IFCT0109. SEGURIDAD INFORMÁTICA

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

ANEXO

GESTIÓN DE RIESGOS

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. INTRODUCCIÓN

LA GESTIÓN DE RIESGOS ESTÁ PRESENTE EN DISTINTOS ÁMBITOS DE LA SOCIEDAD Y LA EMPRESA.

SON ALGUNOS **EJEMPLOS** LA GESTIÓN DE RIESGOS:

- LABORALES
- ALIMENTARIOS
- BANCARIOS, FINANCIEROS
- CORPORATIVOS, DE PROYECTOS
- MEDIOAMBIENTALES
- DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

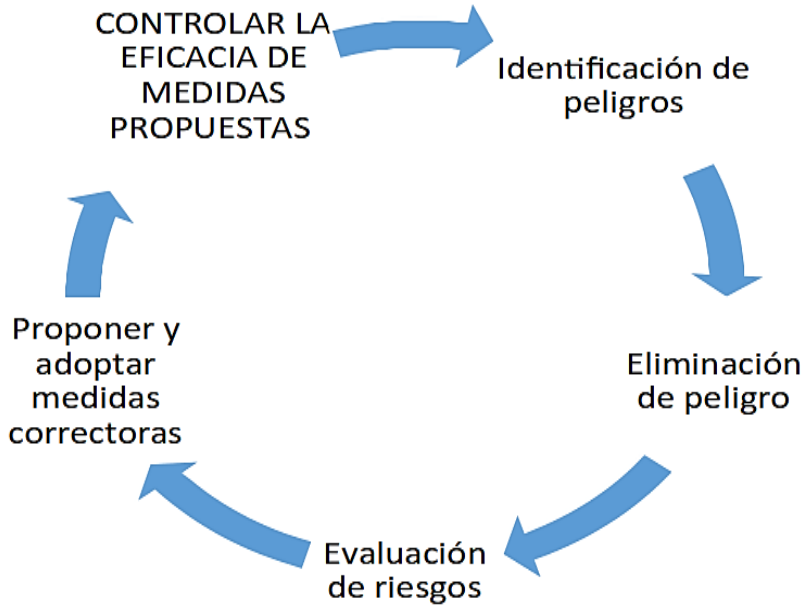
LOS RESPONSABLES SON **CONSCIENTES DE LA EXISTENCIA DE AMENAZAS** QUE SUPONEN UN PELIGRO PARA LA CONSECUCIÓN DE SUS OBJETIVOS.

DEDICAN **ESFUERZOS Y RECURSOS** A **MANTENER ESTOS RIESGOS POR DEBAJO DE UN LÍMITE CONSENSUADO** EN SUS ORGANIZACIONES.

1. INTRODUCCIÓN

PARA MAXIMIZAR LOS BENEFICIOS DE DICHA GESTIÓN Y CONTAR CON GARANTÍAS DE ÉXITO, **LOS ESFUERZOS HAN DE SER EMPLEADOS DE FORMA METÓDICA, ESTRUCTURADA Y**, SOBRE TODO, **SIGUIENDO UN PROCESO DE EVALUACIÓN Y MEJORA CONTINUA**.

LAS ORGANIZACIONES SE ENCUENTRAN EN UN **ENTORNO EN CAMBIO CONSTANTE**. LOS LOGROS OBTENIDOS ANTE LAS AMENAZAS DE HOY NO SUPONEN NINGUNA GARANTÍA DE ÉXITO PARA LAS AMENAZAS DE MAÑANA.



CONTENIDOS

1. INTRODUCCIÓN
2. **CONCEPTOS**
3. GESTIÓN DE RIESGOS
4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

2. CONCEPTOS

ACTIVO

CUALQUIER **RECURSO** DE LA EMPRESA **NECESARIO PARA DESEMPEÑAR LAS ACTIVIDADES** DIARIAS **Y CUYA NO DISPONIBILIDAD O DETERIORO SUPONE UN AGRAVIO O COSTE**.

LA NATURALEZA DE LOS ACTIVOS DEPENDERÁ DE LA EMPRESA, PERO SU PROTECCIÓN ES EL FIN ÚLTIMO DE LA GESTIÓN DE RIESGOS. LA VALORACIÓN DE LOS ACTIVOS ES IMPORTANTE PARA LA EVALUACIÓN DE LA MAGNITUD DEL RIESGO.

ESTE TÉRMINO EN LAS NUEVAS NORMAS SE GENERALIZA PARA DENOMINARSE **FUENTE DE RIESGO** SIENDO EL ELEMENTO QUE SÓLO O CON OTROS PUEDE ORIGINAR UN RIESGO.

2. CONCEPTOS

AMENAZA

CIRCUNSTANCIA DESFAVORABLE QUE PUEDE OCURRIR Y QUE **CUANDO SUCEDE TIENE CONSECUENCIAS NEGATIVAS SOBRE LOS ACTIVOS** PROVOCANDO SU INDISPONIBILIDAD, FUNCIONAMIENTO INCORRECTO O PÉRDIDA DE VALOR.

EN LA EVOLUCIÓN DE LAS NORMAS ESTE CONCEPTO SE AMPLÍA PARA DENOMINARSE **SUCESO**.

VULNERABILIDAD

DEBILIDAD QUE PRESENTAN LOS ACTIVOS Y QUE FACILITA LA MATERIALIZACIÓN DE LAS AMENAZAS.

2. CONCEPTOS

IMPACTO

CONSECUENCIA DE LA MATERIALI-ZACIÓN DE UNA AMENAZA SOBRE UN ACTIVO APROVECHANDO UNA VULNERABILIDAD. EL IMPACTO SE SUELE ESTIMAR EN PORCENTAJE DE DEGRADACIÓN QUE AFECTA AL VALOR DEL ACTIVO, EL 100% SERÍA LA PÉRDIDA TOTAL DEL ACTIVO.

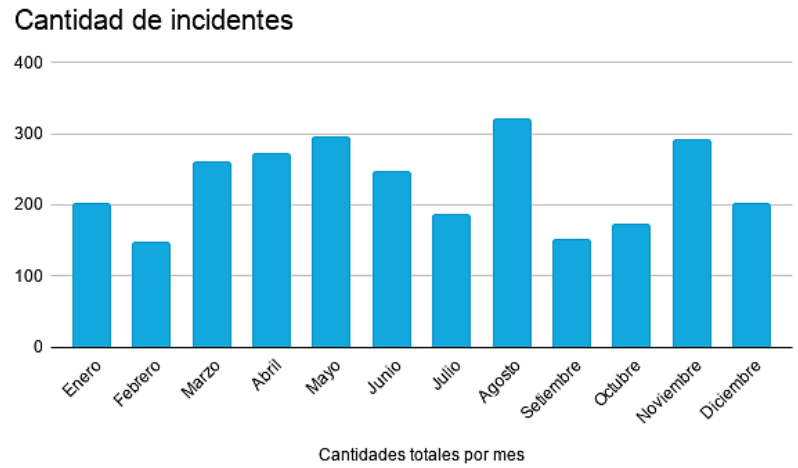
2. CONCEPTOS

PROBABILIDAD

ES LA **POSIBILIDAD DE OCURRENCIA DE UN HECHO**, SUCESO O ACONTECIMIENTO.

LA FRECUENCIA DE OCURRENCIA IMPLÍCITA SE CORRESPONDE CON LA AMENAZA.

