SALVAGUARDAS. PARTE I

AUTOR: LUIS RAMÍREZ LORÍA

MARZO: 2021

San Marcos

Tabla de contenido

Introducción

Dentro de los distintos modelos y normas de gestión de riesgo informático y sistemas de gestión de seguridad informática, analizados en las lecturas anteriores, se han establecido mecanismos y procesos clave como la definición de activos, la determinación y análisis de riesgos informáticos, la determinación de amenazas y los esquemas de tratamiento.

También se han analizado las recomendaciones y prácticas de Gestión de Seguridad promovidas en el Marco COBIT 5, las recomendaciones de las normas de Gobierno como la NIST 800-30, MAGERIT y OCTAVE y propiamente en nuestro país se han mencionado las Normas técnicas para la gestión y el control de las tecnologías de información de la Contraloría General de la República, todas herramientas que señalan recomendaciones para mejorar o asegurar los activos y recursos de tecnologías de información de las organizaciones.

Adicionalmente, en estos estudios y análisis se ha determinado que un factor crítico de éxito para que las organizaciones puedan responder a los riesgos y amenazas es el establecimiento de salvaguardas o contramedidas, las cuales se abordarán en esta lectura las asociadas con salvaguardas tales como:

- Salvaguardas lógicas en el acceso
- Salvaguardas lógicas por cifrado
- Salvaguardas técnicas en redes de cibernegocios
- Salvaguardas organizativas en el cibernegocio
- Salvaguardas preactivas en redes: antivirus, filtros, anti-intrusión
- Salvaguardas para desastres: planes y respaldo
- Salvaguardas de gestión: modelos de riesgos

Introducción Aplicación de las salvaguardas jurídico-organizativas: documento de seguridad

En el libro 1 sobre métodos, MAGERIT establece las salvaguardas de la siguiente forma:

> *"Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otras seguridad física y, por último, está la política de personal"* (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Durante la actividad de identificación de salvaguardas efectivas se requiere que la organización estime la eficacia que tiene cada una de estas contramedidas para mitigar los riesgos o amenazas.

En la metodología definida como MAGERIT existen varias etapas en las cuales se realiza un estudio de las contramedidas, buscando que puedan abarcar periodos cortos de tiempo o periodos largos (semestrales o anuales), entre estas fases están:

- Primera etapa: Potencial
  - Identificación de salvaguardas
  - Valoración de salvaguardas
- Segunda etapa. Situación actual
  - Identificación de salvaguardas
  - Valoración de salvaguardas
- Tercera etapa: Objetivo
  - Identificación de salvaguardas
  - Valoración de salvaguardas

A manera general las salvaguardas se pueden clasificar según su actuación en dos tipos:

- Salvaguardas preventivas, que actúan sobre la vulnerabilidad (antes de la agresión) reduciendo la potencialidad de materialización de la amenaza
- Salvaguardas curativas, que actúan sobre el impacto (tras la agresión) reduciendo su gravedad.

Según señalan los estándares, estos mecanismos se definen como el procedimiento o dispositivo, físico o lógico, que reduce el riesgo de forma preventiva o curativa. Se tipifica también según el recurso empleado por la organización o el grupo de activos del domino al que debe ser incorporado, lo cual será analizado durante el desarrollo de la presente lectura.

Los mecanismos de salvaguarda deben ser seleccionados en función de su efectividad y acordes con el activo o servicio por resguardar. En este sentido el concepto de efectividad del mecanismo de salvaguarda se mide bajo dos perspectivas:

- El grado de cumplimiento de su función o la bondad del mecanismo
- El grado de implementación del mecanismo dentro de los procesos asociados al activo.

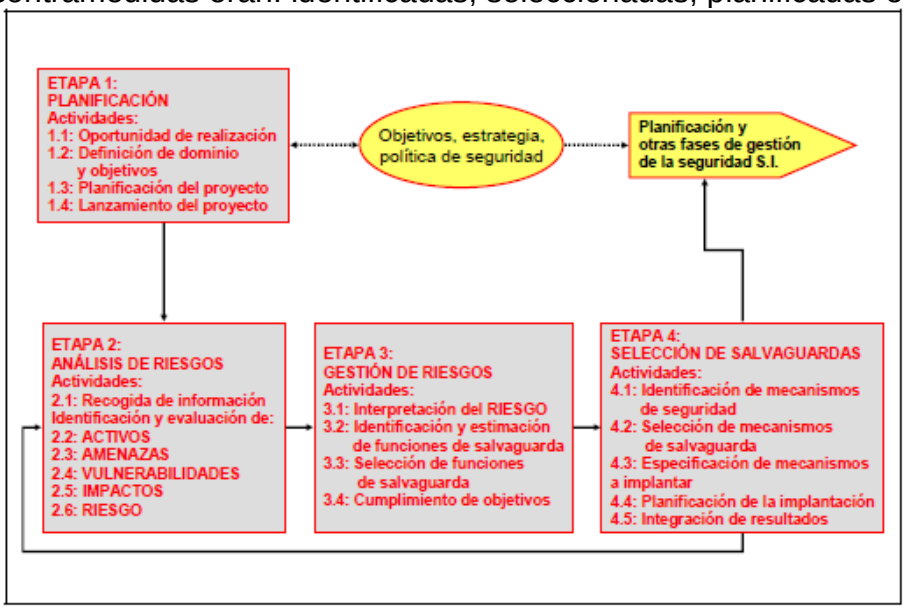
Identificación de salvaguardas

Esta actividad consiste, en la identificación y selección de las salvaguardas que se requieren para la protección de los activos, sistemas o información, para lo cual se requiere del criterio de un especialista en seguridad, quien puede materializar las funciones y servicios seleccionados en función de su efectividad.

La selección de las salvaguardas busca contrarrestar las amenazas identificadas para uno de los activos y busca implementar los mecanismos seleccionados con la ayuda de estándares o mejores prácticas, de forma que se logre definir los componentes del sistema que serán desarrollados, documentados, probados, implantados y aceptados, junto a los procesos de planificación y alineamiento aledaños a la implantación.

Valoración de salvaguardas

Durante la actividad de valoración se busca integrar los resultados de la operación de las salvaguardas, la comparación de costes, comparación entre la suma de los riesgos por amenaza y la suma de los costes de los mecanismos de contramedidas asociados a las amenazas, para evitar contradicciones en su aplicación y en su valoración. En la segunda versión de MAGERIT la etapa de salvaguardas aplicaba como un proceso independiente en el cual estas contramedidas eran: identificadas, seleccionadas, planificadas e integradas.



Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Ahora bien, en metodología MAGERIT v.3, el Paso de Salvaguardas señala: *"se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal."* (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

En este caso se recomienda seguir el siguiente flujo de procesos en lo que respecta a las salvaguardas, resumen tomado de MAGERIT, (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012):

Selección de salvaguardas

Considerar, si es necesario hacer una escogencia o criba inicial para quedarnos con aquellas que son relevantes para lo que hay que proteger, teniendo en cuenta los siguientes aspectos:

1. Tipo de activos a proteger, pues cada tipo se protege de una forma específica
2. Dimensión o dimensiones de seguridad que requieren protección
3. Amenazas de las que necesitamos protegernos
4. Si existen salvaguardas alternativas

Además, se puede establecer un principio de proporcionalidad y tener en cuenta:

1. El mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante
2. La mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes (ver zonas de riesgo)
3. La cobertura del riesgo que proporcionan salvaguardas alternativas

Esto lleva a dos tipos de declaraciones para excluir una cierta salvaguarda del conjunto de las que conviene analizar:

- **No aplica** – se dice cuando una salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración
- N**o se justifica** – se dice cuando la salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger.

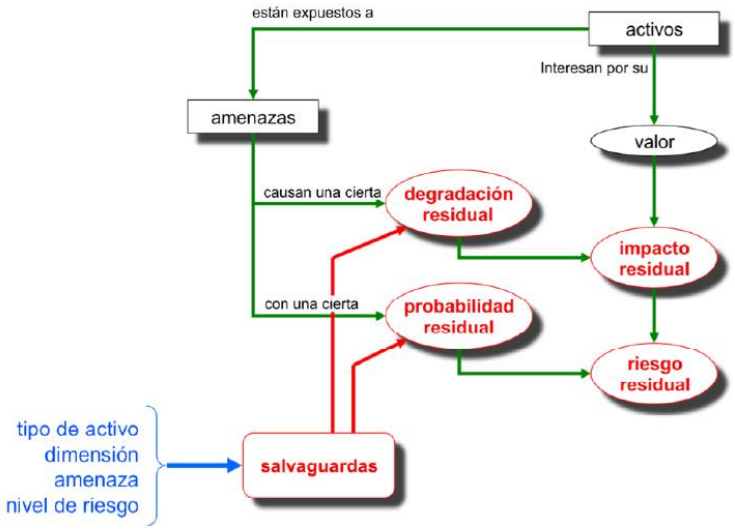
Como resultado se genera una **"declaración de aplicabilidad"** o relación de salvaguardas que deben ser analizadas como componentes nuestro sistema de protección.

Efecto de las salvaguardas

Las salvaguardas entran en el cálculo del riesgo de dos formas:

- Reduciendo la probabilidad de las amenazas.
    - Las salvaguardas preventivas. Llegan a impedir que la amenaza se materialice.

- Limitando el daño causado.
    - Unas limitan la posible degradación, otras permiten detectar inmediatamente el ataque para frenar que la degradación avance.
    - Algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.



Elementos de análisis del riesgo residual

Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Tipos de protección

Los tipos de protección son las posibles respuestas a las salvaguardas o contramedidas y por lo general se clasifican como:

- [PR] Prevención. Son preventivos y reducen la oportunidad de un incidente ocurra.
- [DR] Disuasión. Tiene un efecto tal sobre los atacantes que estos no se atreven o piensan varias veces el ataque.
- [EL] Eliminación. Elimina un incidente cuando impide que tenga lugar.
- [IM] Minimización del impacto. Limita el impacto cuando acota las consecuencias del incidente.
- [CR] Corrección. Repara el daño producido.
- [RC] Recuperación. Permite regresar al estado anterior al incidente.
- [MN] Monitorización. Monitorea lo que ha ocurrido y lo que está ocurriendo.
- [DC] Detección. Detecta e informa cuando un ataque está ocurriendo
- [AW] Concientización. Actividades de formación de las personas con nexos al sistema y que ejercen influencia sobre él.

- [AD] Administración. Componentes de Seguridad el sistema.

efecto	tipo
preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Tipos de salvaguardas

Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Eficacia de la protección

Evalúan la eficacia de la salvaguarda frente al riesgo, si es técnicamente idónea, si se emplea siempre, si es desplegada, configurada y mantenida correctamente, combina 2 factores:

- Desde el punto de vista técnico:
  - Es técnicamente idónea para enfrentarse al riesgo que protege
  - Se emplea siempre
- Desde el punto de vista de operación
  - Está perfectamente desplegada, configurada y mantenida
  - Existen procedimientos claros de uso normal y en caso de incidencias
  - Los usuarios están formados y concienciados
  - Existen controles que avisan de posibles fallos.

Para MAGERIT, medir los aspectos organizativos, se puede realizar empleando una escala de madurez que recoja en forma de factor corrector la confianza que merece el proceso de gestión de la salvaguarda:

factor	nivel	significado
0%	L0	inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	L5	optimizado

Eficacia y madures de las salvaguardas

Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Vulnerabilidades

Es toda debilidad aprovechada por una amenaza, tanto en el activo como en sus medidas de protección. Son vulnerabilidades todas las ausencias o ineficacias de las contramedidas pertinentes para salvaguardar el valor de un activo.

Continuando con el estudio de las salvaguardas, vamos a analizar varias de las más establecidas.

Salvaguardas lógicas en el acceso

En los estándares y mejores prácticas las salvaguardas lógicas en el acceso se categorizan dentro de las protecciones generales y horizontales en las cuales se sugiere que se establezcan controles para:

- Protecciones Generales
- Identificación y autenticación
- Control de acceso lógico
- Segregación de tareas
- Gestión de incidencias
- Herramientas de seguridad
- Herramienta contra código dañino
- Herramienta de detección / prevención de intrusión
- Herramienta de chequeo de configuración
- Herramienta de análisis de vulnerabilidades
- Herramienta de monitorización de tráfico
- Herramienta de monitorización de contenidos
- Herramienta para análisis de logs
- Honey net / honey pot
- Verificación de las funciones de seguridad
- Gestión de vulnerabilidades
- Registro y auditoría

Dentro de las medidas de protección o salvaguardas, las recomendaciones más efectivas son:

1. Mantener sistemas de autenticación fuertes y que incorporen evaluaciones biométricas.

2. Definir una política de control de acceso que permita la identificación de la información del usuario y sus actividades, que existan responsables de conceder, configurar y revocar accesos, con procedimientos para su solicitud, depuración y eliminación.
3. Establecer un registro de usuarios y un registro de accesos realizados, actualizado y con criterios de validación.
4. Gestionar los privilegios de acceso sobre principios de accesos por segregación de funciones (cada uno accede solo lo que necesite).
5. Gestionar claves de usuario, características técnicas, complejidad, prohibición de divulgación.
6. Revisión periódica de derechos de acceso a usuarios y funciones.
7. Establecer responsabilidades del usuario, políticas de uso de claves secretas, incluso la disposición de pantallas, cuando se atienen clientes.
8. Existencia de políticas de uso de servicios de red (internet, correo electrónico, redes sociales y otros)
9. Establecer mecanismos de autenticación y registro remoto, como redes privadas virtuales (VPN)
10. Separación de redes de servicios de información, grupos de usuarios, sistemas.
11. Control de conexiones realizadas desde fuera de la empresa
12. Control de acceso al sistema operativo, establecer un sistema de gestión de contraseñas, restricciones de uso del sistema operativo, cierre de sesiones, limitación de periodos para establecer sesiones.
13. Control de acceso a aplicaciones e información, por roles de lectura, escritura, modificación, incorporando aislamiento de información confidencial, cifrado integrado.
14. Políticas para trabajo en esquemas de movilidad, incluyendo comunicaciones móviles y teletrabajo.

