**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** | 4 |
| **NOMBRE DEL COMPONENTE FORMATIVO** | Estudio de caso |
| **BREVE DESCRIPCIÓN** | Para el desarrollo practico de realizar la valuación de los activos de la organización nos apoyaremos en un caso de estudio que nos permitirá desarrollar el proceso de valuación de activos a partir de la aplicación de una metodología de análisis y valuación de activos. |
| **PALABRAS CLAVE** | Activos, SP830, NIST, confidencialidad, integridad, disponibilidad |

|  |  |  |  |
| --- | --- | --- | --- |
| **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. **Caso de estudio**
  2. **NIST SP 800 - 30. (National Institute of Standards and Technology).**

**2.1. Objetivos**

**2.2. Caracterización del sistema**

**2.2.1. Valuación de Activos**

**2.2.2 Análisis de Riesgos**

**2.2.3 Matriz de Riesgos**

**2.2.4 Plan de tratamiento de Riesgos**

1. **DESARROLLO DE CONTENIDOS:**

**Introducción**

Esta actividad de aprendizaje nos lleva a adquirir los conocimientos sobre metodologías y estándares de análisis y evaluación de activos, y algunas herramientas y técnicas utilizadas para caracterizar y hacer la respectiva valuación de los activos tecnológicos críticos de la organización.

Mediante la aplicación de un estándar del análisis de riesgos como NIST-SP 830 podremos realizar todo el proceso que nos permita construir la matriz de riesgos y poder determinar los controles necesarios para, diseñar un plan de tratamiento de Riesgos.

1. **Caso de Estudio**

La unidad objeto de estudio no es de nueva creación, sino que lleva años tramitando expedientes de forma local, antes manualmente, ahora por medio de un sistema informático propio. A este sistema informático se le ha añadido recientemente una conexión a un archivo central que funciona como “memoria histórica”: permite recuperar datos y conservar los expedientes cerrados. La última novedad consiste en ofrecer un servicio propio de la administración electrónica, en el que los usuarios pueden realizar sus tramitaciones vía web, usando su Número de Identificación Fiscal -NIF como identificación, más una contraseña personal. El mismo sistema de tramitación es usado localmente por un funcionario que atiende a los ciudadanos que se presentan en las dependencias de la unidad.

El responsable del proyecto de administración electrónica, alarmado por las noticias aparecidas en los medios sobre la inseguridad de Internet, y sabiendo que un fallo en el servicio conllevaría un serio daño a la imagen de su unidad, asume el papel de Promotor. En este papel escribe un informe interno, dirigido al director de la unidad, en el que da cuenta de:

* + Los medios informáticos con que se está trabajando y los que se van a instalar.
  + Las incidencias ocurridas desde que la unidad existe.
  + Las incertidumbres que le causa el uso de Internet para la prestación del servicio.

Con base en dicho informe argumenta la conveniencia de lanzar un proyecto al que decide llamar ASEGURA. La Dirección, convencida de la necesidad de tomar medidas antes de que ocurra una desgracia, crea un comité de seguimiento formado por los responsables de los servicios involucrados: atención a usuarios, asesoría jurídica, servicios informáticos y seguridad física.

Se determina que el alcance del proyecto será el servicio de tramitación electrónica, presencial y remota. También se estudiará la seguridad de la información que se maneja: expedientes.

Respecto del equipamiento, se analizarán equipos y redes de comunicaciones. Se toma la decisión de dejar fuera del estudio elementos que pudieran ser relevantes en un análisis más detallado como pudieran ser los datos de identificación y autenticación de los usuarios de los sistemas, las áreas de trabajo del personal que los maneja, la sala de equipos (centro de proceso de datos) y las personas relacionadas con el proceso. Está previsto lanzar un futuro proyecto ASEGURA más detallado que profundice en dichos aspectos.

Explícitamente se excluirá la evaluación de la seguridad de los servicios subsidiarios que se emplean. El análisis es local, circunscrito a la unidad que nos ocupa. Dichos servicios remotos se consideran, a efectos de éste análisis, “opacos”; es decir, que no entraremos en analizar cómo se prestan.

El lanzamiento del proyecto incluye una reunión de la dirección con el comité de seguimiento en la que se exponen los puntos principales del análisis somero realizado por el Promotor que queda habilitado como director del proyecto ASEGURA en el que participaran dos personas de su equipo junto con un contrato de asesoría establecido con una empresa consultora externa.

