETERMINE QUE NO EXISTEN EFECTOS NEGATIVOS Y QUE, POR TANTO, NO SE PUEDE CONSIDERAR RIESGO.

UN PROBLEMA

ES **UN RIESGO QUE YA SE HA MATERIALIZADO**. EN ESTE CASO, NO HAY INCERTIDUMBRE, YA QUE HAY CERTEZA SOBRE SU OCURRENCIA Y, POR TANTO, TAMPOCO SE PUEDE CONSIDERAR RIESGO.

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

Preocupación	• Efectos negativos: NO • Incertidumbres: SÍ
Riesgo	• Efectos negativos: SI • Incertidumbres: SÍ
Problema	• Efectos negativos: SI • Incertidumbres: NO

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

CONCEPTOS BÁSICOS DE LA GESTIÓN DE RIESGOS

LA **GESTIÓN DE RIESGOS** SE DEFINE COMO *EL* ***CONJUNTO DE PROCESOS DESARROLLADOS POR UNA ORGANIZACIÓN CON EL FIN DE DISMINUIR LA PROBABILIDAD Y OCURRENCIA DE AMENAZAS Y DE AUMENTAR LA PROBABILIDAD Y OCURRENCIA DE OPORTUNIDADES CON EFECTOS NEGATIVOS***.

SE TRATA DE **UNA METODOLOGÍA** ENCAMINADA A GESTIONAR CORRECTAMENTE LAS INCERTIDUMBRES DE UNA AMENAZA.

EN EL ÁMBITO DE LA GESTIÓN DE RIESGOS, ENTRA EN JUEGO EL CONCEPTO DE **SEGURIDAD DE LA INFORMACIÓN** (*CONJUNTO DE MEDIDAS Y CAPACIDADES DE LOS SISTEMAS DE INFORMACIÓN PARA RESISTIR A LAS AMENAZAS MANTENIENDO LA DISPONIBILIDAD, AUTENTICIDAD, INTEGRIDAD Y CONFIDENCIALIDAD DE LOS DATOS*).

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

CONCEPTOS BÁSICOS DE LA GESTIÓN DE RIESGOS

UNA CORRECTA GESTIÓN DE RIESGOS UTILIZARÁ UNAS MEDIDAS DE SEGURIDAD QUE PROTEJAN SUS DATOS E INFORMACIÓN EN CUANTO A:

- **DISPONIBILIDAD**
- **INTEGRIDAD**
- **CONFIDENCIALIDAD**
- **AUTENTICIDAD**
- **TRAZABILIDAD**

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

CONCEPTOS BÁSICOS DE LA GESTIÓN DE RIESGOS

DISPONIBILIDAD

LA INFORMACIÓN DEBE ESTAR DISPONIBLE A LOS USUARIOS SIEMPRE QUE SEA NECESARIO. UNA CARENCIA DE DISPONIBILIDAD PROVOCA INTERRUPCIONES DE SERVICIO Y MERMAS DE CALIDAD.

INTEGRIDAD

LA INFORMACIÓN DEBE SER CORRECTA Y COMPLETA. LA SEGURIDAD DEBE IMPEDIR QUE SE MANIPULE, CORROMPA O ELIMINE INFORMACIÓN SIN AUTORIZACIÓN.

CONFIDENCIALIDAD

LA INFORMACIÓN DEBE ESTAR DISPONIBLE SOLO PARA LOS USUARIOS QUE ESTÉN CORRECTAMENTE AUTORIZADOS. LA SEGURIDAD DEBE ENCARGARSE EN TODO MOMENTO DE PROTEGER LA INFORMACIÓN ANTE ACCESOS NO AUTORIZADOS.

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

CONCEPTOS BÁSICOS DE LA GESTIÓN DE RIESGOS

AUTENTICIDAD

GARANTÍA DE LA FUENTE DE LA QUE PROCEDEN LOS DATOS. LA SEGURIDAD DE LA ORGANIZACIÓN DEBE ASEGURAR QUE LOS DATOS PROCEDEN DE SITIOS SEGUROS SIN HABER SUFRIDO MANIPULACIÓN ALGUNA.

TRAZABILIDAD

SE DEBE CONOCER EN TODO MOMENTO QUIÉN Y CUÁNDO HA REALIZADO CADA ACCIÓN CON LA INFORMACIÓN DE LA INFORMACIÓN. ESTA CARACTERÍSTICA ES MUY ÚTIL PARA ANALIZAR LOS INCIDENTES Y PARA DETECTAR A LOS ATACANTES.

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

CONCEPTOS BÁSICOS DE LA GESTIÓN DE RIESGOS

APARTE DE LOS CONCEPTOS REFERENTES A LAS CARACTERÍSTICAS DE LA INFORMACIÓN, PARA UNA CORRECTA COMPRENSIÓN DE LA GESTIÓN DE RIESGOS HAY QUE TENER CLAROS LOS SIGUIENTES CONCEPTOS:

RIESGO

ESTIMACIÓN DE LAS PROBABILIDADES DE QUE UNA AMENAZA SE MATERIALICE SOBRE LOS ACTIVOS DE LA ORGANIZACIÓN, CAUSANDO EFECTOS NEGATIVOS O PÉRDIDAS.

ANÁLISIS DE RIESGOS

PROCESO Y METODOLOGÍA UTILIZADOS PARA ESTIMAR LA MAGNITUD DE LOS RIESGOS A LOS QUE SE EXPONE UNA ORGANIZACIÓN.

TRATAMIENTO DEL RIESGO

PROCESOS REALIZADOS PARA MODIFICAR LOS RIESGOS DE UNA ORGANIZACIÓN.

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

ESTÁNDAR ISO 31000 DE GESTIÓN Y TRATAMIENTO DE RIESGOS

LA NORMA **ISO 31000** PROPONE A LAS ORGANIZACIONES:

PRINCIPIOS FUNDAMENTALES

1. **CREAR VALOR:** LA GESTIÓN DE LOS RIESGOS DEBE CREAR VALOR Y MANTENERLO.
2. **ESTAR INTEGRADAS EN LOS PROCESOS DE LA ORGANIZACIÓN:** LA GESTIÓN DE RIESGOS DEBE SER UNA ACTIVIDAD INTEGRADA DENTRO DE LOS PROCESOS DE LA ORGANIZACIÓN Y NO SER TRATADA COMO UN PROCESO AISLADO.
3. LA GESTIÓN DE RIESGOS **DEBE ESTAR PRESENTE EN LA TOMA DE DECISIONES DE LA ORGANIZACIÓN**.
4. LA GESTIÓN DE RIESGOS **DEBE TRATAR EXPLÍCITAMENTE LA INCERTIDUMBRE**: LAS AMENAZAS Y ASPECTOS INCIERTOS DEBEN SER ANALIZADOS PARA CONOCER EL ORIGEN DE SU INCERTIDUMBRE Y SU POSIBLE TRATAMIENTO.

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

ESTÁNDAR ISO 31000 DE GESTIÓN Y TRATAMIENTO DE RIESGOS

PRINCIPIOS FUNDAMENTALES

5. LA GESTIÓN DE RIESGOS DEBE SER **SISTEMÁTICA**, ESTRUCTURADA Y UTILIZARSE A SU DEBIDO TIEMPO.
6. **DEBE BASARSE EN LA MEJOR INFORMACIÓN DE LA QUE DISPONE**: LA GESTIÓN DE RIESGOS SE DEBE LLEVAR A CABO TOMANDO EN CONSIDERACIÓN LA OPINIÓN DE PROFESIONALES ESPECIALIZADOS Y LA EXPERIENCIA.
7. **DEBE ADAPTARSE A LAS CIRCUNSTANCIAS LOCALES Y ESPECÍFICAS:** PARA UNA CORRECTA GESTIÓN DE RIESGO, LAS ORGANIZACIONES DEBEN TENER EN CUENTA EL SECTOR DE SU ACTIVIDAD Y EL ENTORNO EN EL QUE TRABAJAN.
8. **SE DEBEN VALORAR LOS FACTORES HUMANOS Y CULTURALES** PARA CONOCER LA VISIÓN DE LAS DISTINTAS PARTES IMPLICADAS Y QUE ASÍ COLABOREN CON LA ACTIVIDAD DE LA ORGANIZACIÓN.

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

ESTÁNDAR ISO 31000 DE GESTIÓN Y TRATAMIENTO DE RIESGOS

PRINCIPIOS FUNDAMENTALES

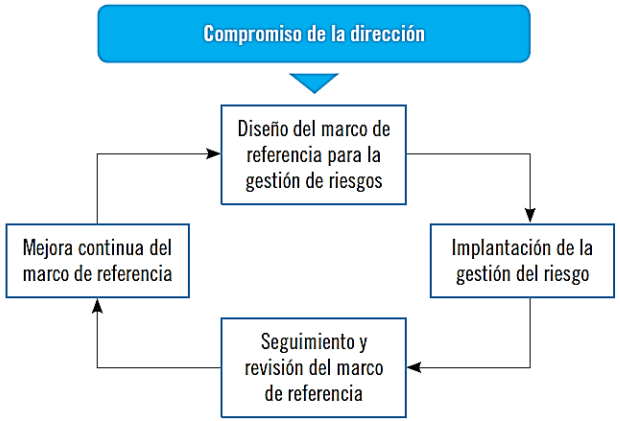
9. LA GESTIÓN DE RIESGOS **DEBE SER TRANSPARENTE E INCLUSIVA**, BASÁNDOSE EN LA COMUNICACIÓN DE LAS PARTES IMPLICADAS Y TENIENDO EN CUENTA SUS OPINIONES.
10. TAMBIÉN DEBE **SER DINÁMICA, ITERATIVA Y SENSIBLE AL CAMBIO**: EN LA GESTIÓN DE RIESGOS DEBE TENERSE EN CUENTA QUE LA ORGANIZACIÓN ESTÁ EN CONTINUO CAMBIO Y DEBE SER CAPAZ DE ADAPTARSE A LAS ALTERACIONES QUE PUEDAN OCURRIR.
11. ADEMÁS, **DEBE FACILITAR LA MEJORA CONTINUA DE LA ORGANIZACIÓN** BASADA EN EL APRENDIZAJE, LA EXPERIENCIA Y LA FORMACIÓN.

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

MARCO DE TRABAJO PARA LA GESTIÓN DEL RIESGO

LA NORMA **ISO 31000** ESTABLECE UN **MARCO DE REFERENCIA PARA LA GESTIÓN DE RIESGOS** FORMADO POR LAS SIGUIENTES ACTIVIDADES:

- LAS ORGANIZACIONES DEBEN DISEÑAR UN **MARCO DE REFERENCIA** PARA LA GESTIÓN DE RIESGOS QUE **TENGA EN CUENTA SUS PROPIAS PECULIARIDADES** Y SU ENTORNO.
- UNA VEZ DISEÑADO EL MARCO DE REFERENCIA, DEBERÁN **IMPLANTAR LA GESTIÓN DEL RIESGO** PARA PODER DISMINUIR LA PROBABILIDAD DE AMENAZAS Y PÉRDIDAS.

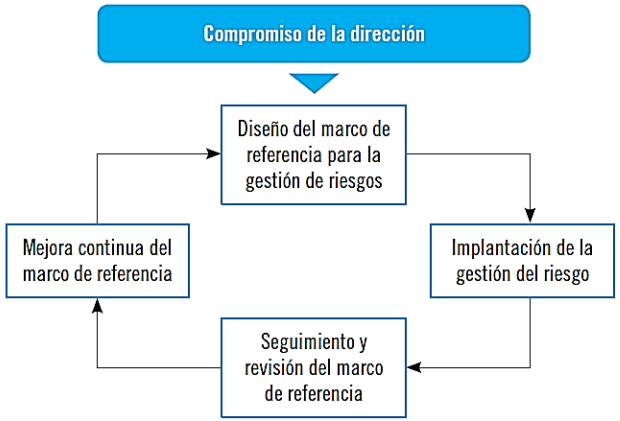


2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

MARCO DE TRABAJO PARA LA GESTIÓN DEL RIESGO

- LA GESTIÓN DE RIESGOS **DEBE SER EVALUADA Y REVISADA PERIÓDICAMENTE** PARA VALORAR SI SIGUE SIENDO EFICIENTE Y ES NECESARIO REALIZAR ALGÚN CAMBIO.
- CON ESTAS REVISIONES PERIÓDICAS, LAS ORGANIZACIONES DEBEN SER **CAPACES DE APRENDER DE LOS FALLOS DETECTADOS Y ENTRAR EN UN PROCESO DE MEJORA CONTINUA** QUE GARANTICE UNA MEJOR GESTIÓN DE RIESGOS.

TODAS ESTAS ACTIVIDADES Y FASES DEBEN **CONTAR CON EL APOYO Y COMPROMISO DE LA DIRECCIÓN** DE LA ORGANIZACIÓN PARA QUE PUEDAN SER IMPLANTADAS DE MODO GLOBAL EN TODAS SUS TAREAS Y PROCEDIMIENTOS.



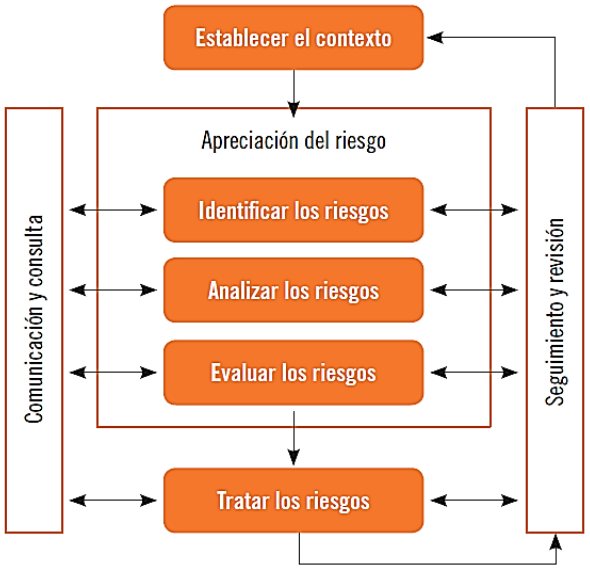
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

PROCESO DE GESTIÓN DEL RIESGO

ISO 31000 ESTABLECE UN PROCESO DE GESTIÓN DEL RIESGO CON UN **CONJUNTO DE FASES Y PASOS** PARA QUE LAS ORGANIZACIONES LO ADAPTEN E IMPLANTEN, MEJORANDO LA EFECTIVIDAD Y PRECISIÓN ANTE POSIBLES AMENAZAS.

ISO 31000 PROPONE UNA SERIE DE FASES O PROCESOS:

- **ESTABLECIMIENTO DEL ENTORNO Y DEL CONTEXTO**
- **APRECIACIÓN DEL RIESGO**
- **IDENTIFICACIÓN DEL RIESGO**
- **ANÁLISIS DEL RIESGO**
- **EVALUACIÓN DEL RIESGO**
- **TRATAMIENTO DEL RIESGO**
- **MONITORIZACIÓN Y REVISIÓN**
- **COMUNICACIÓN Y CONSULTA**

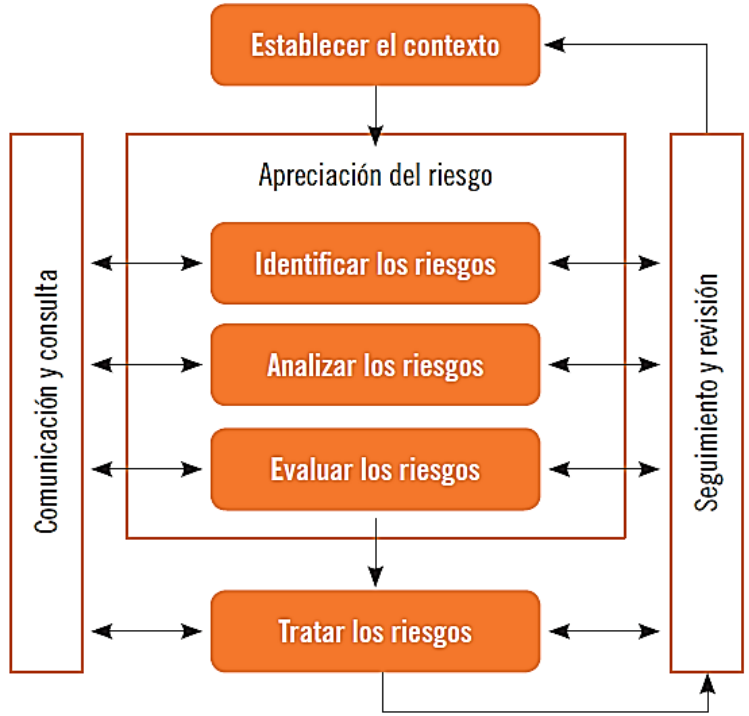


2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

PROCESO DE GESTIÓN DEL RIESGO

ESTABLECIMIENTO DEL ENTORNO Y DEL CONTEXTO

EN UN PRIMER MOMENTO, DEBERÁN **ANALIZARSE** TODAS **LAS PECULIARIDADES DE LA ORGANIZACIÓN**, DEL ENTORNO Y DE SUS SISTEMAS DE INFORMACIÓN PARA **DESARROLLAR UNA ESTRATEGIA** DE GESTIÓN DE RIESGOS **QUE SE ADAPTE A SUS NECESIDADES**.



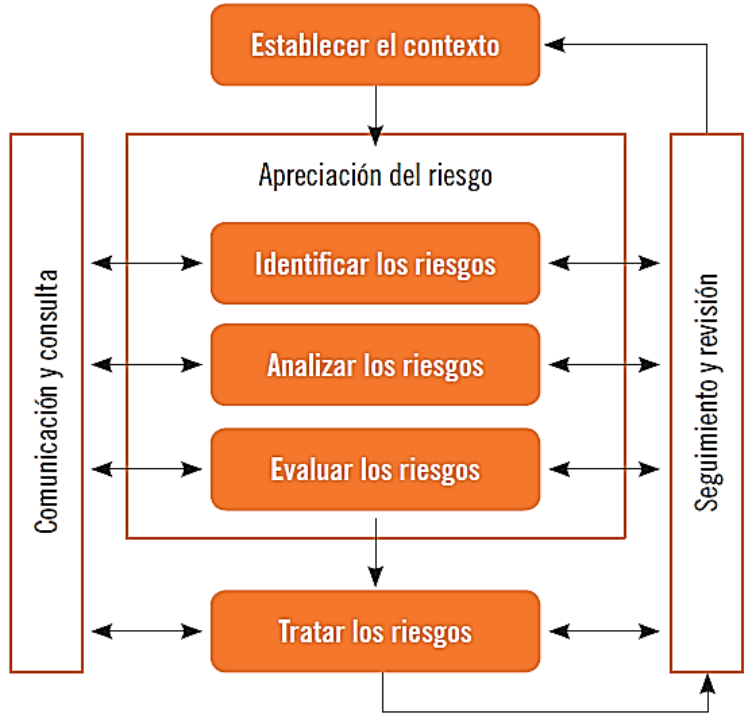
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

PROCESO DE GESTIÓN DEL RIESGO

APRECIACIÓN DEL RIESGO

CONSISTE EN UNA SERIE DE TAREAS RELACIONADAS CON LA **DETECCIÓN E IDENTIFICACIÓN** DE LOS RIESGOS DE UNA ORGANIZACIÓN PARA SU **EVALUACIÓN Y CATEGORIZACIÓN**. DENTRO DE ESTA FASE, SE ENCUENTRAN LAS **SUBFASES** SIGUIENTES:

- **IDENTIFICACIÓN DEL RIESGO**
- **ANÁLISIS DEL RIESGO**
- **EVALUACIÓN DEL RIESGO**



2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

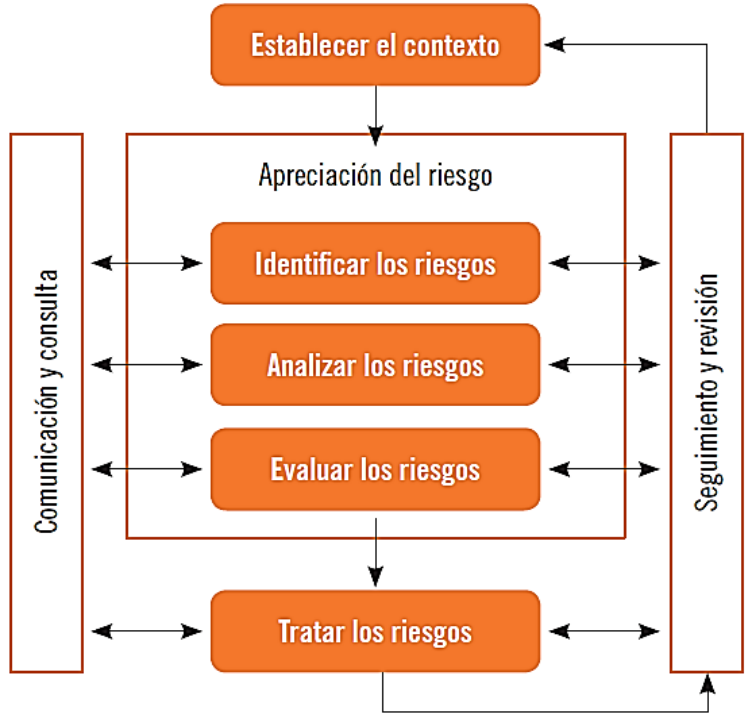
PROCESO DE GESTIÓN DEL RIESGO

APRECIACIÓN DEL RIESGO

IDENTIFICACIÓN DEL RIESGO: HABRÁ QUE IDENTIFICARLO PARA CONOCER SUS CARACTERÍSTICAS BÁSICAS.

ANÁLISIS DEL RIESGO: SERÁ NECESARIO REALIZAR UN ANÁLISIS MÁS PROFUNDO Y DETALLADO PARA CONOCER SUS CARACTERÍSTICAS Y COMPORTAMIENTOS PARTICULARES.

EVALUACIÓN DEL RIESGO: SE TENDRÁN QUE EVALUAR LOS POTENCIALES DAÑOS Y EFECTOS NEGATIVOS QUE PUEDE OCASIONAR PARA DETERMINAR SU IMPORTANCIA Y MAGNITUD.

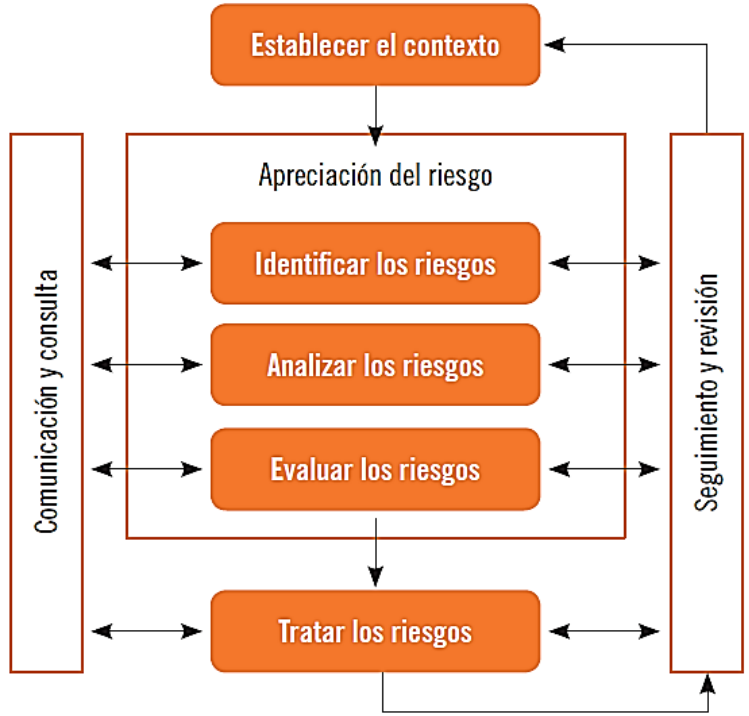


2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

PROCESO DE GESTIÓN DEL RIESGO

TRATAMIENTO DEL RIESGO

SEGÚN LO DETERMINADO EN EL ANÁLISIS Y EVALUACIÓN DEL RIESGO, **SE TOMARÁN** UNA SERIE DE **DECISIONES Y MEDIDAS QUE MINIMICEN LA PROBABILIDAD DE SU OCURRENCIA Y SU DAÑO POTENCIAL**.



2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

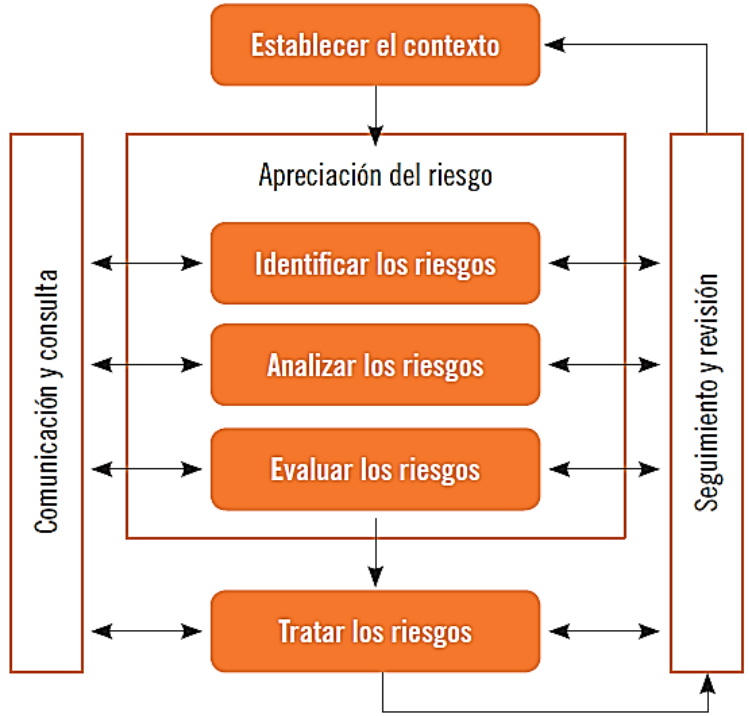
PROCESO DE GESTIÓN DEL RIESGO

MONITORIZACIÓN Y REVISIÓN

CUANDO YA SE HA DECIDIDO E IMPLANTADO LA, HABRÁ QUE **MONITORIZARLA** LO MÁXIMO POSIBLE PARA QUE SE INTEGRE EN LA ORGANIZACIÓN COMO UN PROCESO AUTOMÁTICO.

ADEMÁS**, REQUERIRÁ REVISIONES PERIÓDICAS** PARA DETECTAR POSIBLES FALLOS Y SOLUCIONARLOS EN EL MENOR TIEMPO POSIBLE.

DURANTE LA IMPLANTACIÓN, TAMBIÉN SE RECOMIENDA IR REALIZANDO REVISIONES QUE GARANTICEN SU DESARROLLO CORRECTO.



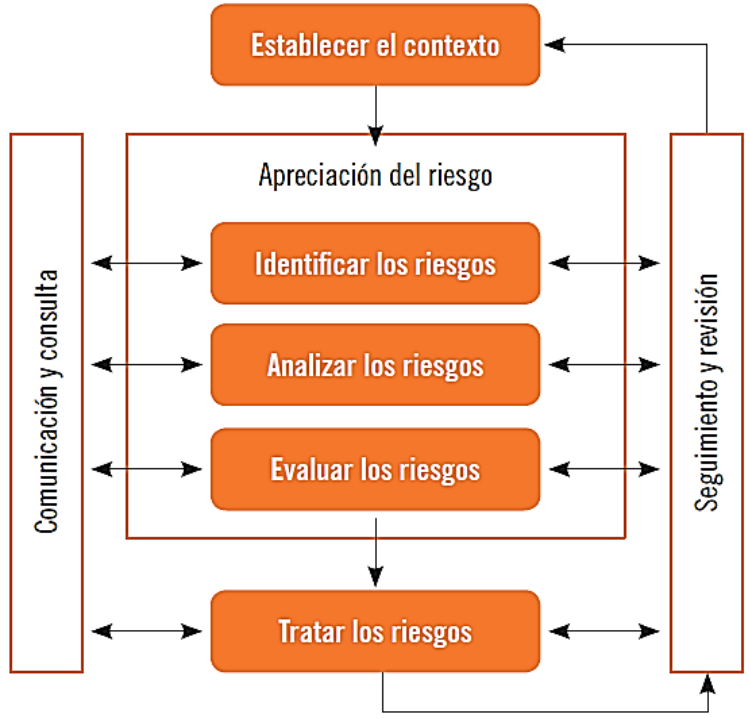
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

PROCESO DE GESTIÓN DEL RIESGO

COMUNICACIÓN Y CONSULTA

LA ORGANIZACIÓN DEBERÁ ESTAR EN **PERMANENTE CONTACTO CON LOS DISTINTOS AGENTES Y PARTICIPANTES** DE SU SISTEMA DE INFORMACIÓN CON UNA SERIE DE **OBJETIVOS**:

- AYUDAR A ESTABLECER EL CONTEXTO ADECUADAMENTE.
- GARANTIZAR LOS INTERESES DE LAS PARTES INTERESADAS Y ASEGURARSE QUE ESTÁN BIEN INFORMADAS.
- AYUDAR A ASEGURAR QUE LOS RIESGOS ESTÁN IDENTIFICADOS CORRECTAMENTE.
- DAR APOYO AL SISTEMA DE GESTIÓN DE RIESGOS.
- DESARROLLAR UNA CORRECTA POLÍTICA DE COMUNICACIÓN INTERNA Y EXTERNA DE LA ORGANIZACIÓN, PARA QUE TODOS LOS AGENTES TENGAN LA POSIBILIDAD DE CONSULTAR LOS RIESGOS DEL SISTEMA DE INFORMACIÓN Y SUS CONSECUENCIAS.



CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. **PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA**
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA

PARA UNA CORRECTA Y COMPLETA GESTIÓN DEL RIESGO DE UN SISTEMA DE INFORMACIÓN, HAY QUE **PRESTAR ATENCIÓN A LOS DISTINTOS TIPOS DE AGENTES E INCIDENCIAS** QUE PUEDEN AFECTAR AL FLUJO DE DATOS.

LOS MÁS IMPORTANTES A CONSIDERAR **SON LAS VULNERABILIDADES O FALLOS DE PROGRAMA Y LOS PROGRAMAS MALICIOSOS** (**SOFTWARE MALICIOSO**).

3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA

PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

UNA **VULNERABILIDAD ES UN FALLO DE SEGURIDAD EN UN PROGRAMA O EN UN SISTEMA DE INFORMACIÓN**.

NO TODOS LOS FALLOS DE PROGRAMAS SON DE SEGURIDAD, HAY ERRORES QUE PROVOCAN QUE FUNCIONE INCORRECTAMENTE O QUE TENGA COMPORTAMIENTOS INESPERADOS, SIN QUE SUPONGA UN RIESGO PARA LA INFORMACIÓN QUE MANEJAN.

NO OBSTANTE, **LAS VULNERABILIDADES** SON, EN NUMEROSAS OCASIONES, EL ORIGEN DE MUCHOS FALLOS DE SEGURIDAD Y **DEBEN TOMARSE EN CONSIDERACIÓN** CUANDO SE PLANIFICA LA GESTIÓN DE RIESGOS DEL SISTEMA DE INFORMACIÓN.

3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA

PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

LA VARIEDAD DE VULNERABILIDADES Y FALLOS DE PROGRAMA ES DE LO MÁS EXTENSA Y SE DISTINGUE SU TIPOLOGÍA ATENDIENDO A SUS CARACTERÍSTICAS ESPECIALES. ENTRE LAS VULNERABILIDADES MÁS IMPORTANTES, CABE DESTACAR LAS QUE SE DESCRIBEN A CONTINUACIÓN.

VULNERABILIDADES DE CONFIGURACIÓN

SON VULNERABILIDADES **GENERADAS POR UNA MALA GESTIÓN DEL SOFTWARE** POR PARTE DEL USUARIO FINAL.

NO SE ORIGINAN POR UN FALLO DEL DISEÑO EN SÍ, SINO QUE SE ORIGINAN EN EL MOMENTO EN EL QUE **EL USUARIO CONFIGURA EL SISTEMA ERRÓNEAMENTE**.

3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA

PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

VALIDACIÓN DE ENTRADA

SE TRATA DE UNA VULNERABILIDAD QUE **SE GENERA CUANDO LA APLICACIÓN NO COMPRUEBA ADECUADAMENTE LA ENTRADA DE DATOS** QUE PROVIENEN DESDE EL EXTERIOR.

SALTO DE DIRECTORIO

ES UNA VULNERABILIDAD QUE SE **APROVECHA DE LA FALTA DE SEGURIDAD DE LOS SERVICIOS DE RED PARA MOVERSE POR LOS DIRECTORIOS DE LA APLICACIÓN HASTA LLEGAR A SU DIRECTORIO RAÍZ**.

EN CASO DE SISTEMAS OPERATIVOS, ESTA VULNERABILIDAD PUEDE OCASIONAR QUE USUARIOS NO AUTORIZADOS ACCEDAN A SU DIRECTORIO RAÍZ Y PUEDAN CONECTARSE A ELLOS PARA EJECUTAR ACCIONES DE MODO REMOTO.

3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA

PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

INYECCIÓN DE COMANDOS EN EL SISTEMA OPERATIVO

LA INYECCIÓN DE COMANDOS EN EL SISTEMA OPERATIVO CONSISTE EN LA **CAPACIDAD** QUE TIENE EL USUARIO **PARA EJECUTAR COMANDOS EN EL SISTEMA OPERATIVO** QUE PUEDAN PONER EN PELIGRO SU INTEGRIDAD.

INYECCIÓN SQL

SE TRATA DE UNA VULNERABILIDAD QUE SE LOCALIZA EN EL NIVEL DE BASE DE DATOS DEL PROGRAMA O APLICACIÓN. SE PRODUCE CUANDO **EL FILTRADO DE LAS VARIABLES UTILIZADAS CON CÓDIGO SQL NO SE REALIZA CORRECTAMENTE**.

AL REALIZARSE UN FILTRADO INCORRECTO, **LOS ATACANTES PUEDEN INYECTAR NUEVO CÓDIGO SQL PARA MODIFICAR EL COMPORTAMIENTO DE LA APLICACIÓN** E, INCLUSO, INTRODUCIR CÓDIGO MALICIOSO EN EL SISTEMA.

3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA

PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

ERROR DE BÚFER

UN BÚFER ES UN ESPACIO DE LA MEMORIA DE UN DISCO O DE UN INSTRUMENTO DIGITAL RESERVADA PARA EL ALMACENAMIENTO DE INFORMACIÓN DIGITAL DE FORMA TEMPORAL HASTA QUE ESTA SE PROCESE.

SE PRODUCEN ERRORES DE BÚFER **CUANDO SE INTENTAN ALMACENAR DATOS DE FORMA INCONTROLADA EN SU ESPACIO** (PROVOCANDO DAÑOS EN ZONAS DE LA APLICACIÓN) **O CUANDO LA VELOCIDAD DE ENTRADA DE DATOS EN EL BÚFER ES INFERIOR A LA VELOCIDAD DE LECTURA** DE LOS MISMOS (PROVOCANDO FALLOS Y LA DETENCIÓN MOMENTÁNEA DE LA EJECUCIÓN DE LA APLICACIÓN).

3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA

PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

FALLO DE AUTENTICACIÓN

VULNERABILIDAD QUE SE ORIGINA **CUANDO EL PROGRAMA NO PUEDE AUTENTICAR CORRECTAMENTE** AL USUARIO QUE INTENTA ACCEDER EN ÉL.

ERROR EN LA GESTIÓN DE RECURSOS

OCURRE CUANDO **EL FALLO DE PROGRAMA PERMITE AL USUARIO NO AUTORIZADO PROVOCAR UNA GESTIÓN DEFICIENTE DE LOS RECURSOS DEL SISTEMA,** PROVOCANDO UN CONSUMO EXCESIVO EN ESTOS.

CUANDO ESTO SUCEDE**, LA APLICACIÓN** SUELE DEJAR DE RESPONDER E **INTERRUMPE EL SERVICIO.**

3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA

PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

ERROR DE DISEÑO

SON VULNERABILIDADES OCASIONADAS CUANDO EL PROGRAMADOR REALIZA EL **DISEÑO DE LA APLICACIÓN CON FALLOS Y ERRORES**, TANTO EN EL DISEÑO INICIAL COMO EN SU DESARROLLO POSTERIOR.

ESTOS ERRORES PUEDEN LLEVAR A UN MAYOR **RIESGO DE ENTRADA DE ATACANTES** QUE INTENTEN APROVECHARSE DE LOS FALLOS DE DISEÑO **PARA INTRODUCIR CÓDIGO MALICIOSO EN LA APLICACIÓN.**

3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA

PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE

UN **PROGRAMA MALICIOSO O MALWARE** ES UN TIPO DE PROGRAMA ***DISEÑADO PARA QUE USUARIOS NO AUTORIZADOS ACCEDAN A UN SISTEMA DE INFORMACIÓN SIN AUTORIZACIÓN DE SU PROPIETARIO Y PRODUCIR EFECTOS INDESEADOS EN ESTE***.

DENTRO DE ESTOS PROGRAMAS SE ENGLOBAN UNA GRAN VARIEDAD DE SOFTWARE: ***VIRUS, TROYANOS, GUSANOS, SPYWARE****, ETC.*

SUELEN DISEÑARSE PARA **MODIFICAR O ELIMINAR DATOS E INFORMACIÓN** ALMACENADA, INCURRIENDO EN ILEGALIDADES QUE PUEDEN SER PENALIZADAS.