PARA ESTIMAR LA FRECUENCIA PODEMOS BASARNOS EN DATOS EMPÍRICOS (DATOS OBJETIVOS) DEL HISTÓRICO DE LA EMPRESA, O EN OPINIONES DE EXPERTOS O DEL EMPRESARIO (DATOS SUBJETIVOS).



2. CONCEPTOS

EL SIGUIENTE DIAGRAMA MUESTRA LAS RELACIONES ENTRE ESTOS CONCEPTOS

2. CONCEPTOS

¿CÓMO SE MIDE EL NIVEL DE RIESGO?

EL **IMPACTO** NOS INDICA LAS CONSECUENCIAS DE LA MATERIALIZACIÓN DE UNA AMENAZA.

EL **NIVEL DE RIESGO** ES UNA ESTIMACIÓN DE LO QUE PUEDE OCURRIR Y SE VALORA, DE FORMA **CUANTITATIVA**, COMO EL PRODUCTO DEL IMPACTO, (CONSECUENCIA), ASOCIADO A UNA AMENAZA (SUCESO), POR LA PROBABILIDAD DE LA MISMA.

2. CONCEPTOS

¿CÓMO SE MIDE EL NIVEL DE RIESGO?

EL IMPACTO Y EL RIESGO **SE VALORAN EN TÉRMINOS DEL COSTE DERIVADO DEL VALOR DE LOS ACTIVOS AFECTADOS CONSIDERANDO, ADEMÁS DE LOS DAÑOS** PRODUCIDOS EN EL PROPIO ACTIVO:

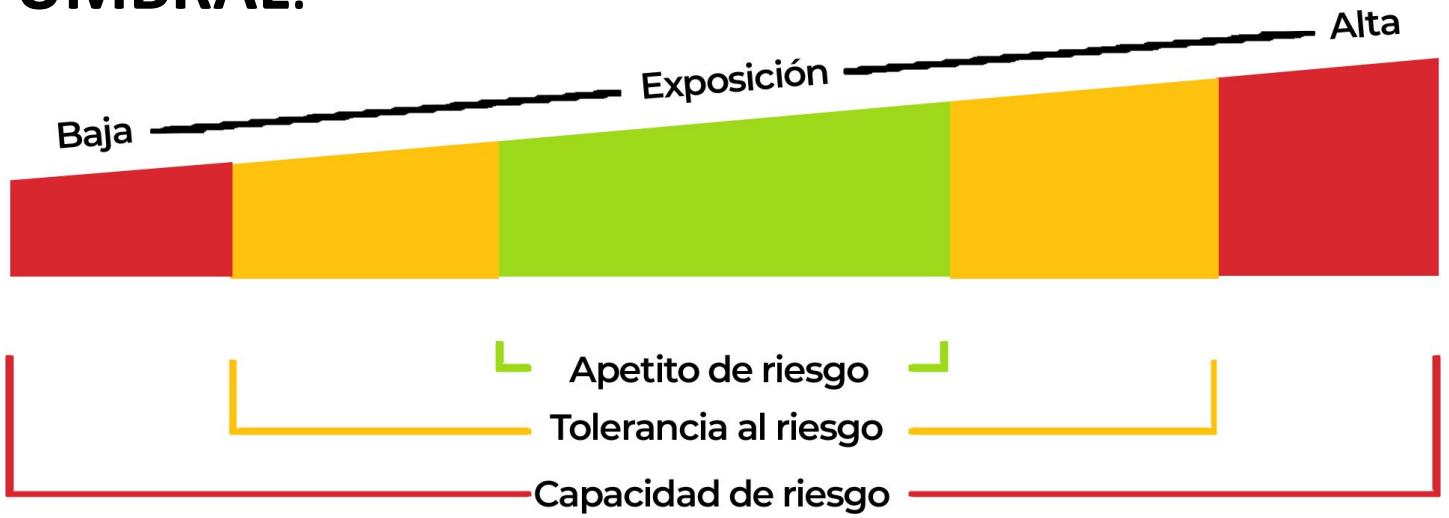
- DAÑOS PERSONALES
- PÉRDIDAS FINANCIERAS
- INTERRUPCIÓN DEL SERVICIO
- PÉRDIDA DE IMAGEN Y REPUTACIÓN
- DISMINUCIÓN DEL RENDIMIENTO

2. CONCEPTOS

¿CÓMO SE MIDE EL NIVEL DE RIESGO?

TRABAJAR CON MAGNITUDES ECONÓMICAS FACILITA A LAS ORGANIZACIONES ESTABLECER EL LLAMADO **UMBRAL DE RIESGO**, O **APETITO AL RIESGO**: *EL NIVEL MÁXIMO DE RIESGO QUE LA EMPRESA ESTÁ DISPUESTA A SOPORTAR*.

LA GESTIÓN DE RIESGOS DEBE MANTENER EL NIVEL DE RIESGO SIEMPRE POR DEBAJO DEL UMBRAL.

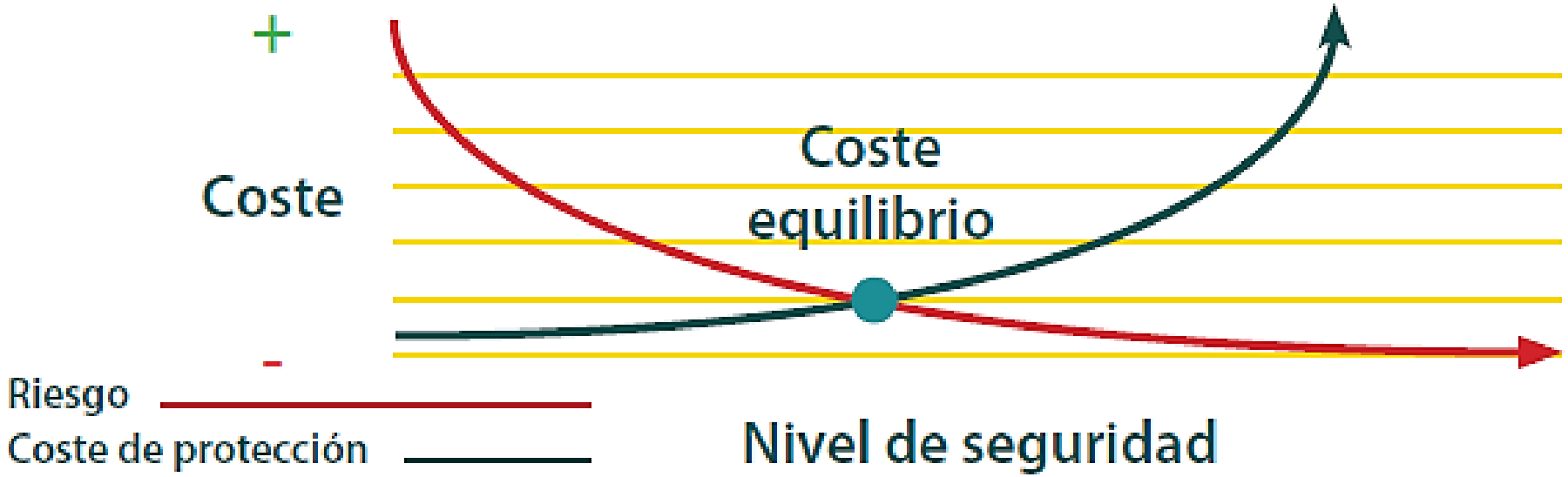


2. CONCEPTOS

¿CÓMO SE MIDE EL NIVEL DE RIESGO?