Uno de los miembros del equipo interno tendrá un perfil técnico: ingeniero de sistemas. A la consultora externa se le exige identificar nominalmente a las personas que van a participar y firmar un acuerdo de confidencialidad.

El proyecto se anuncia internamente mediante comunicación general a todo el personal de la unidad y notificación personal a aquellas personas que se verán directamente afectadas. En estas comunicaciones se identifican las personas responsables del proyecto.

A continuación, se hace una presentación de los servicios ofrecidos por la empresa

**Servicio de tramitación**

El servicio de tramitación se presta por medio de una aplicación informática desarrollada en el pasado sobre una base de datos. A esta aplicación se accede a través de una identificación local del usuario que controla sus privilegios de acceso. En la faceta de tramitación presencial, es la persona que está atendiendo al usuario final la que se identifica frente al sistema. En el caso de la tramitación remota, es el propio administrado quien se identifica.

Toda la tramitación incluye una fase de solicitud (y entrada de datos) y una fase de respuesta (y entrega de datos). El usuario realiza su solicitud y espera una notificación para recoger la respuesta. La notificación es por correo, certificado en el caso de tramitación presencial, y electrónico en el caso de tramitación electrónica.

Iniciar una tramitación supone abrir un expediente que se almacena localmente en la oficina. También supone recabar una serie de datos del archivo central de información, datos que se copian localmente. Al cierre del expediente, los datos y un informe de las actuaciones realizadas se remiten al archivo central para su custodia, eliminándose la información de los equipos locales.

El personal de la unidad se identifica por medio de su cuenta de usuario, mientras que los usuarios remotos se identifican por su NIF. En ambos casos el sistema requiere una contraseña para autenticarlos.

Por último, hay que destacar el papel que presta la mensajería electrónica en todo el proceso de tramitación, usado tanto como medio interno de comunicación entre el personal, y como mecanismo de notificación a los usuarios externos. Como norma, no se debe emplear el correo como transporte de documentos; estos siempre serán servidos por medio de accesos web.

**Servicio de archivo central**

En forma de intranet, se presta un servicio centralizado de archivo y recuperación de documentos. Los usuarios acceden por medio de una interfaz web local, que se conecta por medio de una red privada virtual con el servidor remoto, identificándose por medio de su NIF. Este servicio sólo está disponible para el personal de la unidad y para el empleado virtual que presta el servicio de tramitación remota.

**Equipamiento informático**

La unidad dispone de varios equipos personales de tipo PC situados dentro de los locales. Estos equipos disponen de un navegador web, de un cliente de correo electrónico sin almacenamiento local de los mensajes y un paquete ofimático estándar (procesador de textos y hoja de cálculo).

Para la valuación de los activos nos podemos apoyar en varias metodologías dispuestas para este propósito, para este ejemplo trabajaremos con SP-830.

1. **NIST SP 800 – 30. (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 con 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 con categorías que entre otras pueden ser:

* Instalaciones
* Comunicaciones
* Equipamiento
* Aplicaciones
* Personal
* Activos esenciales
* entre otros

En esta etapa se hace un levantamiento de información a partir de la utilización de diferentes técnicas de recolección de información como la entrevista, la encuesta, la observación directa, la entrevista dirigida, entre otras, que nos facilitaran la identificación de los diferentes activos de TI que hacen parte de la organización y particularmente que estén involucrados en el cumplimiento misional de la organización.

Como lo indica la metodología Se denominan activos los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

Para obtener una mejor categorización de activos y de acuerdo con las categorías planteadas se dividirán los activos dentro de los siguientes grupos:

* Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
* Las aplicaciones informáticas (software) que permiten manejar los datos.
* Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
* Los soportes de información que son dispositivos de almacenamiento de datos.
* El equipamiento auxiliar que complementa el material informático.
* Las redes de comunicaciones que permiten intercambiar datos.
* Las instalaciones que acogen equipos informáticos y de comunicaciones.
* Las personas que explotan u operan todos los elementos anteriormente citados.

Realizado el análisis del caso de estudio se identifican los siguientes activos:

**Servicios:**

* Servicio web local: Utilizado en el servicio de archivo central al cual se conectan los usuarios mediante acceso centralizado al archivo de recuperación de datos.
* VPN: utilizada para permitir la conexión al personal de la unidad de tramitación y al empleado Virtual.
* Correo electrónico: usado tanto como medio interno de comunicación entre el personal, y como mecanismo de notificación a los usuarios externos.