Salvaguardas lógicas por cifrado

Las salvaguardas lógicas por cifrado ofrecen seguridad para aspectos tales como la suplantación de identidad, manipulación de la configuración y se recomienda por tanto emplear técnicas de criptografía para evitar una posible falla de pérdida de confidencialidad.

En la técnica de cifrado por sustitución quien envía el mensaje original, también llamado mensaje claro o mensaje plano, debe encriptarlo; es decir, escribirlo con una serie de claves o acomodos del texto plano, de tal forma que nadie lo pueda entender; en tanto, el receptor del mensaje deberá conocer cómo descifrar el mensaje a fin de entender con claridad el mensaje original o texto plano.

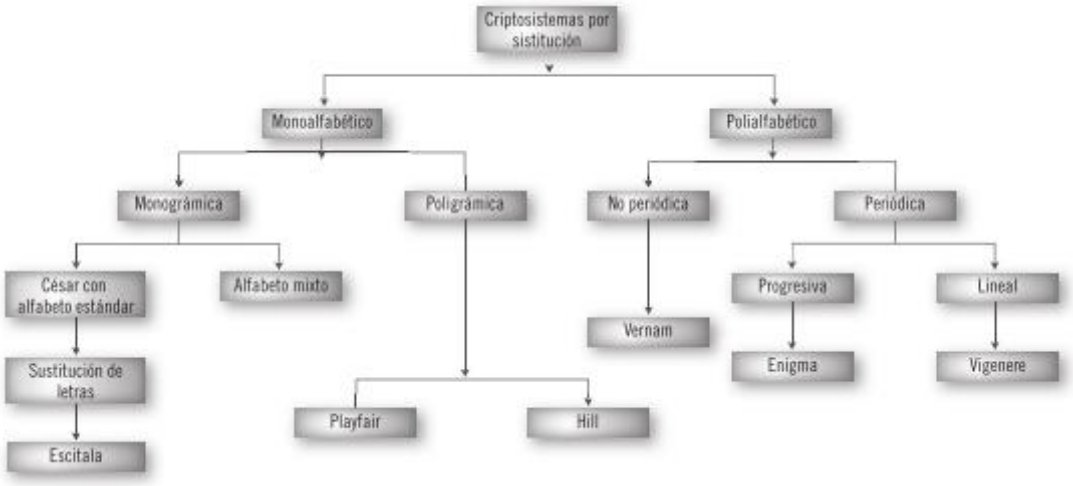
n la técnica de sustitución quien envía el mensaje original, también llamado mensaje claro o mensaje plano, debe encriptarlo; es decir, escribirlo con una serie de claves o acomodos del texto plano, de tal forma que nadie lo pueda entender; en tanto, el receptor del mensaje deberá conocer cómo descifrar el mensaje a fin de entender con claridad el mensaje original o texto plano.

“Lo importante de cifrar un mensaje es que la forma de descifrarlo sea por completo aleatoria; es decir, que una computadora en los tiempos actuales no sea capaz de encontrar la forma en la cual fue hecho, por lo que de ningún modo tendrá manera de descifrar el mensaje escrito.” (Baca Urbina, 2016). Estas salvaguardas se aplican a riesgos tales como:

- Intercepción de las comunicaciones.
- Análisis de tráfico.
- Protección de la Información.
- Copias de seguridad de los datos (backup).
- Aseguramiento de la integridad.
- Cifrado de la información.
- Uso de firmas electrónicas.
- Uso de servicios de fechado electrónico (time stamping).
- Gestión de claves criptográficas.
- Gestión de claves de cifra de información.
- Gestión de claves de firma de información.
- Gestión de claves para contenedores criptográficos.
- Gestión de claves de comunicaciones.
- Gestión de certificados

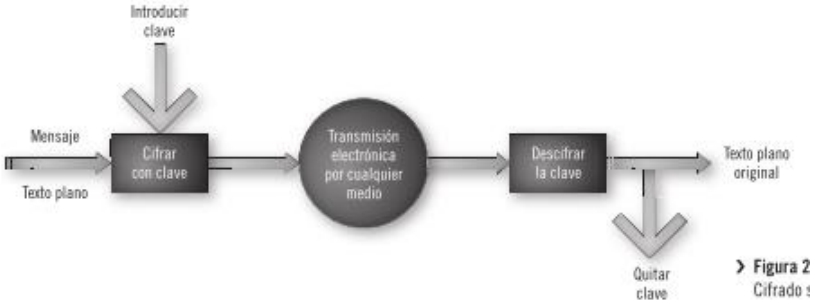
Dentro de las medidas de protección de cifrado, las tradicionales son, según Bacca:

1. Criptografía clásica: "Se conoce con este nombre a todos los métodos utilizados para encriptar información y que han pasado a la historia por alguna razón, ya sea porque fueron de los primeros de los que se tiene registro, porque los utilizó algún personaje famoso, porque en su tiempo se creían indescifrables y/o porque se utilizaron en conflictos bélicos y su descifrado determinó hacia cuál de los bandos beligerantes se inclinó la guerra” (Baca Urbina, 2016). Estos mecanismos no se aplican en el mundo de la computación, pero son una buena referencia para entender a qué se refiere el cifrado, pueden investigarse los más conocidos como el Cifrador de Hill, el Cifrador de Vigenere, Cifrador Playfair.



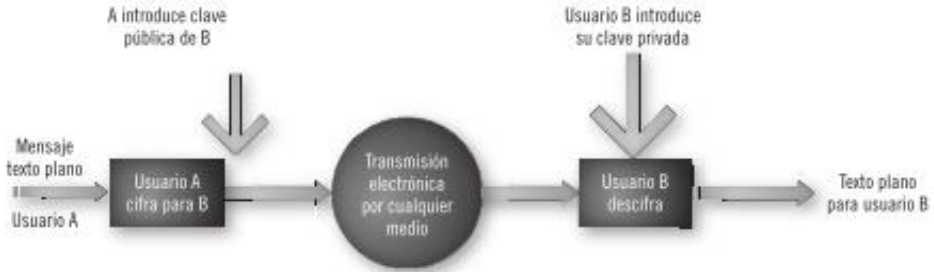
Criptosistemas clásicos por sustitución. Fuente: (Baca Urbina, 2016)

2. Cifrado DES (conocido por lo general como Triple DES, TDES, 3DES): Es un algoritmo para proteger datos mediante el uso de claves privadas de cifrado en 64 bits. *"En el cifrado o criptografía simétrica, tanto el emisor como el receptor del mensaje claro tienen una llave o clave secreta que se utiliza ya sea para cifrar o para descifrar el mensaje claro. Como el mensaje se transmite a través de medios inseguros y la información se considera muy importante, se hace necesario protegerla."* (Baca Urbina, 2016)



