**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| **PROGRAMA DE FORMACIÓN** | **Tecnología en Desarrollo e Implementación de Soluciones para la Transformación Digital** |

|  |  |
| --- | --- |
| **NÚMERO DEL COMPONENTE FORMATIVO** | 3 |
| **NOMBRE DEL COMPONENTE FORMATIVO** | Metodologías de Análisis y Valuación de Riesgos |
| **BREVE DESCRIPCIÓN** | En este componente formativo hablaremos de algunas de las metodologías de análisis y valuación de activos más usadas en el desarrollo de sistemas de gestión de seguridad de la información, y en particular a manera de ejemplo mostraremos el proceso utilizando para ello NIST SP-830. |
| **PALABRAS CLAVE** | Activos, SP830, NIST, confidencialidad, integridad, disponibilidad, CISO, activo, riesgo, amenaza, vulnerabilidad, impacto |

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPETENCIA** | 220501108 diagnóstico del estado actual de la ciberseguridad de la organización. | **RESULTADOS DE APRENDIZAJE** | 220501108-02 Construir el plan de tratamiento de riesgos de ciberseguridad acorde con metodologías de análisis y valoración. |

|  |  |
| --- | --- |
| **AREA OCUPACIONAL** | No Aplica |
| **IDIOMA** | Español |

1. **TABLA DE CONTENIDOS:**

**Introducción**

* 1. **Caracterización de las metodologías de análisis y valuación de riesgos**
  2. Objetivos de las metodologías de análisis y valuación de riesgos
  3. Que es el análisis de Riesgos

1.3 Determinar el contexto

1.3.1 Concepto

1.3.2 Dominio o grupos de controles

1.3.3 Objetivo de control

1.3.4 Objetivos

1.3.5 Alcance

1.3.6 Aplicabilidad

1.3.7 Técnicas de planificación

1.3.8 Conceptos a tener en cuenta

1.3.9 Tipos de objetivos de seguridad.

1.3.10 Características

1. **Metodologías de Análisis y valuación de Activos**
   1. **Magerit**
      1. Objetivos de Magerit
         1. Directos
         2. Indirectos
   2. **Octave**

2.2.1 Objetivos

2.2.2 Equipo de Análisis de Riesgos

2.2.3 Fases del método propuesto por Octave

**2.3 Metodología CORAS (COnstruct a platform for Risk Analysis of Security critical system)**

**2.4 Metodología MEHARI**

2.4.1 Introducción general de la utilización de MEHARI

2.4.2 Fases de la metodología MEHARI

2.4.2.1 Análisis o evaluación de Riesgos

2.4.2.2 Evaluaciones de Seguridad

2.4.2.3 Análisis de Amenazas

**2.5 Nist SP-830 . (National Institute of Standards and Technology)**

**2.5.1** Objetivos

2.5.2 Caracterización del sistema

2.5.3 Valuación de Activos

2.5.4 Identificación de amenazas

2.5.5 Valuación de amenazas

2.5.6 Identificación de vulnerabilidades

2.5.7 Análisis de controles

2.5.8 Determinación de probabilidades

2.5.9 Análisis de Impacto

2.5.10 Determinación del riesgo

2.5.11 Recomendaciones de Controles

2.5.12 Documentación de Resultados

1. **DESARROLLO DE CONTENIDOS:**

**Introducción**

Esta actividad de aprendizaje nos lleva a adquirir los conocimientos referentes a las metodologías de análisis y valuación de activos de mayor uso y en la aplicación de una de estas a partir del caso de estudio propuesto en el componente formativo anterior.

1. **Características de las metodologías de Análisis y Valuación de Riesgos**

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

El análisis de riesgos es el primer punto de la gestión de la seguridad de la información de una organización, y es necesario para realizar la gestión de los riesgos, es decir, tomar la decisión de eliminarlos, ignorarlos, transferirlos o mitigarlos y controlarlos, es decir realizar la gestión de riesgos.

Por esta razón se hace imprescindible la utilización o adopción de una metodología que le permita al personal de tecnología realizar el proceso de una manera más ordenada, especializada y ajustada a las necesidades propias de cada organización.

* 1. **Objetivos de las metodologías de análisis y valuación de activos**

Tanto en las metodologías acá estudiadas como la que se desarrollará el ejemplo tienen por objetivo los siguientes puntos:

* Planificación de la reducción de riesgos
* Planificación de la prevención de accidentes
* Visualización y detección de las debilidades existentes en los sistemas
* Ayuda en la toma de las mejores decisiones en materia de seguridad de la información
  1. **Que es el análisis de Riesgos**

Es la consideración sistemática del daño probable que puede causar en el negocio un fallo en la seguridad de la información con las consecuencias potenciales de perdida de confidencialidad, integridad y la disponibilidad de la información.

Para el proceso de implementación de una estrategia de gestión de la seguridad en una organización, se sugiere hacer uso de la norma ISO/IEC 27001:2022, ya que esta norma nos brinda los lineamientos e instrucciones para su establecimiento, además de presentarnos los fundamentos y aspecto más relevantes para su implementación, nos presenta bajo su anexo A, un esquema de controles de seguridad los cuales buscan abordar los aspectos más importantes para su adopción en el aseguramiento de los activos de información mediante el establecimiento de los objetivos de seguridad.

* 1. **Determinar el contexto**

En el ejercicio de implementación de estrategias de seguridad en las organizaciones es conveniente conocer el contexto sobre el cual se realizarán las acciones que buscan el aseguramiento de los activos de información, esto nos permite valorar los activos, valuar el riesgo presente, dimensionar los controles a utilizar, así como identificar los recursos y tiempo necesario para su implementación.

* + 1. **Concepto**

El estándar ISO/IEC 27001:2012 nos presenta directrices para implementar SGSI en una organización, esta permite llevar a cabo el proceso de implementación, dentro de este proceso se desarrolla un componente de los más críticos e importantes como es el análisis de riesgos, el cual nos permite reconocer el nivel de seguridad previo de los activos de información en una organización; a partir de este análisis se propone un plan de trabajo que involucra la determinación del plan de acción a desarrollar con el objetivo de reducir el riesgo en la organización.

Esta norma cuenta con el anexo A en la cual se definen los Objetivos de Control y Controles de Referencia que permite identificar los controles de seguridad a implementar en la organización y esta se establece mediante el documento denominado Declaración de Aplicabilidad, a continuación, reconoceremos algunos conceptos importantes a tener encuentra en el ejercicio de la determinación del plan de trabajo para la implementación de la ciberseguridad.