**Aplicaciones Informáticas:**

* Software tramitación de expedientes: Utilizado para Iniciar una tramitación que supone abrir un expediente que se almacena localmente en la oficina, también supone recabar una serie de datos del archivo central de información, datos que se copian localmente. Al cierre del expediente, los datos y un informe de las actuaciones realizadas se remiten al archivo central para su custodia, eliminándose la información de los equipos locales.
* Software ofimático básico: procesador de texto y hoja de cálculo
* Sistema de Gestión de Base de Datos

**Equipos Informáticos:**

* PC de escritorio: Utilizado dentro de los locales por las personas a cargo de la operación del sistema de tramitación de expedientes.
* Servidor: Utilizado como servidor de archivos, mensajería, bases de datos y Aplicaciones web.
* Firewall o Cortafuegos: controla la conexión a Internet que limita las comunicaciones a nivel de red.
* Control de Acceso: controla la entrada y salida del personal quienes se identifican y registran su hora de entrada y de salida.
* Sistema de detección y extinción de incendios

**Los soportes de información:**

* Servidor de Archivos: Es el servidor donde se almacena la información crítica de la entidad

**Redes de Comunicaciones:**

* Red de Área Local: Que cubre las dependencias de trabajo y la sala de equipos.
* Conexión ADSL: Provee la conexión a Internet
* Conexión RDSI: Utilizado como un canal de conexión a internet de respaldo.

**Instalaciones:**

* Sala de equipos: Espacio donde se encuentran ubicados los equipos de cómputo o recursos tecnológicos que soportan la operación de la empresa.
* Locales y Planta física: donde se encuentran ubicadas las oficinas y áreas de trabajo.

**Personal:**

* Administrador de sistemas: Persona a Cargo de la administración de los servicios y aplicativos

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

Tabla 1: Clasificación de Activos

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Servicios** | **Aplicaciones Informáticas** | **Equipos Informáticos** | **Soportes de Información** | **Redes de comunicaciones** | **Instalaciones** | **Personal** |
| Web Local | SW de tramitación de expedientes | Servidor | Servidor de Archivos | LAN | Sala de equipos | Administrador de Sistemas |
| VPN | SW ofimático | PC escritorio |  | Conexión DSL | Locales y planta física |  |
| Correo electrónico | SGDB | Firewall |  | Conexión RDSI |  |  |
|  |  | Control de Acceso |  |  |  |  |
|  |  | Sistema de extensión de incendios |  |  |  |  |

* + 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 informática 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.

Tabla 2: Valores de Valuación de activos

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

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.

Tabla 3: Pilares de seguridad - criterios de Valuación

|  |  |  |
| --- | --- | --- |
| **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 |

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.

Tabla 4: Valuación de Activos

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 |
| Firewall | 5 | 5 | 5 | 15 |
| Control de acceso | 3 | 1 | 3 | 7 |
| Sistema de extensión de incendios | 1 | 1 | 1 | 3 |
|  |  |  |  |  |

Como se puede evidenciar en la tabla anterior se concluye que el activo llamado servidor y el activo denominado firewall que aloja la aplicación de tramitación de archivos y control la seguridad para el acceso a los servicios son los más crítico de la categoría seleccionada a manera de ejemplo.

Este proceso debe de realizarse para todos y cada uno de los activos identificados a fin de poder determinar cual o cuales son los activos con mayor valuación esta puede ser considerada para valores entre 12 y 15 , siendo este resultado la suma CID (Confidencialidad, Integridad, Disponibilidad) por cada activo. Después de realizar la valuación se determina que los siguientes activos son de mayor importancia dentro de la empresa para este ejercicio determinamos que es el firewall y el servidor, aunque al hacer la valuación em todos los grupos o categorías seguramente los valores van a cambiar seguramente por que el software de tramitación de expedientes es quizá el más importante ya que es el core del negocio.

* + 1. **Identificación de amenazas**

Teniendo identificados los activos más importantes se pasa a considerar los criterios de posibles causas potenciales de un incidente no relacionado que pueden ocasionar alguna falla dentro de la Empresa. Se realizó una categorización de algunas de las posibles causas o amenazas clasificadas de la siguiente manera:

*Tabla 5: Ejemplo Clasificación de Amenazas*

|  |  |  |
| --- | --- | --- |
| Amenazas Naturales | Amenazas Humanas | Amenazas del Entorno |
| * Terremoto * Inundaciones * Tormentas eléctricas * Vendavales | * Acceso no autorizado a Sistemas * Explotación de errores (usuario y administrador) * Phishing * Interceptación de datos * código malicioso * Abuso de la informática * Virus | * Fallas eléctricas * Polución * Sustancias químicas * Fugas de líquido * 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 |

Categorizadas las amenazas, se procede a definir niveles para encontrar los activos más amenazados, a mayor puntuación el activo puede estar más afectado por una amenaza. Define la puntuación para la valuación de activos con relación a las amenazas.

Tabla 6: Criterios de Valuación de Amenazas

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

De acuerdo con estos valores se procede a identificar que tipo de amenaza y en que nivel de cumplimiento se encuentra dicha amenaza para cada activo identificado, para el caso propuesto siguiendo el ejemplo con los activos críticos quedaría de la siguiente manera:

Tabla 7: Valuación de las Amenazas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Valuación de amenazas de los activos | | | | |
| Activos de información | | | | |
| Categoría: Equipamiento | | | | |
|  | Amenaza natural | Amenaza humana | Amenaza del entorno | Valor de la amenaza |
| Servidor | 2 | 4 | 3 | 9 |
| Firewall | 2 | 5 | 3 | 10 |

Una vez realizada la valuación de amenazas se identifican los activos que se encuentran amenazados y particularmente cuáles son esas amenazas a manera de ejemplo se muestran los siguientes:

Tabla 8: Identificación de las Amenazas

|  |  |  |
| --- | --- | --- |
| **Activos** | **Tipos de Amenazas** | **Amenazas** |
| Servidor | Amenaza humana | * Errores de Seguridad * Acceso no autorizado (Ingeniería Social y Phising). * Suplantación de identidad |
| Amenaza de entorno | * Polución * Humedad * Incendio * Problemas de temperatura |
| Firewall | Amenaza humana | * Acceso no autorizado (Ingeniería Social y Phising). * Error de Configuración * Error por vencimiento de las firmas o bases de datos. |
|  | Amenaza humana | * Errores de seguridad por mala administración. * Acceso físico no Autorizado por terceras personas |

Otro factor importante en la valuación de amenazas es poder hacer el cálculo de la probabilidad de la materialización de una amenaza determinan si un ataque es inminente que podrían causar perjuicio de disponibilidad, confidencialidad, integridad y autenticidad de la información empresarial. Los criterios para la probabilidad de amenaza se definen en, clasificados en 4 niveles ALTA, MEDIA, BAJA, MUY BAJA.

Tabla 9: Valores 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. |
| **MUY BAJA** | No existen condiciones que impliquen riesgo/ataque. |

Los criterios de la probabilidad de Amenazas anteriormente descritos y estudios previos realizados en la Empresa como la recolección de información permitieron identificar el nivel de probabilidad de una amenaza.

Tabla 10: Ejemplo cálculo de la probabilidad de la Amenaza

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tipo de Amenaza** | **Probabilidad de la Amenaza** | | | |
| **Amenazas Humanas** | **Alta** | **Media** | **Baja** | **Muy Baja** |
| Acceso no autorizado por Ingeniería Social y Phising (Firewall y Servidor) | X |  |  |  |
| Errores de seguridad por mala Administración (Servidor y firewall) | X |  |  |  |
| Acceso físico no Autorizado por terceras personas (INFORMACION) |  | X |  |  |

* + 1. **Identificación de Vulnerabilidades**

Las debilidades pueden ocasionar que una amenaza cause daños a un activo y se afecte el normal funcionamiento de la Empresa por este motivo se procede a la identificación de las vulnerabilidades para ello se consideraron tres áreas que determina la metodología SP 800-30, aunque es importante mencionar que las vulnerabilidades pueden ser identificadas en dos frentes distintos, el primero es el que se hace a partir de las sesiones de auditoria que se realizan con los directores o encargados de las áreas de tecnología donde se haga el proceso utilizando para ellos técnicas como la entrevista, la observación, la entrevista dirigida en otre otras técnicas de recolección de información. El segundo frente es el que utilizamos haciendo uso de identificación de vulnerabilidades ya especificas de cada sistema o recurso informático utilizando para ello herramientas y técnicas de ethical hacking como nexus, owasp zap, nmap y tantas otras disponibles incluso en distribuciones especificas para seguridad como Kali Linux.

* Administración
* Operacional
* Técnica

A continuación, se plantean algunos ejemplos de las vulnerabilidades que pueden ser identificadas para cada una de las áreas que propone SP-830.

Tabla 11: Ejemplo criterios administrativos

|  |  |
| --- | --- |
| **Criterios de Administración** | |
| **Criterio** | **Descripción** |
| Asignación de responsabilidades | No existe claridad frente a la definición de roles y responsabilidades. |
| Revisión periódica de los controles de seguridad | No se hace una revisión periódica de controles de seguridad que protejan los activos. |
| Sistemas de autorización | EL manejo de claves secretas por parte de los usuarios se realiza de manera informal. Falta de procedimiento formal para la revisión de los accesos a los sistemas para mirar usuarios y permisos asignados. |

Tabla 12: Ejemplo de criterios operacionales

|  |  |
| --- | --- |
| **Criterios de Operación** | |
| **Criterio** | **Descripción** |
| Seguridad y capacitación técnica | No se cuenta con un documento donde se estipulen los incidentes y las mejoras en seguridad. |
| Evaluación de riesgos | Algunos riesgos sobre los activos más críticos de la empresa no están plenamente identificados y documentados. |
| Revisión periódica de los controles de seguridad | La existencia de controles de seguridad que protejan los activos es escasa. |

Tabla 13: Ejemplo Criterios técnicos

|  |  |
| --- | --- |
| **Criterios de Operación** | |
| **Criterio** | **Descripción** |
| Comunicaciones (Interconexión se sistemas). | No existen barras de puesta a tierra dentro del cuarto de comunicaciones y en rack. |
| Controles de acceso | no se maneja criterios para el control de longitud contraseñas, tiempos de expiración y cambios de estas. |
| No se manejan controles de autenticación para el ingreso al sitio de procesamiento de información (tarjetas de control con códigos etc). |

**Probabilidad de Vulnerabilidades**

Dentro de las organizaciones 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 de acuerdo con la siguiente tabla.

Tabla 14:Valores probabilidad de las vulnerabilidades

|  |  |
| --- | --- |
| **Nivel de probabilidad** | **Definición de la probabilidad** |
| Alta | El threat-source es altamente motivado y suficientemente capaz, y los controles para evitar la vulnerabilidad de ser ejercidas son ineficaces. |
| Media | El threat-source es motivado y capaz, pero los controles están en el lugar que pueden impedir el ejercicio exitoso de la vulnerabilidad |
| 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. |

Ejemplo de la clasificación de la probabilidad

Tabla 15: Ejemplo cálculo de la probabilidad de ocurrencia de una amenaza

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerabilidad** | **Alta** | **Media** | **Baja** |
| La existencia de controles de seguridad que protejan los activos es escasa. | X |  |  |
| El manejo de aplicaciones está más enfocado a lo funcional y no se tienen controles adecuados de seguridad |  | X |  |
| Algunos riesgos sobre los activos más críticos de la empresa no están plenamente identificados y documentados. |  | X |  |

* + 1. **Análisis de Controles**

El análisis de controles es la actividad que permite la utilización del estándar ISO 270001 en este caso en su versión más reciente la versión 2022 en donde debemos tener en cuenta la nueva distribución de acuerdo con la actualización de la norma.

Para la versión de ISO 27001:2013 esta contaba con un total de 132 controles distribuidos en 14 dominios y 35 objetivos de control, sin embargo, después de la actualización de la norma la nueva versión de ISO 27001:2022 quedo distribuida en 4 grandes grupos de control y 93 controles distribuidos de la siguiente manera:

* Controles administrativos = 37
* Controles de Personas = 8
* Controles Físicos = 14
* Controles tecnológicos = 34

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

Tabla 16: Ejemplos de 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 |

De acuerdo con el ejercicio o ejemplo que se viene desarrollando podemos realizar el siguiente ejemplo:

|  |  |  |  |
| --- | --- | --- | --- |
| **Activo** | **Controles Físicos** | **Controles Técnicos** | **Controles Administrativos** |
| Servidor |  | * Autenticación a nivel de la red * Técnicas de Cifrado y encriptación | * Entrenamiento y conocimiento * Políticas de seguridad |
| Firewall | * Biométrica (incluye huellas digitales, voz, rostro, iris, escritura a mano y otros métodos automatizados utilizados para reconocer individuos) | * Técnicas de Cifrado y encriptación |  |

* + 1. **Análisis del Impacto**
    2. **Determinación del Riesgo**
    3. **Recomendaciones de Controles**
    4. **Documentación de Resultados**

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** |
|  |  |  |
|  |  |  |

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. |
|  |  |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

* 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

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 | Noviembre 19 de 2020 |
|  |  |  |  |

1. **CONTROL DE CAMBIOS**

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

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