Cifrado simétrico. Fuente: (Baca Urbina, 2016)

Cifrado asimétrico: *"requiere de dos claves o llaves: una pública y la otra privada, las cuales están relacionadas matemáticamente. Desde el punto de vista de la computación, es muy difícil conocer la llave privada a través de la clave pública."* (Baca Urbina, 2016)



Cifrado asimétrico. Fuente: (Baca Urbina, 2016)

3. AES (Advanced Encryption Standard), es un cifrador simétrico de bloques, *"el cual tiene bloques de 128 bits y claves de 128, 192 y 256 bits. Dependiendo del tamaño de la clave, en AES las rondas pueden ser 10 si la clave es de 128 bits, 12 si la clave es de 192 bits y 14 si la clave es de 256 bits. El AES fue llamado así por el NIST. Fue publicado en 2001 con el fin de reemplazar al 3DES o TDES"* (Baca Urbina, 2016), Este cifrados realiza cuatro transformaciones matemáticas:
    a. Sustitución no lineal de bytes. Donde cada byte es reemplazado por otro de acuerdo con una tabla predeterminada de búsqueda.
    b. Mover de lugar las filas. En esta transformación cada fila es rotada de manera cíclica en determina número de veces.
    c. Combinar los cuatro bytes de cada columna utilizando una transformación lineal.
    d. Combinación de cada byte con la clave que se generó en cada ronda. Cada una de estas claves es una derivación de la clave de cifrado, efectuado una iteración de la clave mediante el uso de la operación XOR.

Funcionamiento del sistema de cifrado AES. Fuente: (Baca Urbina, 2016)

4. Otros sistemas de cifrado asimétrico son: DSA y ElGamal. En estos a pesar que la clave pública la puede obtener cualquier interesado, es imposible obtener la clave privada a partir de la clave pública. En la actualidad se han desarrollado claves asimétricas basadas en curvas elípticas que son menos costosa basadas en un logaritmo discreto, utilizando menos memoria y recursos de hardware para cifrar y descifrar.

Salvaguardas técnicas en redes de cibernegocios

A nivel de los negocios electrónicos, tan promovidos en los últimos años, es importante asegurar algunas condiciones relacionadas a las salvaguardas técnicas en las redes, los expertos de "Business Intelligence Limitada" nos recomiendan:

1. *“Mecanismos de cifrado y negocio electrónico. La protección de la confidencialidad, es percibida por los usuarios como esencial para sus asuntos, también para los electrónicos. La disponibilidad no es menos importante, como se ha visto con los citados ataques para conseguir la negación de servicio en los principales portales mundiales.*
2. Subestados de seguridad y funciones de información:
    a. Cibernegocio Cerrado: Se conoce como ‘Cibernegocio cerrado’ las transacciones entre empresas (Business to Business, BtoB, popularmente B2B). Éstas siguen constituyendo el 80% del Negocio electrónico con ayuda de las facilidades que aporta el Cibernegocio (red abierta y software asequible a las entidades pequeñas y medias). Las características más importantes del Cibernegocio Cerrado desde el punto de vista de la seguridad se ligan al carácter formalizado, bien reglamentado (a menudo contractualmente) y bilateral (relación uno a uno) entre unas entidades que suelen mantener relaciones repetitivas y diferidas (no interactivas). Estas características se dan igualmente en las transacciones entre Entidades Públicas (A2A, Administration to Administration, por ejemplo, la interconexión de Registros entre Administraciones) o entre una empresa y una Entidad Pública (B2A, Business to Administration)
    b. Cibernegocio abierto: Se conocen como ‘Cibernegocio abierto’ las transacciones entre entidades y consumidores ‘cibernautas’ (Business to Consumer, B2C) con posible venta ‘al por menor’. La venta de intangibles por este medio comporta procesos de negocio totalmente remodelados, con inclusión de micro transacciones y alquileres (pay per view, etc.). El pago suele ofrecer todas las variantes, agregadas o no (con micro pago antes o después del consumo), tarjetas de crédito o débito y monedero electrónico. Se pueden cubrir todos los escenarios de la venta (página-escaparate, portal-galería comercial, entrada en tienda-compra) y puede cambiar toda la cadena de valor en cuanto a la distribución, los productos intangibles o los servicios pre y postventa. Unos intermediarios desaparecen, pero pueden aparecer otros (tecnólogos, financieros, consultores).*” (Business Intelligent Limitada, 2020)

Salvaguardas organizativas en el cibernegocio

Las salvaguardas organizativas son mecanismos de prevención y gestión de las incidencias. Para la revista IT NOW, las 5 principales maneras de proteger la ciberseguridad de su empresa son:

1. *“Cifrado PGP*
    a. *Datos altamente sensibles como los números de seguro social, detalles de tarjetas de crédito y documentos que contenían secretos comerciales deben ser cifrados durante la transmisión de los datos, así como en el almacenamiento y copia de seguridad.*

b. *Hay muchos tipos de cifrado, la encriptación PGP (Pretty Good Privacy) es ampliamente utilizada para el intercambio de mensajes de correo electrónico de forma segura. Cuando se desea enviar PGP cifrado de correos electrónicos o archivos, primero debe obtener su clave pública para cifrar los datos. Al cifrar, se elige a quien desea descifrar los datos, y sólo aquellos que se designe pueden hacerlo. Cuando las personas reciben los datos cifrados con su clave pública, utilizan su clave privada para descifrarlo.*

2. *Firewalls y software UTM*

   a. *Un servidor de seguridad es uno de los puntos más cruciales de seguridad en una red, la protección de la red a un acceso no autorizado y de Internet.*

   b. *Los firewalls típicamente incluyen enrutamiento y otras funciones básicas del servidor de red. Además, muchos de ellos también incluyen lo que se conoce como Gestión Unificada de Amenazas (UTM), lo que proporciona una mayor protección de red, como antivirus, antispam, opciones portal cautivo (que exigen a los usuarios interactuar con una página Web intermedia, a menudo un inicio de sesión de página, antes de que puedan acceder a la Web) y filtrado de contenidos.*

3. *Informática forense*

   a. *Su objetivo es la investigación de sistemas de información para poder detectar cualquier clase de evidencia de vulnerabilidad que puedan tener. Asimismo, se persiguen diferentes objetivos de prevención, intentando anticiparse a lo que pudiera pasar, así como establecer una solución rápida cuando las vulnerabilidades ya se han producido.*

   b. *El papel que tiene la informática forense es principalmente preventivo y nos ayuda, mediante diferentes técnicas a probar que los sistemas de seguridad que tenemos implementados son los adecuados para poder corregir errores y poder mejorar el sistema además de conseguir la elaboración de políticas de seguridad y la utilización de determinados sistemas para poder mejorar tanto el rendimiento como la seguridad del sistema de información.*

4. *Análisis de vulnerabilidad*

   a. *El análisis de vulnerabilidad comprueba a través de herramientas de software y servicios de consultoría la debilidad o fortaleza ante el conjunto de amenazas conocidas al día de la evaluación tanto para elementos externos (Servicios SAAS, Servicios de Cloud Computing, Servicios BYOD, Usuarios no autorizados, sniffers,) como para elementos internos (Usuarios, sistemas implementados, estaciones de trabajo, dispositivos móviles, sistemas operativos, etc.)*

   b. *Un correcto análisis de vulnerabilidades no solo detecta las áreas de mejora, sino que también propone la correcta arquitectura necesaria para proteger la infraestructura de una organización y los diferentes cambios de políticas de*

seguridad que se requiere implementar para asegurar una continuidad de operación, la asistencia que se debe proveer cuando se ve comprometida la seguridad informática y la recuperación ante desastres ante amenazas e intrusiones.