* + 1. **Dominio o grupos de controles**

categorías de seguridad que abordan los principales dominios a tener presente en el establecimiento de la seguridad, la norma actualmente se encuentra estructurada por 4 grandes grupos de controles y un total de 93 controles que representan los niveles de seguridad como son: organizativos, de personas, físicos y tecnológicos, y que estos también se pueden identificar desde el ámbito estratégico como como operativo como se puede observar en la Imagen No. 1



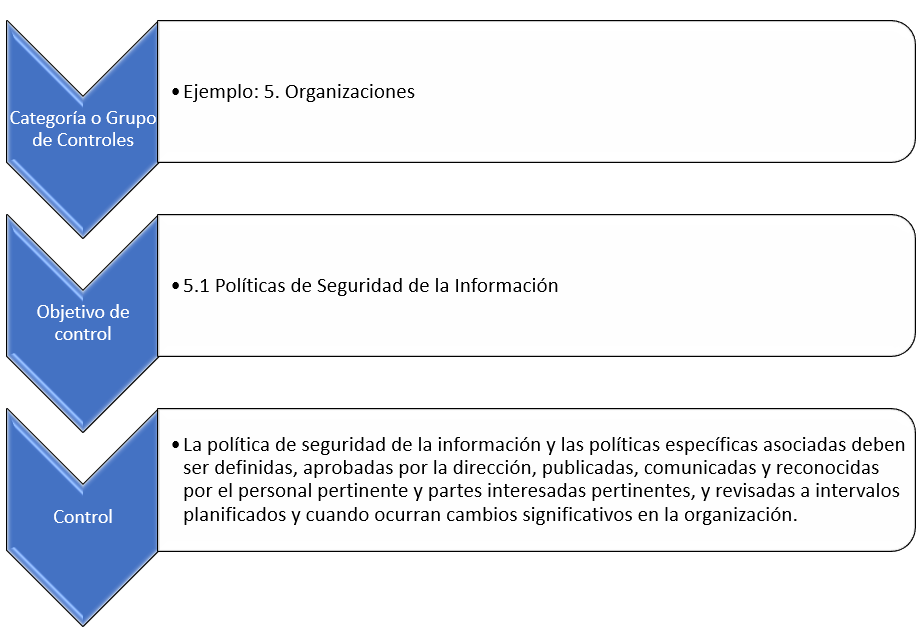
Imágen : Distribución de controles ISO 27001:2022 Tomado de https://www.cynthus.com.mx/actualizacion-del-estandar-iso-27001/

* + 1. **Objetivo de control**

Cada uno de los dominios de seguridad que nos presenta la norma ISO/IEC 27001:2022 descritos anteriormente, se encuentra dividido en categorías denominadas Objetivos de control el cual nos brinda los objetivos principales de los controles de seguridad que se implementaran.

Control: Son acciones que se deben implementar bajo un proceso o procedimiento, para garantizar los objetivos de seguridad de la organización.

En este orden de ideas, la estructura de los objetivos de control se presenta de acuerdo con la imagen 2.



Imágen : Estructura de los Objetivos de Control: Fuente propia

* + 1. **Objetivos**

Los dominios de seguridad que proponen esta norma se encuentran estructurados de acuerdo a los componentes y elementos más relevantes para el mejoramiento de los activos de información y estos proponen los objetivos de control estudiados en el componente formativo numero 2 denominado: CF2 Clasificación, valuación de activos y modelos de referencia.

En una organización se deben de gestionar los activos de información de manera segura y responsable, por ello la norma nos recomienda que se cuente con policiacas claras que apoyen el ejercicio de identificación y aseguramiento de los activos de la información.

Estos objetivos de control en profundidad pueden ser consultados en la Norma ISO/IEC 27001:2022 – Anexo A para identificar aspectos más en profundidad sobre los controles de seguridad.

* + 1. **Alcance**

En el ejercicio para la determinación de los controles que se desean aplicar, es importante determinar el alcance de su implementación, es decir, dependiendo del análisis de riesgos realizados a los activos de información, buscando la mitigación de estos y evitando un impacto negativo.

El establecimiento de los controles debe estar enfocados en garantizar el normal funcionamiento de la organización garantizando los niveles aceptables en la confidencialidad, integridad y disponibilidad de la información

Para determinar el alcance, es importante contar con los detalles sobre los activos de información con el fin de determinar los controles necesarios; desde el enfoque del control encontramos los siguientes tipos:

* **Controles de Gestión:** este tipo de controles buscan controlas los riesgos que afectan la organización en cuanto a su estructura y dinámica de trabajo.
* **Controles Técnicos:** Estos controles son aquellos que se relacionan con factores tecnológicos, basados en software, hardware, controles técnicos, de seguridad perimetral o a las comunicaciones entre otros.
* **Controles Operacionales**: Estos controles buscan reducir los riesgos a partir de directrices o lineamientos para el desarrollo de actividades o funciones propias de la organización de manera segura.
* **Controles de cumplimiento:** Estos controles buscan mejorar el cumplimiento y adaptación por parte de la organización en el desarrollo de sus funciones o actividades.

Así mismo desde la finalidad del control, estos se pueden clasificar de la siguiente manera:

* **Controles Disuasorios:** Son aquellos que buscan prevenir a un atacante potencial.
* **Controles Preventivos**: Buscan minimizar la probabilidad de que un incidente se presente en la organización.
* **Controles de Detección:** Buscan identificar el momento más exacto de cuando sucede un incidente.
* **Controles Correctivos:** Se establecen para dar solución una vez que se presente un incidente en la organización.

Podemos identificar algunos controles sugeridos por la norma ISO/IEC 27001:2022 dentro del anexo A.

* + 1. **Aplicabilidad**

Una vez identificados y establecidos los controles a implementar en los procesos de la organización, estos deben de declararse mediante un documento denominado Declaración de Aplicabilidad (Statement of Aplicability SoA) el cual nos da un punto de partida sobre los controles.

Este documento es construido durante el establecimiento del sistema de gestión de la seguridad de la información, por lo que se considera un documento de referencia tanto para la implementación de controles, así como para su evaluación.

En la imagen 3, podemos observar un ejemplo de documento de Declaración de Aplicabilidad, en donde se establece los controles, su aplicación, su justificación, responsable, así como el plan de acción a realizar para su implementación

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente con confianza media

Imágen : Ejemplo de Declaración de aplicabilidad (SOA). Recuperado de <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiw9JuJjrWBAxUOnGoFHYQ_B-AQFnoECDQQAQ&url=https%3A%2F%2Fiso27001security.com%2FISO27k_SGSI_6.1_SoA_2022_Espanol_Rev03_2022.xlsx&usg=AOvVaw0ewJMSh-3SXojjoV1nlqUL&opi=89978449>

* + 1. **Técnicas de planificación**

Como lo mencionamos anteriormente, el proceso de planificación para la implementación de la estrategia de seguridad debe abarcar una revisión y verificación del informe de análisis de riesgos que permita determinar en primer lugar los activos de información que se desean proteger en la organización, así como las amenazas a las cuales están expuestos; este ejercicio conlleva al establecimiento de los objetivos de seguridad con los cuales se busca garantizar una mejora considerable de los niveles de seguridad de los activos en la organización.

.

* + 1. **Conceptos a tener en cuenta**

A partir del establecimiento de los objetivos de seguridad se favorece la planificación para la implementación de estrategias que permitan mejorar los niveles de seguridad en los activos de información de una organización; esta planificación deberá contar con alcances y etapas que involucren la implementación de controles para que garanticen los pilares de la información.

* **Activo de información**: Un activo de información de acuerdo con la norma ISO/IEC 27001:2022 es “algo que una organización valora y por lo tanto debe proteger”
* **Objetivo de seguridad**: Son objetivos que se plantean a partir de los resultados de la evaluación de riesgos y reflejan la medida en la que se alcanzan los niveles de protección de los activos de información para determinar la eficacia de los controles implementados.
* **Registro**: Son evidencias o anotaciones relacionadas con el desarrollo y ejecución de un control de acuerdo con lo propuesto.
* **Recurso:** Corresponde a los elementos o insumos necesarios para la implementación de un control y se convierte en un aspecto fundamental en el ejercicio de establecer las acciones a implementar.
* **Métrica:** Las métricas son instrumentos que permiten verificar el nivel de cumplimiento de un control de seguridad de acuerdo con lo esperado y propuesto en la estrategia de seguridad.

Como ejemplo para aplicar las métricas encontramos las siguientes:

|  |  |  |
| --- | --- | --- |
| **Estado** | | **Significado** |
| **? Desconocido** | No ha sido siquiera revisado aún | |
| **Inexistente** | Ausencia completa de una política, procedimiento, control, etc legible. | |
| **Inicial** | El desarrollo apenas ha comenzado y requerirá un trabajo significativo para satisfacer los requisitos | |
| **Limitado** | Progresando bien pero no completado aún | |
| **Definido** | El desarrollo está más o menos completo, aunque con ausencia de detalles y/o no está aún implementado, en cumplimiento vigente ni activamente avalado por la alta dirección. | |
| **Gestionado** | El desarrollo está completo, el proceso / control ha sido implementado y recientemente comenzó a operar | |
| **Optimizado** | El requisito está plenamente conforme, está plenamente operativo como se espera, está siendo activamente supervisado y mejorado, y hay evidencia sustancial para demostrar todo lo antedicho a los auditores | |
| **No Aplica** | TODOS los requerimientos en el cuerpo principal de la norma ISO/IEC 27001 son obligatorios SI su SGSI va a ser certificado. Caso contrario, la gerencia a cargo, puede ignorarlos | |

Tabla :Ejemplo de metricas para medir el nivel de cumplimiento

* + 1. **Tipos de objetivos de seguridad.**

La planificación de la estrategia de seguridad se debe realizar mediante la construcción de los objetivos de seguridad, estos se deben de proponer a partir del análisis de riesgos realizado a los activos de información y establecen las acciones que se deben de adelantar para tratar los riesgos de seguridad, estos objetivos buscan garantizar los pilares de la información.

Para el establecimiento de los objetivos de seguridad es importante tener presente aspectos como son:

* Los recursos que se necesitan para realizar la implementación.
* La persona, área o dependencia responsable del cumplimiento del objetivo.
* El método de evaluación, con el fin de identificar si el objetivo se está cumpliendo.

Además, debe tener presente que todo el ejercicio de la construcción y ejecución del objetivo de control debe estar documentado, así como:

* Definir cada objetivo y su finalidad.
* Las evaluaciones y seguimiento a la ejecución y verificación del control verificando que este se cumpla.
  + 1. **Características**

De acuerdo con las características de la estrategia de seguridad y controles de información que se vayan a implementar en la organización, se deben establecer los objetivos de seguridad los cuales deben de contar con características que permitan validar si fueron cumplidos; de acuerdo a la norma ISO/IEC 27001:2022, los objetivos de seguridad deben de presentar las siguientes características:

* Estar alineadas a la política de seguridad de la información.
* Se deben de poder medir
* Tener presente el contexto de la estrategia de seguridad, así como el resultado del ejercicio de valoración de riesgos.
* Estos deben ser informados a todos los interesados.
* Deben ser evaluados y actualizados de acuerdo con las necesidades.

Adicionalmente, se deberá de tener presente las siguientes condiciones durante el proceso de su planificación:

* Se debe conservar la información documentada sobre los objetivos de la seguridad de la información.
* En el momento de realizar la planificación para garantizar el alcance de los objetivos propuestos en relaciona a la seguridad de la información, se debe tener presente:
* Acciones para desarrollar.
* Recursos necesarios.
* Persona, área o dependencia responsables.
* Tiempo necesario para culminar.
* Método de evaluación.

La información documentada deberá de ser conservada para su revisión en procesos de auditoria tanto internas como externas para cumplimiento como verificación.

1. **Metodologías de Análisis y valuación de Activos**
   1. **Magerit**

Magerit es una metodología que se esfuerza por enfatizarse en dividir los activos de la organización en variados grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier inconveniente.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

En el periodo transcurrido desde la publicación de la primera versión de Magerit (1997) hasta la fecha, el análisis de riesgos se ha venido consolidando como paso necesario para la gestión de la seguridad.

La Evaluación del riesgo es fundamental para llevar a cabo planes de seguridad y de contingencia dentro de la organización, para poder gestionarlos y hacerse riguroso frente a posibles ataques a los datos y la información tanto de la organización, como de los servicios que presta.

* + 1. **Objetivos de Magerit**
       1. **Directos**
    - Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de corregirlos a tiempo.
    - Ofrecer un método sistemático para analizar tales riesgos.
    - Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
      1. **Indirectos**
* Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

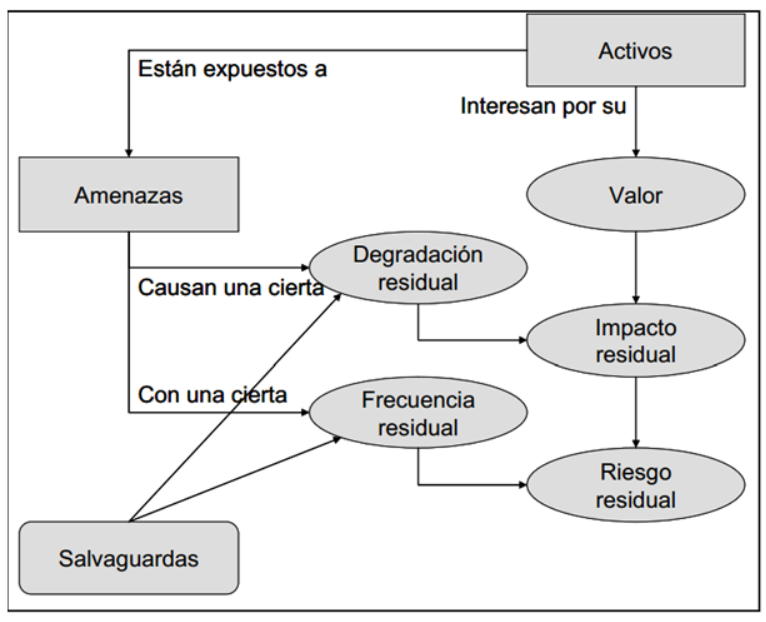
La metodología MAGERIT es una de las más utilizadas ya que se encuentra en español. MAGERIT está basado en tres submodelos:

* Submodelo de elementos: Es este submodelo se clasifican 6 elementos básicos que son: activos, amenazas, vulnerabilidades, impacto, riesgo, salvaguarda.
* Submodelo de eventos: Aquí se clasifican los elementos anteriores en tres formas: dinámico físico, dinámico organizativo y estático.
* Submodelo de procesos: Se definen en 4 etapas: análisis de riesgo, planificación, gestión de riesgo y selección de salvaguardas.

La metodología consta de tres volúmenes:

* Volumen I – Método, es el volumen principal en el que se explica detalladamente la metodología.
* Volumen II – Catálogo de elementos, complementa el volumen principal proporcionando diversos inventarios de utilidad en la aplicación de la metodología. Los inventarios que incluye son:
  + Tipos de activos
  + Dimensiones y criterios de valoración
  + Amenazas
  + Salvaguardas
* Volumen III – Guía de técnicas, complementa el volumen principal proporcionando una introducción de algunas de técnicas a utilizar en las distintas fases del análisis de riesgos. Las técnicas que recoge son:
* Análisis mediante tablas
* Análisis algorítmico
* Árboles de ataque
* Técnicas generales o
* Análisis coste-beneficio
* Diagramas de flujo de datos (DFD)
* Diagramas de procesos
* Técnicas gráficas
* Planificación de proyectos
* Sesiones de trabajo: entrevistas, reuniones y presentaciones
* Valoración Delphi

La metodología MAGERIT se puede resumir gráficamente de la siguiente forma:



Imágen : : Metodologia Magerit

* 1. **Metodología OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)**

Es un método de evaluación y de gestión de los riesgos para garantizar la seguridad del sistema informático, desarrollado por el estándar internacional ISO270001.

El núcleo central de OCTAVE es un conjunto de criterios (principios, atributos y resultados) a partir de los cuales se pueden desarrollar diversas metodologías.

* + 1. **Objetivos**
* Permitir la comprensión del manejo de los recursos
* Identificación y evaluación de los riesgos que afectan la seguridad dentro de una organización.
* Exige llevar la evaluación de la organización y del personal de la tecnología de información

Octave divide los activos en dos tipos que son:

* Sistemas, (Hardware. Software y Datos)
* Personas
  + 1. **Equipo de Análisis de Riesgos**

Debe existir un equipo de Análisis el cual tiene las siguientes funciones:

* Identificación recursos importantes mediante encuestas y entrevistas
* Enfoque actividades de análisis de riesgos
* Relación de amenazas y vulnerabilidades
* Evaluación riesgos
* Creación estrategia de protección, planes de mitigación y diseño de políticas de seguridad
  + 1. **Fases del método propuesto por Octave**
* Visión de organización: Donde se definen los siguientes elementos: activos, vulnerabilidades de organización, amenazas, exigencias de seguridad y normas existentes.
* Visión tecnológica: se clasifican en dos componentes o elementos: componentes claves y vulnerabilidades técnicas.
* Planificación de las medidas y reducción de los riesgos: se clasifican en los siguientes elementos: evaluación de los riesgos, estrategia de protección, ponderación de los riesgos y plano de reducción de los riesgos.

El método Octave se resume en las siguientes fases



Imágen : Fases del Metodo Octave

* 1. **Metodología CORAS (COnstruct a platform for Risk Analysis of Security critical system)**

Desarrollado a partir de 2001 por SINTEF, un grupo de investigación noruego financiado por organizaciones del sector público y privado. Se desarrolló en el marco del Proyecto CORAS (IST-2000-25031) financiado por la Unión europea.

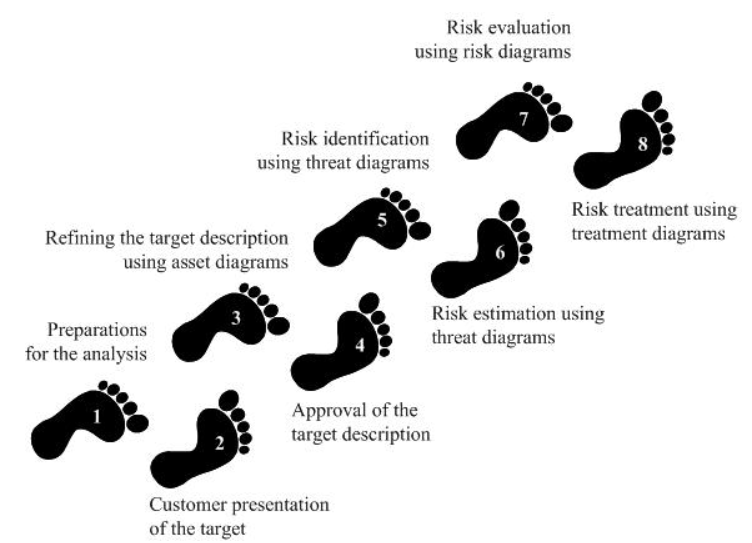
El método CORAS proporciona:

* Una metodología de análisis de riesgos basado en la elaboración de modelos, que consta de siete pasos, basados fundamentalmente en entrevistas con los expertos.
* Un lenguaje gráfico basado en UML (Unified Modelling Language) para la definición de los modelos (activos, amenazas, riesgos y salvaguardas), y guías para su utilización a lo largo del proceso. El lenguaje se ha definido como un perfil UML.
* Un editor gráfico para soportar la elaboración de los modelos, basado en Microsoft Visio.
* Una biblioteca de casos reutilizables.
* Una herramienta de gestión de casos, que permite su gestión y reutilización.
* Representación textual basada en XML (eXtensible Mark-up Language) del lenguaje gráfico.
* Un formato estándar de informe para facilitar la comunicación de distintas partes en el proceso de análisis de riesgos.

El método propone 7 pasos que son:

* Paso 1, Presentación: Reunión inicial, para presentar los objetivos y el alcance del análisis y recabar información inicial.
* Pasó 2, Análisis de alto nivel: Entrevistas para verificar la comprensión de la información obtenida y la documentación analizada. Se identifican amenazas, vulnerabilidades, escenarios e incidentes.
* Pasó 3, Aprobación: Descripción detallada de los objetivos, alcance y consideraciones, para su aprobación por parte del destinatario del análisis de riesgos.
* Pasó 4, Identificación de riesgos: Identificación detallada de amenazas, vulnerabilidades, escenarios e incidentes.
* Pasó 5, Estimación de riesgo: Estimación de probabilidades e impactos de los incidentes identificados en el paso anterior.
* Pasó 6, Evaluación de riesgo: Emisión del informe de riesgos, para su ajuste fino y correcciones.
* Pasó 7, Tratamiento del riesgo: Identificación de las salvaguardas necesarias, y realización de análisis coste/beneficio.

A continuación se muestra el resumen grafico del método CORAS



Imágen : Pasos del método CORAS

* 1. **Metodología MEHARI**

MEHARI es una metodología desarrollada por CUSIF (Club de la Securité De L’information Français) en 1998 que pasó a ser Open Source en 2007.

El objetivo de esta metodología es permitir un análisis directo e individual de situaciones de riesgos descritas en diferentes escenarios y proporcionar un completo conjunto de herramientas específicamente diseñadas para la gestión de la seguridad a corto, medio y largo plazo, adaptables a diferentes niveles de madurez.

* + 1. **Introducción general de la utilización de MEHARI**

La principal orientación de MEHARI es la evaluación y reducción de riesgos. Sus bases de datos de conocimiento, mecanismos y herramientas se han creado con ese objetivo.

Asimismo, en la mente de los diseñadores del conjunto de la metodología, la necesidad de un método estructurado para el análisis y reducción de riesgos puede ser, en función de la organización:

* Un método permanente de trabajo – la línea base para un grupo especializado,
* Un método de trabajo utilizado en paralelo junto a otras prácticas de gestión de la Seguridad,
* Un método de trabajo utilizado de forma ocasional para complementar otras prácticas regulares.

Con esto en mente, MEHARI proporciona un conjunto de enfoques y herramientas que permiten realizar un análisis de riesgos cuando es necesario.

La metodología MEHARI, que comprende las bases de datos de conocimiento, los manuales y las guías que describen los diferentes módulos (amenazas, riesgos, vulnerabilidades), se encuentra disponible para ayudar a las personas implicadas en la gestión de la seguridad (CISO, responsables de riesgos, auditores, CIO,), en sus diferentes tareas y actividades.

MEHARI es un conjunto de herramientas y funcionalidades metodológicas para la gestión de la seguridad y de las medidas asociadas, basado en un análisis de riesgos preciso. Los aspectos fundamentales de MEHARI son:

* Su modelo de riesgos (cualitativo y cuantitativo),
* el examen de la eficacia de las medidas de seguridad en vigor o previstas,
* la capacidad para evaluar y simular los niveles de riesgo derivados de medidas adicionales
  + 1. **Fases de la metodología MEHARI**
       1. **Análisis o evaluación de Riesgos**

Una situación de riesgo se puede caracterizar por diferentes factores:

* Factores estructurales (u organizacionales), los cuales no dependen de las medidas de seguridad, sino de la actividad principal de la organización, su entorno y su contexto.
* Factores de la reducción de riesgo, que son función directa de las medidas de seguridad implementadas.

Para ello, integra herramientas (como criterios de evaluación, fórmulas, etc.) y bases de datos de conocimiento (en particular para el diagnóstico de las medidas de seguridad), como complemento esencial al marco de análisis de riesgos.

Es necesario realizar un enfoque estructurado que permita identificar todas las situaciones potenciales de riesgo, con el fin de analizar las más críticas y poder identificar las acciones para reducir el riesgo a niveles aceptables.

* + - 1. **Evaluaciones de Seguridad**

MEHARI integra cuestionarios de controles de seguridad, lo que permite evaluar el nivel de calidad de los mecanismos y soluciones encaminadas a la reducción del riesgo. Los controles o medidas de seguridad se agrupan en servicios y en dominios de seguridad. Para realizar esta evaluación es necesario seguir los siguientes pasos:

* Revisión de vulnerabilidades o evaluación de los servicios de seguridad: MEHARI proporciona un modelo de riesgos estructurado que considera los factores de reducción del riesgo en forma de servicios de seguridad.

El resultado de la evaluación de la vulnerabilidad tendrá el fin de garantizar que los servicios de seguridad cumplen realmente su cometido.

La evaluación se basa en una base de datos experta de conocimientos proporcionada por MEHARI para evaluar el nivel de calidad de las medidas de seguridad.

* Planes de seguridad basados en la revisión de vulnerabilidades: se realizará la confección de planes de seguridad como resultado directo de la evaluación del estado de los servicios de seguridad.

El proceso de gestión de la seguridad se enfoca en ejecutar una evaluación y decidir mejorar todos aquellos servicios que no tienen un suficiente nivel de calidad.

MEHARI proporciona unos cuestionarios de diagnóstico que se pueden utilizar para este tipo de enfoque.

* Apoyo en las BBDD en la creación de un marco de referencia de seguridad: las bases de datos de conocimiento de MEHARI se pueden utilizar directamente para crear un marco de referencia de seguridad que contendrá y describirá el conjunto de reglas e instrucciones de seguridad que debe seguir la organización.

Los cuestionarios de evaluación de MEHARI son una buena base de trabajo para los responsables de seguridad para decidir lo que debe ser aplicado en la organización.

La creación de un conjunto de reglas, a través de un marco de referencia de seguridad, se enfrenta a menudo a dificultades en la implementación local, por lo que se deben gestionar exenciones y excepciones.

* Dominios cubiertos por el módulo de evaluación de vulnerabilidades: desde un punto de vista de análisis de riesgo, en base a la identificación de todas las situaciones de riesgo y con el deseo de cubrir todos aquellos riesgos inaceptables, MEHARI no se limita simplemente al dominio IT.

El módulo de evaluación cubre, además de los sistemas de información, todo el conjunto de la organización, como la protección del sitio en general, el entorno de trabajo y los aspectos legales y regulatorios.

* + - 1. **Análisis de Amenazas**

Sea cual sea la orientación de la política de seguridad, hay un principio en el que coinciden todos los responsables: debe existir un equilibrio entre las inversiones de seguridad por un lado y la importancia de los principales retos empresariales por el otro.

Esto significa que la comprensión de las amenazas del negocio es fundamental, y que el análisis del contexto de seguridad merece un nivel prioritario y un método estricto y riguroso de evaluación.

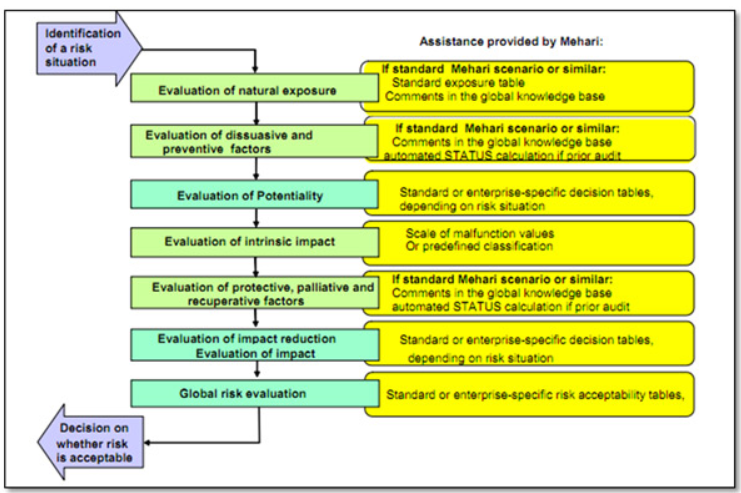
El fin del análisis de las amenazas de seguridad es responder a la siguiente doble pregunta ¿Qué puede suceder, y si sucede, puede ser serio?

MEHARI proporciona un módulo de análisis de amenazas con dos tipos de resultados:

* Una escala de valores de posibles malfuncionamientos en sus procesos operacionales.
* Una clasificación de la información y de los activos TI: consiste en la definición, para cada tipo de información, para cada tipo de activo TI, y para cada criterio de clasificación (habitualmente Confidencialidad, Integridad y Disponibilidad). La clasificación de la información de los activos es la escala de los valores de malfuncionamiento definida anteriormente traducido a indicadores de sensibilidad asociados con los activos TI.

La escala de valores de malfuncionamiento y la clasificación de la información y activos son dos formas distintas de expresar las amenazas de seguridad. El primero es más detallado y proporciona más información a los CISO y el segundo es más generalista y resulta más útil para las campañas de sensibilización e información.

La siguiente imagen resume las características y procesos de mehari.



Imágen : Fases y Caracteristicas de MEHARI

* 1. **Nist SP-830 . (National Institute of Standards and Technology)**

Guía de gestión de riesgo para sistemas de tecnología de la información – Recomendaciones del Instituto Nacional de Estándares y Tecnología. Es una guía que propone un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos como parte de la gestión de la seguridad de la información; sin embargo, esto no es suficiente, pues se necesita del apoyo de toda la organización para que los objetivos y alcance de la gestión de riesgos concluyan con éxito.

Esta metodología abarca 9 pasos:

1. Caracterización del sistema
2. Identificación de amenazas
3. Identificación de vulnerabilidades
4. Análisis de controles
5. Determinación de probabilidades
6. Análisis del impacto
7. Determinación del riesgo
8. Recomendaciones de controles
9. Documentación de resultados
   * 1. **Objetivos**

* El objetivo de desempeño de la gestión de riesgos es habilitar la organización para cumplir su misión
* Mejorar el aseguramiento del sistema TI que almacena, procesa o transmite información organizacional.
* Permitir la gestión de riesgos para tomar decisiones bien fundamentadas de gestión y justificar los gastos que forman parte de un presupuesto de TI.
* Asistir a la administración en lo que se autoriza (o acredita) a los sistemas de TI sobre la base de la documentación de soporte a partir de los resultados de la gestión de riesgos.

A manera de ejemplo se realizará una parte de cada uno de los pasos propuestos por SP- 830, para este caso utilizaremos las dos primeras actividades que incluye la caracterización de los activos y su valuación de acuerdo a los principios de la seguridad.

* + 1. **Caracterización del sistema**

La primera parte consiste en identificar cuáles son los activos con que cuenta la empresa, para esta parte tomaremos como ejemplo los propuestos en el caso de estudio, para realizar de manera más ordenada y clara se recomienda caracterizar los activos de acuerdo a categorías que entre otras pueden ser:

Instalaciones, comunicaciones, equipamiento, aplicaciones, personal, activos esenciales, entre otros que se consideren nos faciliten su clasificación y posterior valuación de los activos.

Podemos crear tablas que nos faciliten el agrupamiento de activos en cada una de las categorías antes mencionadas.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Instalaciones** | **Comunicaciones** | **Equipamiento** | **Aplicaciones** | **Personal** | **Activos Esenciales** |
| Edificio empresa | Conexión a Internet  Conexión de red LAN  Servicio de Correo electrónico | Servidor  Computadores de escritorio  Impresora  Fotocopiadora | Software tramitación de archivos.  … | Operador software  … | Bases de Datos  … |

Tabla : Clasificación de Activos

* + 1. **Valuación de Activos**

Dentro de la etapa de caracterización de la infraestructura, luego de la identificación y clasificación de los activos por categorías se realiza la valuación de estos. Esta valuación se hace teniendo como punto de partida los pilares de la seguridad informativa y para cada uno de ellos se definen diferentes niveles de cumplimiento como se consigna en la tabla siguiente. El nivel más alto indicaría que se cumple a cabalidad con un determinado pilar de la seguridad informática.

|  |  |
| --- | --- |
| **Criterios de Valuación de los activos** | |
| Muy Alto | 5 |
| Alto | 4 |
| Medio | 3 |
| Bajo | 2 |
| Muy bajo | 1 |

Tabla : Valores de Valuación de activos

Para determinar el valor de la valuación de los activos se debe de considerar los siguientes criterios de acuerdo con los pilares de la seguridad de la información.

|  |  |  |
| --- | --- | --- |
| **Criterios para la Valuación de activos** | | |
| Confidencialidad | Integridad | Disponibilidad |
| Los componentes del sistema TI serán accesibles sólo por aquellos usuarios autorizados. | Los componentes del sistema TI sólo pueden ser creados y modificados por los usuarios autorizados. | Los usuarios deben tener disponibles todos los componentes del sistema TI cuando así lo requieran |

Tabla : : Pilares de seguridad - criterios de Valuación

El siguiente paso es realizar el proceso de valuación de los activos identificados a fin de determinar cuáles son los más sensibles o críticos, a manera de ejemplo se realizará la valuación para algunos de los activos identificados.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Proceso de valuación de Activos** | | | | |
| **Categoría: Equipamiento** | | | | |
| Activo | Confidencialidad | Integridad | Disponibilidad | Valor del Activo |
| Servidor | 5 | 5 | 5 | 15 |
| Computador de escritorio | 4 | 4 | 3 | 11 |
| Impresora | 3 | 1 | 1 | 5 |
| Fotocopiadora | 1 | 1 | 1 | 3 |

Tabla : Ejemplo Valuación de Activos

Como se puede evidenciar en la tabla anterior se concluye que el activo llamado servidor que aloja la aplicación de tramitación de archivos es el más crítico de la categoría seleccionada.

* + 1. **Identificación de amenazas**

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad informática, los Elementos de Información.

Para el caso de SP-830 estas se categorizan en tres tipos: Humanas, naturales y del entorno, y las siguientes son algunos ejemplos.

|  |  |  |
| --- | --- | --- |
| **Valuación de las Amenazas** | | |
| **Naturales** | **Humanas** | **Entorno** |
| * Terremoto * Inundaciones * Tormentas eléctricas * Vendavales * Huracanes | * Acceso no autorizado a la infraestructura * Explotación de errores (usuario y administrador) * Ingeniería social * Malicia * Virus informático (malware) * Phishing * Ingeniería social * Denegación de servicio * Spoofing | * Fallas eléctricas * Polución * Temperatura * Incendios * Control de humedad * Edificaciones Cercanas * Accidente de tránsito. * Protección de los equipos en el sitio * Fuentes de Potencia * Seguridad de cableados * Mantenimiento de equipos * Ingreso no autorizado * Aseguramiento de oficinas, recintos y espacios físicos. * Fallas de equipos |

Tabla : : Criterios de valuación de Amenazas

A continuación, se muestra un ejemplo de cómo se identifican las amenazas

|  |  |  |  |
| --- | --- | --- | --- |
| Activo | A. Naturales | A. Humanas | A. Entorno |
| Servidor | Inundación | Acceso no autorizado  Denegación de servicio  Virus  Suplantación de seguridad | Humedad  Polvo |

Tabla : Ejemplo de identificación de amenazas

* + 1. **Valuación de amenazas**

El proceso de valuación de las amenazas se hace para cada activo en cada una de las categorías al igual que en el caso anterior tomaremos como ejemplo una categoría para realizar el proceso.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Valuación de Amenazas** | | | | |
| **Activo** | **A. Naturales** | **A. Humanas** | **A. Entorno** | **Valor Amenaza** |
| Servidor | 1 | 5 | 3 | 9 |
| Computador de escritorio | 1 | 4 | 3 | 8 |
| Impresora | 1 | 1 | 2 | 4 |
| Fotocopiadora | 1 | 1 | 2 | 4 |

Tabla : Valuación de Amenazas

De la tabla anterior se puede concluir que el activo llamado servidor es que el mayor valor en las amenazas tiene.

* + 1. **Identificación de vulnerabilidades**

Las vulnerabilidades son debilidad de cualquier tipo que compromete la seguridad del sistema informático, para la identificación de vulnerabilidades se puede recurrir a dos estrategias distintas pero complementarias que son a partir de la utilización de herramientas tecnológicas que de manera automática pueden identificarlas, este proceso se realiza mediante el cumplimiento de técnicas de ethical hacking siguiendo una metodología para este proceso como ISAF, OWASP, OSSTMM, entre otras.

Sin embargo, existen vulnerabilidades que deben identificadas y que ninguna herramienta tecnológica las puede detectar como las que se generan por problemas eléctricos, de control de acceso físico a servidores y equipos, falta de documentación de los procesos y procedimientos, entre otros que solo pueden identificarse mediante un análisis personal, observación directa, entrevista dirigida y otras estrategias de manera presencial.



Imágen : Ejemplo de Análisis de Vulerabilidad Ilustración

* + 1. **Análisis de controles**

En este apartado el estándar propone una actividad que corresponde a identificar y seleccionar los controles actuales y los controles planificados.

Los controles los podemos clasificar en técnicos, físicos y administrativos a continuación se mencionan algunos ejemplos de estos controles.

|  |  |  |
| --- | --- | --- |
| Controles de seguridad | | |
| Controles Físicos | Controles Técnicos | Controles administrativos |
| Cámaras de circuito cerrado  Sistemas de alarmas térmicos o de movimiento  Guardias de seguridad  Identificación con fotos  Puertas de acero con seguros especiales  Biométrica (incluye huellas digitales, voz, rostro, iris, escritura a mano y otros métodos automatizados utilizados para reconocer individuos) | Encriptación  Tarjetas inteligentes  Autenticación a nivel de la red  Listas de control de acceso (ACLs)  Software de auditoría de integridad de archivos | Entrenamiento y conocimiento  Planes de recuperación y preparación para desastres.  Estrategias de selección de personal y separación.  Registro y contabilidad de personal.  Políticas de seguridad |

Tabla : Ejemplos de algunos controles

* + 1. **Determinación de probabilidades**

Las probabilidades permiten medir en que porcentajes se pueden llegar a presentar algún tipo de incidente que ponga en riesgo el correcto funcionamiento de los recursos tecnológicos.

Al igual que con las variables anteriores para su medición nos apoyaremos en las siguientes características:

|  |  |
| --- | --- |
| **Criterios para medir la probabilidad de las amenazas** | |
| Alta | La realización del ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque. |
| MEDIA | Existen condiciones que hacen poco probable un ataque en el corto plazo pero que no son suficientes para evitarlo en el largo plazo |
| BAJA | Existen condiciones que hacen muy lejana la posibilidad del ataque. |

Tabla :Crietrios medición probabilidad

Dentro de la empresa existen una serie de vulnerabilidades que pueden ser explotadas por las amenazas por lo tanto se hace necesario definir criterios que permitan determinar el nivel de probabilidad de las vulnerabilidades; tres niveles son definidos con este fin como se observa en la tabla siguiente:

|  |  |
| --- | --- |
| **Criterios para medir la probabilidad de las vulnerabilidades** | |
| Alta | El threat-source es altamente motivado y suficientemente capaz, y los controles para evitar la vulnerabilidad de ser ejercidas son ineficaces |
| MEDIA | Existen condiciones que hacen poco probable un ataque en el corto plazo pero que no son El threat-source es altamente motivado y suficientemente capaz, y los controles para evitar la vulnerabilidad de ser ejercidas son ineficaces |
| BAJA | El threat-source carece de motivación o capacidad, o los controles existen para prevenir, o al menos obstaculicen de manera significativa la vulnerabilidad de ser ejercida |

Tabla : Criterios para medir la probabilifdad de la Vulnerabilidad

A continuación, se muestra a manera de ejemplo como es el proceso de identificación de las probabilidades en las amenazas y vulnerabilidades.

|  |  |  |  |
| --- | --- | --- | --- |
| **Tipo de amenaza** | **Probabilidad de amenaza** | | |
|  | **alta** | **media** | **baja** |
| Amenaza de entorno |  | X |  |
| Amenaza humana | X |  |  |
| Control de humedad (Cuarto de telecomunicaciones) |  | X |  |
| Polución (cuarto de telecomunicaciones) |  | X |  |
| Falta de cumplimiento de la normatividad de cableado estructurado (Armario) | X |  |  |

Tabla : Probabilidad en las amenazas

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerabilidad** | **Alta** | **Media** | **Baja** |
| No se tiene un canal de backup con ISP en caso de fallo de canal principal | X |  |  |
| Cableado de red y eléctrico junto en algunos sitios. | X |  |  |
| No existen barras de puesta a tierra dentro del cuarto de comunicaciones y en rack. | X |  |  |
| No se tiene un plano adecuado para mirar distancias de puntos de red, pero por observación de algunas oficinas se sobrepasa la distancia máxima. |  | X |  |
| Falta de etiquetas adecuadas de equipos activos y servidores. |  | X |  |
| No se maneja un mecanismo de control de humedad |  | X |  |
| No se tiene un diagrama lógico de conexión de equipos | X |  |  |

Tabla : Probabilidad en las vulnerabilidades

* + 1. **Análisis de Impacto**

Para determinar el establecimiento de prioridades en la protección y prevención, se requiere conocer cual o cuales activos pueden ser potencialmente afectados por incidentes de seguridad.

En caso de que hallan afectaciones a los activos se debe determinar cuál es la afectación y grado de problema que podría causar en la organización, este grado de afectación puede medirse desde las consecuencias económicas, indisponibilidades de acceso entre otras.

El impacto debe medirse con base a los tres principios de la seguridad: la confidencialidad, la integridad y la disponibilidad.

El impacto se puede medir en tres niveles que son:

|  |  |
| --- | --- |
| Alto | En el corto plazo desmoviliza o desarticula a la organización. |
| Medio | Provoca la desarticulación de un componente de la organización. Si no se atiende a tiempo, a largo plazo puede provocar la desarticulación de la organización. |
| Bajo | Causa daño aislado, que no perjudica a ningún componente de la organización. |

Tabla : Criterios para determinar el Impacto

A continuación, se presenta a manera de ejemplo como se puede realizar el proceso de evaluación del impacto.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Activos Amenazados** | **Principios de la Seguridad Informática** | | | **Impacto** | | |
|  | **Confidencialidad** | **Integridad** | **Disponibilidad** | **Alto** | **Medio** | **Bajo** |
| Servidor | X | X | X | X |  |  |
| Estaciones de trabajo | X | X | X | X | X |  |
| Impresora | X | X | X | X |  | X |

Tabla : Ejemplo Medicion del Impacto

* + 1. **Determinación del riesgo**

El riesgo es el efecto negativo cuando se produce un impacto sobre un activo, teniendo en cuenta tanto la probabilidad de la amenaza y el impacto de esta. Una efectiva administración de riesgos se necesita para evaluar y mitigar los riesgos identificados en la empresa.

Dentro de este ámbito la Probabilidad de Amenaza e Impacto de las amenazas están considerados por medio de los siguientes niveles o escalas.

* 2 = Baja
* 3 = Mediana
* 4 = Alta

El Riesgo, se calcula como el producto de la multiplicación Probabilidad de Amenaza por el Impacto de la amenaza, está agrupado en tres rangos, y para su mejor visualización, se aplica diferentes colores.

* Bajo Riesgo = 6 – 9 (Verde)
* Medio Riesgo = 10-12 (Naranja)
* Alto Riesgo = 13– 16 (Rojo)

|  |  |
| --- | --- |
| Alto | En el corto plazo desmoviliza o desarticula a la organización. |
| Medio | Provoca la desarticulación de un componente de la organización. Si no se atiende a tiempo, a largo plazo puede provocar la desarticulación de la organización. |
| Bajo | Causa daño aislado, que no perjudica a ningún componente de la organización. |

Tabla : Criterios para la medición del Riesgo

A continuación, se presenta a manera de ejemplo como sería el proceso general de la valuación del riesgo.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ANALISIS DE RIESGOS** | | | | | | |
| **IMPACTO** |  | **PROBABILIDAD DE AMENAZA (alto=4, Medio=3, Bajo=2)** | | | | |
|  | **HUMANA** | **ENTORNO** | | | |
| **ESCALA PARA IMPACTO (Alto=4, Medio=3, Bajo=2)** | **Amenaza humana** | **Amenaza de entorno** | **Control de humedad (Cuarto de telecomunicaciones)** | **Polución (cuarto de telecomunicaciones)** | **Falta de cumplimiento de la normatividad de cableado estructurado (Armario)** |
|  |  | **4** | **3** | **3** | **3** | **4** |
| Servidor | **4** | **16** | **12** | **12** | **12** | **16** |
| Estaciones de trabajo | **3** | **12** | **9** | **9** | **9** | **12** |
| Impresora | **4** | **16** | **12** | **12** | **12** | **16** |
|  | **4** | **16** | **12** | **12** | **12** | **16** |
| Rack | **4** | **16** | **12** | **12** | **12** | **16** |

Tabla : Ejemplo Valuación del Riesgo

* + 1. **Recomendaciones de Controles**

Como la revisión de las políticas de seguridad, actualización de antivirus, cambio periódico de contraseñas, instalación de firewalls o sanciones en caso de incumplimiento de la normativa vigente.

Los controles pueden ser preventivos, correctivos o detectivos los cuales deben responder a las necesidades de mitigación a los riesgos identificados.

Una vez calculado el riesgo, debemos tratar aquellos riesgos que superen un límite que nosotros mismos hayamos establecido. Por ejemplo, trataremos aquellos riesgos cuyo valor sea igual o superior a “16” o superior a “Medio” en caso de que hayamos hecho el cálculo en términos cualitativos. A la hora de tratar el riesgo, existen cuatro estrategias principales:

* Transferir el riesgo a un tercero. Por ejemplo, contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.
* Eliminar el riesgo. Por ejemplo, eliminando un proceso o sistema que está sujeto a un riesgo elevado. En el caso práctico que hemos expuesto, podríamos eliminar la wifi de cortesía para dar servicio a los clientes si no es estrictamente necesario.
* Asumir el riesgo, siempre justificadamente. Por ejemplo, el coste de instalar un grupo electrógeno puede ser demasiado alto y por tanto, la organización puede optar por asumir.
* Implantar medidas para mitigarlo. Por ejemplo, contratando un acceso a internet de respaldo para poder acceder a los servicios en la nube en caso de que la línea principal haya caído.
  + 1. **Documentación de Resultados**

En esta fase realizamos el informe correspondiente a la valoración de riesgos que incluye la valuación, el plan de tratamiento de riesgos incluyendo los controles a implementar.

1. **ACTIVIDADES DIDÁCTICAS (OPCIONALES SI SON SUGERIDAS)**

|  |  |
| --- | --- |
| **DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA** | |
| Nombre de la Actividad | NA |
| Objetivo de la actividad |  |
| Tipo de actividad sugerida |  |
| **Archivo de la actividad**  **(Anexo donde se describe la actividad propuesta)** |  |

1. **MATERIAL COMPLEMENTARIO:**

|  |  |  |
| --- | --- | --- |
| **Referencia APA del Material** | **Tipo de material**  **(Video, capítulo de libro, articulo, otro)** | **Enlace del Recurso o**  **Archivo del documento o material** |
| Anexo1. Declaración de Aplicabilidad SOA ISO 27001:2022 | Archivo de hoja de calculo | En el link de materiales de formación |
|  |  |  |

1. **GLOSARIO:**

|  |  |
| --- | --- |
| **TERMINO** | **SIGNIFICADO** |
| NIST | del National Institute of Standard Technology (Instituto Nacional de Estándares y Tecnología). |
| ACTIVO TECNOLOGICO | Todo equipo tecnológico o relacionado con la tecnología requerido para que la organización cumpla con su función o misión. |
| SP-830 | Special Publication 830, Guía de gestión de riesgo para sistemas de tecnología de la información – recomendaciones del instituto nacional de estándares y tecnología |
| Confidencialidad | Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados |
| Integridad | Propiedad de salvaguardar la exactitud y estado completo de los activos |
| Disponibilidad | Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. |
| CISO | chief information security officer(Oficial de seguridad de la Información) |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

* CERT - Software Engineering Institute - Carnegie Mellon University. (s.f.). CERT. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). Recuperado el 08 de Marzo de 2014, de <http://www.cert.org/octave/>
* Autrey, A. C. (2001). OCTAVE Criteria Versión 2.0. ittsburgh: Carniege Mellon – Software Engineering Institute.
* SGSI - 08 Análisis y valoración de riesgos. Metodologías. (2010, 12 mayo). [Vídeo]. YouTube. https://www.youtube.com/watch?v=g7EPuzN5Awg
* Calder, A. (2018). NIST Cybersecurity Framework: Una guía de bolsillo . IT Governance Publishing Ltd.
* NIST Framework for Improving Critical Infrastructure Cybersecurity https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
* Seguridad 7”A”Metodología NIST SP 800-30 (National Institute of Standards and Technology), Disponible en: http://seguridades7a.blogspot.com/p/ nist-sp-800-30.html.
* M. Juan. (2009), Análisis de Riesgos de Seguridad, [On line]. Disponible en: http://oa.upm.es/1646/1/ PFC\_JUAN\_MANUEL\_MATALOBOS\_VEIGAa.pdf
* MAGERIT “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información” está disponible tanto en español como en inglés.
* OCTAVE: “Operationally Critical Threat, Asset, and Vulnerability Evaluation” Metodología de Análisis y Gestión de Riesgos desarrollada por el CERT;
* NIST SP 800-39 “Gestión de Riesgos de los Sistemas de Información, una perspectiva organizacional”;

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Nombre** | **Cargo** | **Dependencia**  ***(Para el SENA indicar Regional y Centro de Formación)*** | **Fecha** |
| **Autor (es)** | Henry Eduardo Bastidas Paruma | Instructor | Regional Cauca, Centro de teleinformática y producción industrial | Septiembre 18 de 2023 |
|  |  |  |  |

1. **CONTROL DE CAMBIOS**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** | **Razón del Cambio** |
| **Autor (es)** |  |  |  |  |  |