SE DENOMINA **COSTE DE PROTECCIÓN** AL COSTE QUE SUPONE PARA LAS ORGANIZACIONES LOS RECURSOS Y ESFUERZOS QUE DEDICAN PARA MANTENER EL NIVEL DE RIESGO POR DEBAJO DEL UMBRAL DESEADO.

EN LA SIGUIENTE GRÁFICA PODEMOS VER COMO AMBOS CONCEPTOS, RIESGO Y COSTE DE PROTECCIÓN, SE RELACIONAN.



EL PUNTO EN EL QUE EL COSTE DE PROTECCIÓN ES EL ADECUADO PARA MANTENER LOS RIESGOS POR DEBAJO DEL UMBRAL FIJADO DE RIESGO ES EL **COSTE DE EQUILIBRIO**

2. CONCEPTOS

¿QUÉ HACER CON LOS RIESGOS?

LAS ACTIVIDADES CUYO OBJETIVO ES MANTENER EL RIESGO POR DEBAJO DEL UMBRAL FIJADO SE ENGLOBAN EN LO QUE SE DENOMINA **GESTIÓN DEL RIESGO**.

LAS ORGANIZACIONES QUE DECIDAN GESTIONAR EL RIESGO PARA SU ACTIVIDAD DEBERÁN REALIZAR DOS GRANDES TAREAS:

- **ANÁLISIS DE RIESGO**
- **TRATAMIENTO DE LOS RIESGOS**

Gestión de riesgos = **Análisis de riesgos + Tratamiento de riesgos**

2. CONCEPTOS

¿QUÉ HACER CON LOS RIESGOS?

ANÁLISIS DE RIESGO

CONSISTE EN AVERIGUAR EL NIVEL DE RIESGO QUE LA EMPRESA ESTÁ SOPORTANDO.

PARA ELLO, TRADICIONALMENTE LAS METODOLOGÍAS PROPONEN QUE:

- SE REALICE UN INVENTARIO DE ACTIVOS
- SE DETERMINEN LAS AMENAZAS
- SE CALCULEN LAS PROBABILIDADES DE QUE OCURRAN Y LOS POSIBLES IMPACTOS

Gestión de riesgos = **Análisis de riesgos + Tratamiento de riesgos**

2. CONCEPTOS

¿QUÉ HACER CON LOS RIESGOS?

TRATAMIENTO DE LOS RIESGOS

PARA AQUELLOS RIESGOS CUYO NIVEL ESTÁ POR ENCIMA DEL UMBRAL DESEADO LA EMPRESA DEBE DECIDIR CUÁL ES EL MEJOR TRATAMIENTO QUE PERMITA DISMINUIRLOS.

ESTA DECISIÓN SIEMPRE HA DE PASAR UN FILTRO ECONÓMICO DONDE EL COSTE DEL TRATAMIENTO, O COSTE DE PROTECCIÓN, NO SUPERE EL COSTE DE RIESGO DISMINUIDO.

Gestión de riesgos = **Análisis de riesgos + Tratamiento de riesgos**

2. CONCEPTOS

¿QUÉ HACER CON LOS RIESGOS?

PARA EL TRATAMIENTO DE RIESGOS LAS EMPRESAS CUENTAN, ENTRE OTRAS, CON LAS SIGUIENTES **OPCIONES**:

- **EVITAR O ELIMINAR EL RIESGO**
- **REDUCIRLO O MITIGARLO**
- **TRANSFERIRLO, COMPARTIRLO O ASIGNARLO A TERCEROS**
- **ACEPTARLO**

2. CONCEPTOS

¿QUÉ HACER CON LOS RIESGOS?

EVITAR O ELIMINAR EL RIESGO

POR EJEMPLO, SUSTITUYENDO EL ACTIVO POR OTRO QUE NO SE VEA AFECTADO POR LA AMENAZA O ELIMINANDO LA ACTIVIDAD QUE LO PRODUCE.

REDUCIRLO O MITIGARLO

TOMANDO LAS MEDIDAS OPORTUNAS PARA QUE EL NIVEL DE RIESGO SE SITÚE POR DEBAJO DEL UMBRAL. PARA CONSEGUIRLO SE PUEDE:

- **REDUCIR LA PROBABILIDAD O FRECUENCIA DE OCURRENCIA**: TOMANDO, POR EJEMPLO, MEDIDAS PREVENTIVAS
- **REDUCIR EL IMPACTO DE LA AMENAZA O ACOTAR EL IMPACTO**, ESTABLECIENDO POR EJEMPLO CONTROLES Y REVISANDO EL FUNCIONAMIENTO DE LAS MEDIDAS PREVENTIVAS

2. CONCEPTOS

¿QUÉ HACER CON LOS RIESGOS?

TRANSFERIRLO, COMPARTIRLO O ASIGNARLO A TERCEROS

EN OCASIONES LA EMPRESA NO TIENE LA CAPACIDAD DE TRATAMIENTO Y PRECISA LA CONTRATACIÓN DE UN TERCERO CON CAPACIDAD PARA REDUCIR Y GESTIONAR EL RIESGO DEJÁNDOLO POR DEBAJO DEL UMBRAL.

ACEPTARLO

SE ASUME EL RIESGO, BIEN PORQUE ESTÁ DEBAJO DEL UMBRAL ACEPTABLE DE RIESGO BIEN EN SITUACIONES EN LAS QUE LOS COSTES DE SU TRATAMIENTO SON ELEVADOS Y AUN SIENDO RIESGOS DE IMPACTO ALTO SU PROBABILIDAD DE OCURRENCIA ES BAJA O PORQUE AUN A PESAR DEL RIESGO LA EMPRESA NO QUIERE DEJAR DE APROVECHAR LA OPORTUNIDAD QUE PARA SU NEGOCIO SUPONE ESA ACTIVIDAD ARRIESGADA.

2. CONCEPTOS

¿QUÉ HACER CON LOS RIESGOS?

EN LA ACTUALIDAD **EXISTEN DIVERSAS METODOLOGÍAS Y GUÍAS DE BUENAS PRÁCTICAS**, TANTO **GENERALISTAS** COMO **ESPECIALIZADAS**.

GENERALISTAS

- **COSO,** ORGANIZACIÓN AMERICANA DEDICADA A LA CREACIÓN DE GUÍAS Y MARCOS DE TRABAJO EN EL ÁMBITO DE LA GESTIÓN DE RIESGOS EMPRESARIALES.
- **ISO 31000,** NORMA GLOBAL, NO CERTIFICABLE, QUE APORTA METODOLOGÍA, PRINCIPIOS Y DIRECTRICES EN MATERIA DE GESTIÓN DE RIESGOS.

2. CONCEPTOS

¿QUÉ HACER CON LOS RIESGOS?

ESPECÍFICAS DE GESTIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN

- **MAGERIT**, METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN, CREADA POR EL MINISTERIO DE ADMINISTRACIONES PÚBLICAS ESPAÑOL.
- **ISO/IEC 27005,** NORMA QUE APORTA DIRECTRICES PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.
- **NIST SP - 800-30,** METODOLOGÍA CREADA EN ESTE CASO POR EL GOBIERNO NORTEAMERICANO.

