IFCT0109. SEGURIDAD INFORMÁTICA

MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

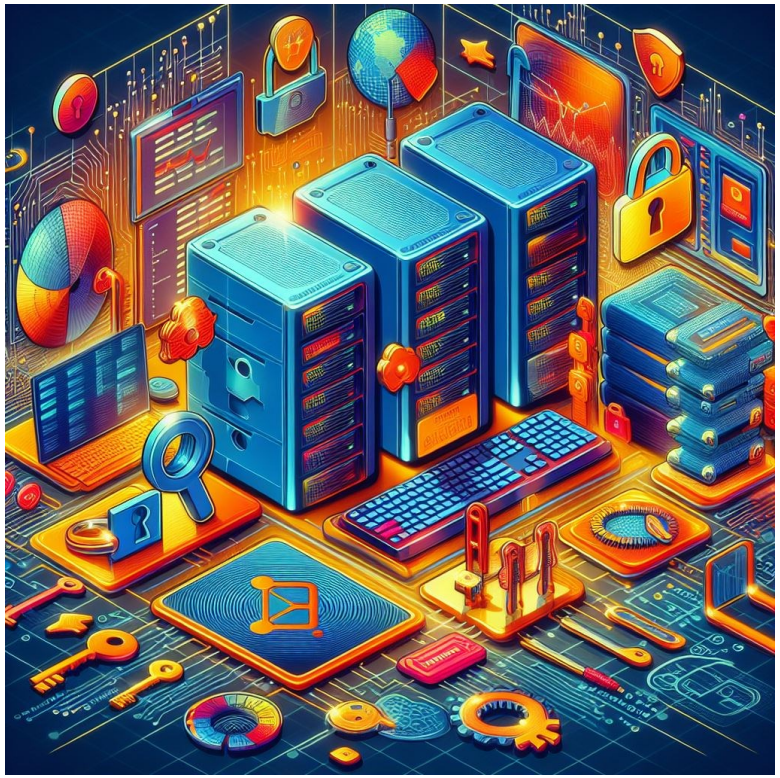
ANEXO

FUGA DE INFORMACIÓN Y PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)

INTRODUCCIÓN

DENTRO DE LA EMPRESA **EXISTEN INTANGIBLES** COMO LA *CARTERA DE CLIENTES, LAS TARIFAS, EL CONOCIMIENTO COMERCIAL, LA PROPIEDAD INTELECTUAL, ETC*.

LA INFORMACIÓN **CONSTITUYE UNO DE LOS ACTIVOS MÁS IMPORTANTES DE UNA ORGANIZACIÓN**.



INTRODUCCIÓN

ESTA INFORMACIÓN **ES UTILIZADA COMO ARMA DE DESPRESTIGIO, HERRAMIENTA DE PRESIÓN O ELEMENTO DE VALOR QUE SE COMERCIALIZA Y VENDE** A ESCALA GLOBAL EN TODO TIPO DE ÁMBITOS Y SECTORES.

INTRODUCCIÓN

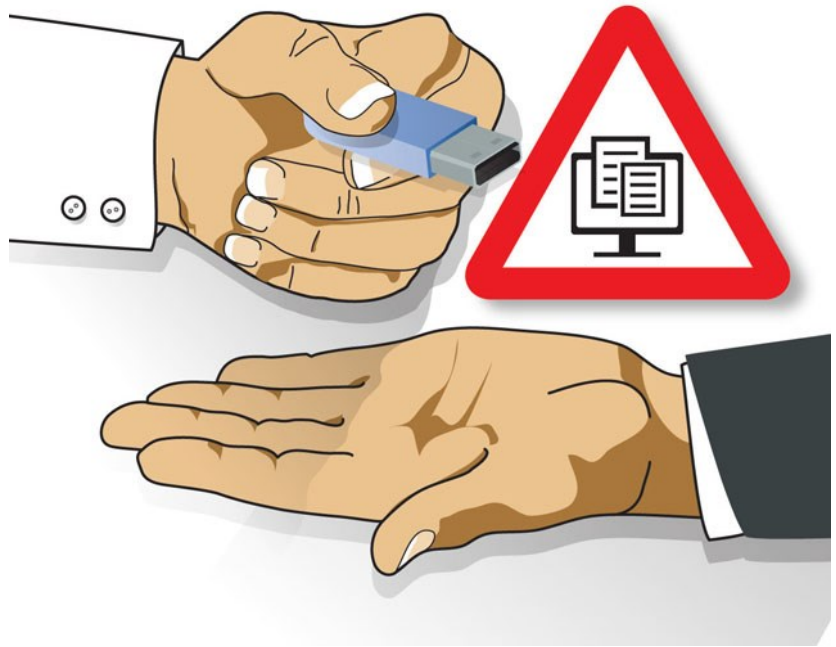
TODO ELLO ESTÁ CONVIRTIENDO A **LA FUGA DE INFORMACIÓN** EN **UNA DE LAS MAYORES AMENAZAS** E INSTRUMENTO DE FUERZA Y PRESIÓN.

LA FUGA DE INFORMACIÓN TIENE UN COMPONENTE SOCIAL Y HUMANO MUY IMPORTANTE.

DETRÁS DE UNA BUENA PARTE DE LOS INCIDENTES DE FUGA DE INFORMACIÓN SE ESCONDEN *MOTIVACIONES PERSONALES, ECONÓMICAS, DAÑO A LA IMAGEN DE LA ORGANIZACIÓN O SIMPLES ERRORES*, ENTRE OTRAS.

INTRODUCCIÓN

PODEMOS DEFINIR LA **FUGA DE INFORMACIÓN** COMO LA *PÉRDIDA DE CONFIDENCIALIDAD DE LA INFORMACIÓN DE UNA ORGANIZACIÓN, EMPRESA O INDIVIDUO, MEDIANTE LA OBTENCIÓN DE LA MISMA O EL CONOCIMIENTO DEL CONTENIDO DE ESTA POR PARTE DE PERSONAS NO AUTORIZADAS PARA ELLO*.

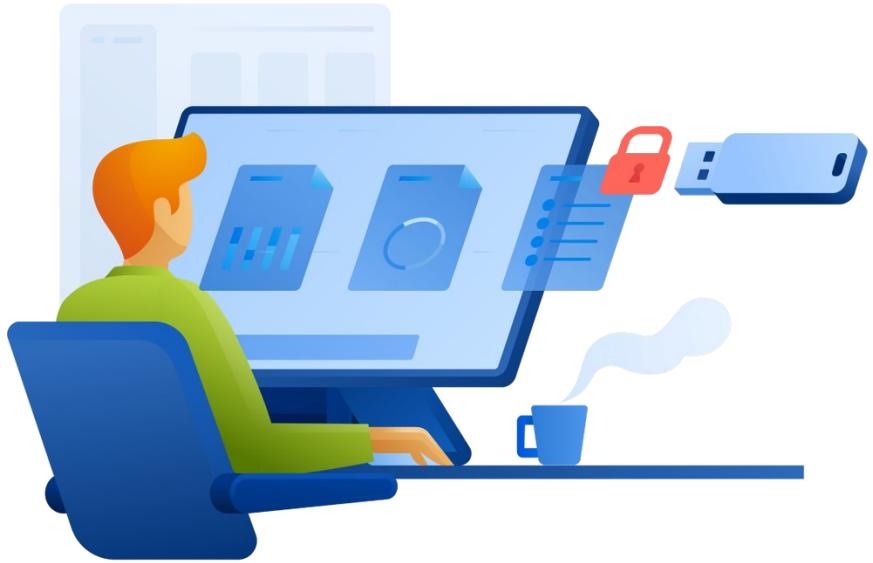


INTRODUCCIÓN

ESTA PUEDE SUCEDER POR **CAUSAS INTERNAS** (PERSONAL QUE TRABAJA EN LA EMPRESA) O POR **CAUSAS EXTERNAS** (PERSONAL EXTERNO A LA EMPRESA, COMO POR EJEMPLO UN PROVEEDOR), ADEMÁS PUEDEN SER **DELIBERADAS O INVOLUNTARIAS**.