OTRO DE SUS OBJETIVOS ES **CONSEGUIR EL CONTROL DEL SISTEMA DE INFORMACIÓN** EN EL QUE CONSIGUEN ACCEDER PARA ENVÍOS MASIVOS DE SPAM POR CORREO ELECTRÓNICO O PARA ALOJAR INFORMACIÓN ILEGAL, ENTRE OTRAS UTILIDADES NO AUTORIZADAS.

3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA

PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE

EL SOFTWARE MALICIOSO **ESTÁ EN CONTINUA ACTUALIZACIÓN** PARA CONSEGUIR MAYOR DAÑO, MAYOR IMPACTO O SIMPLEMENTE PARA ACCEDER A MÁS SISTEMAS DE INFORMACIÓN.

POR ELLO**, ES NECESARIA LA ACTUALIZACIÓN PERIÓDICA DE ANTIVIRUS**, DE OTRAS **HERRAMIENTAS** QUE COMBATEN ESTE TIPO DE SOFTWARE **Y** DE TODAS **LAS APLICACIONES Y SISTEMAS OPERATIVOS** DEL SISTEMA DE INFORMACIÓN PARA MINIMIZAR EL RIESGO DE ACCESO DE USUARIOS NO AUTORIZADOS Y DE DAÑOS EN LA INFORMACIÓN DEL SISTEMA.

CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. **PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES**
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES

ELEMENTOS DEL ANÁLISIS DE RIESGOS

CUANDO SE PRETENDE **IMPLANTAR UN PROCESO DE GESTIÓN DE RIESGOS** EN LA ORGANIZACIÓN PARA AUMENTAR EL NIVEL DE SEGURIDAD DE LA INFORMACIÓN, **DEBEN CONOCERSE** PREVIAMENTE **UNA SERIE DE CONCEPTOS** Y LAS RELACIONES EXISTENTES ENTRE ELLOS.

EL PROCESO DE GESTIÓN DE RIESGOS CONLLEVA EL ANÁLISIS DE UNA SERIE DE ELEMENTOS IMPORTANTES DEL SISTEMA DE INFORMACIÓN.

SE DESCRIBEN **LOS PRINCIPALES ELEMENTOS DEL ANÁLISIS** A TENER EN CUENTA **EN EL PROCESO DE GESTIÓN DE RIESGOS.**

4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES

ELEMENTOS DEL ANÁLISIS DE RIESGOS

ACTIVO

UN ACTIVO **ES UN RECURSO DEL SISTEMA DE INFORMACIÓN**, NECESARIO PARA GARANTIZAR EL CORRECTO FUNCIONAMIENTO DE LOS PROCESOS DE LA ORGANIZACIÓN.

LOS ACTIVOS TAMBIÉN **SON FUNDAMENTALES PARA LOGRAR LOS OBJETIVOS DEFINIDOS POR LA ORGANIZACIÓN Y REQUIEREN DE UNA ESPECIAL PROTECCIÓN**.

CUALQUIER AMENAZA QUE PUEDA AFECTAR A UN ACTIVO PUEDE PONER EN PELIGRO LA ACTIVIDAD DE LA ORGANIZACIÓN Y SU SERVICIO AL CLIENTE.

4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES

ELEMENTOS DEL ANÁLISIS DE RIESGOS

AMENAZA

UNA AMENAZA **ES CUALQUIER EVENTO QUE PUEDE AFECTAR AL ACTIVO** DE UN SISTEMA DE INFORMACIÓN, **PROVOCANDO UN INCIDENTE DE SEGURIDAD Y** PRODUCIENDO **EFECTOS ADVERSOS** O PÉRDIDAS DE INFORMACIÓN.

LAS AMENAZAS **AFECTAN DIRECTAMENTE A LAS PROPIEDADES DE LA INFORMACIÓN**: INTEGRIDAD, DISPONIBILIDAD, CONFIDENCIALIDAD Y AUTENTICIDAD.

LAS AMENAZAS **PUEDEN SER DE ORIGEN EXTERNO O INTERNO.**

LAS DE ORIGEN INTERNO PROVIENEN DE PROCESOS INTERNOS, DEL PROPIO PERSONAL O DE LAS CONDICIONES TÉCNICAS DEL SISTEMA DE INFORMACIÓN

LAS DE ORIGEN EXTERNO PROVIENEN DE AGRESIONES HUMANAS, TÉCNICAS O DE AGENTES DE CARÁCTER NATURAL.

4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES

ELEMENTOS DEL ANÁLISIS DE RIESGOS

AMENAZA

LAS AMENAZAS SE CLASIFICAN EN TRES GRUPOS:

Tipos de amenazas

Grupo	Definición
Criminalidad	Acciones causadas por humanos que incumplen requerimientos legales. Son ejemplos el sabotaje, el robo, el espionaje, el fraude, etc.
Sucesos de origen físico	Eventos de origen natural y/o técnico, además de eventos causados por humanos de forma indirecta. Por ejemplo: inundaciones, sobrecargas eléctricas, fallos de corriente, incendios, etc.
Negligencia y decisiones institucionales	Acciones realizadas por personas con poder e influencia sobre el sistema de información. Por ejemplo: gestión deficiente de contraseñas y permisos de usuario, falta de protocolo y normas de actuación, falta de formación, falta de capacitación, etc.

4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES

ELEMENTOS DEL ANÁLISIS DE RIESGOS

RIESGO

UN **RIESGO ES LA POSIBILIDAD DE QUE UNA AMENAZA SE MATERIALICE** CAUSANDO EFECTOS NEGATIVOS O POSITIVOS.

CONTROL ATENUANTE

SE CONSIDERAN ATENUANTES AQUELLOS **ACTIVOS Y MEDIDAS QUE CONSIGUEN REDUCIR** LAS POSIBILIDADES DE AMENAZAS Y, POR TANTO, **EL NIVEL DE RIESGO** DEL SISTEMA DE INFORMACIÓN DE LA ORGANIZACIÓN.

4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES

ELEMENTOS DEL ANÁLISIS DE RIESGOS

IMPACTO

EL IMPACTO **ES LA MAGNITUD DEL DAÑO QUE PROVOCA UN ATAQUE EXITOSO** EN EL QUE SE HAN PERJUDICADO LA CONFIDENCIALIDAD, LA DISPONIBILIDAD, LA INTEGRIDAD Y LA AUTENTICIDAD DE LA INFORMACIÓN DEL SISTEMA.

DEPENDIENDO DE LOS DAÑOS CAUSADOS Y LOS ACTIVOS AFECTADOS, EL IMPACTO SERÁ MAYOR O MENOR: ES POSIBLE QUE UNA AMENAZA COMPROMETA A UN ACTIVO PRESCINDIBLE DEL SISTEMA (**IMPACTO BAJO**) O QUE, SIN EMBARGO, COMPROMETA A UN ACTIVO IMPORTANTE, OCASIONANDO EFECTOS GRAVES EN EL CORRECTO FUNCIONAMIENTO DE UNA ORGANIZACIÓN (**IMPACTO MUY ELEVADO**).

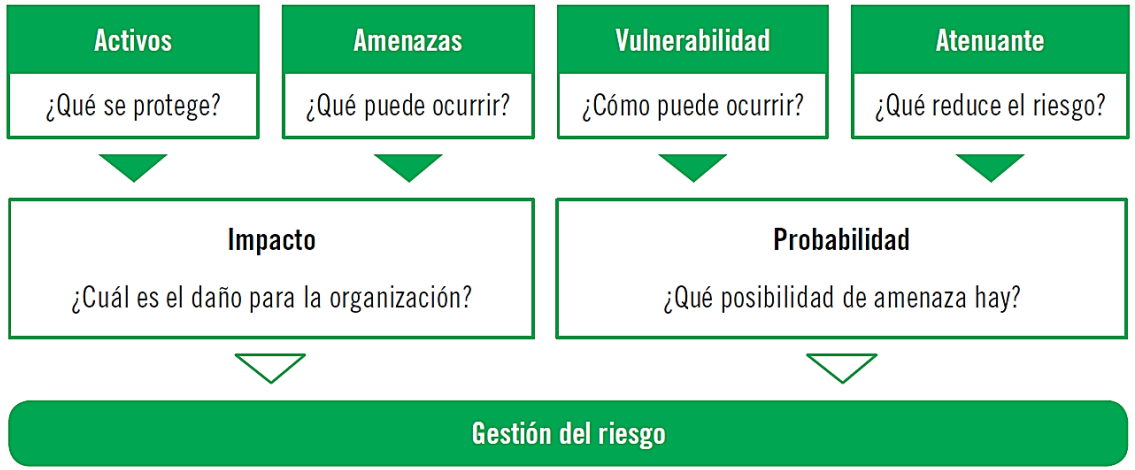
PROBABILIDAD

LA PROBABILIDAD SE DEFINE COMO **LA ESTIMACIÓN DE POSIBILIDADES DE QUE SE MATERIALICE EL RIESGO** O, LO QUE ES LO MISMO, QUE SE PRODUZCA UNA AMENAZA REAL.

4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES

MODELOS DE RELACIONES DE CONCEPTOS DE GESTIÓN DE RIESGOS

UNA CORRECTA **GESTIÓN DEL RIESGO** SE CONSIGUE CON **LA DETERMINACIÓN DEL IMPACTO Y DE LA PROBABILIDAD DE UN RIESGO POTENCIAL**



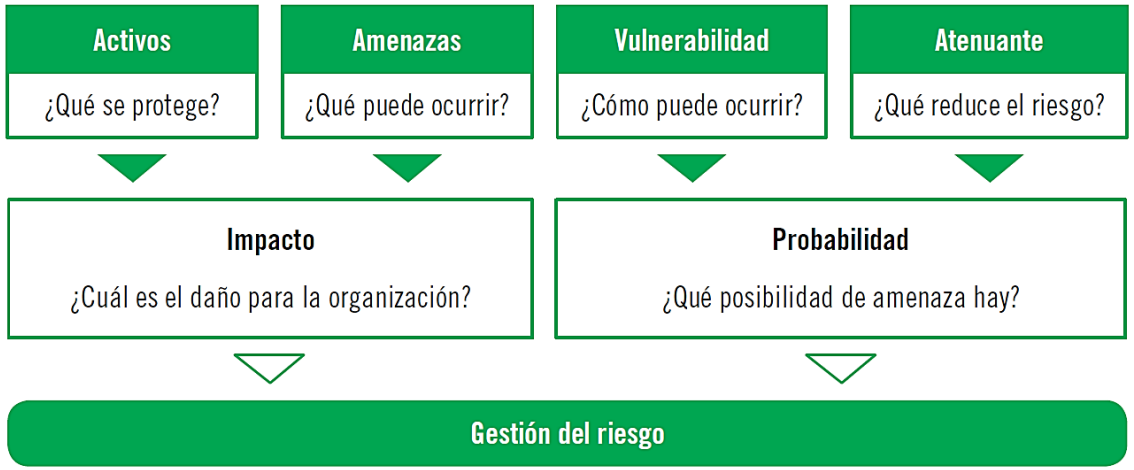
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES

MODELOS DE RELACIONES DE CONCEPTOS DE GESTIÓN DE RIESGOS

EL **IMPACTO** DE UNA POSIBLE AMENAZA DEBERÁ **CALCULARSE CON UN ANÁLISIS** PROFUNDO **DE LOS DISTINTOS ACTIVOS** DE LA ORGANIZACIÓN **Y** DE **LAS AMENAZAS** QUE PUEDEN AFECTAR A ESTOS.

A **MAYORES AMENAZAS Y ACTIVOS** MÁS RELEVANTES, **MAYOR IMPACTO** PARA LA ORGANIZACIÓN.

Y, POR EL CONTRARIO, A **MENOR NIVEL DE AMENAZAS Y AFECTACIÓN A ACTIVOS** MENOS RELEVANTES, **MENOR IMPACTO**.

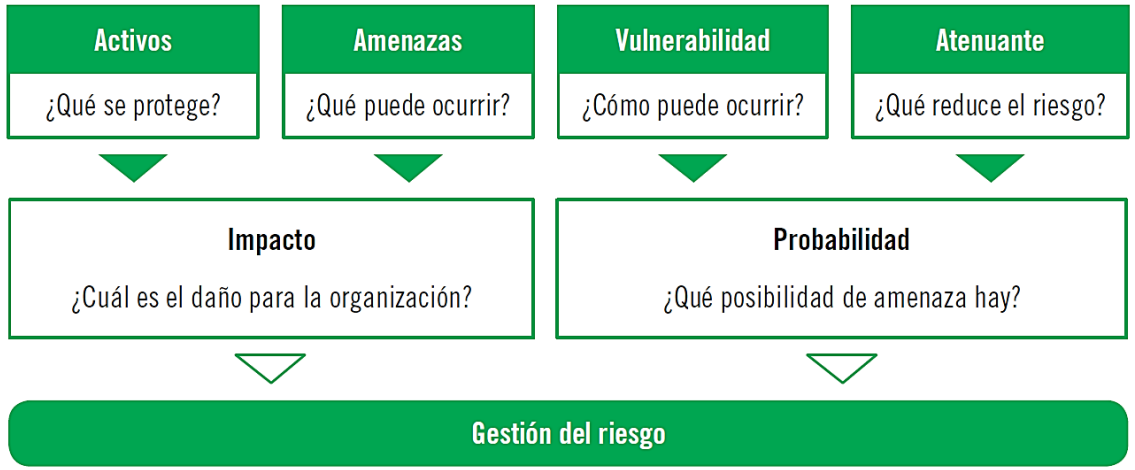


4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES

MODELOS DE RELACIONES DE CONCEPTOS DE GESTIÓN DE RIESGOS

POR OTRO LADO, DEBERÁ CALCULARSE TAMBIÉN **LA PROBABILIDAD** DE OCURRENCIA DE UNA AMENAZA.

ESTA PROBABILIDAD VENDRÁ DETERMINADA POR UN **ANÁLISIS DE LAS VULNERABILIDADES** DE LA ORGANIZACIÓN **Y** DE **LOS ATENUANTES** DE LOS QUE SE DISPONE.

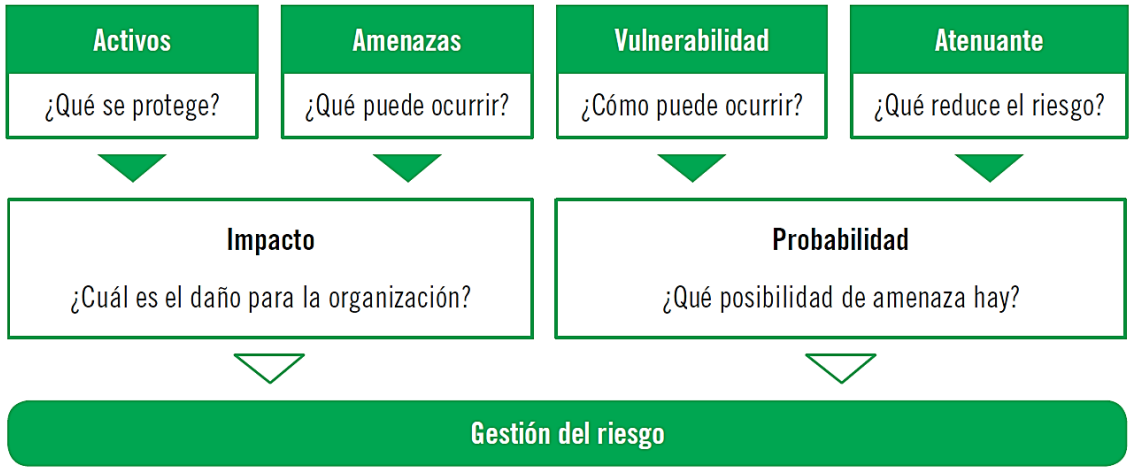


4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES

MODELOS DE RELACIONES DE CONCEPTOS DE GESTIÓN DE RIESGOS

A MENOR NIVEL DE VULNERABILIDADES Y MAYORES ATENUANTES, MENOR PROBABILIDAD DE AMENAZAS.

A MAYOR NIVEL DE VULNERABILIDADES Y MENORES ATENUANTES, MAYOR PROBABILIDAD DE AMENAZAS Y, POR TANTO, MAYOR RIESGO.



CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. **METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS**
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS

UN **CONTROL DE SEGURIDAD** ES **UN CONJUNTO DE MEDIDAS ENCARGADAS DE PALIAR LAS VULNERABILIDADES Y REDUCIR EL RIESGO** DE UN SISTEMA DE INFORMACIÓN. EN LA ACTUALIDAD, SE DISTINGUEN CUATRO **TIPOS DE CONTROLES**, MOSTRADOS EN LA TABLA SIGUIENTE:

Tipos de controles de seguridad

Control	Descripción
Disuasorio	Su finalidad principal es reducir la probabilidad de recibir un ataque.
Preventivo	Su finalidad es proteger al sistema de información de sus vulnerabilidades, intentando impedir el acceso de los atacantes o reduciendo el impacto de los daños causados.
Correctivo	Tienen como finalidad principal reducir el impacto de una amenaza.
Detectivo	Se encargan de detectar e impedir posibles ataques.

5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS

UNA **METODOLOGÍA** SE DEFINE COMO **EL PROCEDIMIENTO Y EL CONJUNTO DE TÉCNICAS UTILIZADAS PARA EL ANÁLISIS DEL RIESGO**

LA GESTIÓN DE RIESGOS DEBE SER CAPAZ DE DETERMINAR CUÁLES DE ESTOS CONTROLES SON LOS MÁS ADECUADOS, EFICIENTES Y RENTABLES Y, PARA ELLO, **EXISTEN DOS METODOLOGÍAS** DISTINTAS PARA REALIZAR EL ANÁLISIS DE RIESGOS:

- **METODOLOGÍA CUANTITATIVA**
- **METODOLOGÍA CUALITATIVA**

5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS

METODOLOGÍA CUANTITATIVA DE ANÁLISIS DE RIESGOS

EL ENFOQUE CUANTITATIVO DEL ANÁLISIS DE RIESGOS **TIENE EN CUENTA DOS ELEMENTOS:**

- **LA PROBABILIDAD** DE OCURRENCIA DE UN EVENTO
- **EL IMPACTO** QUE PUEDE PROVOCAR EN CASO DE QUE SUCEDA.

PARA DETERMINAR Y ANALIZAR LOS RIESGOS, LA METODOLOGÍA CUANTITATIVA **SE BASA EN UN MODELO MATEMÁTICO** QUE SIRVA DE APOYO A LA TOMA DE DECISIONES.

5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS

METODOLOGÍA CUANTITATIVA DE ANÁLISIS DE RIESGOS

VENTAJAS

- **FACILITA COMPARACIONES** ENTRE VULNERABILIDADES CON CARACTERÍSTICAS MUY DIFERENCIADAS.
- **APOYA NUMÉRICAMENTE LA TOMA DE DECISIONES** Y LAS OPINIONES CREADAS.
- SIRVE COMO **JUSTIFICANTE PARA LA APLICACIÓN DE MEDIDAS** DE GESTIÓN DE RIESGOS.