5. *Establecer un sistema de detección de intrusos*
    a. *Un sistema de detección de intrusión (IDS) es complementario a un servidor de seguridad. Un servidor de seguridad ofrece una protección similar a un muro alrededor de su red; puede designar ciertos puertos TCP o UDP, donde sólo el tráfico específico de Internet y de la red puede pasar. Otros puertos y el tráfico están bloqueados, pero un firewall básico no alerta que usted rompa los intentos o detenga el tráfico no autorizado para entrar en la red a través de otros medios. Un IDS, por otro lado, es como tener guardias de seguridad colocados alrededor de la pared y el interior de la zona restringida para detectar y detener otras numerosas amenazas."* (Editorial IT NOW, 2019)

Salvaguardas preactivas en redes: antivirus, filtros, anti-intrusión

A nivel de los negocios electrónicos, tan promovidos en los últimos años, es importante asegurar algunas condiciones relacionadas a las salvaguardas técnicas en las redes, los expertos de "Business Intelligence Limitada" nos recomiendan:

1. *"Filtros y cortafuegos (firewall): Para controlar el acceso, rutas y accesibilidad de terceros a los flujos de información, se instalan mecanismos de filtro en los nodos-conectores de las redes. El firewall es un dispositivo lógico, más o menos sofisticado (simple encaminador o con capacidad de cómputo) que separa un dominio de red de otro; aplica operaciones de filtrado de paquetes en los niveles 3/4 de red/transporte y permite tomar decisiones de seguridad basadas en la información de los 'sobres' o 'cabeceras' de dichos paquetes (dirección fuente y número de puerto). El cortafuegos tiene por tanto funciones de separación, limitación y análisis del flujo de la información que circula entre sus dos puertas a ambos dominios. Como ejerce un control de acceso centralizado, su efectividad exige que lo atraviese todo usuario interno/exterior/remoto para acceder desde/a las redes internas protegidas.*
2. *Proxy: Un cortafuegos al nivel de la aplicación se suele llamar sistema 'proxy· porque trata como 'apoderado' de los usuarios-clientes internos que solicitan servicios con los servidores externos de Internet. Si se configura bien, controla el acceso a servicios individuales simulando ser el origen de todo el tráfico entrante (que no tienen en cuenta el destinatario final del servicio) e incluso puede hacerse cargo del tráfico interno. Requiere un módulo proxy específico para cada tipo de servicio). Su mayor coste y seguridad se compensa con ciertas ventajas: puede configurarse como la única dirección de computador visible para la red externa; proporciona un registro (logging) detallado; al usar proxies distintos para los servicios protege incluso contra los computadores internos mal configurados o no seguros; y soporta autentificación 'fuerte' del usuario en dos niveles, el clásico de identificador+contraseña (poco*

robusto contra ataques de 'husmeadores' o sniffers) y otro más sofisticado, con técnicas de retrollamada (call-back), de claves de un sólo uso (one time passwords, OTPs) o de Claves públicas certificadas (que se verán en el capítulo de cifrado).

3. *Firewall Agente - Un cortafuegos al nivel de agente activo, llega a poder controlar el contenido de los accesos a los servicios (por ejemplo, evitando virus, impidiendo el acceso a servicios de carácter no profesional, imponiendo límites al volumen de información en tránsito, etc.). Se apoya en arquitecturas hibridas de los dos niveles citados.*
4. *Scanners. Estos mecanismos son paquetes integrados que combinan la nueva generación de 'proxies adaptativos' con mecanismos 'patrulladores' (scanners) por el sistema protegido (no sólo defensores de su perímetro, como hacen los cortafuegos originales) con administradores de la red interna (que reaccionan a los fallos internos con alertas y/o acciones) y con Sistemas Detectores de Intrusiones IDS (que reaccionan a los intentos de ataque exterior con alertas y/o acciones).*
5. *Sensores. El mecanismo central de estos mecanismos es un 'orquestador de eventos' que recibe entradas de varios ¶sensores· externos e internos (antivirus, patrullador-detector de puntos de vulnerabilidad) y se configura para cumplir una política de seguridad con varios tipos de reglas registradas (adecuadas a los escenarios detectables) para desembocar en distintos ¶actuadores· o salidas (informes, centro de comunicaciones de seguridad con consulta en línea o help-desk, disparo de acciones, etc.)."* (Business Intelligent Limitada, 2020)

Salvaguardas para desastres: planes y respaldo

Acorde con la metodología MAGERIT existen una serie de amenazas sobre los activos de un sistema de información que pueden deberse a desastres de distintas naturalezas, tales como:

- Desastres naturales: Catalogados como sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta de la acción de la naturaleza, tales como fuego o incendios, daños por agua, inundaciones, rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, fenómeno de origen volcánico, entre otros.
- Desastres industriales: desastres debidos a la actividad humana tales como explosiones, derrumbes, efectos de la contaminación química, efectos de las sobrecargas eléctricas, fluctuaciones eléctricas, accidentes de tráfico o tránsito.
- Contaminación mecánica: Vibraciones, polvo, suciedad.
- Condiciones inadecuadas: Temperatura, humedad, deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad.
- Emanaciones electromagnéticas: El cual se caracteriza por el hecho de poner vía

radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.

Según Romero Castro y otros, la forma de establecer salvaguardas para este tipo de amenazas es el establecimiento de planes de mitigación de riesgo, modelos de respaldo y alta disponibilidad de las infraestructuras de servicios. Acorde a estos autores se deben establecer:

- Protocolos y políticas de actuación o respuesta a eventos.
- Planes de recuperación de desastres.
- Planes de contingencia
- Protocolos de gestión de incidentes. Asignado un organigrama de responsabilidades a cada equipo de trabajo y ocupándose de la comunicación de los mismos, así como de las normas que deben cumplirse a toda la plantilla de la organización.