CONTENIDOS

1. INTRODUCCIÓN
2. CONCEPTOS
3. **GESTIÓN DE RIESGOS**
4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

3. GESTIÓN DE RIESGOS

EN ESTE APARTADO SE DESCRIBE EL PROCESO Y LAS ACTIVIDADES NECESARIOS PARA LLEVAR A CABO LA GESTIÓN DE RIESGOS DE ACUERDO A LA NORMA **ISO 31000.** VEAMOS:

- **PRINCIPIOS**
- **MARCO DE TRABAJO**
- **ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS**

3. GESTIÓN DE RIESGOS

PRINCIPIOS

ESTOS SON LOS PRINCIPIOS BÁSICOS QUE DEBE CUMPLIR LA GESTIÓN DE RIESGOS SI QUEREMOS QUE CUMPLA SU COMETIDO:

- PROTEGER EL VALOR, ES DECIR, CONTRIBUIR A LA CONSECUCIÓN DE LOS OBJETIVOS Y LA MEJORA DEL DESEMPEÑO
- SER UNA PARTE INTEGRAL DE TODOS LOS PROCESOS DE LA EMPRESA
- FORMAR PARTE DE LA TOMA DE DECISIONES
- TRATAR EXPLÍCITAMENTE LA INCERTIDUMBRE
- SER SISTEMÁTICA, ESTRUCTURADA Y OPORTUNA
- BASARSE EN LA MEJOR INFORMACIÓN DISPONIBLE
- ADAPTARSE, ALINEÁNDOSE CON EL CONTEXTO INTERNO Y EXTERNO Y CON LOS PERFILES DEL RIESGO

3. GESTIÓN DE RIESGOS

PRINCIPIOS

- INTEGRAR FACTORES HUMANOS Y CULTURALES
- SER TRASPARENTE Y PARTICIPATIVA
- SER DINÁMICA, ITERATIVA Y RESPONDE A LOS CAMBIOS
- FACILITAR LA MEJORA CONTINUA

3. GESTIÓN DE RIESGOS

MARCO DE TRABAJO

LA GESTIÓN DE RIESGOS HA DE ESTAR PLENAMENTE INTEGRADA EN LOS PROCESOS DE LA EMPRESA Y REQUIERE UN COMPROMISO FUERTE Y SOSTENIDO DE LA DIRECCIÓN, ASÍ COMO DEL ESTABLECIMIENTO DE UNA RIGUROSA PLANIFICACIÓN ESTRATÉGICA, **UN MARCO DE TRABAJO**.

ESTE **HA DE SER OBJETO DE SEGUIMIENTO Y REVISIÓN PERIÓDICA** QUE PERMITAN **MEDIR EL PROGRESO Y ADAPTARSE A LOS CAMBIOS** DEL ENTORNO, **TOMANDO LAS DECISIONES** OPORTUNAS **PARA LA MEJORA CONTINUA**.

3. GESTIÓN DE RIESGOS

MARCO DE TRABAJO

PARA CONSEGUIR UNA BUENA GESTIÓN DEL RIESGO EL MARCO DE TRABAJO DEFINIDO HA DE:

- COMPRENDER LA EMPRESA Y SU CONTEXTO
- ESTABLECER UNA POLÍTICA DE GESTIÓN DE RIESGOS
- IDENTIFICAR AUTORIDADES Y COMPETENCIAS
- DEFINIR LA INTEGRACIÓN EN LOS PROCESOS DE NEGOCIO COMO PLAN ESTRATÉGICO PARA QUE SEA RELEVANTE, EFICAZ Y EFICIENTE
- PROPORCIONAR LOS RECURSOS NECESARIOS:
- PERSONAS, FORMACIÓN
  - PROCESOS Y PROCEDIMIENTOS
  - MÉTODOS Y HERRAMIENTAS
- ESTABLECER MECANISMOS DE COMUNICACIÓN INTERNA Y EXTERNA

3. GESTIÓN DE RIESGOS

MARCO DE TRABAJO

ESTE MARCO DE TRABAJO SE IMPLEMENTARÁ DEFINIENDO UN CALENDARIO Y ESTRATEGIA DE IMPLEMENTACIÓN Y REVISIÓN QUE PERMITA:

- ESTABLECER Y DESARROLLAR LOS OBJETIVOS
- APLICAR LA POLÍTICA Y EL PROCESO
- CUMPLIR CON LA LEGISLACIÓN Y NORMATIVA
- ORGANIZAR LA FORMACIÓN Y LA COMUNICACIÓN Y CONSULTA A LOS INTERESADOS

3. GESTIÓN DE RIESGOS

MARCO DE TRABAJO

POLÍTICA DE GESTIÓN DE RIESGOS

VA A SER CLAVE PARA UNA GESTIÓN DE RIESGOS EFICAZ. LA POLÍTICA TRATARÁ ESTAS CUESTIONES:

- MOTIVOS PARA LLEVAR A CABO LA GESTIÓN DE RIESGOS
- RELACIÓN CON OTRAS POLÍTICAS DE LA EMPRESA
- RESPONSABILIDADES Y RENDICIÓN DE CUENTAS EN EL PROCESO DE GESTIÓN DE RIESGOS
- RECURSOS DISPONIBLES
- MEDICIÓN DEL DESEMPEÑO
- COMPROMISO DE REVISIÓN DEL MARCO DE TRABAJO Y DE LA POLÍTICA

3. GESTIÓN DE RIESGOS

ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS

EN EL PROCESO DE GESTIÓN DE RIESGOS SE DISTINGUEN LAS SIGUIENTES ACTIVIDADES:

3. GESTIÓN DE RIESGOS

ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS

COMUNICACIÓN Y CONSULTA

ESTA ACTIVIDAD ES LA PRIMERA Y ABARCA TODAS LAS SIGUIENTES PUES SE HA DE REALIZAR EN TODAS LAS ETAPAS.

EN ELLA **SE FOMENTA LA PARTICIPACIÓN Y SE COORDINAN LAS ACTUACIONES DE TODAS LAS PARTES IMPLICADAS**, TANTO INTERNAS COMO EXTERNAS, EN LA GESTIÓN DE RIESGOS.

3. GESTIÓN DE RIESGOS

ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS

DETERMINAR EL CONTEXTO

ES ESENCIAL QUE LA GESTIÓN DE RIESGOS SE INTEGRE TANTO CON EL RESTO DE LAS ÁREAS DE LA EMPRESA COMO CON SU ENTORNO EXTERNO.

HAY QUE **DETERMINAR LOS CONDICIONANTES TANTO INTERNOS COMO EXTERNOS QUE DEFINEN EL MARCO DE TRABAJO**.

A **NIVEL INTERNO** SE TENDRÁN EN CUENTA: *LA CULTURA, RECURSOS, PROCESOS Y OBJETIVOS DEL NEGOCIO*.

A *NIVEL EXTERNO* SE CONSIDERAN DIFERENTES ASPECTOS RELATIVOS AL *ENTORNO SOCIAL, ECONÓMICO O LEGISLATIVO*.

3. GESTIÓN DE RIESGOS

ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS

DETERMINAR EL CONTEXTO

COMO RESULTADO DE ESTA FASE SE ESTABLECEN:

- LOS OBJETIVOS DE LA GESTIÓN DE RIESGO
- LOS CRITERIOS QUE SE EMPLEARÁN PARA LA EVALUACIÓN DE LOS RIESGOS, EL MÉTODO A UTILIZAR EN EL ESTABLECIMIENTO DE PROBABILIDADES, ASÍ COMO LAS MAGNITUDES DE LOS IMPACTOS
- EL ALCANCE DE LA GESTIÓN DE RIESGOS, LOS ROLES Y LA ASIGNACIÓN DE RESPONSABILIDADES

3. GESTIÓN DE RIESGOS

ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS

VALORACIÓN O APRECIACIÓN DE RIESGOS

UNA VEZ DEFINIDO EL CONTEXTO **SE HAN DE VALORAR LOS RIESGOS**.

EN ESTA ETAPA **SE DETERMINAN LOS RIESGOS QUE VAN A SER CONTROLADOS** POR MEDIO DE SU IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN.

TODOS AQUELLOS RIESGOS QUE NO SEAN IDENTIFICADOS QUEDARÁN COMO **RIESGOS OCULTOS O NO CONTROLADOS**.

3. GESTIÓN DE RIESGOS

ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS

VALORACIÓN O APRECIACIÓN DE RIESGOS

SE REALIZAN EN ESTA FASE LAS SIGUIENTES **ACTIVIDADES**:

- **IDENTIFICACIÓN DEL RIESGO**, CUYO OBJETIVO ES BÚSQUEDA, RECONOCIMIENTO Y DESCRIPCIÓN DE TODOS LOS POSIBLES PUNTOS DE PELIGRO TANTO INTERNOS COMO EXTERNOS.PARA CADA UNO DE ELLOS SE DETERMINARÁ SU IMPACTO Y PROBABILIDAD

  ESTA FASE RESPONDE A LAS SIGUIENTES PREGUNTAS:

  - ¿QUÉ PUEDE PASAR?
  - ¿CUÁNDO Y DÓNDE?
  - ¿CÓMO Y POR QUÉ?

3. GESTIÓN DE RIESGOS

ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS

VALORACIÓN O APRECIACIÓN DE RIESGOS

SE REALIZAN EN ESTA FASE LAS SIGUIENTES **ACTIVIDADES**:

- **ANÁLISIS DE RIESGOS**, ES LA ETAPA EN LA CUAL **SE CALIFICAN CADA LOS RIESGOS** IDENTIFICADOS TANTO DE FORMA CUANTITATIVA COMO CUALITATIVA PARA PRIORIZAR NUESTROS ESFUERZOS. TAMBIÉN SE PERSIGUE COMPRENDER CÓMO SE DESARROLLAN LOS RIESGOS, ESTUDIANDO SUS CAUSAS Y CONSECUENCIAS, ASÍ COMO EVALUANDO LA EFICACIA DE LOS DIFERENTES MEDIOS DE CONTROL IMPLANTADOS EN LA EMPRESA.

  SE MIDE EL NIVEL DE RIESGO SEGÚN LA FÓRMULA:

  RIESGO = IMPACTO X PROBABILIDAD

3. GESTIÓN DE RIESGOS

ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS

VALORACIÓN O APRECIACIÓN DE RIESGOS

SE REALIZAN EN ESTA FASE LAS SIGUIENTES **ACTIVIDADES**:

- **EVALUACIÓN DEL RIESGO**, CUYO OBJETIVO ES **DETERMINAR PRIORIDADES EN EL USO DE LOS RECURSOS** A EMPLEAR EN LA GESTIÓN DE RIESGOS.

  EN ESTA FASE SE AMPLÍA LA CALIFICACIÓN DEL ANÁLISIS ANTERIOR INCLUYENDO VALORACIONES EN TÉRMINOS DE ESTRATEGIA DE NEGOCIO QUE PERMITAN ESTABLECER QUÉ RIESGOS SON ACEPTABLES Y CUÁLES NO.

3. GESTIÓN DE RIESGOS

ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS

TRATAMIENTO DEL RIESGO

A CONTINUACIÓN, **SE IDENTIFICAN Y EVALÚAN LAS OPCIONES EXISTENTES DE TRATAMIENTO DE CADA UNO DE LOS RIESGOS** QUE SEA NECESARIO TRATAR SEGÚN SE DETERMINÓ EN LA FASE ANTERIOR.

ALGUNAS DE LAS **OPCIONES DE TRATAMIENTO** SON: **EVITARLO, REDUCIRLO O MITIGARLO, TRANSFERIRLO O COMPARTIRLO Y ACEPTARLO**.

3. GESTIÓN DE RIESGOS

ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS

SEGUIMIENTO Y REVISIÓN

PARA CONSEGUIR UNA MEJORA CONTINUA **SE SUPERVISA LO QUE ESTÁ OCURRIENDO EN LA PRÁCTICA** Y **SE REALIZAN LAS CORRECCIONES** QUE FUERA PRECISO.

TAMBIÉN SE HA DE EVALUAR EL PROPIO SISTEMA DE GESTIÓN, DETECTANDO POSIBLES DEFICIENCIAS Y OPORTUNIDADES DE MEJORA.

LA REVISIÓN DE LOS CAMBIOS DEL ENTORNO ESTÁ INCLUIDA EN ESTA ETAPA, REALIMENTANDO LA FASE DE DETERMINACIÓN DEL CONTEXTO.

CONTENIDOS

1. INTRODUCCIÓN
2. CONCEPTOS
3. **GESTIÓN DE RIESGOS**
4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

LAS COMPAÑÍAS SON CONSCIENTES DEL PROTAGONISMO DE LA INFORMACIÓN EN SUS PROCESOS PRODUCTIVOS.

HA CAMBIADO TAMBIÉN LAS CON CLIENTES, PROVEEDORES, ORGANISMOS OFICIALES, DONDE INTERNET JUEGA UN IMPORTANTE PAPEL COMO MEDIO DE COMUNICACIÓN.

LAS EMPRESAS DEBEN PREOCUPARSE Y ASIGNAR RECURSOS PARA LA GESTIÓN DE LOS RIESGOS ASOCIADOS A SU INFORMACIÓN Y A LAS INFRAESTRUCTURAS QUE LA SOPORTAN.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL ACTIVO A PROTEGER ES LA **INFORMACIÓN**.

HABLAMOS TANTO DE INFORMACIÓN DIGITAL **CONTENIDA EN NUESTROS SISTEMAS DE INFORMACIÓN** COMO AQUELLA **CONTENIDA EN CUALQUIER OTRO SOPORTE** COMO POR EJEMPLO EL PAPEL.

LA GESTIÓN DEBE **OCUPARSE DE TODO EL CICLO DE VIDA DE LA INFORMACIÓN** Y NO SÓLO DE SU EXPLOTACIÓN, CONSIDERANDO ETAPAS COMO LA DE CAPTURA O DESTRUCCIÓN DE LA INFORMACIÓN.

LA **INFORMACIÓN** ES EL **ACTIVO PRINCIPAL** PERO **TAMBIÉN DEBEMOS CONSIDERAR**:

INFRAESTRUCTURA INFORMÁTICA, EQUIPOS AUXILIARES, REDES DE COMUNICACIONES, INSTALACIONES Y PERSONAS.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

CUANDO HABLAMOS DE SEGURIDAD DE LA INFORMACIÓN HABLAMOS DE PROTEGERLA DE RIESGOS EN SUS PRINCIPALES PROPIEDADES:

- **CONFIDENCIALIDAD** LA INFORMACIÓN SOLO TIENE QUE SER ACCESIBLE O DIVULGADA A AQUELLOS QUE ESTÁN AUTORIZADOS.
- **INTEGRIDAD** LA INFORMACIÓN DEBE PERMANECER CORRECTA (INTEGRIDAD DE DATOS) Y COMO EL EMISOR LA ORIGINÓ (INTEGRIDAD DE FUENTE) SIN MANIPULACIONES POR TERCEROS.
- **DISPONIBILIDAD** LA INFORMACIÓN DEBE ESTAR SIEMPRE ACCESIBLE PARA AQUELLOS QUE ESTÉN AUTORIZADOS.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

LAS **AMENAZAS** A LAS QUE SE ENFRENTA LA INFORMACIÓN DE NUESTRAS ORGANIZACIONES PUEDEN SER MUY VARIADAS, A MODO DE EJEMPLO:

- **DE ORIGEN NATURAL**: INUNDACIONES, TERREMOTOS, INCENDIOS, RAYOS
- **FALLOS DE LA INFRAESTRUCTURA AUXILIAR**: FALLOS DE SUMINISTRO ELÉCTRICO, REFRIGERACIÓN, CONTAMINACIÓN...
- **FALLOS DE LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIONES**: FALLOS EN LAS APLICACIONES, HARDWARE O EQUIPOS DE TRANSMISIONES
- **ERROR HUMANO**: ERRORES ACCIDENTALES O DELIBERADOS DE LAS PERSONAS QUE INTERACTÚAN CON LA INFORMACIÓN, POR EJEMPLO:
  - ACCIONES NO AUTORIZADAS COMO USO DE SOFTWARE O HARDWARE NO AUTORIZADOS
  - FUNCIONAMIENTO INCORRECTO POR ABUSO O ROBO DE DERECHOS DE ACCESO O ERRORES EN EL USO, FALTA DE DISPONIBILIDAD, ETC.
  - INFORMACIÓN COMPROMETIDA POR ROBO DE EQUIPOS, DESVELADO DE SECRETOS, ESPIONAJE, ETC.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

LAS **VULNERABILIDADES** DEPENDEN DE LA NATURALEZA DE LOS MISMOS.. ALGUNOS **EJEMPLOS** SON:

- EQUIPAMIENTO INFORMÁTICO SUSCEPTIBLE A VARIACIONES DE TEMPERATURA O HUMEDAD
- SISTEMAS OPERATIVOS QUE POR SU ESTRUCTURA, CONFIGURACIÓN O MANTENIMIENTO SON MÁS VULNERABLES A ALGUNOS ATAQUES
- LOCALIZACIONES QUE SON MÁS PROPENSAS A DESASTRES NATURALES COMO POR EJEMPLO INUNDACIONES O QUE ESTÁN EN LUGARES CON VARIACIONES DE SUMINISTRO ELÉCTRICO
- APLICACIONES INFORMÁTICAS, QUE, POR SU DISEÑO, SON MÁS INSEGURAS QUE OTRAS
- PERSONAL SIN LA FORMACIÓN ADECUADA, AUSENTE O SIN SUPERVISIÓN

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN ES UN PROCESO QUE CONSISTE EN:

- **COMUNICACIÓN**
- **ESTABLECIMIENTO DEL CONTEXTO**
- **VALORACIÓN DEL RIESGO**
- **TRATAMIENTO DEL RIESGO Y ACEPTACIÓN DEL RIESGO**
- **REVISIÓN Y MONITORIZACIÓN**

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

COMUNICACIÓN

LAS ACCIONES DE COMUNICACIÓN SE SUCEDERÁN PARA MANTENER INFORMADA A LA DIRECCIÓN Y A LA PLANTILLA. IGUALMENTE SE RECIBIRÁ INFORMACIÓN DE LOS PROCESOS Y LOS INTERESADOS. ESTAS ACCIONES DE COMUNICACIÓN SON IMPORTANTES PARA:

- IDENTIFICAR LOS RIESGOS
- VALORARLOS EN FUNCIÓN DE LAS CONSECUENCIAS PARA EL NEGOCIO Y LA PROBABILIDAD DE
- QUE OCURRAN
- COMPRENDER LA PROBABILIDAD Y CONSECUENCIAS DE LOS RIESGOS
- ESTABLECER PRIORIDADES PARA EL TRATAMIENTO DE RIESGOS
- INFORMAR Y CONTRIBUIR A QUE SE INVOLUCREN LAS ÁREAS INTERESADAS
- MONITORIZAR LA EFECTIVIDAD DEL TRATAMIENTO DE LOS RIESGOS
- REVISAR CON REGULARIDAD EL PROCESO Y SU MONITORIZACIÓN
- CONCIENCIAR A LA PLANTILLA Y A LA DIRECCIÓN SOBRE ESTOS RIESGOS Y SU FORMA DE MITIGARLOS

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

ESTABLECIENDO EL CONTEXTO DE SEGURIDAD DE LA INFORMACIÓN

EN FUNCIÓN DEL CONTEXTO, **SE DEFINEN LOS CRITERIOS BÁSICOS** PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

ADEMÁS, SIRVE PARA **SER CONSCIENTES DE LAS LEYES** QUE SE DEBEN CUMPLIR, ASÍ COMO REQUISITOS DE **CONTRATOS** CON TERCEROS **Y NORMATIVA APLICABLE.**

LAS DISTINTAS ÁREAS IMPLICADAS HARÁN VALER SUS EXPECTATIVAS, LOS RECURSOS DISPONIBLES Y CÓMO VALORAN LAS POSIBLES CONSECUENCIAS DE LOS RIESGOS.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

ESTABLECIENDO EL CONTEXTO DE SEGURIDAD DE LA INFORMACIÓN

ASÍ QUEDARÁN DEFINIDOS LOS CRITERIOS PARA:

- **EVALUACIÓN DE RIESGOS**:
  - CUÁLES SON LOS ACTIVOS DE INFORMACIÓN CRÍTICOS.
  - LA IMPORTANCIA DE LOS MISMOS EN CUANTO A DISPONIBILIDAD, INTEGRIDAD Y CONFIDENCIALIDAD.
  - EL VALOR ESTRATÉGICO DE LOS PROCESOS DE INFORMACIÓN DEL NEGOCIO.
- **NIVELES DE CLASIFICACIÓN DE LOS IMPACTOS**
- **ESCALAS DE ACEPTACIÓN DE RIESGOS**

POR ÚLTIMO, SE DEFINE **EL ÁMBITO** Y LOS LÍMITES DE ESTA GESTIÓN, ES DECIR A QUÉ PARTE DE LA ORGANIZACIÓN AFECTA, QUE PROCESOS, QUE OFICINAS O QUE PARTE DE LA ESTRUCTURA.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

VALORANDO LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

ESTA ES LA FASE CENTRAL DE LA GESTIÓN DE RIESGOS. CONSTA A SU VEZ DE:

- **IDENTIFICACIÓN**
- **ANÁLISIS**
- **EVALUACIÓN**

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

IDENTIFICANDO LOS RIESGOS

PARA LA EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN PRIMER LUGAR SE HAN DE IDENTIFICAR LOS ACTIVOS DE INFORMACIÓN. EN GENERAL ESTOS PUEDEN SER DE DOS TIPOS:

- **PRIMARIOS**
- **DE SOPORTE**

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

IDENTIFICANDO LOS RIESGOS

- **PRIMARIOS**
  - **INFORMACIÓN**: ESTRATÉGICA, DE CARÁCTER PERSONAL O QUE ESTÉ SUJETA A LEGISLACIÓN QUE LA PROTEJA, ESENCIAL PARA EL DESARROLLO DEL NEGOCIO, DE DIFÍCIL O MUY COSTOSA REPOSICIÓN, ETC
  - **ACTIVIDADES Y PROCESOS DE NEGOCIO**: QUE TIENEN QUE VER CON PROPIEDAD INTELECTUAL, LOS QUE SI SE DEGRADAN HACEN IMPOSIBLE LA EJECUCIÓN DE LAS TAREAS DE LA EMPRESA, LOS NECESARIOS PARA EL CUMPLIMIENTO LEGAL O CONTRACTUAL, ETC
- **DE SOPORTE**
  - **HARDWARE**: PC, PORTÁTILES, SERVIDORES, IMPRESORAS, DISCOS, DOCUMENTOS EN PAPEL
  - **SOFTWARE**: SISTEMAS OPERATIVOS, PAQUETES, APLICACIONES,...
  - **REDES**: CONMUTADORES, CABLEADO, PUNTOS DE ACCESO,...
  - **PERSONAL**: USUARIOS, DESARROLLADORES, RESPONSABLES,...
  - **EDIFICIOS**, SALAS, Y SUS SERVICIOS
  - **ESTRUCTURA ORGANIZATIVA**: RESPONSABLES, ÁREAS, CONTRATISTAS,...

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

IDENTIFICANDO LOS RIESGOS

DESPUÉS DE TENER UNA RELACIÓN CON TODOS LOS ACTIVOS SE HAN DE CONOCER LAS AMENAZAS QUE PUEDEN CAUSAR DAÑOS EN LA INFORMACIÓN, LOS PROCESOS Y LOS SOPORTES.

LA IDENTIFICACIÓN DE LAS AMENAZAS Y LA VALORACIÓN DE LOS DAÑOS QUE PUEDEN PRODUCIR SE PUEDE OBTENER PREGUNTANDO A LOS PROPIETARIOS DE LOS ACTIVOS, USUARIOS, EXPERTOS, ETC.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

IDENTIFICANDO LOS RIESGOS

PARA VALORAR LOS DAÑOS ESTAS SON ALGUNAS DE LAS PREGUNTAS:

- ¿QUÉ VALOR TIENE ESTE ACTIVO PARA LA EMPRESA?
- ¿CUÁNTO CUESTA SU MANTENIMIENTO?
- ¿CÓMO REPERCUTE EN LOS BENEFICIOS DE LA EMPRESA?
- ¿CUÁNTO VALDRÍA PARA LA COMPETENCIA?
- ¿CUÁNTO COSTARÍA RECUPERARLO O VOLVERLO A GENERAR?
- ¿CUÁNTO COSTÓ ADQUIRIRLO O SU DESARROLLO?
- ¿A QUÉ RESPONSABILIDADES LEGALES O CONTRACTUALES NOS ENFRENTAMOS SI SE VE COMPROMETIDO?

SI YA SE HAYAN TOMADO CONTRAMEDIDAS PARA ESTAS AMENAZAS ES IMPORTANTE TENERLAS EN CUENTA PARA NO DUPLICAR ESFUERZOS.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

IDENTIFICANDO LOS RIESGOS

AL LLEGAR AQUÍ TENDREMOS, UN LISTADO DE ACTIVOS, SUS AMENAZAS Y LAS MEDIDAS QUE YA SE HAN TOMADO.

A CONTINUACIÓN, REVISAREMOS LAS VULNERABILIDADES QUE PUEDEN APROVECHAR LAS AMENAZAS Y CAUSAR DAÑOS A NUESTROS ACTIVOS DE INFORMACIÓN.

- EXISTEN DISTINTOS MÉTODOS PARA ANALIZAR AMENAZAS :
- ENTREVISTAS CON USUARIOS Y CUESTIONARIOS
- INSPECCIÓN FÍSICA
- USO DE HERRAMIENTAS PARA EL ESCANEO AUTOMATIZADO

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

IDENTIFICANDO LOS RIESGOS

PARA CADA UNA DE LAS AMENAZAS ANALIZAREMOS LAS **VULNERABILIDADES** QUE PUEDE EXPLOTAR.

FINALMENTE SE HAN DE CONCRETAR LAS **CONSECUENCIAS**, ES DECIR, CÓMO ESTAS AMENAZAS Y VULNERABILIDADES AFECTAN A LA DISPONIBILIDAD, INTEGRIDAD Y CONFIDENCIALIDAD DE LOS ACTIVOS DE INFORMACIÓN.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

ESTIMANDO LOS RIESGOS

LOS CRITERIOS PARA ESTIMAR LOS RIESGOS ESTABLECIDOS EN LA FASE DE ESTABLECIMIENTO DEL CONTEXTO SON LOS QUE SERVIRÁN PARA MEDIR EL IMPACTO EN LOS ACTIVOS. ESTOS CRITERIOS SE CONCRETAN EN ESCALAS PARA VALORAR:

- PÉRDIDAS FINANCIERAS
- COSTES DE REPARACIÓN O SUSTITUCIÓN
- INTERRUPCIÓN DEL SERVICIO
- PÉRDIDA DE REPUTACIÓN Y CONFIANZA DE LOS CLIENTES
- DISMINUCIÓN DEL RENDIMIENTO
- INFRACCIONES LEGALES O RUPTURA DE CONDICIONES CONTRACTUALES
- PÉRDIDA DE VENTAJA COMPETITIVA
- DAÑOS PERSONALES

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

ESTIMANDO LOS RIESGOS

EJEMPLO:

Rango impacto / Descripción		Descripción	Pérdidas financieras	Pérdida del activo(s)	Reputación e imagen	Disminución de rendimiento
5	Catastrófico	> 6 % del presupuesto	Total	Mayor que un mes	Alta y muy extendida	> 50 % de variación en los indicadores
4	Desastroso	6% del Presupuesto	Muy gran impacto	De una semana a un mes	Media y muy extendida	25-50 % variación en los indicadores
3	Serio	2% del presupuesto	Gran impacto	De un día a una semana	Media y poco extendida	10-25% variación en los indicadores
2	Menor	1% del presupuesto	Impacto menor	½ día o 1 día	Baja y muy extendida	5-10 % variación enl os indicadores
1	Insignificante	< 0,5 % del presupuesto	Casi sin impacto	Menor de ½ día	Baja y poco extendida	Hasta 5% variación en los indicadores

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

ESTIMANDO LOS RIESGOS

LOS MÉTODOS PARA REALIZARLA INCLUYEN **ESTIMACIONES CUALITATIVAS Y CUANTITATIVAS** O UNA COMBINACIÓN DE AMBAS.

EN LA **ESTIMACIÓN CUALITATIVA** SE CALIFICAN LAS POTENCIALES CONSECUENCIAS Y LA PROBABILIDAD **SEGÚN NIVELES** (ALTO, MEDIO, BAJO) SUBJETIVOS.

EN LA **CUANTITATIVA** SE UTILIZA UNA ESCALA CON **VALORES NUMÉRICOS**, APOYÁNDOSE EN DATOS DE DISTINTAS FUENTES POR EJEMPLO INCIDENTES DEL PASADO, EXPERIENCIA PREVIA, ESTUDIOS, ETC.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

ESTIMANDO LOS RIESGOS

ADEMÁS DE MEDIR LAS POSIBLES CONSECUENCIAS SE HA DE **ESTIMAR LA PROBABILIDAD** DE QUE OCURRAN LOS INCIDENTES.

TAMBIÉN EN ESTE CASO SE UTILIZAN TÉCNICAS CUALITATIVAS Y CUANTITATIVAS QUE CONSIDERAN:

- ESTADÍSTICAS DE LOS INCIDENTES EN EL PASADO, DE ESTUDIOS O DEL SECTOR
- FACTORES GEOGRÁFICOS O ESTACIONALES (TEMPERATURA, INUNDACIONES, ...)
- MOTIVACIONES DE LOS POSIBLES ATACANTES (ATRACTIVO DE LOS DATOS QUE SE MANEJAN, CLIMA LABORAL, ...)
- VULNERABILIDADES EXISTENTES
- MEDIDAS QUE YA SE HAN TOMADO Y SU RESULTADO

COMO RESULTADO TENDREMOS LA VALORACIÓN DE LAS CONSECUENCIAS Y SU PROBABILIDAD, CON LAS QUE PODREMOS **ESTIMAR EL NIVEL DEL RIESGO**

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

EVALUANDO LOS RIESGOS

UNA VEZ SE HAN VALORADO LAS CONSECUENCIAS O IMPACTOS Y LA PROBABILIDAD DE LOS INCIDENTES PARA LOS ACTIVOS DEL ÁMBITO ELEGIDO, **SE HA DE REALIZAR EL PRODUCTO DE AMBOS PARA CALCULAR LOS RIESGOS**.

LOS RESULTADOS OBTENIDOS SE COMPARARÁN CON LOS CRITERIOS DE ACEPTACIÓN DE RIESGO.

LA SIGUIENTE TABLA MUESTRA UN EJEMPLO DE UN MAPA DE CALOR CON EL QUE COMPARAR LAS VALORACIONES REALIZADAS.

SITUAREMOS CADA RIESGO EN LA TABLA, ANTES Y DESPUÉS DE CONSIDERAR COMO HAN AFECTADO LAS MEDIDAS QUE YA SE HABÍAN PUESTO EN MARCHA.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

EVALUANDO LOS RIESGOS

ESTE TIPO DE TABLAS TAMBIÉN SERVIRÁ PARA ESTIMAR QUÉ TRATAMIENTO DAR A CADA RIESGO. POR EJEMPLO, LOS RIESGOS EN LA ZONA ROJA SERÍAN INACEPTABLES PERO LOS DE LA ZONA BLANCA PODEMOS ELEGIR SOPORTARLOS.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

TRATANDO Y ACEPTANDO RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

DE LA ETAPA ANTERIOR **TENDREMOS UNA LISTA ORDENADA DE RIESGOS O UNA TABLA**. AHORA DEBEMOS **ELEGIR QUÉ HACER** CON CADA UNO DE ELLOS **EN VIRTUD DE SU VALORACIÓN Y DE LOS CRITERIOS ESTABLECIDOS**.

ES DECIR, TENDREMOS QUE SITUAR LA ***LÍNEA ROJA*** DE NUESTRO UMBRAL O NIVEL DE TOLERANCIA AL RIESGO.

EN ESTA FASE **SE SELECCIONARÁ LA OPCIÓN DE TRATAMIENTO** ADECUADA (EVITAR, REDUCIR O MITIGAR, TRANSFERIR O ACEPTAR) **PARA CADA RIESGO** DE LA LISTA.

SON PREFERIBLES LAS OPCIONES QUE APORTEN UNA **REDUCCIÓN CONSIDERABLE DEL RIESGO DE LA FORMA MÁS ECONÓMICA**.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

TRATANDO Y ACEPTANDO RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

EL NIVEL DE TOLERANCIA DE RIESGO SE ESTABLECE EN BASE A **CRITERIOS DE COSTE-BENEFICIO.**

VEMOS UN EJEMPLO:

Coste-Beneficio	Tratamiento
El coste del tratamiento es muy superior a los beneficios.	**Evitar el riesgo**, por ejemplo, dejando de realizar esa actividad.
El coste del tratamiento es adecuado a los beneficios.	**Reducir o mitigar el riesgo**: seleccionando e implementando los controles o medidas adecuadas que hagan que se reduzca la probabilidad o el impacto.
El coste del tratamiento por terceros es más beneficioso que el tratamiento directo.	**Transferir el riesgo, por ejemplo**, contratando un seguro o subcontratando el servicio.
El nivel de riesgo está muy alejado del nivel de tolerancia.	**Retener o aceptar el riesgo** sin implementar controles adicionales. Monitorizarlo para confirmar que no se incrementa.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

TRATANDO Y ACEPTANDO RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

PARA **REDUCIR O MITIGAR LOS RIESGOS** SE REALIZAN ESTAS **ACCIONES**:

- INSTALAR PRODUCTOS O CONTRATAR SERVICIOS
- ESTABLECER CONTROLES DE SEGURIDAD
- MEJORAR LOS PROCEDIMIENTOS
- CAMBIAR EL ENTORNO
- INCLUIR MÉTODOS DE DETECCIÓN TEMPRANA
- IMPLANTAR UN PLAN DE CONTINGENCIA Y CONTINUIDAD
- REALIZAR FORMACIÓN Y SENSIBILIZACIÓN.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

TRATANDO Y ACEPTANDO RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

EL RESULTADO DE ESTA FASE SE CONCRETA EN UN **PLAN DE TRATAMIENTO DE RIESGOS,** ES DECIR, LA SELECCIÓN Y JUSTIFICACIÓN DE UNA O VARIAS OPCIONES PARA CADA RIESGO IDENTIFICADO.

A ESTE PLAN SE AÑADIRÁ UNA **RELACIÓN DE RIESGOS RESIDUALES**, ES DECIR, AQUELLOS QUE AÚN SIGUEN EXISTIENDO A PESAR DE LAS MEDIDAS TOMADAS.

ADICIONALMENTE SE INCLUYE EN ALGUNOS MODELOS UNA ETAPA DE **ACEPTACIÓN DEL RIESGO** PARA GARANTIZAR QUE LA DIRECCIÓN ES CONSCIENTE DE LOS RIESGOS RESIDUALES.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

MONITORIZANDO LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

PERIÓDICAMENTE SE REVISARÁN POSIBLES CAMBIOS EN EL VALOR DE LOS ACTIVOS, IMPACTOS, AMENAZAS, VULNERABILIDADES Y PROBABILIDADES.

LOS RIESGOS NO SON ESTÁTICOS Y PUEDEN CAMBIAR SIN PREVIO AVISO. POR ELLO ES NECESARIA UNA **SUPERVISIÓN CONTINUA** QUE DETECTE:

- NUEVOS ACTIVOS O MODIFICACIONES EN EL VALOR DE LOS ACTIVOS
- NUEVAS AMENAZAS
- CAMBIOS O APARICIÓN DE NUEVAS VULNERABILIDADES
- AUMENTO DE LAS CONSECUENCIAS O IMPACTOS
- INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

MONITORIZANDO LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

DE FORMA ANÁLOGA SE REVISARÁ EL PROPIO PROCESO DE GESTIÓN DE RIESGOS PARA ADECUARLO AL CONTEXTO. ESTA REVISIÓN AFECTA ENTRE OTROS A:

- LAS CATEGORÍAS DE ACTIVOS
- LOS CRITERIOS DE EVALUACIÓN DE RIESGOS
- LOS NIVELES DE CLASIFICACIÓN DE LOS IMPACTOS
- LAS ESCALAS DE ACEPTACIÓN DE RIESGOS
- LOS RECURSOS NECESARIOS.

4. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

EL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

MONITORIZANDO LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

COMO RESULTADO DE LA GESTIÓN DE RIESGOS TENEMOS IDENTIFICADOS LOS RIESGOS Y SU FORMA DE TRATARLOS. ESTE ES UN BUEN **PUNTO DE PARTIDA PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN** EN LA EMPRESA DE FORMA AMPLIA.

LA GESTIÓN DE RIESGOS ES EL PROCESO CENTRAL PARA PONER EN MARCHA UN **PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN**. EN ESTE PLAN SE DEFINEN Y PRIORIZAN, EN BASE A UNA EVALUACIÓN DE RIESGOS, LOS PROYECTOS QUE SE HAYAN DE IMPLANTAR PARA REDUCIR LOS RIESGOS A QUE ESTÁ EXPUESTA LA EMPRESA.

ESTO ES TODO