DESVENTAJAS

- SE UTILIZAN METODOLOGÍAS DE ANÁLISIS DE RIESGOS ESTÁNDARES, **NO OFRECE LA POSIBILIDAD DE PERSONALIZARLAS** SEGÚN LAS PARTICULARIDADES DEL SISTEMA DE INFORMACIÓN.
- **DEBEN SER DESARROLLADAS** OBLIGATORIAMENTE **POR PROFESIONALES ESPECIALIZADOS** PARA QUE PROPORCIONEN RESULTADOS FIABLES.
- RESULTAN **DIFÍCILES DE MANTENER Y DE MODIFICAR.**
- **SOLO PERMITEN LA ESTIMACIÓN DE PÉRDIDAS CUANDO ESTAS DEPENDEN DE VALORES CUANTIFICABLES**. EN EL MOMENTO QUE ENTRA UN VALOR INDEFINIDO O QUE NO PERMITE CUANTIFICACIÓN, LA ESTIMACIÓN DE LAS PÉRDIDAS NO SERÁ VÁLIDA.

5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS

METODOLOGÍA CUALITATIVA DE ANÁLISIS DE RIESGOS

SE BASA EN EL RACIOCINIO HUMANO PARA CALCULAR LAS PÉRDIDAS POTENCIALES ESTIMADAS SIN NECESIDAD DE UTILIZAR MÉTODOS PROBABILÍSTICOS.

ES **LA METODOLOGÍA UTILIZADA CON MÁS FRECUENCIA** PARA EL ANÁLISIS DE RIESGOS.

TAMBIÉN REQUIEREN LA PARTICIPACIÓN DE UN PROFESIONAL, PERO **EL COSTE** EN RECURSOS HUMANOS IMPLICADOS **ES** SUMAMENTE **INFERIOR**.

ESTA METODOLOGÍA **SUELE UTILIZARSE CUANDO EL NIVEL DE RIESGO NO ES ELEVADO O** CUANDO **LOS DATOS NUMÉRICOS NO SON ADECUADOS** PARA UNA CORRECTA ESTIMACIÓN DEL RIESGO.

TAMBIÉN **SE UTILIZA COMO BASE INICIAL** PARA DEFINIR LA METODOLOGÍA CUANTITATIVA A UTILIZAR EN EL ANÁLISIS.

5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS

METODOLOGÍA CUALITATIVA DE ANÁLISIS DE RIESGOS

VENTAJAS

- PERMITE **UNA ORGANIZACIÓN DEL TRABAJO FLEXIBLE** Y CON CAPACIDAD DE REACCIÓN.
- **INCLUYE VALORES Y ACTIVOS INCUAN**TIFICABLES.
- SE ENFOCA PRINCIPALMENTE EN **LA IDENTIFICACIÓN DE LOS EVENTOS OCURRIDOS O POTENCIALES**.

DESVENTAJAS

- **DEPENDE DE LA CALIDAD, PROFESIONALIDAD Y HABILIDAD DE LOS PROFESIONALES** PARTICIPANTES EN EL ANÁLISIS.
- SEGÚN EL NIVEL DE CONOCIMIENTOS DEL PROFESIONAL**, ES POSIBLE QUE SE PASEN POR ALTO RIESGOS IMPORTANTES** DESCONOCIDOS.
- **EXIGE LA** OPINIÓN **E INTERVENCIÓN DE UN PROFESIONAL**.
- IDENTIFICA LOS EVENTOS CON MAYOR CLARIDAD, PERO **NO PUEDE DETERMINAR LA PROBABILIDAD REAL DE OCURRENCIA.**

CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. **IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN**
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. 1DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN

FASES DEL PROCESO DE ANÁLISIS Y GESTIÓN DE RIESGOS

EL PROCESO DE ANÁLISIS Y GESTIÓN DE RIESGOS ESTÁ FORMADO POR UNA SERIE DE FASES:

1. IDENTIFICACIÓN DE LOS ACTIVOS
2. VALORACIÓN DE LOS ACTIVOS
3. IDENTIFICACIÓN DE LAS AMENAZAS
4. DETERMINACIÓN DEL IMPACTO DE UNA AMENAZA
5. DETERMINACIÓN DEL RIESGO
6. ESTABLECIMIENTO DE SALVAGUARDAS (ATENUANTES)
7. REVISIÓN DEL IMPACTO Y DETERMINACIÓN DEL IMPACTO RESIDUAL
8. REVISIÓN DEL RIESGO Y DETERMINACIÓN DEL RIESGO RESIDUAL

ESTE APARTADO **SE VA A CENTRAR** PRINCIPALMENTE **EN LAS FASES 1 Y 2** DEL PROCESO, LA IDENTIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS.

6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN

IDENTIFICACIÓN DE LOS ACTIVOS

UN ACTIVO **ES EL CONJUNTO DE RECURSOS DEL SISTEMA DE INFORMACIÓN O RELACIONADOS CON ESTE QUE SON NECESARIOS PARA EL CORRECTO FUNCIONAMIENTO DE LA ORGANIZACIÓN** Y PARA QUE SE ALCANCEN LOS OBJETIVOS DEFINIDOS POR ESTA.

EL ACTIVO MÁS IMPORTANTE QUE MANEJA UNA ORGANIZACIÓN **ES LA INFORMACIÓN**. NO HAY QUE OLVIDAR **OTROS ACTIVOS** QUE TAMBIÉN PUEDEN SER RELEVANTES:

6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN

IDENTIFICACIÓN DE LOS ACTIVOS

- LOS SERVICIOS PRESTADOS CON LA UTILIZACIÓN DE DICHA INFORMACIÓN.
- LOS SERVICIOS NECESARIOS PARA PODER UTILIZAR Y TRATAR LA INFORMACIÓN.
- LOS EQUIPOS Y SOPORTES DE INFORMACIÓN QUE PERMITEN ALMACENAR LA INFORMACIÓN: ORDENADORES, DISPOSITIVOS DE ALMACENAMIENTO EXTERNOS, ETC.
- LOS EQUIPOS INFORMÁTICOS QUE PERMITEN LA GESTIÓN DE LA INFORMACIÓN.
- LAS APLICACIONES QUE PERMITEN GESTIONAR LA INFORMACIÓN Y LOS SERVICIOS QUE SE PROPORCIONAN A TRAVÉS DE ESTA.
- LAS REDES DE COMUNICACIONES QUE PERMITEN Y FACILITAN EL INTERCAMBIO DE INFORMACIÓN.
- LAS INSTALACIONES EN LAS QUE SE UBICAN Y PROTEGEN LOS EQUIPOS INFORMÁTICOS, DISPOSITIVOS, SISTEMAS DE ALMACENAMIENTO Y REDES DE COMUNICACIONES NECESARIOS PARA GESTIONAR LA INFORMACIÓN Y OFRECER EL SERVICIO.
- LOS RECURSOS HUMANOS QUE UTILIZAN TODOS LOS ELEMENTOS ANTERIORES.

6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN

VALORACIÓN DE LOS ACTIVOS

LA IMPORTANCIA DE LOS ACTIVOS DE UN SISTEMA DE INFORMACIÓN **DEPENDERÁ DE SU VALORACIÓN.**

SI UN ACTIVO NO TIENE VALOR, **ES** COMPLETAMENTE **PRESCINDIBLE.**

POR OTRA PARTE, **SI UN ACTIVO ES NECESARIO** PARA EL CORRECTO FUNCIONAMIENTO DEL SISTEMA, **ES QUE TIENE CIERTO VALOR**.

LO QUE HABRÁ QUE CALCULAR ES CUÁL ES EL VALOR DE DICHO ACTIVO.

LA **VALORACIÓN DEL ACTIVO** VIENE DEFINIDA COMO **EL COSTE QUE IMPLICARÍA RECUPERARSE DE UN FALLO DEL ACTIVO PROVOCADO POR ALGUNA INCIDENCIA**.

ESTA VALORACIÓN **DEPENDE DE MUCHOS FACTORES** QUE VARIARÁN, POR SUPUESTO, SEGÚN LA ORGANIZACIÓN Y EL SISTEMA DE INFORMACIÓN IMPLANTADO.

6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN

VALORACIÓN DE LOS ACTIVOS

LOS FACTORES MÁS IMPORTANTES A CONSIDERAR SON:

- **COSTE DEL PERSONAL** ESPECIALIZADO **NECESARIO PARA RECUPERAR EL ACTIVO** (*COSTE DE MANO DE OBRA*).
- **LOS INGRESOS PERDIDOS** POR EL FALLO DEL ACTIVO.
- **COSTE DE ADQUISICIÓN E INSTALACIÓN DE UN ACTIVO NUEVO** EN CASO DE QUE EL ANTERIOR HAYA RESULTADO INSERVIBLE (*COSTE DE REPOSICIÓN*).
- **PÉRDIDA DE PERCEPCIÓN DE CONFIANZA Y CALIDAD** DE LOS CLIENTES Y PROVEEDORES PROVOCADOS POR UNA INTERRUPCIÓN DEL SERVICIO PROVOCADA POR EL FALLO DEL ACTIVO.
- **INFRACCIONES COMETIDAS Y SANCIONES** CORRESPONDIENTES AL INCUMPLIMIENTO DE REQUERIMIENTOS LEGALES O DE OBLIGACIONES CONTRACTUALES DEBIDAS AL FALLO DEL ACTIVO.
- **DAÑOS** Y EFECTOS PERJUDICIALES **PROVOCADOS** POR EL ACTIVO **A OTROS ACTIVOS**, TANTO PROPIOS COMO AJENOS A LA ORGANIZACIÓN.
- **DAÑOS MEDIOAMBIENTALES** CAUSADOS POR EL ACTIVO.
- **DAÑOS A OTRAS PERSONAS** CAUSADOS POR EL ACTIVO.

6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN

TIPOS DE VALORACIONES DE ACTIVOS

LA VALORACIÓN DE UN ACTIVO, DEL MISMO MODO QUE LA METODOLOGÍA DE GESTIÓN DE RIESGOS, PUEDE REALIZARSE DE DOS MODOS:

VALORACIÓN CUANTITATIVA

SE CALCULA EL VALOR DEL ACTIVO **UTILIZANDO CANTIDADES NUMÉRICAS**, VALORES EXACTOS.

VALORACIÓN CUALITATIVA

SE ASIGNA EL VALOR A LOS ACTIVOS, **UTILIZANDO UNA ESCALA DE NIVELES**. POR EJEMPLO: PUEDE UTILIZARSE UNA ESCALA TIPO “VALOR NULO, VALOR BAJO, VALOR MEDIO, VALOR ALTO, VALOR MUY ALTO” PARA CLASIFICAR LOS DISTINTOS ACTIVOS EN CADA UNO DE LOS NIVELES DE VALORACIÓN.

6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN

TIPOS DE VALORACIONES DE ACTIVOS

SEA CUAL SEA LA METODOLOGÍA DE VALORACIÓN DE ACTIVOS UTILIZADA, **HAY QUE TENER EN CUENTA DOS ASPECTOS** BÁSICOS:

HOMOGENEIDAD

ES NECESARIO **PODER ESTABLECER COMPARACIONES DE LOS VALORES DE LOS ACTIVOS**, AUNQUE SEAN DE DIFERENTES DIMENSIONES PARA DETERMINAR LA RELEVANCIA DE CADA UNO DE ELLOS.

RELATIVIDAD

ES VITAL QUE EXISTA LA **POSIBILIDAD DE RELATIVIZAR EL VALOR DE UN ACTIVO CUANDO SE COMPARA CON LOS DEMÁS**. ES POSIBLE QUE UN ACTIVO CONLLEVE MUCHOS COSTES DE REPOSICIÓN Y QUE TENGA UN VALOR ELEVADO, PERO QUE, AL COMPARARLO CON LOS DEMÁS ACTIVOS DEL SISTEMA DE INFORMACIÓN, SU VALORACIÓN SEA RELATIVAMENTE REDUCIDA (QUE LOS OTROS ACTIVOS TENGAN COSTES DE REPOSICIÓN MUCHO MÁS ELEVADOS QUE ESTE).

6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN

LAS DIMENSIONES DE VALORACIÓN DE LOS ACTIVOS

CUANDO SE PROCEDE A REALIZAR LA VALORACIÓN DE LOS ACTIVOS, NO PUEDE CALCULARSE TOMANDO SOLO UNA DE SUS DIMENSIONES, SINO **QUE DEBEN TENERSE EN CUENTA TODAS Y CADA UNA DE ELLAS**:

DIMENSIONES DE VALORACIÓN DE LOS ACTIVOS

Dimensión	Descripción
Disponibilidad	¿Cuál sería la importancia del activo si este no estuviera disponible?
Integridad	¿Qué importancia tendría que el activo sufriera modificaciones descontroladas?
Confidencialidad	¿Cuál sería la importancia del conocimiento del activo por usuarios no autorizados?
Autenticidad	¿Cuál sería la importancia del acceso al activo por parte de personas no autorizadas?
Trazabilidad	¿Cuál sería la importancia de la falta de constancia de la utilización del activo?

CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. **IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE**
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE

UNA AMENAZA ES UN CONJUNTO DE HECHOS Y EVENTOS QUE PUEDEN OCURRIR Y QUE PUEDEN PROVOCAR EFECTOS PERJUDICIALES A LOS ACTIVOS DEL SISTEMA DE INFORMACIÓN.

POR ELLO, TIENE **PRIORIDAD PROTEGER A LOS ACTIVOS DE DICHAS AMENAZAS**.

LA MANERA DE PROTEGER LOS ACTIVOS DE LAS AMENAZAS ES **REDUCIENDO SU RIESGO**, INTENTANDO REDUCIR AL MÁXIMO LA POSIBILIDAD DE QUE ESTAS OCURRAN.

PARA ELLO, SERÁ NECESARIO **IDENTIFICAR LAS POSIBLES AMENAZAS** DEL SISTEMA DE INFORMACIÓN Y **VALORARLAS**

HAY QUE TENER EN CUENTA QUE PUEDEN SER **ACCIDENTALES O DELIBERADAS**.

7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE

AMENAZAS ACCIDENTALES

AMENAZAS NATURALES (TERREMOTOS, INUNDACIONES, ETC.)

AMENAZAS INDUSTRIALES (FALLOS ELÉCTRICOS, FALLOS DE COMUNICACIÓN, ETC.)

AMENAZAS HUMANAS (ERRORES PROVOCADOS SIN DELIBERACIÓN PREVIA U OMISIONES DE ACCIONES QUE SON IMPORTANTES PARA EL FUNCIONAMIENTO DEL SISTEMA).

AMENAZAS DELIBERADAS

LA *INTRUSIÓN*

EL ESPIONAJE

EL ROBO DE INFORMACIÓN

EL FRAUDE, ETC.

7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE

IDENTIFICACIÓN DE LAS AMENAZAS

PARA IDENTIFICAR LAS AMENAZAS, ES NECESARIO **CONOCER LOS ACTIVOS DE QUE DISPONE LA ORGANIZACIÓN Y SUS CARACTERÍSTICAS PRINCIPALES**:

- TIPO DE ACTIVO (DISPOSITIVO DE ALMACENAMIENTO, RED DE COMUNICACIÓN, ETC.)
- LAS DIMENSIONES DEL ACTIVO QUE HACEN QUE TENGA UN VALOR CONSIDERABLE
- LA EXPERIENCIA DE LA ORGANIZACIÓN EN RELACIÓN A ANTERIORES INCIDENCIAS OCURRIDAS CON EL ACTIVO
- LOS DEFECTOS DEL ACTIVO NOTIFICADOS POR SU FABRICANTE DE ORIGEN

7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE

IDENTIFICACIÓN DE LAS AMENAZAS

UNA VEZ DESCRITAS LAS CARACTERÍSTICAS DEL ACTIVO, HABRÁ QUE REGISTRAR **INFORMACIÓN DETALLADA DE LA AMENAZA**:

- EFECTOS DE LA AMENAZA DEBIDAMENTE EXPLICADOS.
- ENTREVISTAS REALIZADAS QUE HAN APORTADO INFORMACIÓN PARA LA DETECCIÓN DE LA AMENAZA.
- HISTORIAL DE AMENAZAS RELEVANTES, TANTO DE LA ORGANIZACIÓN COMO DE OTRAS ORGANIZACIONES.

7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE

IDENTIFICACIÓN DE LAS AMENAZAS

EJEMPLOS DE AMENAZAS FRECUENTES

- **SUPLANTACIÓN:** ESTA AMENAZA SE PRODUCE CUANDO UN USUARIO NO AUTORIZADO SUPLANTA LA IDENTIDAD DE OTRO USUARIO HACIÉNDOSE PASAR POR ESTE.
- **ALTERACIÓN:** MODIFICACIÓN Y ALTERACIÓN DE LA INFORMACIÓN O DE ALGÚN DATO CONCRETO DEL SISTEMA DE INFORMACIÓN.
- **REPUDIO:** NEGACIÓN DE LA PRODUCCIÓN DE UN HECHO. ES FRECUENTE QUE UN EMPLEADO REALICE ALGUNA ACCIÓN PERJUDICIAL PARA LA ORGANIZACIÓN Y QUE, POSTERIORMENTE, LO NIEGUE.
- **DIVULGACIÓN DE INFORMACIÓN:** COMUNICACIÓN DE INFORMACIÓN CONFIDENCIAL O DE VALOR A TERCEROS QUE NO DEBERÍAN CONOCERLA.
- **DENEGACIÓN DEL SERVICIO:** INCAPACIDAD DE ACCEDER A UN SERVICIO DETERMINADO DEL SISTEMA DE INFORMACIÓN. SUELE PRODUCIRSE POR SATURACIÓN DE DATOS DE ENTRADA.
- **ELEVACIÓN DE PRIVILEGIOS:** UTILIZACIÓN DE PRIVILEGIOS DE MAYOR NIVEL POR USUARIOS NO AUTORIZADOS PARA ELLO.

7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE

VALORACIÓN DE LAS AMENAZAS

CUANDO SE PRODUCE UNA AMENAZA, LOS EFECTOS SOBRE LOS ACTIVOS NO SON IGUAL DE PERJUDICIALES PARA TODAS SUS DIMENSIONES, PUDIENDO, POR EJEMPLO, AFECTAR GRAVEMENTE A LA INTEGRIDAD DE LA INFORMACIÓN, PERO NO TENER EFECTOS SOBRE SU CONFIDENCIALIDAD.

LAS AMENAZAS SE VALORARÁN ATENDIENDO A LOS EFECTOS PERJUDICIALES QUE PUEDEN PROVOCAR A LOS ACTIVOS DEL SISTEMA DE INFORMACIÓN O, LO QUE ES LO MISMO, A **SU IMPACTO**.

EL IMPACTO DE UNA AMENAZA SE DEFINE COMO LA MEDICIÓN DEL DAÑO PROVOCADO SOBRE UNO O VARIOS ACTIVOS.

7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE

VALORACIÓN DE LAS AMENAZAS

SU VALORACIÓN SE CALCULARÁ TOMANDO COMO REFERENCIA LOS SIGUIENTES ELEMENTOS:

- DAÑOS PRODUCIDOS EN LOS ACTIVOS DE LA ORGANIZACIÓN.
- CAPACIDAD DE REPRODUCCIÓN Y EXPANSIÓN DE LA AMENAZA A OTROS ACTIVOS DEL SISTEMA.
- CAPACIDAD DE EXPLOTACIÓN DE LA AMENAZA.
- USUARIOS QUE SE PUEDEN VER AFECTADOS EN CASO DE PRODUCIRSE LA AMENAZA.
- CAPACIDAD DE DETECCIÓN Y DESCUBRIMIENTO DE LA AMENAZA CUANDO ESTA SE PRODUZCA.

7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE

VALORACIÓN DE LAS AMENAZAS

ADEMÁS DEL IMPACTO, LA VALORACIÓN DE LA AMENAZA VENDRÁ TAMBIÉN DETERMINADA POR LA VULNERABILIDAD DEL ACTIVO, QUE SE VERÁ AFECTADO EN DOS ASPECTOS:

DEGRADACIÓN DEL ACTIVO: VALORACIÓN DEL PERJUICIO SUFRIDO POR EL ACTIVO POR LA OCURRENCIA DE LA AMENAZA.

FRECUENCIA DE LA AMENAZA: CANTIDAD DE VECES QUE SE PRODUCE LA AMENAZA EN UN PERÍODO DE TIEMPO DETERMINADO.

DE ESTE MODO, **LA VALORACIÓN DE LA AMENAZA VENDRÁ DADA POR SU IMPACTO, LA DEGRADACIÓN DE LOS ACTIVOS AFECTADOS Y SU FRECUENCIA**.

CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. **ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA**
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA

PARA IDENTIFICAR Y ESTIMAR UNA VULNERABILIDAD, DEBE PARTICIPAR UN PROFESIONAL QUE CONOZCA PROFUNDAMENTE LOS DISTINTOS ACTIVOS DEL SISTEMA DE INFORMACIÓN Y LAS AMENAZAS Y RIESGOS QUE PUEDEN SUFRIR**. SE CONSIDERAN TRES TIPOS DE VULNERABILIDADES:**

- **VULNERABILIDAD INTRÍNSECA**

  VULNERABILIDAD QUE PROVIENE DIRECTA Y EXCLUSIVAMENTE DEL ACTIVO Y DE LA AMENAZA.

- **VULNERABILIDAD EFECTIVA**

  QUE SE HA GENERADO A RAÍZ DE UNA SALVAGUARDA YA EXISTENTE EN EL SISTEMA DE INFORMACIÓN.

- **VULNERABILIDAD RESIDUAL**

  GENERADA POR LA APLICACIÓN DE SALVAGUARDAS IMPLANTADAS SIGUIENDO EL RESULTADO DEL PROCESO DE ANÁLISIS Y GESTIÓN DE RIESGOS.

8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA

ALGUNOS ***EJEMPLOS*** DE VULNERABILIDADES SON:

- *VULNERABILIDADES DE SEGURIDAD FÍSICA:*
  - ACCESOS DE PERSONAL NO AUTORIZADO AL RECINTO.
  - DESASTRES NATURALES (RAYOS, INUNDACIONES, ETC.).
  - INCENDIOS.
- *VULNERABILIDADES EN LAS CONEXIONES DE RED:*
  - FALLOS EN EL CORTAFUEGOS O FIREWALL.
  - INTRUSIONES Y ACCESOS NO AUTORIZADOS A TRAVÉS DE LA RED.
- *VULNERABILIDADES EN LA INFRAESTRUCTURA DE RED:*
  - FALLOS Y VULNERABILIDADES PRESENTES EN DISPOSITIVOS DE RED COMO ROUTERS, HUBS, SWITCHES, ETC.
- *VULNERABILIDADES EN EL CORREO ELECTRÓNICO.*
- *VULNERABILIDADES EN LAS APLICACIONES DE GRAN VALOR Y EN S.O.*

8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA

VALORACIÓN DE LA VULNERABILIDAD

SE MEDIRÁ CONSIDERANDO EL PERIODO DE TIEMPO TRANSCURRIDO ENTRE LA AMENAZA POTENCIAL Y SU MATERIALIZACIÓN REAL EN EL ACTIVO DEL SISTEMA DE INFORMACIÓN. TENDRÁ TAMBIÉN QUE CALCULARSE LA FRECUENCIA EN LA QUE SE MATERIALIZA LA AMENAZA.

PARA LA MEDICIÓN DE LA VULNERABILIDAD **SE UTILIZAN ESCALAS QUE VALORARÁN LA FRECUENCIA DE OCURRENCIA Y SU PROBABILIDAD**. UN EJEMPLO DE TABLA DE VALORES DE VULNERABILIDADES PODRÍA SER EL SIGUIENTE:

Valor de la vulnerabilidad	Frecuencia	Probabilidad
Muy frecuente	Varias veces al día.	Entre el 75 y el 100 %.
Bastante frecuente	Una vez al día.	Entre el 50 y el 75 %.
Frecuente	Una vez en semana.	Entre el 25 y el 50 %.
Poco frecuente	Una vez al mes.	25 % o menos.

8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA

PARA DETECTAR Y ANALIZAR LAS VULNERABILIDADES DE UN SISTEMA DE INFORMACIÓN, SE UTILIZAN CIERTAS HERRAMIENTAS Y TÉCNICAS DE ANÁLISIS DE LAS QUE CABE DESTACAR LAS SIGUIENTES:

- **ANÁLISIS LOCAL**
- **ANÁLISIS REMOTO DE CAJA BLANCA**
- **ANÁLISIS DE CAJA NEGRA**

8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA

ANÁLISIS LOCAL

SE REALIZA MEDIANTE **LA EJECUCIÓN DE PRUEBAS DE SOFTWARE PARA OBTENER INFORMACIÓN OBJETIVA SOBRE LA CALIDAD DE LAS DISTINTAS APLICACIONES Y SISTEMAS OPERATIVOS** DEL SISTEMA DE INFORMACIÓN. PUEDEN SER DE DOS TIPOS:

PRUEBAS ESTÁTICAS: PRUEBAS QUE NO REQUIEREN LA EJECUCIÓN DEL CÓDIGO DE LA APLICACIÓN PARA PODER REALIZARSE.

PRUEBAS DINÁMICAS: NECESITAN QUE SE ESTÉ EJECUTANDO LA APLICACIÓN EN EL MOMENTO DE LA REALIZACIÓN DE LA PRUEBA. SU PRINCIPAL VENTAJA ES SU MAYOR PRECISIÓN EN EL MOMENTO DE EVALUAR EL COMPORTAMIENTO DE LA APLICACIÓN ANALIZADA.

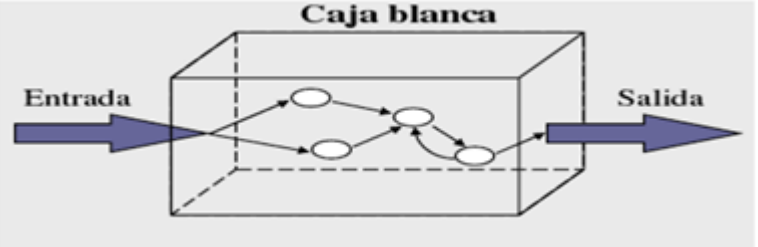
AMBAS PRUEBAS **UTILIZAN UNA SERIE DE HERRAMIENTAS Y MÉTODOS** QUE PERMITIRÁN LA DETECCIÓN DE LAS VULNERABILIDADES Y SU POSTERIOR MEDICIÓN

8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA

ANÁLISIS REMOTO DE CAJA BLANCA

SE REALIZA CON LA **EJECUCIÓN DE PRUEBAS QUE EXAMINAN LA ESTRUCTURA INTERNA DE LA APLICACIÓN Y DE LOS COMPONENTES DEL SISTEMA**.

ANTES DE LA EJECUCIÓN DE LAS PRUEBAS DE CAJA **BLANCA, LOS AUDITORES INFORMÁTICOS DEBERÁN RECOPILAR TODA LA INFORMACIÓN QUE SEA POSIBLE PARA LA EVALUACIÓN DE LA SEGURIDAD Y DE LAS VULNERABILIDADES DEL SISTEMA DE INFORMACIÓN**: CÓDIGO FUENTE DE LAS APLICACIONES, ARCHIVOS DE CONFIGURACIÓN, ETC.

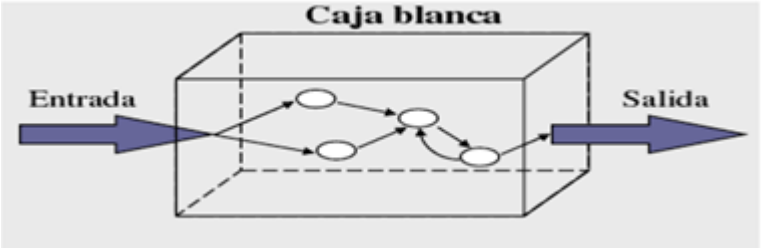


8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA

ANÁLISIS REMOTO DE CAJA BLANCA

CON ESTA INFORMACIÓN, ADEMÁS DE DETECTAR LAS VULNERABILIDADES MÁS PRÓXIMAS, TAMBIÉN SE PUEDEN DETECTAR VULNERABILIDADES POTENCIALES MÁS PROFUNDAS CON UNA REVISIÓN EXTENSA DEL SISTEMA.

ESTAS PRUEBAS **SUELEN REQUERIR MÁS RECURSOS** POR PARTE DEL AUDITOR Y DE LA ORGANIZACIÓN, PERO TAMBIÉN **OFRECEN RESULTADOS MÁS PRECISOS.**



8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA

ANÁLISIS REMOTO DE CAJA BLANCA

VENTAJAS

- LAS PRUEBAS SON MUY MINUCIOSAS Y LOS RESULTADOS OBTENIDOS MÁS PRECISOS.
- LAS RECOMENDACIONES OBTENIDAS DE LOS RESULTADOS DE ESTAS PRUEBAS TAMBIÉN SON MÁS PRECISAS Y EFICACES.
- DETECTA TANTO LAS VULNERABILIDADES MÁS INMEDIATAS COMO LAS MÁS PROFUNDAS (DE CONFIGURACIÓN Y DE DISEÑO DE LA APLICACIÓN).

DESVENTAJAS

- REQUIERE MUCHOS Y COSTOSOS RECURSOS
- NO HAY SIMULACIÓN DE INTRUSIÓN PARA VERIFICAR SU EFECTIVIDAD

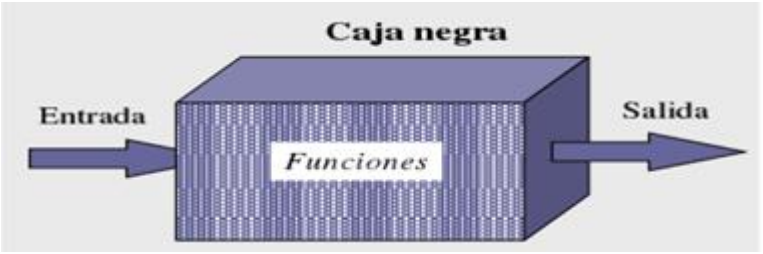
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA

ANÁLISIS REMOTO DE CAJA NEGRA

CONSISTEN EN **UNA SERIE DE PRUEBAS QUE EVALÚAN EXCLUSIVAMENTE LAS ENTRADAS Y SALIDAS DEL SISTEMA DE INFORMACIÓN.**

SU FINALIDAD PRINCIPAL ES CONSEGUIR **SIMULAR LOS ATAQUES DE UN INTRUSO**:

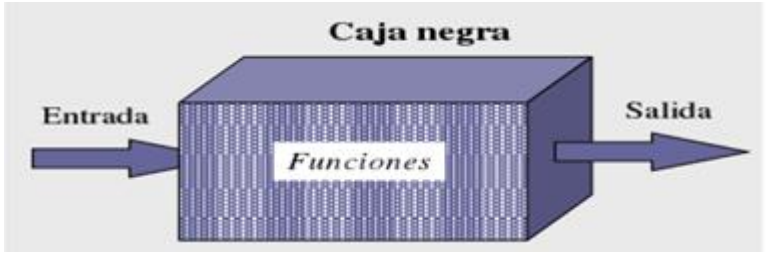
IMITAN LO QUE EL INTRUSO HARÍA Y OBTIENEN INFORMACIÓN BASTANTE REAL SOBRE LOS RIESGOS A LOS QUE SE EXPONE EL SISTEMA EVALUADO.



8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA

ANÁLISIS REMOTO DE CAJA NEGRA

LA IDEA DE ESTAS PRUEBAS ES QUE**, SI UN AUDITOR** DE SEGURIDAD **INFORMÁTICA ES CAPAZ DE DETECTAR ALGUNA VULNERABILID**AD CON ESTAS PRUEBAS DE CAJA NEGRA, **UN INTRUSO TAMBIÉN PODRÍA** DETECTARLAS CON FACILIDAD.



SE PUEDEN OBTENER DATOS DEL SISTEMA COMO:

- LAS FUNCIONES QUE REALIZA EL SISTEMA.
- EL GRADO DE CUMPLIMIENTO DE LOS OBJETIVOS DEL SISTEMA.
- LAS REACCIONES DEL SISTEMA ANTE LA PRESENCIA DE INTRUSIONES.

8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA

ANÁLISIS REMOTO DE CAJA NEGRA

VENTAJAS

- FACILITA INFORMACIÓN QUE PERMITE REALIZAR ESTIMACIONES REALES DE LAS AMENAZAS.
- OBTIENE LA INFORMACIÓN A TRAVÉS DEL ANÁLISIS DE INFORMACIÓN PÚBLICA (INTERNA Y EXTERNA).
- LOS RECURSOS DE LA ORGANIZACIÓN UTILIZADOS PARA ESTE TIPO DE PRUEBAS SON BASTANTE REDUCIDOS.

DESVENTAJAS

- RECOPILAR TODA LA INFORMACIÓN PÚBLICA NECESARIA PUEDE SER UN TRABAJO BASTANTE LABORIOSO.
- LAS VULNERABILIDADES MÁS PROFUNDAS Y OCULTAS PUEDEN SER PASADAS POR ALTO EN EL ANÁLISIS.
- LAS RECOMENDACIONES FORMULADAS A PARTIR DE LOS RESULTADOS DE ESTA PRUEBA SON DE CARÁCTER GENERAL.

CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. **OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA**
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA

UNA VEZ REALIZADA LA GESTIÓN DEL RIESGO DEL SISTEMA DE INFORMACIÓN, **YA SE CONOCEN CON MÁS PROFUNDIDAD LAS VULNERABILIDADES** A LAS QUE ESTÁ EXPUESTO.

CON ESTA INFORMACIÓN Y LAS VULNERABILIDADES DETECTADAS, SE PUEDEN **PROPONER UNA SERIE DE RECOMENDACIONES** QUE LAS ELIMINEN O QUE REDUZCAN SU PROBABILIDAD DE MATERIALIZACIÓN.

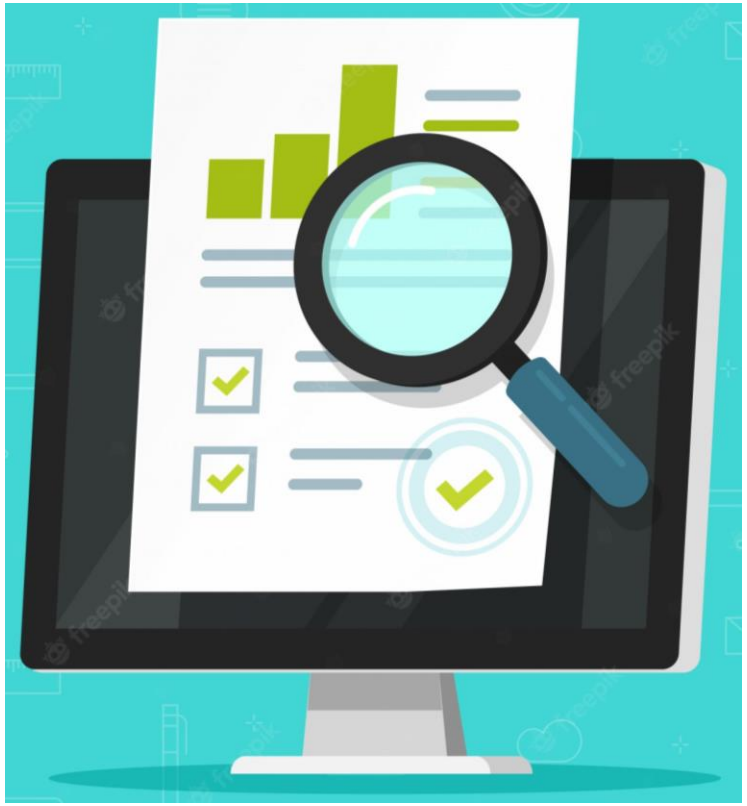
DE ESTE MODO, EL PROCESO DE AUDITORÍA EN FUTURAS EVALUACIONES SE IRÁ OPTIMIZANDO, YA QUE **EL NÚMERO DE VULNERABILIDADES Y DEFECTOS DEL SISTEMA DETECTADOS DEBERÍA SER MENOR SI LAS MEDIDAS CORRECTORAS SE APLICAN CORRECTAMENTE**.

9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA

EL INFORME DE AUDITORÍA

CON LA CORRECCIÓN DE LAS VULNERABILIDADES DETECTADAS Y LA CONTINUA EVALUACIÓN DE LOS SISTEMAS DE INFORMACIÓN, **DEBE PRODUCIRSE UN PROCESO DE APRENDIZAJE QUE DEBERÁ REFLEJARSE EN EL INFORME DE AUDITORÍA**, PERMITIENDO ASÍ UNA OPTIMIZACIÓN CONSTANTE Y PROGRESIVA DEL PROCESO DE AUDITORÍA.

EL INFORME DEBERÁ CONTENER EL HISTÓRICO DE LAS VULNERABILIDADES DETECTADAS, SU PROGRESIÓN Y LAS POSTERIORES MODIFICACIONES DEL SISTEMA DE INFORMACIÓN IMPLANTADAS SIGUIENDO LAS RECOMENDACIONES DE LA AUDITORÍA.



9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA

EL INFORME DE AUDITORÍA

ES UN DOCUMENTO FORMALIZADO QUE CONTIENE LOS OBJETIVOS DE LA AUDITORÍA, LAS METODOLOGÍAS UTILIZADAS, LOS RESULTADOS OBTENIDOS Y LAS CONCLUSIONES Y RECOMENDACIONES DE LOS AUDITORES.

TIENE QUE SER CLARO, CONCISO, OPORTUNO, OBJETIVO E IMPARCIAL Y DEBE SER ELABORADO POR AUDITORES INDEPENDIENTES.

EN CUANTO A LA **GESTIÓN DE RIESGOS**, **EL INFORME** DE AUDITORÍA **DEBERÁ CONTENER** TAMBIÉN **LOS ACTIVOS** DE LA ORGANIZACIÓN **Y SU VALORACIÓN**, JUNTO CON **LAS VULNERABILIDADES, AMENAZAS Y RIESGOS** DETECTADOS EN EL SISTEMA DE INFORMACIÓN DETECTADO.

CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. **IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS**
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS

LAS MEDIDAS DE SALVAGUARDA O DE SEGURIDAD **SON MEDIDAS CUYA FUNCIÓN** FUNDAMENTAL **ES REDUCIR O ELIMINAR UN RIESGO DE DOS FORMAS**:

- **LA REDUCCIÓN DE LA PROBABILIDAD DE MATERIALIZACIÓN DE LAS AMENAZAS**
- **LA REDUCCIÓN DEL IMPACTO DE LAS AMENAZAS SOBRE LA ORGANIZACIÓN**

10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS

REDUCCIÓN DE LA PROBABILIDAD DE MATERIALIZACIÓN DE LAS AMENAZAS

SON SALVAGUARDAS PREVENTIVAS. LA SALVAGUARDA IDEAL SERÍA AQUELLA QUE IMPIDIESE COMPLETAMENTE QUE SE MATERIALIZARA CUALQUIER TIPO DE AMENAZA.

REDUCCIÓN DEL IMPACTO DE LAS AMENAZAS SOBRE LA ORGANIZACIÓN

LIMITAN O REDUCEN LA DEGRADACIÓN DEL ACTIVO ANTE LA PRESENCIA DE ALGUNA AMENAZA, IMPIDIENDO QUE EL DAÑO OCASIONADO SE EXPANDA.

CIERTAS AMENAZAS TAMBIÉN PUEDEN LLEGAR A RESTAURAR EL SISTEMA CUANDO ALGUNA AMENAZA LO HA PUESTO EN PELIGRO O HA DAÑADO ALGUNO DE SUS ACTIVOS.

PARA QUE ESTAS SALVAGUARDAS ACTÚEN**, DEBE HABERSE MATERIALIZADO LA INCIDENCIA O AMENAZA** Y, EN CUALQUIER CASO, LA **SALVAGUARDA LIMITA LOS EFECTOS NOCIVOS Y SU EXPANSIÓN** SOBRE LOS ACTIVOS QUE FORMAN PARTE DEL SISTEMA DAÑADO.

10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS

SE CLASIFICAN EN VARIOS TIPOS, ATENDIENDO A CRITERIOS DIFERENTES.

ATENDIENDO AL **MOMENTO DE ACTUACIÓN DE LA SALVAGUARDA**:

- **ACTIVAS:** AQUELLAS QUE REDUCEN O ELIMINAN EL RIESGO DE UNA AMENAZA.
- **PASIVAS:** AQUELLAS QUE REDUCEN EL IMPACTO SOBRE LA ORGANIZACIÓN, UNA VEZ YA SE HA PRODUCIDO EL INCIDENTE DE SEGURIDAD.

ATENDIENDO A SU **COMPOSICIÓN Y AL TIPO DE PROTECCIÓN QUE OFRECEN**:

- **FÍSICAS:** AQUELLAS QUE PROTEGEN EL ACCESO FÍSICO A LOS ACTIVOS Y LAS CONDICIONES AMBIENTALES EN LAS QUE ESTOS SE UTILIZAN.
- **LÓGICAS:** SE ENCARGAN DE PROTEGER LOS ACTIVOS A TRAVÉS DE HERRAMIENTAS, TÉCNICAS Y PROGRAMAS INFORMÁTICOS.

10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS

UNA SALVAGUARDA EFICAZ AL 100% SERÍA LO IDEAL, PERO, PARA ELLO, **DEBERÍA CUMPLIR UNA SERIE DE PRECEPTOS:**

- SU IMPLANTACIÓN, CONFIGURACIÓN Y MANTENIMIENTO DEBEN SER PERFECTOS.
- DEBE EMPLEARSE EN TODO MOMENTO.
- SU PROTOCOLO DE USO NORMAL DEBE SER CLARO Y, EN CASO DE OCURRIR CUALQUIER INCIDENCIA, EL PERSONAL DEBE ESTAR CORRECTAMENTE FORMADO PARA REACCIONAR DE UN MODO RÁPIDO Y EFICAZ.
- DEBEN ESTAR IMPLANTADOS UNA SERIE DE CONTROLES QUE AVISEN CUANDO SE DETECTE CUALQUIER TIPO DE FALLO.

LAS ORGANIZACIONES DEBEN **INTENTAR CONSEGUIR UNAS SALVAGUARDAS QUE TENGAN UN CIERTO GRADO DE EFICACIA** QUE PERMITA EL CUMPLIMIENTO DE LOS OBJETIVOS DE SEGURIDAD MARCADOS, CALCULANDO UNA ESTIMACIÓN REAL CUANDO SE QUIERA ESTIMAR LA GESTIÓN DE RIESGOS.

10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS

LAS SALVAGUARDAS Y LOS ACTIVOS

EXISTE LA POSIBILIDAD DE QUE **ALGUNAS SALVAGUARDAS PASEN A FORMAR PARTE DEL EQUIPAMIENTO DE UN SISTEMA DE INFORMACIÓN**.

EL COSTE DE IMPLANTACIÓN DE LA SALVAGUARDA HACE QUE EL ACTIVO AL QUE PROTEGE AUMENTE DE VALOR, CONVIRTIÉNDOSE EN PARTE DE ÉL.

HAY QUE TENER EN CUENTA QUE, EN EL MOMENTO EN QUE PASA A FORMAR PARTE DE UN ACTIVO, **TAMBIÉN ESTÁ EXPUESTO A LOS RIESGOS DEL SISTEMA Y PUEDE TENER VULNERABILIDADES**, A LA VEZ QUE PUEDE SUFRIR LAS MISMAS AMENAZAS QUE LOS OTROS ACTIVOS.

10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS

LAS SALVAGUARDAS Y LOS ACTIVOS

POR ESO, CUANDO SE IMPLANTAN SALVAGUARDAS QUE FORMAN PARTE DEL ACTIVO, ***HAY QUE REALIZAR UN NUEVO ANÁLISIS DE RIESGOS*** *CON EL NUEVO SISTEMA DESPLEGADO PARA ASEGURARSE DE QUE EL RIESGO AL QUE SE EXPONE EL SISTEMA ES INFERIOR A AQUEL AL QUE ESTABA EXPUESTO ANTES DE IMPLANTARSE LA SALVAGUARDA*.

AUNQUE SE INCORPORE LA SALVAGUARDA AL SISTEMA, SU FINALIDAD DEBE SER LA MISMA: REDUCIR EL RIESGO DEL SISTEMA GENERAL Y DE LA ORGANIZACIÓN.

CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. **ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE**
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE

CUANDO YA SE HAN IDENTIFICADO Y VALORADO LOS ACTIVOS, AMENAZAS, VULNERABILIDADES Y SALVAGUARDAS, **LA SIGUIENTE FASE EN EL PROCESO DE GESTIÓN DEL RIESGO ES EL ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO** O, LO QUE ES LO MISMO, LA **ESTIMACIÓN DEL ESTADO DEL RIESGO.**

EL OBJETIVO PRINCIPAL DE ESTA FASE SE DIVIDE EN DOS PUNTOS FUNDAMENTALES:

- **ESTIMAR EL IMPACTO POTENCIAL AL QUE SE SOMETE EL SISTEMA DE INFORMACIÓN.**
- **ESTIMAR EL IMPACTO RESIDUAL AL QUE SE SOMETE EL SISTEMA DE INFORMACIÓN.**

11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE

ESTIMACIÓN DEL IMPACTO POTENCIAL

EL IMPACTO POTENCIAL **ESTÁ FORMADO POR EL CONJUNTO DE EFECTOS PERJUDICIALES QUE PUEDEN SUFRIR LOS ACTIVOS** DEL SISTEMA DE INFORMACIÓN **EN EL CASO DE MATERIALIZARSE UNA AMENAZA.**

PARA EL CÁLCULO DEL **ESCENARIO ACTIVO-AMENAZA** DERIVADO DEL IMPACTO POTENCIAL, DEBERÁN TENERSE EN CUENTA LOS ASPECTOS SIGUIENTES:

- **ACTIVOS IDENTIFICADOS Y SU VALORACIÓN**
- **AMENAZAS IDENTIFICADAS Y SU VALORACIÓN**

11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE

ESTIMACIÓN DEL IMPACTO POTENCIAL

TENIENDO EN CUENTA EL ***PAR ACTIVO-AMENAZA***, PUEDEN ESTABLECERSE UNA SERIE DE ESCENARIOS DE IMPACTO TENIENDO EN CUENTA LA DEGRADACIÓN DEL ACTIVO PROVOCADA POR LA AMENAZA Y LA VALORACIÓN DE DICHO ACTIVO.

SE CATEGORIZA EL VALOR DE LOS ACTIVOS EN:

- **MUY ALTO**
- **ALTO**
- **MEDIO**
- **BAJO**
- **MUY BAJO**

11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE

ESTIMACIÓN DEL IMPACTO POTENCIAL

POR OTRO LADO, **SE CATEGORIZA SU DEGRADACIÓN PROVOCADA POR LA AMENAZA** EN:

- **DEGRADACIÓN INFERIOR AL 1 % DE SU VALOR.**
- **DEGRADACIÓN ENTRE EL 1 Y EL 10% DE SU VALOR.**
- **DEGRADACIÓN DE MÁS DEL 10 % DE SU VALOR.**

CON LAS DISTINTAS COMBINACIONES DE LAS CATEGORÍAS DESCRITAS ARRIBA, SE FORMA UNA **TABLA DE ESCENARIOS**.

11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE

ESTIMACIÓN DEL IMPACTO POTENCIAL

IMPACTO		Degradación del activo		
		Inferior al 1 %	1-10 %	Superior al 10 %
Valor del activo	Muy alto	MEDIO	ALTO	MUY ALTO
	Alto	BAJO	MEDIO	ALTO
	Medio	MUY BAJO	BAJO	MEDIO
	Bajo	MUY BAJO	MUY BAJO	BAJO
	Muy bajo	MUY BAJO	MUY BAJO	MUY BAJO

11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE

ESTIMACIÓN DEL IMPACTO RESIDUAL

EL IMPACTO RESIDUAL **TIENE EN CUENTA LA ACTUACIÓN DE LAS SALVAGUARDAS** SOBRE EL RIESGO DEL SISTEMA DE INFORMACIÓN.

SE DEFINE **EL IMPACTO RESIDUAL** COMO *LOS DAÑOS A LOS QUE SE EXPONE EL SISTEMA DE INFORMACIÓN CUANDO ESTE ESTÁ PROTEGIDO POR LAS SALVAGUARDAS IMPLANTADAS*.

DE ESTE MODO, **PARA SU ESTIMACIÓN SE AÑADE UN ELEMENTO MÁS AL CÁLCULO**, SIENDO SUS ELEMENTOS PRINCIPALES:

- LA IDENTIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS.
- LA IDENTIFICACIÓN Y VALORACIÓN DE LAS AMENAZAS.
- **LA IDENTIFICACIÓN Y VALORACIÓN DE LAS SALVAGUARDAS.**

11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE

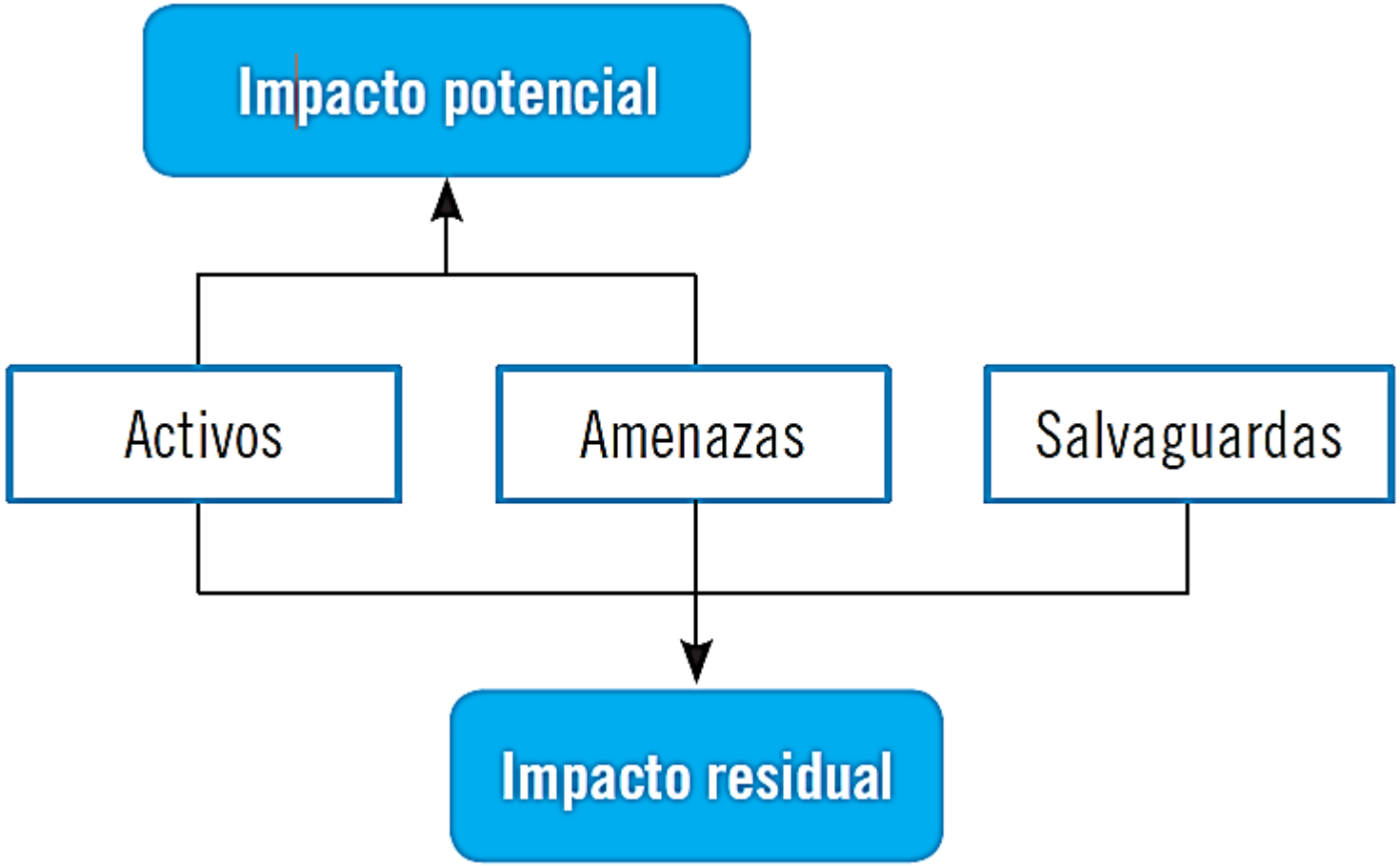
ESTIMACIÓN DEL IMPACTO RESIDUAL

SI LA ACTUACIÓN DE LAS SALVAGUARDAS FUESE EFICAZ Y CORRECTA**, EL IMPACTO RESIDUAL DE UNA AMENAZA SOBRE LOS ACTIVOS DEL SISTEMA DE INFORMACIÓN DEBERÁ SER MENOR QUE SU IMPACTO POTENCIAL.**

SI NO FUESE ASÍ, DEBERÍA INICIARSE UNA EVALUACIÓN DE LAS SALVAGUARDAS PARA CONOCER SUS VULNERABILIDADES Y LOS EFECTOS DE ESTAS E IMPLANTAR MEDIDAS CORRECTORAS QUE PERMITAN UNA MAYOR EFICIENCIA Y UN MENOR IMPACTO ANTE INCIDENCIAS DE SEGURIDAD.

11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE

IMPACTO POTENCIAL Y RESIDUAL



CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. **DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS**
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS

PARA ESTABLECER EL NIVEL DE RIESGO DE CADA **PAR DE ACTIVO/AMENAZA**, PREVIAMENTE HAY QUE DETERMINAR:

- **LA PROBABILIDAD**
- **EL IMPACTO**

DE **MATERIALIZACIÓN DE LOS ESCENARIOS**.

12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS

PROBABILIDAD DE MATERIALIZACIÓN DE LOS ESCENARIOS DE RIESGO

LA PROBABILIDAD DE MATERIALIZACIÓN DE UN ESCENARIO SE DEFINE CON **LAS POSIBILIDADES REALES QUE HAY DE PRODUCIRSE UNA INCIDENCIA DE SEGURIDAD Y LA FRECUENCIA CON LA QUE SE PUEDE PRODUCIR.** ESTA PROBABILIDAD VIENE CLASIFICADA EN CINCO CATEGORÍAS DISTINTAS:

- **RARO:** CON PROBABILIDADES CASI NULAS DE MATERIALIZARSE LA AMENAZA; ENTRE 0 Y 20% DE PROBABILIDAD.
- **IMPROBABLE:** CON POCAS PROBABILIDADES DE MATERIALIZARSE LA AMENAZA: ENTRE 20 Y 40%.
- **PROBABLE:** TANTO PUEDE MATERIALIZARSE LA AMENAZA COMO NO MATERIALIZARSE; ENTRE 40 Y 60%.
- **ALTAMENTE PROBABLE:** CON ELEVADAS POSIBILIDADES DE MATERIALIZARSE LA AMENAZA; ENTRE 60 Y 80%.
- **CASI CERTEZA:** ES PRÁCTICAMENTE SEGURO QUE SE PRODUZCA LA AMENAZA; ENTRE 80 Y 100%.

12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS

PROBABILIDAD DE MATERIALIZACIÓN DE LOS ESCENARIOS DE RIESGO

PROBABILIDAD	ESCALA	DESCRIPCIÓN	CALIFICACIÓN
Raro	0-20 %	Eventualidad casi nula	1
Improbable	20-40 %	Solo ocurre en ocasiones excepcionales	2
Probable	40-60 %	Puede ocurrir o no ocurrir	3
Altamente probable	60-80 %	Puede ocurrir bastantes veces	4
Casi certeza	80-100 %	Casi siempre ocurre	5

12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS

IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS DE RIESGO

EL IMPACTO VENDRÁ DETERMINADO POR LOS **EFECTOS NEGATIVOS QUE PUEDE PRODUCIR LA MATERIALIZACIÓN DE UNA AMENAZA** Y SE CLASIFICARÁ EN:

- **MUY BAJO:** EL VALOR DE LOS ACTIVOS AFECTADOS ES MUY BAJO Y LA DEGRADACIÓN QUE PUEDEN SUFRIR ANTE INCIDENCIAS ES PRÁCTICAMENTE NULA.
- **BAJO:** EL IMPACTO DE LA MATERIALIZACIÓN DE LA AMENAZA ES BASTANTE IRRELEVANTE PARA LA ORGANIZACIÓN.
- **MEDIO:** EL IMPACTO DE MATERIALIZACIÓN DE LA AMENAZA YA MERECE ATENCIÓN POR PARTE DE LA ORGANIZACIÓN, BIEN PORQUE LOS ACTIVOS TIENEN UN VALOR CONSIDERABLE O BIEN PORQUE SU NIVEL DE DEGRADACIÓN TAMBIÉN ES BASTANTE ELEVADO.
- **ALTO:** LA MATERIALIZACIÓN DE LA AMENAZA PUEDE OCASIONAR DAÑOS IMPORTANTES PARA EL SISTEMA DE INFORMACIÓN Y PARA LA ORGANIZACIÓN EN GENERAL.
- **MUY ALTO:** LOS DAÑOS QUE PUEDE OCASIONAR LA AMENAZA SI SE MATERIALIZA PUEDEN SER MUY GRAVES, QUEDANDO LA ORGANIZACIÓN GRAVEMENTE DAÑADA; LOS ACTIVOS AFECTADOS SON DE GRAN VALOR Y SU DEGRADACIÓN ES PRÁCTICAMENTE TOTAL.

12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS

IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS DE RIESGO

Impacto	DESCRIPCIÓN	CALIFICACIÓN
Muy bajo	Impacto insignificante.	1
Bajo	Efectos mínimos para la organización.	2
Medio	Efectos considerables sobre los activos.	3
Alto	Efectos muy considerables para la organización en general.	4
Muy alto	Efectos irreparables o difícilmente reparables para la organización.	5

CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. **ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA**
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA

CUANDO YA SE HAN CATEGORIZADO LOS ***PARES ACTIVO/AMENAZA*** Y ESTABLECIDOS LOS DISTINTOS NIVELES DE IMPACTO Y PROBABILIDAD DE UNA AMENAZA, EL SIGUIENTE PASO ES LA **ESTIMACIÓN DEL RIESGO.**

LOS DATOS DE ENTRADA QUE SE DEBERÁN UTILIZAR PARA LA ESTIMACIÓN DEL RIESGO SERÁN LOS SIGUIENTES:

- IDENTIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS.
- IDENTIFICACIÓN Y VALORACIÓN DE LAS AMENAZAS.
- IDENTIFICACIÓN Y VALORACIÓN DE LAS SALVAGUARDAS.
- **IMPACTO ESTIMADO CON LOS PARES ACTIVO/AMENAZA IDENTIFICADOS.**

13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA

LA ESTIMACIÓN DEL RIESGO PUEDE SER DE RIESGO RESIDUAL O DE RIESGO POTENCIAL:

- **EL RIESGO POTENCIAL** SERÁ EL RIESGO AL QUE ESTÁ SOMETIDO EL SISTEMA DE INFORMACIÓN SIN CONTAR CON LAS SALVAGUARDAS ESTABLECIDAS. SOLO SE TIENEN EN CUENTA LOS ACTIVOS, LAS AMENAZAS Y EL IMPACTO POTENCIAL.
- **EL RIESGO RESIDUAL,** POR EL CONTRARIO, SE ESTIMARÁ TOMANDO COMO FACTORES DE CÁLCULO LAS SALVAGUARDAS ESTABLECIDAS EN EL SISTEMA Y EL IMPACTO RESIDUAL, ADEMÁS DE LOS ACTIVOS Y LAS AMENAZAS.

13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA

NIVEL DE RIESGO DE LOS ESCENARIOS DE LOS PARES ACTIVO/AMENAZA

LOS DISTINTOS ESCENARIOS QUE PUEDEN PRODUCIRSE CON **LAS COMBINACIONES** DE LAS CATEGORÍAS **DEL IMPACTO** SOBRE LOS ACTIVOS DE UNA ORGANIZACIÓN **Y LA PROBABILIDAD** DE MATERIALIZACIÓN DE LAS AMENAZAS ESTABLECEN **VARIAS CATEGORÍAS DE RIESGO** DIVIDIDAS EN CINCO NIVELES:

- **NIVEL DE RIESGO DESPRECIABLE**
- **NIVEL DE RIESGO BAJO**
- **NIVEL DE RIESGO MODERADO**
- **NIVEL DE RIESGO IMPORTANTE**
- **NIVEL DE RIESGO CRÍTICO**

LA UBICACIÓN DE CADA RIESGO EN UNA U OTRA CATEGORÍA SE CALCULARÁ CON EL PRODUCTO DE LAS CALIFICACIONES DE SU IMPACTO Y DE SU PROBABILIDAD:

RIESGO = IMPACTO X PROBABILIDAD

13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA

NIVEL DE RIESGO DE LOS ESCENARIOS DE LOS PARES ACTIVO/AMENAZA

Probabilidad	Nivel de riesgos o Nivel de Severidad				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi Certeza	MODERADO	ALTO	ALTO	EXTREMO	EXTREMO
Muy Probable	BAJO	MODERADO	ALTO	ALTO	EXTREMO
Posible	BAJO	MODERADO	MODERADO	ALTO	ALTO
Improbable	BAJO	BAJO	MODERADO	MODERADO	ALTO
Rara	BAJO	BAJO	BAJO	BAJO	MODERADO
	Impacto				

CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. **DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO**
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO

PARA EVALUAR EL RIESGO ESTIMADO DE CADA PAR ACTIVO/AMENAZA, DEBERÁ TENERSE EN CUENTA SU UBICACIÓN EN LA MATRIZ DE RIESGOS.

LOS CRITERIOS A TENER EN CUENTA SON LOS SIGUIENTES:

- **SI EL RIESGO ESTÁ SITUADO EN UNA ZONA DE RIESGO CRÍTICO**
- **SI EL RIESGO ESTÁ SITUADO EN UNA ZONA DE RIESGO DESPRECIABLE**
- **SI EL RIESGO ESTÁ SITUADO EN OTRAS ZONAS (RIESGO BAJO, MODERADO E IMPORTANTE)**

14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO

SI EL RIESGO ESTÁ SITUADO EN UNA ZONA DE RIESGO CRÍTICO

LOS EFECTOS PARA LA ORGANIZACIÓN PUEDEN SER MUY PERJUDICIALES PARA EL CORRECTO DESARROLLO DE SU ACTIVIDAD

SE ACONSEJA ELIMINAR LA ACTIVIDAD QUE OCASIONA EL RIESGO SIEMPRE QUE SEA POSIBLE O, POR LO MENOS, REDUCIRLA.

LA ORGANIZACIÓN DEBERÁ DISEÑAR PLANES DE CONTINGENCIA QUE PERMITAN LA RESTAURACIÓN DEL SISTEMA DE INFORMACIÓN LO ANTES POSIBLE EN CASO DE MATERIALIZARSE LA AMENAZA.

14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO

SI EL RIESGO ESTÁ SITUADO EN UNA ZONA DE RIESGO DESPRECIABLE

SERÁ UN RIESGO ASUMIBLE POR LA ORGANIZACIÓN Y NO SERÁ NECESARIA LA IMPLANTACIÓN DE MEDIDAS ADICIONALES QUE LO REDUZCAN O LO ELIMINEN.

SI EL RIESGO ESTÁ SITUADO EN OTRAS ZONAS (RIESGO BAJO, MODERADO E IMPORTANTE)

LA ORGANIZACIÓN DEBERÁ VALORAR LA IMPORTANCIA Y EL COSTE DE ESTABLECER MEDIDAS CORRECTIVAS QUE DISMINUYAN O ELIMINEN LOS RIESGOS DE CADA ACTIVO.

SE TENDRÁ QUE EVALUAR CASO POR CASO PARA DETERMINAR SI LA IMPLANTACIÓN DE LA MEDIDA CORRECTIVA COMPENSA PARA LA REDUCCIÓN DE RIESGO QUE SE PUEDE OBTENER CON ELLO.

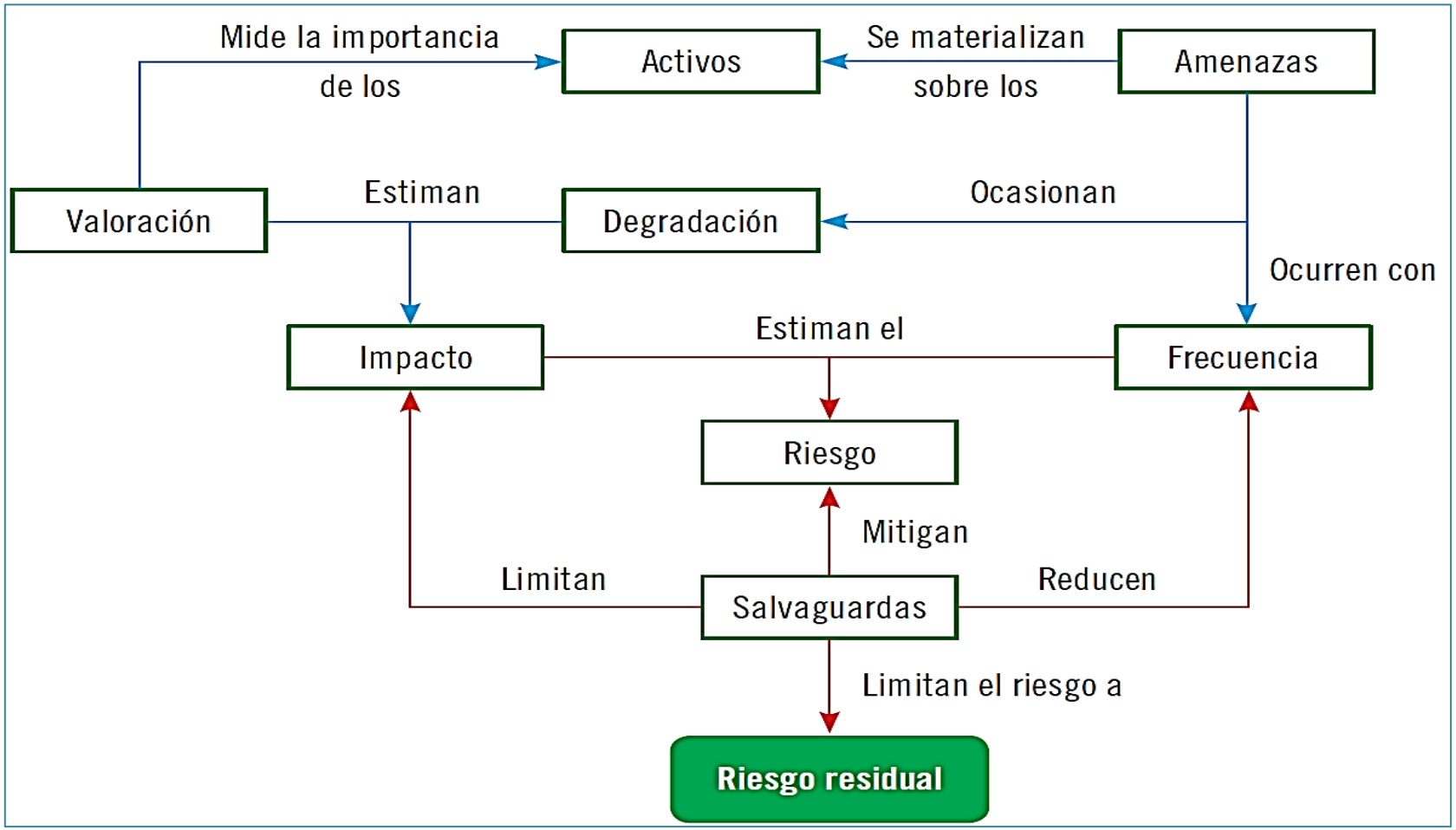
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO

CON LA EVALUACIÓN DE CADA RIESGO POR SEPARADO, LA ORGANIZACIÓN OBTENDRÁ INFORMACIÓN VALIOSA QUE LE PERMITIRÁ:

- **ESTABLECER LA PROBABILIDAD DE MATERIALIZACIÓN DE AMENAZAS** QUE PUEDAN AFECTAR A LA CORRECTA ACTIVIDAD DE LA ORGANIZACIÓN Y QUE PUEDAN OBSTACULIZAR EL CUMPLIMIENTO DE SUS OBJETIVOS.
- **CALCULAR Y ESTIMAR EL IMPACTO DE LAS AMENAZAS** SOBRE LAS PERSONAS Y LOS DEMÁS ACTIVOS Y RECURSOS DE LA ORGANIZACIÓN. CON ELLO, PODRÁ SELECCIONAR LOS ACTIVOS CON MÁS IMPACTO Y ESTABLECER MEDIDAS QUE LES OTORGUEN UNA MAYOR PROTECCIÓN ANTE POSIBLES AMENAZAS.
- **ESTABLECER CRITERIOS DE VALORACIÓN, CALIFICACIÓN Y EVALUACIÓN DE LOS RIESGOS** QUE PERMITA REALIZAR UNA TOMA DE DECISIONES DE SEGURIDAD ADECUADAS PARA GARANTIZAR EL CORRECTO FUNCIONAMIENTO DE LA ORGANIZACIÓN.

14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO

VISIÓN GENERAL DE LA GESTIÓN DE RIESGOS



LAS AMENAZAS SE MATERIALIZAN SOBRE LOS ACTIVOS, A LOS QUE DEGRADAN, Y OCURREN CON UNA FRECUENCIA ESTIMADA.

EL VALOR DE LOS ACTIVOS ES LO QUE LES DA IMPORTANCIA DENTRO DE UNA ORGANIZACIÓN.

EL VALOR DE LOS ACTIVOS Y SU DEGRADACIÓN SON LOS QUE PERMITEN CALCULAR EL IMPACTO DE UNA AMENAZA.

POR OTRO LADO, LA FRECUENCIA CON LA QUE SE MATERIALIZA LA AMENAZA Y EL IMPACTO DE ESTA SOBRE UN ACTIVO DETERMINARÁN SU NIVEL DE RIESGO.

PARA MITIGAR EL RIESGO ESTÁN LAS SALVAGUARDAS, QUE LO LLEVARÁN A CABO LIMITANDO EL IMPACTO O REDUCIENDO LA FRECUENCIA DE LA AMENAZA, LLEGANDO ASÍ A LA ESTIMACIÓN DEL RIESGO RESIDUAL (NIVEL DE RIESGO REDUCIDO POR LA PROTECCIÓN DE LAS SALVAGUARDAS).

CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. **RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS**
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS

EN FUNCIÓN DEL NIVEL DEL RIESGO AL QUE SE SOMETEN LOS DISTINTOS ACTIVOS DEL SISTEMA DE INFORMACIÓN DE UNA ORGANIZACIÓN, **SE ENCUENTRAN VARIAS ALTERNATIVAS PARA PROCEDER A SU GESTIÓN.**

ESTAS ALTERNATIVAS **SE FUNDAMENTAN EN LOS CONTROLES**, AQUELLAS MEDIDAS DE SEGURIDAD CUYO OBJETIVO FUNDAMENTAL ES REDUCIR O LIMITAR EL RIESGO TODO LO POSIBLE.

LA POLÍTICA DE GESTIÓN DE RIESGOS DE LA ORGANIZACIÓN DECIDIRÁ QUÉ TIPO DE CONTROL SE VA A IMPLANTAR EN SU SISTEMA DE INFORMACIÓN, DISTINGUIENDO ENTRE:

- **CONTROLES DISUASORIOS**
- **CONTROLES PREVENTIVOS**
- **CONTROLES DETECTORES**
- **CONTROLES CORRECTIVOS**

15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS

CONTROLES DISUASORIOS

SE TRATA DE CONTROLES CUYA FUNCIÓN PRINCIPAL **ES REDUCIR LA PROBABILIDAD DE OCURRENCIA DEL INCIDENTE** (DE MATERIALIZACIÓN DE LA AMENAZA). UN EJEMPLO SERÍA EL ESTABLECIMIENTO DE CONTROLES DE ACCESO PARA EVITAR INTRUSIONES NO DESEADAS.

CONTROLES PREVENTIVOS

TIENEN COMO OBJETIVO **REDUCIR LA VULNERABILIDAD DE LOS ACTIVOS Y DE SUS SALVAGUARDAS PARA LIMITAR LAS POSIBILIDADES DE ENTRADA DE CUALQUIER AMENAZA**. EJEMPLO DE ELLO SON LAS ACTUALIZACIONES Y PARCHES DE LAS APLICACIONES QUE, INSTALÁNDOLOS PERIÓDICAMENTE, PERMITEN LA REDUCCIÓN DE SUS VULNERABILIDADES LO MÁXIMO POSIBLE.

15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS

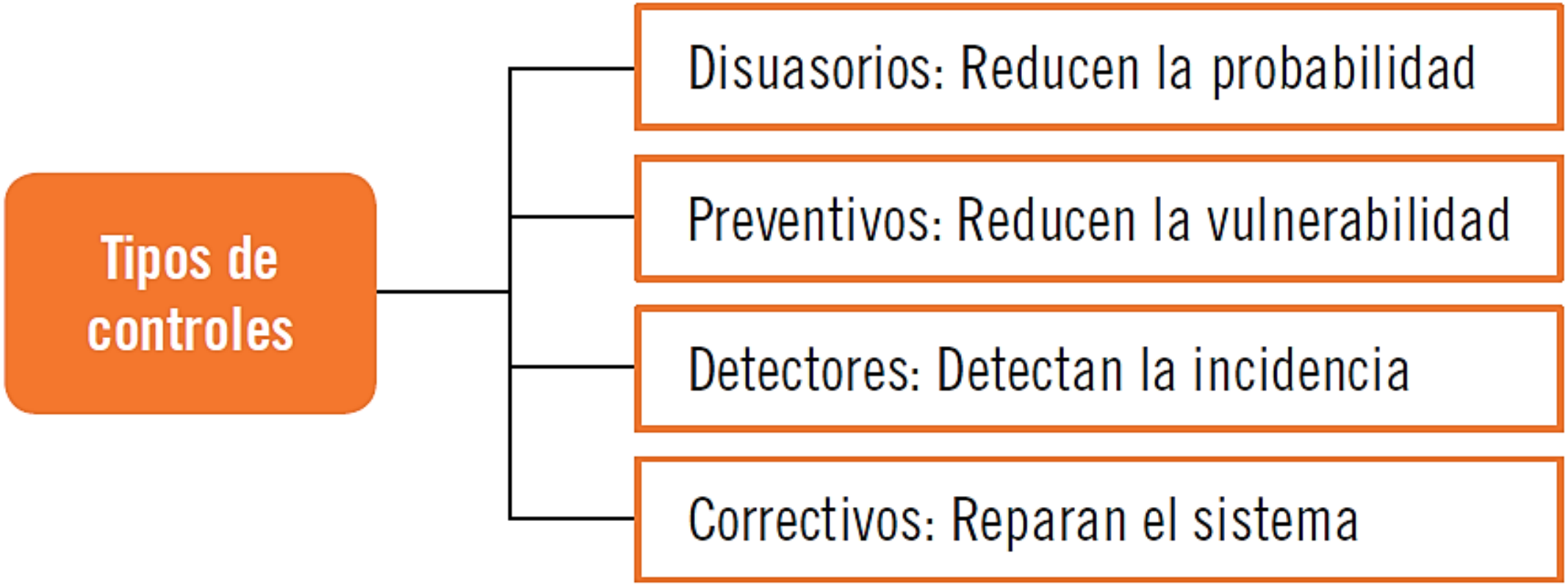
CONTROLES DETECTORES

DETECTAN EL INCIDENTE CUANDO ESTE SE ESTÁ PRODUCIENDO O YA SE HA PRODUCIDO. POR EJEMPLO, CUANDO UN ANTIVIRUS DETECTA LA ENTRADA DE UN VIRUS EN EL SISTEMA, LA INCIDENCIA YA SE HA PRODUCIDO, PERO HA SIDO IDENTIFICADA POR UN CONTROL (EN ESTE CASO, EL ANTIVIRUS).

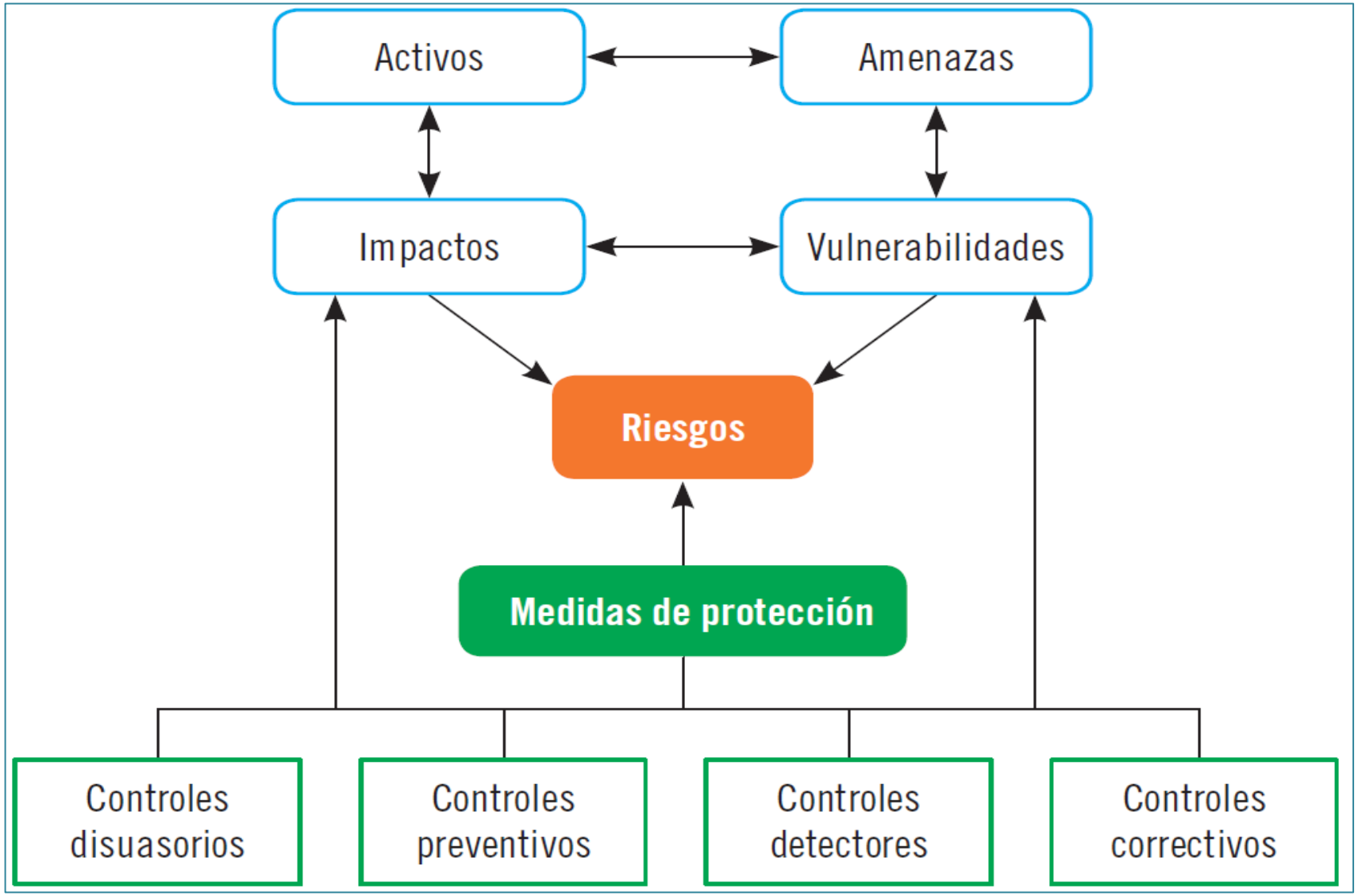
CONTROLES CORRECTIVOS

SU ACTUACIÓN SE LIMITA A MOMENTOS POSTERIORES DEL INCIDENTE. SE ENCARGAN DE LIMITAR SUS EFECTOS PERJUDICIALES, **DE INTENTAR RECUPERAR LA SITUACIÓN ANTERIOR A LA MATERIALIZACIÓN DE LA AMENAZA**. UN EJEMPLO CLARO DE CONTROL CORRECTIVO ES LA UTILIZACIÓN DE COPIAS DE RESPALDO.

15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS



15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS



EL ESTABLECIMIENTO CONJUNTO DE TODAS LAS TIPOLOGÍAS DE CONTROLES PERMITIRÁ LA REDUCCIÓN DEL RIESGO GENERAL DE LA ORGANIZACIÓN AL REDUCIR TODOS SUS COMPONENTES FUNDAMENTALES.

AL REDUCIR EL IMPACTO DE LAS AMENAZAS Y LA APARICIÓN DE VULNERABILIDADES, SE REDUCE LA PROBABILIDAD DE MATERIALIZACIÓN DE AMENAZAS Y, COMO CONSECUENCIA, LA DEGRADACIÓN DE LOS ACTIVOS, DISMINUYENDO ASÍ EL NIVEL GENERAL DE RIESGO DEL ACTIVO.

CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. **GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS**

16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

RECOMENDACIONES BÁSICAS PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS:

1. CONOCER Y ENTENDER EL FUNCIONAMIENTO DE LA ADMINISTRACIÓN DE RIESGOS
2. DEFINIR LAS ACCIONES DEL PLAN DE GESTIÓN DE RIESGOS
3. CONSEGUIR EL APOYO DE LA DIRECCIÓN Y DE PROFESIONALES EXTERNOS
4. IDENTIFICAR LAS CONSECUENCIAS DE CADA RIESGO
5. DESCARTAR LAS AMENAZAS IRRELEVANTES
6. INVENTARIAR LOS ACTIVOS SUSCEPTIBLES DE RIESGO
7. ASIGNAR PROBABILIDADES
8. ASIGNAR EL IMPACTO
9. DETERMINAR EL RIESGO PARA CADA ACTIVO
10. CLASIFICAR LOS RIESGOS
11. CALCULAR EL RIESGO TOTAL
12. DISEÑAR ESTRATEGIAS DE REDUCCIÓN DE RIESGOS
13. DESARROLLAR PLANES DE CONTINGENCIA
14. ANALIZAR LA EFECTIVIDAD DE LAS ESTRATEGIAS IMPLANTADAS

16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

RECOMENDACIONES BÁSICAS PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

1. **CONOCER Y ENTENDER EL FUNCIONAMIENTO DE LA ADMINISTRACIÓN DE RIESGOS**
   LA ORGANIZACIÓN DEBE *TENER CLAROS Y BIEN DEFINIDOS LOS CONCEPTOS QUE FORMAN PARTE DE LA GESTIÓN DE RIESGOS*: RIESGO, AMENAZA, VULNERABILIDAD, ACTIVO, SALVAGUARDA, ETC. SOBRE TODO, DEBE CONOCER TODOS LOS FACTORES NECESARIOS PARA LA DEFINICIÓN Y ESTIMACIÓN DE LOS RIESGOS:
   - **AMENAZA:** ¿QUÉ PUEDE SUCEDER?
   - **PROBABILIDAD:** ¿QUÉ POSIBILIDADES HAY DE QUE SUCEDA? ¿CON QUÉ FRECUENCIA?
   - **IMPACTO:** ¿QUÉ EFECTOS PERJUDICIALES PUEDE OCASIONAR LA AMENAZA SI SE MATERIALIZA?
   - **ACTIVO:** ¿QUÉ RECURSOS PUEDEN VERSE AFECTADOS?
   - **SALVAGUARDA:** ¿CÓMO PUEDE REDUCIRSE EL RIESGO?

16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

RECOMENDACIONES BÁSICAS PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

2. **DEFINIR LAS ACCIONES DEL PLAN DE GESTIÓN DE RIESGOS**
   DEBEN ESTABLECERSE ACCIONES COMO LOS *ACTIVOS QUE SE QUIEREN EVALUAR, LAS POSIBLES AMENAZAS QUE SE PUEDEN MATERIALIZAR, QUÉ METODOLOGÍA SE VA A UTILIZAR, CUÁLES SERÁN LOS UMBRALES DE RIESGO ACEPTABLES, ETC.*

3. **CONSEGUIR EL APOYO DE LA DIRECCIÓN Y DE PROFESIONALES EXTERNOS**
   EN CASOS EN LOS QUE LA REDUCCIÓN O ELIMINACIÓN DEL RIESGO CONLLEVA UN COSTE ELEVADO, SE *RECOMIENDA RECURRIR A PROFESIONALES EXTERNOS QUE PERMITAN LA GESTIÓN DEL RIESGO CON MENORES COSTES Y DELEGACIÓN DE RESPONSABILIDADES*.

   POR OTRO LADO, LOS ENCARGADOS DE LA GESTIÓN DE RIESGOS *DEBEN CONTAR CON EL APOYO DE LA DIRECCIÓN* PARA QUE LA ACTUACIÓN SEA ACORDE CON LA MISIÓN GLOBAL DE LA DIRECCIÓN Y SE INTEGRE COMO UNA ACTIVIDAD DE ESTA.

16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

RECOMENDACIONES BÁSICAS PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

4. **IDENTIFICAR LAS CONSECUENCIAS DE CADA RIESGO**
   TENIENDO EN CUENTA QUE CADA RIESGO CONLLEVA CONSECUENCIAS CON PERJUICIOS DISTINTOS, *DEBEN PODER IDENTIFICARSE Y VALORAR PARA CONOCER QUÉ RIESGOS ES NECESARIO PRIORIZAR Y ATAJAR CON MÁS INMEDIATEZ*.
5. **DESCARTAR LAS AMENAZAS IRRELEVANTES**
   DEBERÁN DESCARTARSE AQUELLAS AMENAZAS CUYO IMPACTO Y PROBABILIDAD DE OCURRENCIA SEAN MÍNIMOS PARA CONCENTRAR LOS RECURSOS Y ESFUERZOS EN AMENAZAS QUE PUEDAN AFECTAR A ACTIVOS DE ALTO VALOR, CON LA ELABORACIÓN DE UN PLAN DE CONTINGENCIA.

16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

RECOMENDACIONES BÁSICAS PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

6. **INVENTARIAR LOS ACTIVOS SUSCEPTIBLES DE RIESGO**
   PARA TENER CONTROLADOS LOS RIESGOS, *SE RECOMIENDA TENER UN INVENTARIO DE TODOS LOS ACTIVOS DE VALOR* SUSCEPTIBLES DE SUFRIR ALGUNA AMENAZA. EL INVENTARIO DEBERÁ ACTUALIZARSE CON CIERTA PERIODICIDAD.
7. **ASIGNAR PROBABILIDADES**
   PARA CADA ACTIVO, *DEBERÁN ASIGNARSE LAS PROBABILIDADES DE MATERIALIZACIÓN DE CADA ACTIVO Y LA FRECUENCIA CON LA QUE SE PUEDEN PRODUCIR*.
8. **ASIGNAR EL IMPACTO**
   UNA VEZ ASIGNADAS LAS PROBABILIDADES, *HAY QUE ASIGNAR EL GRADO DE DEGRADACIÓN* QUE SUFRIRÍA CADA ACTIVO EN CASO DE PRODUCIRSE LA AMENAZA.

16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

RECOMENDACIONES BÁSICAS PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

9. **DETERMINAR EL RIESGO PARA CADA ACTIVO**
   CON LAS PROBABILIDADES Y LOS IMPACTOS ESTIMADOS PARA CADA ACTIVO, DEBERÁ CALCULARSE UNA COMBINACIÓN DE AMBOS FACTORES PARA *ESTIMAR EL RIESGO POTENCIAL DE CADA ACTIVO.*
10. **CLASIFICAR LOS RIESGOS**
    CON LOS RIESGOS CALCULADOS PARA CADA ACTIVO, *DEBERÁ ELABORASE UNA LISTA CON TODOS ELLOS SIGUIENDO UN ORDEN DE PRIORIDAD DE ACTUACIÓN*: A MAYOR RIESGO, MAYOR PRIORIDAD DE ACTUACIÓN Y VICEVERSA.
11. **CALCULAR EL RIESGO TOTAL**
    SE CALCULARÁ EL RIESGO TOTAL DEL SISTEMA DE INFORMACIÓN DE LA ORGANIZACIÓN HACIENDO UN PROMEDIO ARITMÉTICO DE TODOS LOS RIESGOS CALCULADOS DE CADA ACTIVO.

16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

RECOMENDACIONES BÁSICAS PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

12. DISEÑAR ESTRATEGIAS DE REDUCCIÓN DE RIESGOS

PARA REDUCIR EL RIESGO GLOBAL DE LA ORGANIZACIÓN, *DEBERÁN TOMARSE DECISIONES DE ACTUACIÓN SOBRE QUÉ TIPOS DE CONTROLES SE PUEDEN IMPLANTAR Y QUÉ EFECTOS PUEDEN TENER SOBRE LOS RIESGOS DE LA ORGANIZACIÓN.*

13. DESARROLLAR PLANES DE CONTINGENCIA

PARA LOS RIESGOS MÁS IMPORTANTES (QUE AFECTAN A ACTIVOS MÁS VALIOSOS Y OCURREN CON MÁS FRECUENCIA) *DEBERÁ DISEÑARSE UN PLAN DE CONTINGENCIA QUE PERMITA REDUCIRLOS EN EL MENOR TIEMPO POSIBLE* Y RESTITUIR LA SITUACIÓN PREVIA, EVITANDO QUE LOS DAÑOS OCASIONADOS SE EXPANDAN.

16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

RECOMENDACIONES BÁSICAS PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

14. ANALIZAR LA EFECTIVIDAD DE LAS ESTRATEGIAS IMPLANTADAS

UNA VEZ PUESTA EN MARCHA LA GESTIÓN DE RIESGOS Y LAS SALVAGUARDAS Y CONTROLES PREVISTOS, DEBERÁ ANALIZARSE DE NUEVO EL RIESGO PARA CADA ACTIVO Y EL RIESGO GLOBAL DE LA ORGANIZACIÓN. SI LOS RIESGOS NO SE HAN REDUCIDO O LA REDUCCIÓN HA SIDO MÍNIMA, SIGNIFICARÁ QUE LAS MEDIDAS IMPLANTADAS NO SON EFICACES Y SERÁ NECESARIA UNA NUEVA EVALUACIÓN PARA DETECTAR EN QUÉ FALLAN Y CÓMO PUEDEN SOLUCIONARSE.

POR EL CONTRARIO, SI SE CONSIGUE REDUCIR ACEPTABLEMENTE EL RIESGO, SIGNIFICARÁ QUE LOS CONTROLES Y SALVAGUARDAS SON LOS CORRECTOS Y QUE LA GESTIÓN DE RIESGOS SE ESTÁ LLEVANDO A CABO DE UN MODO ADECUADO.

CONTENIDOS

1. INTRODUCCIÓN
2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA
9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS
16. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

RESUMEN

UN **RIESGO** ES CUALQUIER TIPO DE *EVENTO O CONJUNTO DE EVENTOS QUE PUEDE PONER EN RIESGO UN PROYECTO DE LA ORGANIZACIÓN O IMPEDIR EL CUMPLIMIENTO DE SUS OBJETIVOS*.

A PESAR DE EXISTIR VARIOS TIPOS DE RIESGO, LA **GESTIÓN DE RIESGOS** *ES UN CONJUNTO DE PROCESOS CON LA FINALIDAD DE DISMINUIR LA PROBABILIDAD DE AMENAZAS Y ATAQUES SOBRE LOS ACTIVOS* MÁS IMPORTANTES DE LA ORGANIZACIÓN.

EL PROCEDIMIENTO DE GESTIÓN DE RIESGOS SIGUE UNAS FASES BIEN MARCADAS.

EN PRIMER LUGAR, **SE IDENTIFICAN Y VALORAN LOS ACTIVOS** DE LA **ORGANIZACIÓN Y LA DEGRADACIÓN** QUE PUEDEN SUFRIR EN CASO DE MATERIALIZARSE UNA AMENAZA (**IMPACTO**).

UNA VEZ IDENTIFICADOS LOS ACTIVOS Y LOS IMPACTOS SE DEBEN **IDENTIFICAR Y ANALIZAR LAS VULNERABILIDADES** DE ESTOS CON EL FIN DE **ESTIMAR LA FRECUENCIA Y PROBABILIDAD** DE MATERIALIZACIÓN DE AMENAZAS Y CÓMO PODER REDUCIRLAS.

RESUMEN

CON EL IMPACTO Y LAS PROBABILIDADES ESTIMADAS, SE PUEDE PROCEDER A **CALCULAR EL RIESGO POTENCIAL DE CADA ACTIVO Y**, CONJUNTAMENTE, **EL RIESGO POTENCIAL** GLOBAL DE LA ORGANIZACIÓN.

ADEMÁS, **CON EL ANÁLISIS DE LAS SALVAGUARDAS SE PODRÁ CONOCER EL RIESGO RESIDUAL** Y EVALUAR SI ESTAS ESTÁN CUMPLIENDO CON SU COMETIDO O SI, POR EL CONTRARIO, NECESITAN TAREAS DE REVISIÓN.

EL ANÁLISIS Y GESTIÓN DE RIESGOS PERMITE A LAS ORGANIZACIONES DEFINIR ESTRATEGIAS PARA REDUCIR LA PROBABILIDAD DE OCURRENCIA DE AMENAZAS Y EL DAÑO QUE ESTAS PUEDEN CAUSAR EN CASO DE MATERIALIZARSE.

POR ELLO, NO SON POCOS LOS ORGANISMOS ENCARGADOS DE DISEÑAR HERRAMIENTAS Y METODOLOGÍAS QUE SIRVAN DE GUÍA A LAS ORGANIZACIONES PARA QUE ESTAS ELABOREN POLÍTICAS PROPIAS DE GESTIÓN DE RIESGOS; A DESTACAR LA METODOLOGÍA **MAGERIT** (DE CARÁCTER NACIONAL) Y LA METODOLOGÍA **NIST** SP 800-30 (DE CARÁCTER INTERNACIONAL).


ESTO ES
TODO