Plan de seguridad informática. Fuente: (Romero Castro, y otros, 2018)

Por su parte, Francisco nos señala sobre el riesgo de desastres o catástrofes naturales, riesgos de incendio, riesgos como inundaciones, fallas de suministro eléctrico y otros que suponen indisponibilidad de nuestros servicios en línea, deben incorporarse como amenazas y deben ser incluidos en el plan de gestión debe atenderlos por igual. El autor nos da la siguiente clasificación:

- *"Vulnerabilidad: cualquier situación o debilidad latente en el sistema o algunos de sus componentes que hace posible que una amenaza se materialice. Así, por ejemplo, puertos de switch sin asegurar, sistemas operativos sin los parches de seguridad actualizados, firewall desactivados, usuarios de la red que dejan sus sesiones abiertas, empleados que no actualizan de forma frecuente sus credenciales de acceso, personal de confianza y manejo que administra opciones de seguridad sin contar con la preparación o madurez requeridas, entre muchas otras debilidades que deben detectar de forma oportuna en un sistema de gestión de seguridad informática orientada al riesgo.*
- *Superficie de ataque: la sumatoria total de las vulnerabilidades en un sistema que hacen posible que un atacante pueda acceder a él o causar afectaciones. Desde la perspectiva de esta definición, si el sistema operativo de un PC con*

Windows 8 no se encuentra actualizado con los últimos parches de seguridad y en su navegador web el nivel de confianza se encuentra con niveles bajos o también si está desactualizado, esta es una superficie de ataque.

- *Exploits: programas, herramientas o técnicas que se pueden usar para acceder a información o a un sistema al que no se tiene acceso autorizado al aprovechar vulnerabilidades que se han detectado previamente o durante el momento del ataque. Los exploits se catalogan como remotos o locales. En el caso de los remotos, se ejecuta el intento de ataque sin contar con acceso al sistema que se desea comprometer, es decir, el atacante no tiene acceso previo al sistema a través de ningún método físico o lógico. Los locales se ejecutan desde una cuenta de usuario o desde un usuario autorizado en el sistema atacado, no necesariamente se debe ejecutar desde un equipo al interior del sistema, pero para su ejecución se requieren credenciales o acceso a la red o al sistema.* (López, 2018)

Salvaguardas de gestión: modelos de riesgos.

Para determinar adecuadamente lo que refieren las mejores prácticas como el COBIT o el RISK IT, la norma ISO 31000 o el estándar de COSO (con la Gestión de Riesgo Empresarial (ERM)), sobre la optimización de los riesgos, primero debemos recordar algunas definiciones iniciales.

En este sentido acorde a los señalado por Helena, tenemos las siguientes definiciones:

- *Riesgo se define como: "el potencial que una amenaza dada aprovechará las vulnerabilidades de un activo o grupo de activos para causar pérdida o daño a los activos."*
- *Riesgo residual se define como: "Riesgo que permanece después de que se han implementado las salvaguardas."*
- *Análisis de riesgo se define como "el proceso de identificar los riesgos de seguridad, determinar su magnitud e identificar las áreas que necesitan salvaguardas".*
- *Gestión del riesgo es "el proceso de evaluar y cuantificar el riesgo y establecer un nivel aceptable de riesgo para la organización"*
- *Principios de gobernanza sobre riesgos:*
  - *"La gestión de riesgos de TI debe formar parte integral de la gestión de riesgos corporativa".*
  - *"Comités de riesgo y auditoría deben asistir a la junta en el cumplimiento de sus responsabilidades de TI"* (Garbarino Alberti, 2014)

Una adecuada gestión del riesgo de las TI, inicia por la identificación de la utilidad de su gestión por parte de la alta administración (conciencia del riesgo), de manera que se genere el apetito por el riesgo en la organización, y se logre comprender el beneficio del cumplimiento de objetivos de gestión de riesgos, establecer modelos de transparencia en

el tratamiento de riesgos (al inicio lo más relevantes por impacto, visibilidad o criticidad del negocio), definir claramente las responsabilidades de su gestión en la organización, de forma que se puede administrar o gerenciar el riesgo (evaluar, mitigar, evitar o aceptar), abarcando desde los procesos críticos de negocio hasta la seguridad de la información (sumamente relevante en la actual revolución 4.0).

Gestionar los riesgos, en la mayor parte de los marcos y mejores prácticas implica en primer lugar establecer los elementos a considerar en el perfil de riesgos de la empresa, mediante una completa descripción de las implicaciones para el negocio, el desarrollo de hipótesis, de métodos para describir los riesgos de forma homologada y comprender las técnicas para cuantificar riesgos y cuáles son los factores que los generan. Complementándose con el alineamiento de los riesgos con los objetivos del negocio y con el establecimiento de la comunicación e impacto de los riesgos de TI.

Otra acción fundamental es propiamente la definición del proceso de gestión de riesgos, sus fundamentos, modelo de gestión, procesos, cadena de valor y de responsabilidades, según los ámbitos estratégicos, tácticos (carteras, portafolios, proyectos), operativos, lo cual implica a nivel de gobernanza de las TI cubrir aspectos como el gobierno del riesgo, la evaluación y las acciones de respuesta, concordando su definición con el alineamiento a los objetivos de negocio.

COBIT 5.

Dentro del modelo de referencia de procesos de COBIT 5, existen una serie de agrupaciones de la mejores prácticas y recomendaciones relacionados con el Gobierno de TI que engloban procesos relacionados con los dominios de Evaluación, Orientación y Supervisión (EDM), Alineamiento, Planificación y Organización (APO), Construcción, Adquisición e Implementación (BAI), Entregar, Dar Servicio y Soportar (DSS) y por último Supervisar, Evaluar y Valorar (MEA), dentro de los cuales se establecen las recomendaciones correspondientes para Gestionar el Riesgo, y para el Aseguramiento de la Optimización del Riesgo.

APO12 Gestionar el riesgo

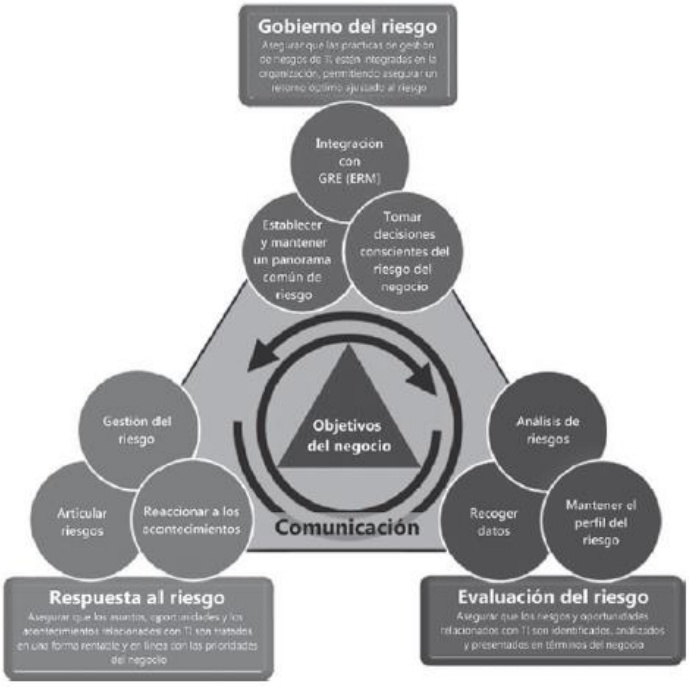
El proceso descrito por ISACA, (ISACA®, 2012), sobre la gestión del riesgo, dispone prácticas adecuadas para identificar, evaluar y reducir los riesgos de TI de una forma continua, y busca mantener estos riesgos / consecuencias, dentro de los niveles de tolerancia establecidos por la dirección de la empresa, incorporando para ellos seis procesos:

1. APO12.01 Recopilar datos
2. APO12.02 Analizar el riesgo
3. APO12.03 Mantener un perfil de riesgo
4. APO12.04 Expresar el riesgo

5. APO12.05 Definir un portafolio de acciones para la gestión de riesgos
6. APO12.06 Responder al riesgo.

RISK TI o RISK FOR COBIT

El marco para la gestión de riesgos de TI, conocido como RISK IT, es también una iniciativa de ISACA, y fue desarrollada como un complemento de COBIT, teniendo en cuenta el marco de controles planteados sobre el Gobierno de TI. Este marco de riesgos (RISK-IT) es un conjunto de principios, guías, procesos de negocio y directrices, el cual está conformado por tres ámbitos y nueve procesos interrelacionados, tal cual se puede ver en la siguiente figura resumida por ISACA:



Fuente: (ISACA IT RISK, 2009)

Según ISACA, (ISACA IT RISK, 2009), "*RISK IT se define y se basa en una serie de guías para la gestión eficaz de los riesgos de TI. Dichas guías se basan en los principios comúnmente aceptados en ERM, que se han aplicado en el ámbito de las TI. El modelo del proceso de los riesgos de TI está diseñado y estructurado para que las organizaciones puedan poner los principios en práctica y comparar sus resultados.*

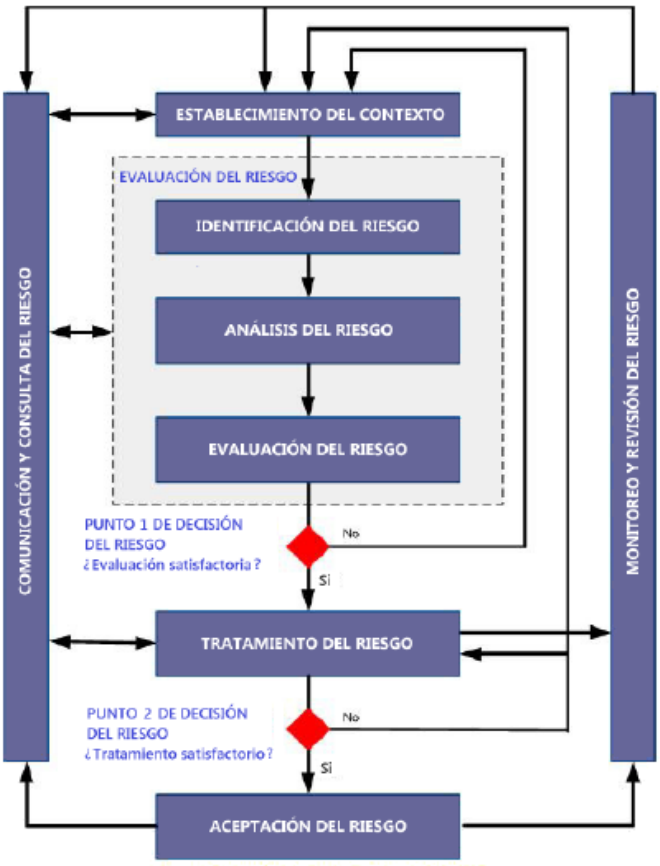
ISO/IEC 27000 / 27005

Al igual que otras normas ISO es utilizada para la estandarización y certificación en las directrices asociadas a la gestión de riesgos en los procesos asociados con las Tecnologías

de Información, en cuanto a aspectos de sistemas de gestión de seguridad de la información, estas se ubican en la norma ISO/IEC 27001:2013 y a nivel de estructura este es muy similar a la ISO 31000 la cual se explicará adelante en el curso, y propiamente a nivel de directrices sobre gestión de riesgos de seguridad de la información se ubican en la ISO/IEC 27005.

Procedimiento ISO/IEC 27005

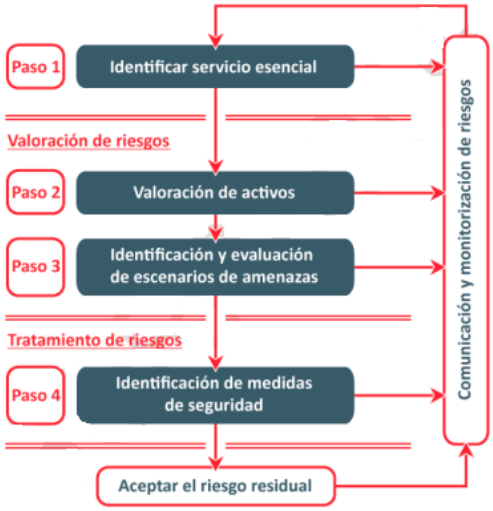
Este procedimiento consiste en a) establecer el contexto (asociado a los procesos de negocio y al riesgo), b) evaluar el riesgo o los riesgos existentes (bajo los pasos de identificación, análisis y evaluación de riesgos), c) establecer el esquema, modelo o acciones de tratamiento del riesgo, d) acepta o gestionar el riesgo residual e) comunicar el riesgo a los interesados d) realizar acciones de revisión y monitoreo, estas dos últimas se ejecutan de manera transversal durante todo el proceso como puede verse en la figura:

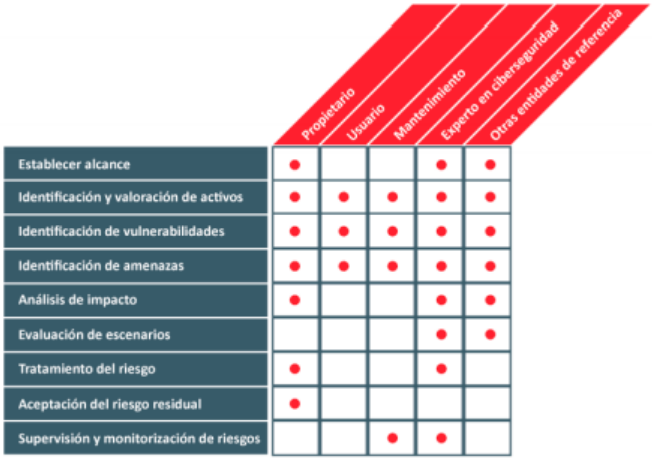


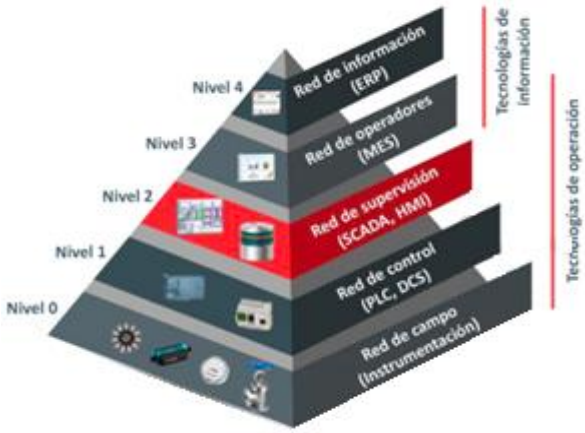
Fuente: (Alfaro Campos, 2017)

Otro de los modelos más orientado al tema de Ciberseguridad es la metodología de Análisis de Riesgos Ligero de Ciberseguridad Industrial (ARLI-CIB), cuyo establecimiento e implementación permiten un acercamiento específico y también ligero, orientado al análisis de riesgos de ciberseguridad en sistemas de control industrial.