INTRODUCCIÓN

LAS **CAUSAS MÁS COMUNES** EN LA FUGA DE INFORMACIÓN SON DEBIDO A LA **FALTA DE CONCIENCIACIÓN** DE LOS EMPLEADOS O SIMPLEMENTE POR LA **FALTA DE SEGURIDAD** EN LOS DISPOSITIVOS.



CONTENIDOS

1. INTRODUCCIÓN
2. **CAUSAS**
3. CONSECUENCIAS
4. PREVENCIÓN
5. GESTIÓN DE LA FUGA DE INFORMACIÓN
6. FORMAS DE DETECTAR LA FUGA DE INFORMACIÓN
7. ACCIONES A REALIZAR

CAUSAS

LA MAYORÍA DE LAS **CAUSAS** DE FUGA DE INFORMACIÓN IMPLICAN LA **AUSENCIA DE ALGÚN TIPO DE MEDIDA** DE SEGURIDAD, PROCEDIMIENTO, HERRAMIENTA, ETC.

ESTO SUPONE LA **FALTA DE CONTROL SOBRE LA INFORMACIÓN** Y **AUMENTA LA PROBABILIDAD DE QUE SE PRODUZCA UN INCIDENTE** DE FUGA DE INFORMACIÓN.

LAS CAUSAS PRINCIPALES DE LOS CASOS DE FUGA DE INFORMACIÓN PUEDEN SER CLASIFICADAS EN DOS **GRUPOS**:

- **ÁMBITO ORGANIZATIVO**
- **ÁMBITO TÉCNICO**

CAUSAS ORGANIZATIVAS

FALTA DE UNA CLASIFICACIÓN DE LA INFORMACIÓN

ES UNO DE LOS PRIMEROS ERRORES QUE SE COMETE.

SE DEBE CLASIFICAR LA INFORMACIÓN, POR EJEMPLO, EN BASE A SU **NIVEL DE CONFIDENCIALIDAD**, EN FUNCIÓN DE DIVERSOS PARÁMETROS:

EL VALOR QUE TIENE PARA LA ORGANIZACIÓN, EL IMPACTO QUE PUEDE GENERAR SU FILTRACIÓN, SU NIVEL DE SENSIBILIDAD O SI SE TRATA DE INFORMACIÓN PERSONAL O NO.

SI SE DESCONOCE EL VALOR DE LA INFORMACIÓN QUE TRATA LA ORGANIZACIÓN, NO SERÁ POSIBLE DISEÑAR Y SELECCIONAR LAS MEDIDAS DE PROTECCIÓN ADECUADAS.

CAUSAS ORGANIZATIVAS

FALTA DE UNA CLASIFICACIÓN DE LA INFORMACIÓN

POR OTRO LADO, **EL ÁMBITO DE DIFUSIÓN** PERMITE ESTABLECER EL PERÍMETRO DENTRO DEL CUAL PODRÁ SER DIFUNDIDA LA INFORMACIÓN.

ESTO, JUNTO CON **EL NIVEL DE CONFIDENCIALIDAD**, HARÁ POSIBLE *DETERMINAR QUIÉN DEBE CONOCER LA INFORMACIÓN Y QUÉ TIPO DE ACCIONES PUEDE REALIZAR SOBRE ESTA*.

ESTO SE CONOCE COMO **PRINCIPIO DEL MÍNIMO CONOCIMIENTO.**

CAUSAS ORGANIZATIVAS

FALTA DE CONOCIMIENTO Y FORMACIÓN

EL EMPLEADO DEBE UTILIZAR LOS RECURSOS QUE LA ORGANIZACIÓN PONE A SU DISPOSICIÓN **DE FORMA RESPONSABLE**, COMO EN EL CASO DE LOS SERVICIOS EN LA NUBE, LOS DISPOSITIVOS MÓVILES, EL CORREO ELECTRÓNICO, LA NAVEGACIÓN WEB, ETC.

POR OTRO LADO, **DEBE DISPONER DE CIERTOS CONOCIMIENTOS Y FORMACIÓN** EN RELACIÓN CON SU ACTIVIDAD DIARIA Y EN MATERIA DE CIBERSEGURIDAD, SIENDO **RESPONSABILIDAD DE LA ORGANIZACIÓN PROPORCIONAR LA FORMACIÓN NECESARIA** DE MANERA QUE EL EMPLEADO PUEDA DESEMPEÑAR SU FUNCIÓN DE FORMA SEGURA.

CAUSAS ORGANIZATIVAS

AUSENCIA DE PROCEDIMIENTOS

ES IMPORTANTE EL **ESTABLECIMIENTO DE POLÍTICAS** QUE INDIQUEN AL USUARIO CLARAMENTE CUÁLES SON LOS LÍMITES DENTRO DE LOS CUALES DEBERÁN DESEMPEÑAR SU ACTIVIDAD.

POR OTRO LADO, **LA DEFINICIÓN DE PROCEDIMIENTOS** PARA LAS ACTIVIDADES DE ESPECIAL IMPORTANCIA O CONFIDENCIALIDAD **DISMINUIRÁN EL RIESGO** PARA QUE SE PRODUZCA UNA FUGA DE INFORMACIÓN.

CAUSAS ORGANIZATIVAS

FALTA DE ACUERDOS DE CONFIDENCIALIDAD

ES IMPORTANTE **SOLICITAR POR ESCRITO LA CONFORMIDAD CON** DIVERSAS NORMAS INTERNAS, COMO **LA POLÍTICA DE CONFIDENCIALIDAD O DE SEGURIDAD**, ENTRE OTRAS, DE MANERA QUE EL FUTURO EMPLEADO, DEJA POR ESCRITO LA ACEPTACIÓN DE LAS CONDICIONES CORRESPONDIENTES.

ADEMÁS, SE CUENTA CON **LEGISLACIÓN QUE PERMITE ESTABLECER LÍMITES LEGALES A LAS ACTIVIDADES DE SUS TRABAJADORES** Y QUE PUEDEN SER UTILIZADAS COMO **MECANISMOS DE DISUASIÓN** PARA EVITAR UN USO MALINTENCIONADO DE LA INFORMACIÓN.

CAUSAS TÉCNICAS

CÓDIGO MALICIOSO O MALWARE

ES **UNA DE LAS PRINCIPALES AMENAZAS**, SIENDO EL ROBO DE INFORMACIÓN UNO DE SUS OBJETIVOS MÁS COMUNES.

EL MALWARE ESTA MUCHAS VECES DISEÑADO UTILIZANDO TÉCNICAS QUE PERMITEN MANTENER OCULTO SU CÓDIGO EN UN SISTEMA, MIENTRAS RECOGE Y ENVÍA INFORMACIÓN.

CAUSAS TÉCNICAS

ACCESO NO AUTORIZADO A SISTEMAS E INFRAESTRUCTURAS

ES **OTRA DE LAS CAUSAS DETRÁS DEL ROBO DE INFORMACIÓN**, YA SEA COMO PARTE DE UNA CAMPAÑA DE DESPRESTIGIO, CON EL ACCESO NO AUTORIZADO A UNA PÁGINA WEB DE UNA ORGANIZACIÓN, O CON MOTIVO DE SUSTRAER INFORMACIÓN SOBRE SECRETOS INDUSTRIALES.

LA ACTUALIZACIÓN SE CONSIDERA PARTE FUNDAMENTAL DE UNA BUENA APLICACIÓN, PUESTO QUE APORTA MAYOR SEGURIDAD Y DENOTA UN TRABAJO DE MEJORA CONTINUA QUE REDUNDA EN BENEFICIO DE LA APLICACIÓN Y, POR EXTENSIÓN, DEL USUARIO.

CAUSAS TÉCNICAS

USO DE SERVICIOS EN LA NUBE

EL USO DE SERVICIOS EN LA NUBE PARA EL ALMACENAMIENTO DE TODO TIPO DE INFORMACIÓN PUEDE CONLLEVAR A LA PERCEPCIÓN DE QUE EN LA NUBE NUESTRA INFORMACIÓN ESTÁ SEGURA.

EL NIVEL DE SEGURIDAD QUE TIENE ES EL DEL ESLABÓN MÁS DÉBIL, QUE, **MUY A MENUDO SON LOS PROPIOS USUARIOS Y SUS CONTRASEÑAS**.

LOS INCIDENTES DE FUGA INFORMACIÓN CAUSADOS POR EL USO INADECUADO DE SERVICIOS EN LA NUBE **SON PARECIDOS A LOS CAUSADOS POR USO DE REDES SOCIALES Y LA FORMA DE TRATARLOS ES MUY SIMILAR**.

CAUSAS TÉCNICAS

USO DE LAS TECNOLOGÍAS MÓVILES PARA EL TRABAJO DIARIO

UN **DISPOSITIVO SUSTRAÍDO**, EN LAS MANOS EQUIVOCADAS, CONTENDRÁ MUCHA INFORMACIÓN QUE PUEDE SER PUBLICADA. ADEMÁS, ESTE TIPO DE INCIDENTES SON DE **DIFÍCIL MITIGACIÓN**.

EL USO DE DISPOSITIVOS MÓVILES HA OCASIONADO LA GENERALIZACIÓN DE MEDIDAS COMO EL **CIFRADO DE LOS DISPOSITIVOS** O EL **USO DE VPN** EN LAS COMUNICACIONES.

LAS MEDIDAS DE SEGURIDAD DEBEN HABERSE TOMADO CON ANTERIORIDAD AL INCIDENTE, PORQUE UNA VEZ ESTE OCURRE HAY POCO MARGEN DE MANIOBRA.

CAUSAS MÁS COMUNES

LAS **CAUSAS MÁS COMUNES** DE LA FUGA DE INFORMACIÓN PUEDEN SER VARIADAS. ALGUNOS EJEMPLOS INCLUYEN:

- EL **EXTRAVÍO DE UNIDADES DE MEMORIA EXTERNAS** CON INFORMACIÓN CONFIDENCIAL DE LA EMPRESA
- **LA EXFILTRACIÓN DE BASES DE DATOS DE CLIENTES SIN CIFRAR** (COMO LAS QUE SUELEN ACOMPAÑAR MUCHOS CASOS DE RANSOMWARE),
- EL **ESPIONAJE INDUSTRIAL**
- LA **FILTRACIÓN DE DATOS PERSONALES** DE EMPLEADOS O CLIENTES DE UNA EMPRESA CONSECUENCIA DE UNA BRECHA DE SEGURIDAD SUFRIDA POR UN PROVEEDOR.

CAUSAS MÁS COMUNES

OTRAS CAUSAS COMUNES PUEDEN SER:

- LA **REVELACIÓN DE INFORMACIÓN CONFIDENCIAL** POR PARTE DE UN EMPLEADO (BIEN PARA GANAR ALGÚN BENEFICIO O BIEN PARA CAUSAR ALGÚN PERJUICIO A LA EMPRESA)
- LA **FILTRACIÓN ACCIDENTAL DE DATOS CONFIDENCIALES**.
- LA **FALTA O PÉRDIDA DE CONCIENCIACIÓN Y DISCIPLINA EN LAS BUENAS PRÁCTICAS Y MEDIDAS DE SEGURIDAD** PARA EL TRATAMIENTO DE LA INFORMACIÓN TAMBIÉN PUEDE SER UNA CAUSA COMÚN.

CAUSAS MÁS COMUNES

EN RESUMEN, LAS **CAUSAS** MÁS COMUNES DE LA FUGA DE INFORMACIÓN PUEDEN SER **VARIADAS**, **DESDE DESCUIDOS HASTA CIBERATAQUES**.

CONTENIDOS

1. INTRODUCCIÓN
2. CAUSAS
3. **CONSECUENCIAS**
4. PREVENCIÓN
5. GESTIÓN DE LA FUGA DE INFORMACIÓN
6. FORMAS DE DETECTAR LA FUGA DE INFORMACIÓN
7. ACCIONES A REALIZAR

CONSECUENCIAS

COMPRENDER LAS POSIBLES CONSECUENCIAS DE UN INCIDENTE DE FUGA DE INFORMACIÓN ES UN **ASPECTO ESENCIAL Y NECESARIO** PARA LA ADECUADA GESTIÓN DE INCIDENTES DE ESTE TIPO.

ASÍ SERÁ POSIBLE **DISEÑAR UNA ESTRATEGIA**, DE FORMA QUE EN CASO DE QUE FINALMENTE SE PRODUZCA, SE TOMEN LAS DECISIONES Y MEDIDAS ADECUADAS PARA MINIMIZAR EL IMPACTO DEL INCIDENTE.

DETERMINAR LAS CONSECUENCIAS Y EL IMPACTO DE UN INCIDENTE DE FUGA DE INFORMACIÓN ES UNA TAREA MUY COMPLEJA QUE **DEPENDE DE MUCHOS FACTORES**.

CONSECUENCIAS

FACTORES

TIPO DE ORGANIZACIÓN

ADMINISTRACIÓN PÚBLICA

EL POSIBLE DAÑO E IMAGEN ES UN FACTOR IMPORTANTE. LAS CONSECUENCIAS ECONÓMICAS, ASÍ COMO LAS SANCIONES DEBIDAS A INCUMPLIMIENTO DE LA LEGISLACIÓN, SON LIMITADAS.

ENTIDADES DEL SECTOR PRIVADO

EL SECTOR PRIVADO SÍ ESTÁ EXPUESTO A SANCIONES ECONÓMICAS. POR OTRA PARTE, UN INCIDENTE PUEDE SUPONER LA PÉRDIDA DE CONFIANZA DE LOS INVERSORES O DE SUS CLIENTES.

CONSECUENCIAS

FACTORES

TIPO DE INFORMACIÓN

INFORMACIÓN CONFIDENCIAL

AQUELLA INFORMACIÓN QUE CONSIDEREMOS CRÍTICA PARA LOS PROCESOS DE NUESTRA ENTIDAD. POR EJEMPLO, DATOS DE CLIENTES, CONTABILIDAD, DATOS DE LOS PROPIOS TRABAJADORES.

INFORMACIÓN NO CONFIDENCIAL

EL HECHO DE SU DIVULGACIÓN IMPACTARÍA EN LA IMAGEN DE LA EMPRESA, PERO EL PESO DEL IMPACTO ECONÓMICO SERÁ MENOR.

CONSECUENCIAS

FACTORES

TIPO DE DATOS

DATOS DE CARÁCTER PERSONAL

CUALQUIER DATO QUE IDENTIFIQUE O QUE PUEDA SER ASOCIADO A UNA PERSONA IDENTIFICADA. SU DIVULGACIÓN O DIFUSIÓN PUEDEN CONLLEVAR SANCIONES PARA LA ORGANIZACIÓN QUE HA SUFRIDO EL INCIDENTE.

OTROS DATOS

SERÁN AQUELLOS QUE NO SON DATOS DE CARÁCTER PERSONAL, GENERALMENTE RELACIONADOS CON TERCEROS, INFORMACIÓN TÉCNICA U OPERATIVA.

CONSECUENCIAS

PARA OBTENER UNA ESCALA DE VALOR DE LAS CONSECUENCIAS, **ES NECESARIO CONTAR CON UNA VALORACIÓN OBJETIVA** TANTO DE LOS FACTORES COMENTADOS COMO DE OTROS FACTORES, SIGUIENDO UN PROCEDIMIENTO DE **ANÁLISIS DE RIESGOS**.

TENDREMOS EN CUENTA EL ACTIVO A PROTEGER DE LA FUGA DE INFORMACIÓN, **LA AMENAZA**, **LA PROBABILIDAD** DE QUE OCURRA **Y EL IMPACTO** PARA PODER OBTENER EL DATO REAL DE RIESGO.

CONSECUENCIAS

ALGUNOS **EJEMPLOS** DE ESTAS SON:

- **DAÑOS REPUTACIONALES**
- **CONSECUENCIAS REGULATORIAS**
- **CONSECUENCIAS ECONÓMICAS**
- **OTRAS CONSECUENCIAS**

CONSECUENCIAS

EJEMPLOS:

DAÑOS REPUTACIONALES

AL TENER UNA FUGA DE INFORMACIÓN SE GENERA UN IMPACTO EN LA IMAGEN DE LA EMPRESA QUE PUEDE LLEGAR A AFECTAR A LA CONFIANZA DE CLIENTES Y PROVEEDORES.

CONSECUENCIAS

EJEMPLOS:

CONSECUENCIAS REGULATORIAS

ESTE INCIDENTE PUEDE CAUSAR QUE LA EMPRESA SE LLEVE UNA SANCIÓN PENAL, ADMINISTRATIVA O DEONTOLÓGICA QUE CONLLEVA NORMALMENTE EL PAGO DE UN ELEVADO IMPORTE.

CONSECUENCIAS

EJEMPLOS:

CONSECUENCIAS ECONÓMICAS

ESTÁN RELACIONADAS CON LA ANTERIOR Y SUPONEN UN IMPACTO NEGATIVO A NIVEL ECONÓMICO, DISMINUCIÓN DE INVERSIÓN, ETC.

CONSECUENCIAS

EJEMPLOS:

OTRAS CONSECUENCIAS

SON AQUELLAS QUE PUEDEN SUPONER UN IMPACTO NEGATIVO EN OTROS ÁMBITOS COMO: POLÍTICO, DIPLOMÁTICO, INSTITUCIONAL O GUBERNAMENTAL.

CONTENIDOS

1. INTRODUCCIÓN
2. CAUSAS
3. CONSECUENCIAS
4. **PREVENCIÓN**
5. GESTIÓN DE LA FUGA DE INFORMACIÓN
6. FORMAS DE DETECTAR LA FUGA DE INFORMACIÓN
7. ACCIONES A REALIZAR

PREVENCIÓN

LAS PRINCIPALES MEDIDAS DE PREVENCIÓN DEBEN ORIENTARSE HACIA EL COMPONENTE HUMANO Y ORGANIZATIVO QUE SE ENCUENTRA DENTRO DE LAS CAUSAS DE ESTE TIPO DE INCIDENTES.

LA PREVENCIÓN DE LA FUGA DE INFORMACIÓN PASA POR LA APLICACIÓN DE MEDIDAS DE SEGURIDAD DESDE TRES PUNTOS DE VISTA:

- **ORGANIZATIVO**
- **TÉCNICO**
- **LEGAL**

PREVENCIÓN

MEDIDAS ORGANIZATIVAS

- PONER EN MARCHA BUENAS PRÁCTICAS PARA LA GESTIÓN DE FUGA DE LA INFORMACIÓN
- DEFINIR UNA POLÍTICA DE SEGURIDAD Y PROCEDIMIENTOS PARA TODO EL CICLO DE VIDA DE LOS DATOS
- ESTABLECER UN SISTEMA DE CLASIFICACIÓN DE LA INFORMACIÓN, PARA LIGARLO A ROLES Y NIVELES DE ACCESO
- LLEVAR A CABO ACCIONES DE FORMACIÓN E INFORMACIÓN INTERNA EN CIBERSEGURIDAD
- IMPLANTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PREVENCIÓN

MEDIDAS TÉCNICAS

- CONTROL DE ACCESO E IDENTIDAD
- SOLUCIONES ANTI-MALWARE Y ANTI-FRAUDE, SEGURIDAD PERIMETRAL Y PROTECCIÓN DE LAS TELECOMUNICACIONES.
- CONTROL DE CONTENIDOS, CONTROL DE TRÁFICO Y COPIAS DE SEGURIDAD.
- CONTROL DE ACCESO A LOS RECURSOS, ACTUALIZACIONES DE SEGURIDAD Y PARCHES.

PREVENCIÓN

MEDIDAS LEGALES

- SOLICITUD DE ACEPTACIÓN DE LA POLÍTICA DE SEGURIDAD Y DE LA DE CONFORMIDAD POR PARTE DE LOS EMPLEADOS
- MEDIDAS RELATIVAS A LA ADECUACIÓN Y CUMPLIMIENTO DE LA LEGISLACIÓN APLICABLE (LOPDGDD, LSSI, ETC.)
- OTRAS MEDIDAS DE CARÁCTER DISUASORIO EN BASE A LA LEGISLACIÓN.

PREVENCIÓN

CADA ORGANIZACIÓN ES DIFERENTE Y SERÁ NECESARIO BUSCAR UN EQUILIBRIO ENTRE COMPLEJIDAD, COSTE Y RIESGO, EN RELACIÓN CON LA IMPLANTACIÓN DE LAS MEDIDAS DE SEGURIDAD.

PARA EVITAR FUGAS DE INFORMACIÓN CAUSADAS POR EL USO INADECUADO DE **SERVICIOS EN LA NUBE**, DEBEMOS SEGUIR LAS MISMAS MEDIDAS QUE PARA OTROS TIPOS DE INCIDENTES.

PARA LOS INCIDENTES CAUSADOS POR DISPOSITIVOS MÓVILES, LA PREVENCIÓN SE BASA EN IMPLANTAR POLÍTICAS DE USO Y MEDIDAS TÉCNICAS: SOLUCIONES ANTI-MALWARE, CIFRADO, USO DE SISTEMAS VPN, ETC.

CONTENIDOS

1. INTRODUCCIÓN
2. CAUSAS
3. CONSECUENCIAS
4. PREVENCIÓN
5. **GESTIÓN DE LA FUGA DE INFORMACIÓN**
6. FORMAS DE DETECTAR LA FUGA DE INFORMACIÓN
7. ACCIONES A REALIZAR

GESTIÓN DE LA FUGA DE INFORMACIÓN

PARA GESTIONAR CORRECTAMENTE UNA FUGA DE INFORMACIÓN SE PUEDEN SEGUIR LOS SIGUIENTES **PASOS**:

1. **FASE INICIAL**
2. **FASE DE LANZAMIENTO**
3. **FASE DE AUDITORÍA**
4. **FASE DE EVALUACIÓN**
5. **FASE DE MITIGACIÓN**
6. **FASE DE SEGUIMIENTO**

GESTIÓN DE LA FUGA DE INFORMACIÓN

1. FASE INICIAL

AQUÍ **SE DETECTA** EL INCIDENTE, **SE COMUNICA** Y **SE INICIA** EL PROTOCOLO.

LOS **MOMENTOS INMEDIATAMENTE POSTERIORES A LA DETECCIÓN** DE UN INCIDENTE DE FUGA DE INFORMACIÓN SON **ESPECIALMENTE CRÍTICOS**.

UNA **ADECUADA GESTIÓN** EN LAS PRIMERAS FASES PUEDE SUPONER UNA **REDUCCIÓN DEL IMPACTO**.

GESTIÓN DE LA FUGA DE INFORMACIÓN

1. FASE INICIAL

UNO DE LOS MAYORES RETOS A LOS QUE SE ENFRENTAN LAS ORGANIZACIONES ES CONSEGUIR LA **DETECCIÓN TEMPRANA** DEL INCIDENTE, SI ES POSIBLE, **A TRAVÉS DE MEDIOS INTERNOS**.

ADEMÁS, REALIZAR UNA CONSTANTE **MONITORIZACIÓN DE CUALQUIER PUBLICACIÓN SOBRE NUESTRA ENTIDAD**, PARA TOMAR EL CONTROL DE LA SITUACIÓN LO ANTES POSIBLE.

GESTIÓN DE LA FUGA DE INFORMACIÓN

1. FASE INICIAL

EN PRIMER LUGAR, DEBEMOS DE **INFORMAR INTERNAMENTE** DE LA SITUACIÓN, JUNTO CON EL **LANZAMIENTO DEL PROTOCOLO DE ACTUACIÓN**.

ES IMPORTANTE INCIDIR EN LA PRUDENCIA Y REDIRIGIR A UN INTERLOCUTOR PREVIAMENTE DESIGNADO CUALQUIER DUDA O PREGUNTA TANTO DE LOS PROPIOS EMPLEADOS COMO SI LA MISMA PROCEDE DE TERCEROS EL EXTERIOR.

ADEMÁS, SE DEBERÁ **INFORMAR DE LA PUESTA EN MARCHA DEL PROCESO DE GESTIÓN DE LA INCIDENCIA**.

GESTIÓN DE LA FUGA DE INFORMACIÓN

2. FASE DE LANZAMIENTO

REUNIÓN DEL GABINETE DE CRISIS PARA VER LA SITUACIÓN, COORDINACIÓN Y VER LAS PRIMERAS ACCIONES A REALIZAR.

EL PRIMER PASO ES **INICIAR EL PROTOCOLO INTERNO DE GESTIÓN DEL INCIDENTE**, CONVOCANDO A LOS RESPONSABLES QUE FORMAN PARTE DEL EQUIPO DE GESTIÓN QUE DEBEN TOMAR LAS DECISIONES: **EL GABINETE DE CRISIS**.

MANTENER LA **CALMA Y ACTUAR CON ORGANIZACIÓN** ES FUNDAMENTAL PARA EVITAR DECISIONES INCORRECTAS O PROVOCAR CONSECUENCIAS NEGATIVAS ADICIONALES.

GESTIÓN DE LA FUGA DE INFORMACIÓN

2. FASE DE LANZAMIENTO

CADA ORGANIZACIÓN DEBERÁ AJUSTARSE A SUS RECURSOS. SERÁ NECESARIO **CONTAR COMO MÍNIMO CON UN RESPONSABLE CON CAPACIDAD DE DECISIÓN**, QUE SE ENCARGARÁ DE LA GESTIÓN Y COORDINACIÓN DE LA SITUACIÓN.

EN CUALQUIER CASO, **TODAS LAS DECISIONES Y LAS ACTUACIONES** RELATIVAS AL INCIDENTE DEBERÁN SER **TOMADAS Y COORDINADAS POR EL GABINETE DE CRISIS.**

ES FUNDAMENTAL **EVITAR ACTUACIONES POR LIBRE** O QUE NO HAYAN SIDO DEFINIDAS Y ACORDADAS POR EL GABINETE.

GESTIÓN DE LA FUGA DE INFORMACIÓN

3. FASE DE AUDITORÍA

REALIZAR UNA **AUDITORÍA INTERNA Y EXTERNA PARA ELABORAR UN INFORME PRELIMINAR**.

UNA VEZ SE HAN INICIADO LOS PASOS ANTERIORES, DARÍA COMIENZO LA **FASE DE OBTENCIÓN DE INFORMACIÓN SOBRE EL INCIDENTE**. PARA ELLO, SERÁ NECESARIO **INICIAR UNA AUDITORÍA INTERNA**, CON EL OBJETIVO DE DETERMINAR CON EXACTITUD Y EN EL MENOR TIEMPO POSIBLE LO SIGUIENTE:

- DETERMINAR LA **CANTIDAD DE INFORMACIÓN** HA PODIDO SER SUSTRAÍDA.

GESTIÓN DE LA FUGA DE INFORMACIÓN

3. FASE DE AUDITORÍA

- ESTABLECER EL **TIPO DE DATOS** QUE CONTIENE LA INFORMACIÓN QUE HA PODIDO SER SUSTRAÍDA. DEBE CONSIDERARSE ESPECIALMENTE SI SE HAN FILTRADO DATOS DE CARÁCTER PERSONAL Y DE QUÉ NIVEL SEGÚN EL REGLAMENTO DE LA **LOPDGDD**.
- DETERMINAR SI LA INFORMACIÓN ES **RELATIVA A LA PROPIA ORGANIZACIÓN O ES EXTERNA**, ES DECIR, SI POR EL CONTRARIO SE TRATA DE INFORMACIÓN QUE HACE REFERENCIA A ORGANIZACIONES O PERSONAS EXTERNAS A LA ORGANIZACIÓN.

GESTIÓN DE LA FUGA DE INFORMACIÓN

3. FASE DE AUDITORÍA

- ESTABLECER Y ACOTAR LA **CAUSA PRINCIPAL DE LA FILTRACIÓN**, SI TIENE UN ORIGEN TÉCNICO, O HUMANO. SI EL **ORIGEN** ES **TÉCNICO**, DETERMINAR LOS **SISTEMAS QUE ESTÁN AFECTADOS** O EN LOS CUALES SE HA PRODUCIDO LA BRECHA. SI ES **HUMANO**, INICIAR EL PROCESO PARA IDENTIFICAR COMO SE HA PRODUCIDO LA FUGA Y **RESPONSABLES** DE ESA INFORMACIÓN.

GESTIÓN DE LA FUGA DE INFORMACIÓN

3. FASE DE AUDITORÍA

ADEMÁS DE LA AUDITORÍA INTERNA, TAMBIÉN ES NECESARIO **REALIZAR UNA AUDITORÍA EXTERNA**.

EL OBJETIVO DE ÉSTA SERÁ CONOCER EL TAMAÑO, GRAVEDAD Y NIVEL DE DIFUSIÓN DE LA FILTRACIÓN EN EL EXTERIOR DE LA ORGANIZACIÓN.

HAY QUE DISTINGUIR ENTRE INFORMACIÓN QUE HA SIDO SUSTRAÍDA E INFORMACIÓN QUE SE HA HECHO PÚBLICA, YA QUE NO SON NECESARIAMENTE LO MISMO.

GESTIÓN DE LA FUGA DE INFORMACIÓN

3. FASE DE AUDITORÍA

AL MENOS ES NECESARIO:

- DETERMINAR EL ALCANCE DE LA PUBLICACIÓN DE LA INFORMACIÓN SUSTRAÍDA. ESTE PUNTO ES CRÍTICO PARA CERRAR LA BRECHA DE SEGURIDAD Y MITIGAR LA DIFUSIÓN DE LA INFORMACIÓN SUSTRAÍDA.
- ESTABLECER QUÉ INFORMACIÓN SE HA HECHO PÚBLICA Y DETERMINAR LA CANTIDAD DE LA INFORMACIÓN FILTRADA EN EL EXTERIOR DE LA ORGANIZACIÓN.
- RECOGER LAS NOTICIAS QUE HAYAN APARECIDO EN LOS MEDIOS DE COMUNICACIÓN Y EN INTERNET SOBRE EL INCIDENTE.
- CONOCER LAS REACCIONES QUE SE ESTÁN PRODUCIENDO EN RELACIÓN CON EL INCIDENTE.

GESTIÓN DE LA FUGA DE INFORMACIÓN

3. FASE DE AUDITORÍA

EN ESTA FASE, EL TIEMPO DE REACCIÓN ES CRÍTICO.

DE FORMA ORIENTATIVA **ES RECOMENDABLE CONOCER LA MAYOR PARTE DE LOS PUNTOS ANTERIORES EN UN PLAZO NO SUPERIOR A 12 HORAS**, DESDE EL MOMENTO EN QUE SE HA CONOCIDO EL INCIDENTE.

EN CUALQUIER CASO, **UN PERIODO SUPERIOR A LAS 48 HORAS PODRÍA CONSIDERARSE EXCESIVO**, AUNQUE DEPENDERÁ DE LA GRAVEDAD DEL INCIDENTE Y DE OTROS FACTORES.

EN ESTE SENTIDO, REDUCIR LOS TIEMPOS ES FUNDAMENTAL, PERO SIN PERDER DE VISTA QUE DEBE PRIMAR LA OBTENCIÓN DE INFORMACIÓN FIABLE Y NO MERAS HIPÓTESIS O SUPOSICIONES.

GESTIÓN DE LA FUGA DE INFORMACIÓN

4. FASE DE EVALUACIÓN

REUNIÓN DEL **GABINETE DE CRISIS** PARA **ANALIZAR EL INFORME DE LA AUDITORÍA** PARA REALIZAR UNA CORRECTA PLANIFICACIÓN.

SE INICIA EL PROCESO DE VALORACIÓN DEL INCIDENTE, POSIBLES CONSECUENCIAS E IMPACTO.

SE ESTABLECEN LAS **TAREAS PRINCIPALES** CON UNA PLANIFICACIÓN DETALLADA PARA CADA UNA DE ELLAS. AL TRATARSE DE UNA EVALUACIÓN INICIAL LAS TAREAS SE DISEÑAN EN FUNCIÓN DE LA INFORMACIÓN DISPONIBLE, QUE PUEDE SER INCOMPLETA.

TAMBIÉN HAY QUE TENER EN CUENTA LA VENTANA DE TIEMPO DE RESPUESTA DISPONIBLE, PUESTO QUE SE DEBE ACTUAR CON AGILIDAD.

GESTIÓN DE LA FUGA DE INFORMACIÓN

4. FASE DE EVALUACIÓN

LAS **PRINCIPALES TAREAS** QUE SERÁ NECESARIO LLEVAR A CABO SON:

- TAREAS PARA **CORTAR LA FILTRACIÓN** Y EVITAR NUEVAS FUGAS DE INFORMACIÓN.
- TAREAS DE **REVISIÓN DE LA DIFUSIÓN** DE LA INFORMACIÓN Y MITIGACIÓN DE LA MISMA, EN ESPECIAL SI ÉSTA CONTIENE DATOS DE CARÁCTER PERSONAL O SE TRATA DE INFORMACIÓN CONFIDENCIAL.
- TAREAS DE **ACTUACIÓN CON LOS AFECTADOS** POR LA FUGA DE INFORMACIÓN, YA SEAN INTERNOS O EXTERNOS.

GESTIÓN DE LA FUGA DE INFORMACIÓN

4. FASE DE EVALUACIÓN

PRINCIPALES TAREAS:

- TAREAS PARA LA **MITIGACIÓN DE LAS CONSECUENCIAS LEGALES**: POSIBLES INCUMPLIMIENTOS DE NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL O DE OTRA NORMATIVA. TAMBIÉN AQUELLAS TAREAS ENCAMINADAS A LA PREPARACIÓN DE TODA LA INFORMACIÓN NECESARIA ANTE POSIBLES DENUNCIAS POR LOS AFECTADOS, OTRAS ORGANIZACIONES, ETC.
- TAREAS PARA LA **DETERMINACIÓN DE LAS CONSECUENCIAS ECONÓMICAS**, QUE PUEDAN AFECTAR A LA ORGANIZACIÓN Y SU POSIBLE MITIGACIÓN.

GESTIÓN DE LA FUGA DE INFORMACIÓN

4. FASE DE EVALUACIÓN

PRINCIPALES TAREAS:

- TAREAS A **ACOMETER EN LOS ACTIVOS DE LA ORGANIZACIÓN AFECTADOS**, Y SU ALCANCE, EN RELACIÓN CON LOS ACTIVOS DE INFORMACIÓN, INFRAESTRUCTURAS, PERSONAS, ETC.
- **PLANIFICACIÓN DEL CONTACTO Y COORDINACIÓN CON FUERZAS Y CUERPOS DE SEGURIDAD**, DENUNCIA Y OTRAS ACTUACIONES, EN CASO DE SER NECESARIO.
- PLANIFICACIÓN DE **COMUNICACIÓN E INFORMACIÓN DEL INCIDENTE**, TANTO A NIVEL INTERNO COMO EXTERNO, A MEDIOS DE COMUNICACIÓN, Y AFECTADOS, EN CASO DE SER NECESARIO.

GESTIÓN DE LA FUGA DE INFORMACIÓN

4. FASE DE EVALUACIÓN

ESTE CONJUNTO BÁSICO DE ACCIONES COMPONDRÁ EL **PLAN DE EMERGENCIA** DISEÑADO PARA EL INCIDENTE DE FUGA DE INFORMACIÓN. SU EJECUCIÓN DEBERÁ DE ESTAR COMPLETAMENTE **COORDINADA Y SUPERVISADA** EN TODO MOMENTO POR EL **GABINETE DE CRISIS.**

EN FUNCIÓN DEL ESCENARIO Y LOS RECURSOS DE LA ORGANIZACIÓN, LAS ACCIONES INDICADAS ANTERIORMENTE PODRÁN **REALIZARSE DE FORMA SIMULTÁNEA O SECUENCIAL**.

EN CUALQUIER CASO, ESTABLECER LA PRIORIDAD DE LAS TAREAS SERÁ RESPONSABILIDAD DEL GABINETE DE CRISIS.

GESTIÓN DE LA FUGA DE INFORMACIÓN

5. FASE DE MITIGACIÓN

EJECUCIÓN DE PLAN ACORDADO POR EL GABINETE DE CRISIS.

EL **PRIMER PASO** ES **REDUCIR LA BRECHA DE SEGURIDAD Y EVITAR** QUE SE PRODUZCAN **NUEVAS FUGAS** DE INFORMACIÓN.

EN ALGUNOS CASOS ES POSIBLE QUE SEA NECESARIO DESCONECTAR UN DETERMINADO SERVICIO O SISTEMA DE INTERNET.

EL **SIGUIENTE PASO** ES DEBEMOS **MINIMIZAR LA DIFUSIÓN DE LA INFORMACIÓN SUSTRAÍDA**. SE CONTACTARÁ CON LOS SITIOS QUE HAN PUBLICADO INFORMACIÓN Y SE SOLICITARÁ SU RETIRADA, EN ESPECIAL SI SE TRATA DE INFORMACIÓN SENSIBLE O PROTEGIDA POR LA **LOPDGDD**.

GESTIÓN DE LA FUGA DE INFORMACIÓN

5. FASE DE MITIGACIÓN

JUNTO CON EL PASO ANTERIOR, SI SE CONSIDERA NECESARIO, SE LLEVARÁ A CABO LA **COMUNICACIÓN PERTINENTE A LOS MEDIOS**.

LOS MEDIOS DE COMUNICACIÓN PUEDEN APORTAR UN MECANISMO MUY EFICAZ PARA HACER LLEGAR TRANQUILIDAD A LOS AFECTADOS.

DEBE DE EXISTIR UN **ÚNICO PUNTO DE CONTACTO EXTERIOR** DESDE LA ORGANIZACIÓN PARA EVITAR DESCOORDINACIÓN.

EN CASO DE EXISTIR **PERSONAS AFECTADAS** POR LA FUGA DE INFORMACIÓN ES FUNDAMENTAL QUE ESTAS **SEAN INFORMADAS**.

GESTIÓN DE LA FUGA DE INFORMACIÓN

5. FASE DE MITIGACIÓN

SE INFORMARÁ NO SOLO DEL INCIDENTE, SINO TAMBIÉN DE LOS DATOS QUE HAN SIDO SUSTRAÍDOS A FIN DE QUE PUEDAN TOMAR LAS ACCIONES OPORTUNAS PARA SU SEGURIDAD (CAMBIO DE CONTRASEÑAS, REVOCACIÓN DE NÚMEROS DE TARJETAS, SER CAUTELOSOS CON CORREOS DE DESCONOCIDOS, ETC.).

ADEMÁS, SE DEBE **PROPORCIONAR ALGÚN CANAL** PARA QUE LOS **AFECTADOS PUEDAN MANTENERSE INFORMADOS SOBRE LA EVOLUCIÓN DEL INCIDENTE** Y LAS DISTINTAS RECOMENDACIONES QUE PUEDA REALIZAR LA ORGANIZACIÓN A LOS AFECTADOS, CON EL OBJETIVO DE MINIMIZAR LAS CONSECUENCIAS.

GESTIÓN DE LA FUGA DE INFORMACIÓN

5. FASE DE MITIGACIÓN

POSTERIORMENTE SE PONDRÁ EN CONOCIMIENTO DEL INCIDENTE A LAS **FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO**, A TRAVÉS DE LA **PRESENTACIÓN DE UNA DENUNCIA Y OTRAS ACCIONES** QUE PUEDAN DERIVARSE DE LA COORDINACIÓN O LA SOLICITUD DE INFORMACIÓN POR PARTE DE LAS FUERZAS Y CUERPOS DE SEGURIDAD.

HAY QUE TENER EN CUENTA, ADEMÁS, LA NECESIDAD DE INFORMAR A OTROS ORGANISMOS QUE PUEDAN TENER COMPETENCIAS DERIVADAS DE LA INFORMACIÓN FILTRADA, COMO ES EL CASO DE LA **AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS**, EN EL CASO DE DATOS DE CARÁCTER PERSONAL.

GESTIÓN DE LA FUGA DE INFORMACIÓN

6. FASE DE SEGUIMIENTO

VALORACIÓN DE LOS RESULTADOS, GESTIÓN DE CONSECUENCIAS, AUDITORÍA COMPLETA, APLICACIÓN DE MEDIDAS Y MEJORAS.

UNA VEZ COMPLETADAS LAS PRINCIPALES ACCIONES DEL PLAN, SE PROCEDERÁ A **EVALUAR EL RESULTADO Y LA EFECTIVIDAD DE LAS ACCIONES REALIZADAS**, EN RELACIÓN CON LAS CONSECUENCIAS Y SU IMPACTO.

ADEMÁS, EN CASO DE SER NECESARIO, SE DEBERÁ DE **HACER FRENTE A OTRAS CONSECUENCIAS** QUE HAYAN PODIDO GENERARSE DURANTE LA FASE DE MITIGACIÓN DEL INCIDENTE, COMO PUEDAN SER CONSECUENCIAS LEGALES, ECONÓMICAS, ETC.

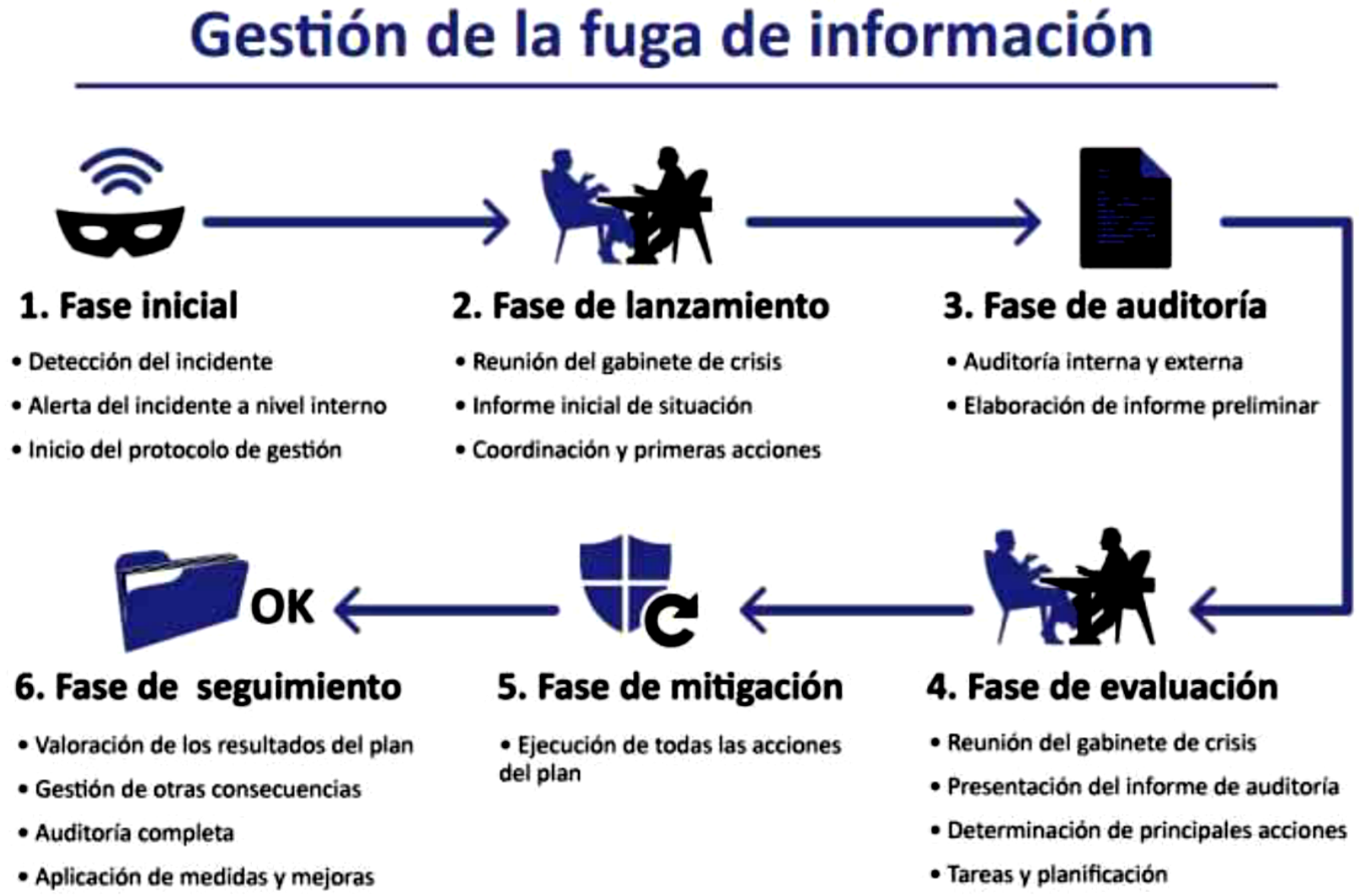
GESTIÓN DE LA FUGA DE INFORMACIÓN

6. FASE DE SEGUIMIENTO

DURANTE ESTA FASE **TAMBIÉN SE INICIARÁ EL PROCESO DE ESTABILIZACIÓN DE LA SITUACIÓN** GENERADA POR EL INCIDENTE.

SE COMENZARÁ CON UN PROCESO DE VALORACIÓN GLOBAL DEL MISMO, QUE SUPONDRÁ UNA AUDITORÍA MÁS COMPLETA A PARTIR DE LA CUAL SE DISEÑARAN E IMPLANTARAN LAS MEDIDAS DEFINITIVAS PARA EVITAR NUEVAS FUGAS Y RESTABLECER EL NORMAL FUNCIONAMIENTO DE LOS SERVICIOS E INFRAESTRUCTURAS QUE PUDIERAN HABERSE VISTO AFECTADAS.

GESTIÓN DE LA FUGA DE INFORMACIÓN



CONTENIDOS

1. INTRODUCCIÓN
2. CAUSAS
3. CONSECUENCIAS
4. PREVENCIÓN
5. GESTIÓN DE LA FUGA DE INFORMACIÓN
6. **FORMAS DE DETECTAR LA FUGA DE INFORMACIÓN**
7. ACCIONES A REALIZAR

FORMAS DE DETECTAR LA FUGA DE INFORMACIÓN

- LA **MONITORIZACIÓN** DE SISTEMAS, REDES Y MOVIMIENTOS DE ARCHIVOS.
- **USAR HERRAMIENTAS QUE RASTREEN INFORMACIÓN CONFIDENCIAL** QUE SE HAYA PODIDO PUBLICAR O PONER A LA VENTA EN INTERNET (INCLUIDA LA DARK WEB).
- IMPLEMENTAR UN **SISTEMA DE ALERTAS E INFORMES EN TIEMPO REAL** QUE ENVIARÁ UNA ALERTA CUANDO SE ACCEDA, MUEVA, MODIFIQUE O BORREN DATOS CONFIDENCIALES O SENSIBLES DE MANERA SOSPECHOSA, O CUANDO SE PRODUZCAN ACCESOS NO AUTORIZADOS.
- **MEDIDAS DE PREVENCIÓN DE PERDIDA DE DATOS**
- **FORMACIÓN Y CONCIENCIACIÓN** DE LOS EMPLEADOS EN CIBERSEGURIDAD.
- **ACUERDOS DE CONFIDENCIALIDAD** CON LOS EMPLEADOS.

CONTENIDOS

1. INTRODUCCIÓN
2. CAUSAS
3. CONSECUENCIAS
4. PREVENCIÓN
5. GESTIÓN DE LA FUGA DE INFORMACIÓN
6. FORMAS DE DETECTAR LA FUGA DE INFORMACIÓN
7. **ACCIONES A REALIZAR**

ACCIONES A REALIZAR

1. CONOCER EL VALOR DE LA PROPIA INFORMACIÓN
2. CONCIENCIAR Y DISUADIR
3. UTILIZAR DEFENSA EN PROFUNDIDAD
4. INCLUIR HERRAMIENTAS TECNOLÓGICAS
5. SEGUIR LOS ESTÁNDARES INTERNACIONALES
6. MANTENER POLÍTICAS Y PROCEDIMIENTOS CLAROS
7. PROCEDIMIENTOS SEGUROS DE CONTRATACIÓN Y DESVINCULACIÓN
8. SEGUIR PROCESOS DE ELIMINACIÓN SEGURA DE DATOS
9. CONSTRUIR UN ENTORNO DE CONFIANZA
10. ACEPTAR Y ENTENDER LA REALIDAD
11. TENER POLÍTICAS DE PREVENCIÓN DE FUGAS DE DATOS (DLP)

ACCIONES A REALIZAR

1. CONOCER EL VALOR DE LA PROPIA INFORMACIÓN

REALIZAR UN ANÁLISIS DE RIESGOS Y UN ESTUDIO DE VALUACIÓN DE ACTIVOS PARA PODER DETERMINAR UN PLAN DE ACCIÓN ADECUADO QUE PERMITA EVITAR POSIBLES FILTRACIONES.

2. CONCIENCIAR Y DISUADIR

DISEÑAR UNA ESTRATEGIA DE CONCIENCIACIÓN QUE INCLUYA LA RESPONSABILIDAD EN EL MANEJO DE LA INFORMACIÓN, QUE FUNCIONE TANTO PARA CAPACITAR A LAS PERSONAS QUE PODRÍAN FILTRAR INFORMACIÓN POR ERROR U OMISIÓN, COMO PARA PERSUADIR A LAS QUE DELIBERADAMENTE INTENTEN HACERLO, MOSTRANDO LAS POTENCIALES CONSECUENCIAS.

ACCIONES A REALIZAR

3. UTILIZAR DEFENSA EN PROFUNDIDAD

CONSIDERAR EL MODELO DE DEFENSA EN CAPAS PARA TOMAR DISTINTAS MEDIDAS DE DIFERENTE NATURALEZA A FIN DE NO CENTRALIZAR LAS SOLUCIONES NI PROMOVER PUNTOS ÚNICOS DE FALLA.

4. INCLUIR HERRAMIENTAS TECNOLÓGICAS

EN ÁMBITOS CORPORATIVOS RESULTA MUY IMPORTANTE CONTAR CON UNA SOLUCIÓN TÉCNICA DE PROTECCIÓN, POR MEDIO DE HARDWARE, SOFTWARE, O COMBINACIÓN DE AMBOS, TANTO A NIVEL DE REDES COMO DE EQUIPOS (SERVIDORES Y ESTACIONES DE TRABAJO). EL CRECIMIENTO DE AMENAZAS COMO EL SPYWARE HACE QUE LOS CÓDIGOS MALICIOSOS TAMBIÉN SEAN POTENCIALES PUNTOS DE FUGA DE INFORMACIÓN.

ACCIONES A REALIZAR

5. SEGUIR LOS ESTÁNDARES INTERNACIONALES

ALINEARSE CON ESTÁNDARES INTERNACIONALES DE GESTIÓN DE LA SEGURIDAD PERMITE DISMINUIR EL RIEGO DE INCIDENTES Y EVITAR QUE EL NEGOCIO SE VEA AFECTADO POR UN DETERMINADO EVENTO DE FILTRACIÓN.

6. MANTENER POLÍTICAS Y PROCEDIMIENTOS CLAROS

RELACIONADO CON EL PUNTO ANTERIOR, SE DEBE TENER UNA CLARA DEFINICIÓN Y COMUNICACIÓN DE LAS POLÍTICAS DE SEGURIDAD Y ACUERDOS DE CONFIDENCIALIDAD, ACEPTADOS Y FIRMADOS POR TODOS LOS USUARIOS. ESTO MINIMIZA POTENCIALES FUGAS DE INFORMACIÓN, AL CONTAR CON UN CONSENTIMIENTO FIRMADO DEL USUARIO PARA NO REALIZAR CIERTAS ACCIONES.

ACCIONES A REALIZAR

7. PROCEDIMIENTOS SEGUROS DE CONTRATACIÓN Y DESVINCULACIÓN

TANTO AL MOMENTO DE LA CONTRATACIÓN COMO EN LA DESVINCULACIÓN DE UNA PERSONA DENTRO DE UNA ORGANIZACIÓN, SE PRODUCE LA CONEXIÓN O DESCONEXIÓN DE UNA NUEVA PIEZA CON EL MOTOR DE LA ORGANIZACIÓN, POR LO QUE DEBEN TENERSE EN CUENTA LOS MÉTODOS DE ACCESO Y REGISTRO DE LOS USUARIOS EN SUS PRIMEROS O ÚLTIMOS MOMENTOS DE TRABAJO.

8. SEGUIR PROCESOS DE ELIMINACIÓN SEGURA DE DATOS

ES FUNDAMENTAL QUE LOS DATOS QUE SE DESEAN ELIMINAR SEAN EFECTIVAMENTE ELIMINADOS Y LOS MEDIOS DE ALMACENAMIENTO ADECUADAMENTE TRATADOS ANTES DE SER REUTILIZADOS.

ACCIONES A REALIZAR

9. CONSTRUIR UN ENTORNO DE CONFIANZA

CONTAR CON PERSONAL CAPACITADO Y RESPONSABLE PARA LA GESTIÓN Y ADMINISTRACIÓN DE INFORMACIÓN SENSIBLE.

10. ACEPTAR Y ENTENDER LA REALIDAD

ESTAS PRÁCTICAS AYUDAN A DISMINUIR LOS RIESGOS DE PÉRDIDA DE INFORMACIÓN VALIOSA Y RESALTAN LA IMPORTANCIA DE TOMAR MEDIDAS CONCRETAS Y DEFINIR UN PLAN REALISTA, ALEJADO DE LA PARANOIA INNECESARIA.

11. TENER POLÍTICAS DE PREVENCIÓN DE FUGAS DE DATOS (DLP)

INCLUYEN REGLAS QUE ESPECIFICAN LAS CONDICIONES Y LAS ACCIONES QUE SE LLEVARÁN A CABO SI NO SE CUMPLEN ESAS REGLAS.

CONTENIDOS

1. INTRODUCCIÓN
2. CAUSAS
3. CONSECUENCIAS
4. PREVENCIÓN
5. GESTIÓN DE LA FUGA DE INFORMACIÓN
6. FORMAS DE DETECTAR LA FUGA DE INFORMACIÓN
7. ACCIONES A REALIZAR

ESTO ES TODO