“ARLI-CIB proporciona una herramienta para facilitar la aplicación, por parte de los operadores de sistemas de control industrial, de la metodología del análisis de riesgos de ciberseguridad.







Fuente: (CERT DE SEGURIDAD E INDUSTRIA, 2016)

El enfoque propuesto por el Modelo de Análisis de Riesgos de Ciberseguridad en Sistemas de Control Industrial desarrollado a lo largo de esta guía, pasa por:

i. Delimitar el alcance del análisis;
ii. Identificar los activos y las amenazas a que puedan estar sujetos;
iii. Estimar el impacto potencial de las mismas;
iv. Evaluar la probabilidad de que los escenarios de riesgo, construidos a partir de esas

amenazas, se materialicen

v. Sugerir una serie de medidas de protección, de aplicación a la instalación objeto de análisis, dentro del alcance definido.

Conclusiones y recomendaciones

Al analizar las distintas salvaguardas recomendadas por los expertos en análisis de riesgos informáticos podemos identificar una amplia gama de naturalezas de riesgo y por tanto, los elementos para brindar respuesta efectiva mediante contramedidas, medidas preventivas, correctivas o de respuesta general abren un gran abanico de posibilidades de acción, lo cual permite a las nuevas organizaciones que ingresan en el mundo de la tecnología o a las organizaciones en general que poseen dependencia de éstas, el analizar, según sus marcos de trabajo y niveles de automatización de procesos o dependencia tecnológica, el establecimiento de aquellos elementos que consideren prioritarios para resguardar o salvaguardar sus activos de información.

Una apropiada gestión de riesgos informáticos debe incluir un plan de respuesta a la materialización de los riesgos y con esto la formulación e implementación de contramedidas que brinde una protección a las organizaciones inmersas en los mundos digitales donde la dependencia de los recursos de tecnología de información y comunicaciones (recursos TIC) implica en sí misma una erogación importante, por lo cual el plan deben priorizar aquellas salvaguardas que mejoren las condiciones de los activos estratégicos de la organización o bien de aquellos elementos y componentes técnicos que coadyuven en mayor medida a la consecución de los objetivos del negocio, la relación con el cliente, los procesos productivos y todas aquellas condiciones que brinden estabilidad y operatividad al negocio.

Con el estudio de estas condiciones y el entendimiento y abordaje de las contramedidas el estudiante se prepara para enfrentarse con un vector diferenciado de las TIC, el establecimiento de medidas de respuesta y salvamento de los activos de información, lo cual genera un conocimiento importante y un nivel de profesionalización muy requerido por los mercados digitales actuales por lo cual la Universidad San Marcos busca posicionar al estudiante como un profesional que sea diferenciado y a la vez requerido en el mercado laboral actual.

Para mejorar los conceptos asociados a salvaguardas de seguridad es importante que el estudiante amplíe los conocimientos mediante la lectura del documento adjunto:

- https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/.
- https://www.incibe-cert.es/sites/default/files/paginas/publicaciones/ensi/ensi_arli-cib_01_metodologia-aarr_borrador.pdf
- Referente Pensamiento Eje 3. ANÁLISIS DE RIESGOS INFORMÁTICOS. Pongamos en práctica

Referencias bibliográficas

- Alfaro Campos, J. C. (2017). *Metodología para la gestión de riesgos de TI basada en COBIT 5.* Cartago, Costa Rica: Instituto Tecnológico de Costa Rica.
- Baca Urbina, G. (2016). *Introducción a la Seguridad Informática* (Primera ed.). México: Grupo Editorial Patria. Obtenido de https://elibro.net/es/ereader/usanmarcos/40458
- Business Intelligent Limitada. (15 de Enero de 2020). *https://www.solucionesalnegocio.com/.* Obtenido de http://www.business-intelligent.com/cibercomercio.pdf
- CERT DE SEGURIDAD E INDUSTRIA. (2016). *ENSI_ARLI-CIB_01- Modelo de Análisis de Riesgos Ligero de Ciberseguridad en Sistemas de Control Industrial (ARLI-CIB).* España: Gobierno de España. Obtenido de https://www.incibe-cert.es/sites/default/files/paginas/publicaciones/ensi/ensi_arli-cib_01_metodologia-aarr_borrador.pdf
- Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT Versión 3.0. Metodología de análisis y gestión de riesgo de los sistemas de información.* Madrid: Gobierno de España.
- Editorial IT NOW. (29 de Abril de 2019). *Revista IT NOW.* Obtenido de https://revistaitnow.com/5-maneras-de-proteger-la-ciberseguridad-de-su-empresa/
- Garbarino Alberti, H. (2014). *Marco de Gobernanza de TI para empresas PyMEs - SMEsITGF.* Madrid: Universidad Politécnica Madrid.
- ISACA IT RISK. (2009). *Marco de Riesgos de TI.* Estados Unidos de América: ISACA.
- ISACA®. (2012). *Cobit 5. Procesos Catalizadores.* Estados Unidos: ISACA.
- LaRepublica.Net. (20 de 02 de 2020). *LaRepublica.net*. Obtenido de https://www.larepublica.net/noticia/costa-rica-registro-casi-32-millones-de-intentos-de-ciberataques-en-primeros-tres-meses
- López, L. F. (2018). *Análisis de riesgos informáticos. Eje 1. Conceptualicemos.* Fundación Universitaria del Área Andina.
- Madrigal Chaves, W. (2019). *SUWA Universidad San Marcos, Repositorio.* Obtenido de http://repositorio.usam.ac.cr/xmlui/
- Real Academia Española. (12 de 12 de 2020). *Diccionario de la Lengua Española*. Obtenido de https://dle.rae.es/
- Red Global de Conocimientos en Auditoría y Control Interno. (01 de 01 de 2021). *www.Auditool.com*. Obtenido de https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque
- Romero Castro, M. I., Figueroa Moran, G. L., Vera Navarrete, D. S., Álava Cruzatty,

J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Alcoy - Alicante, España: Editorial Área de Innovación y Desarrollo,S.L. doi:http://dx.doi.org/10.17993/IngyTec.2018.46

- UNICEM. (22 de 12 de 2020). *El Modelo OSI*. Obtenido de http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica