**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** | 2 |
| **NOMBRE DEL COMPONENTE FORMATIVO** | La clasificación y Valuación de activos. |
| **BREVE DESCRIPCIÓN** | |  | | --- | | El presente componente formativo se centra en conocer todo el proceso para la identificación, categorización y valuación de los activos de información de cualquier organización, así como las diferentes estrategias que podemos utilizar al momento de realizar la recolección de información para la identificación de los activos. | |
| **PALABRAS CLAVE** | Activo, información, clasificación, valoración. |

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPETENCIA** | **220501108 diagnóstico del estado actual de la ciberseguridad de la organización** | **RESULTADOS DE APRENDIZAJE** | 220501108 - 01 Determinar métodos de análisis y valoración de riesgos de ciberseguridad, de acuerdo con estándares internacionales y normatividad nacional |

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

1. **TABLA DE CONTENIDOS:**

**Introducción**

**1.Técnicas de recolección de información**

1.1 Conceptos

1.2 Técnicas

1.2.1 Observación

1.2.1.1 Observación participante o no estructurada

1.2.1.2 Observación no participante o estructurada

1.2.2 Entrevista

1.2.3 Encuestas

1.2.4 Técnica Delphi

1.2.5 Características

**2. La Identificación de los activos**

2.1 Tipos de Activos

2.1.1 Activos Tangibles o Materiales

2.1.2 Activos Intangibles

**3. Actividades para realizar el inventario de activos**

3.1 Inventario de Activos

3.2 Propiedad de los activos

3.3 Clasificación de la Información

3.4 Etiquetado y manipulación de la información

**4 modelos y estándares de Referencia en Ciberseguridad**

4.1 ¿Qué es un estándar?

4.2 Clases

4.3 Familia ISO

4.3.1 ISO/IEC 27001:2022

4.3.1.1 El Anexo A

4.3.2 ISO 27002

4.3.3 Familia NIST

4.3.3.1 Objetivos

4.3.3.2 Alcance

4.3.3.3 Características

4.3.3.4 Aplicación.

4.3.4 Controles de Servicio y Organización 2 (SOC 2)

4.3.4.1 Objetivo

4.3.4.2 Los principios de la norma SOC 2

4.3.5 Modelos COSO

4.3.5.1 Ventajas de Coso

4.3.6 COBIT (Modelo para la auditoría y control de sistemas de información)

4.3.6.1 Principios de COBIT

1. **DESARROLLO DE CONTENIDOS:**

**Introducción**

los lineamientos básicos que deben ser utilizados por los responsables de la seguridad de la información, para poner en marcha la gestión y clasificación de activos de información que son manejados por la entidad, con el fin de determinar que activos posee, de cómo deben ser utilizados, los roles y responsabilidades que tienen los usuarios sobre los mismos y, reconociendo adicionalmente el nivel de clasificación de la información que a cada activo debe dársele.

1. **Técnicas de recolección de información**

Las técnicas de recolección de información involucran los métodos para la captura o toma de datos que se pueden aplicar en las investigaciones o procesos de una organización, los mismos se pueden dar en forma cualitativa o cuantitativa. Es importante resaltar que en la recolección de la información se debe validar la calidad de la información y sus fuentes.

* 1. **Conceptos**

En la recolección de información es importante considerar los siguientes conceptos.

* Información primaria. Es la información que se recolecta directamente por medio de un sujeto directo con su objeto de investigación.
* Información secundaria. Es aquella que se recopila con base en investigaciones realizadas o fuentes de información con propósitos diferentes. La información secundara es recolectada sin tener contacto directo con el objeto de análisis.
* Objeto: Elemento, proceso, área que puede ser objeto de interacción, análisis e investigación por uno o más individuos.
* Sujeto. Actor o individuo que interactúa o participa con un objeto.
  1. **Técnicas**

Existen técnicas de recolección de información, las mismas pueden ser aplicadas en diversos ámbitos y contextos, conocer las mismas es importante para levantar los datos e información necesaria dentro del análisis de riesgos de ciberseguridad. A continuación, se describen las principales técnicas de recolección de información.

* + 1. **Observación**

La técnica de observación permite recolectar datos e información mediante la práctica de examinar o analizar un objeto determinado, aplicando la planeación, ejecución y evaluación. La observación se puede dar participante o no participante, como se explican a continuación.

* + - 1. **Observación participante o no estructurada**

"La técnica de la observación no estructurada es aquella en la cual el investigador tiene, como propósito principal, lograr un conocimiento exploratorio y aproximado de un fenómeno, en vez de tratar de comprobar alguna hipótesis. Se denomina no estructurada en el sentido que el investigador no tiene conocimiento tal del fenómeno que le permita desarrollar un plan específico para hacer las observaciones, antes de empezar a recoger los datos. Aquella observación en la cual el observador o investigador asume el papel de miembro del grupo, comunidad o institución que está investigando, y como tal, participa en su funcionamiento cotidiano." Gallardo y Moreno (1999).

* + - 1. **Observación no participante o estructurada**

"Se refiere a la información que puede ser determinada mediante observaciones directas de la praxis del docente durante los procesos áulicos de enseñanza y aprendizaje, con las mínimas interferencias posibles, considerando las fases de planificación, evaluación y realización; también, considera elementos observables que pueden influir en estos procesos, como la limpieza, la acústica, la iluminación, la distribución espacial, entre otros." Chaves (2009)

* + 1. **Entrevista**

Consiste en la recolección de información por medio de un encuentro en donde se desarrolla un proceso verbal narrativo en donde se plantean una serie de preguntas sobre un tema de estudio en la que un sujeto de análisis responde según los conocimientos, experiencias, opiniones, percepción y explicaciones, que pueden ser soportar en documentación anexa para la validación.

Las entrevistas suelen realizarse planteando principalmente preguntas abiertas y cerradas según el contexto que se requiera. Por ejemplo; Una pregunta abierta en una investigación en seguridad sería, ¿Cómo se desarrolla el análisis de riesgos?, Y una pregunta cerrada sería, Seleccione el tipo de activo de información: a) Software; b) Hardware; c) Datos; e) Personas d) Otro.

* + 1. **Encuestas**

Consiste en la recolección de información de manera estructurada, ordenada en donde al igual que en una entrevista se plantean preguntas abiertas y principalmente cerradas, esto en función obtener los datos o información con la mayor precisión posible para su futuro análisis, toma de decisiones o reportes. En las encuestas se aplican diversos tipos de variables, de tal forma que logren abordar los aspectos necesarios para la recolección de la información requerida.

* + 1. **Técnica Delphi**

Consiste en una técnica repetitiva para llegar a un acuerdo en un grupo de expertos. Esta técnica permite evitar sesgos, los expertos reciben un cuestionario el cual responden y devuelven al investigador, el cual organiza y categoriza los resultados, posteriormente devuelve a los sujetos expertos brindando la opción de cambiar las respuestas, el cambio en las respuestas se debe registrar y justificar, los expertos validaran las respuestas llegando a consensos permitiendo entregar información más precisa en relación a los diferentes aspectos evaluados. Basado en Gallardo y Moreno (1999).

* + 1. **Características.**

Las técnicas de recolección de información pueden apropiar las siguientes características.

* Técnicas Cualitativas: Las mismas pueden presentar alto nivel de entendimiento de los datos e información. La relevancia está dada en las respuestas individuales y su nivel de profundidad. Tienen un alto nivel de subjetividad y dependen del conocimiento, experiencia y percepción que un sujeto tiene sobre el objeto de estudio.
* Técnicas Cuantitativas: Su base fundamental son los datos numéricos que representan características o detalles particulares de un objeto de estudio. Una gran cantidad de datos sobre uno o más atributos de un objeto de estudio que permita generalizar en los resultados obtenidos, facilitando la comprensión y toma de decisiones.
* Registro de datos: Consiste en el proceso de recopilar los datos o información obtenida cuando se aplican técnicas de recolección de información, este es un elemento importante que puede ser aplicado en papel y archivos físicos, en medios digitales tales como documentos de procesadores de texto, registros multimedia (Imagen, audio, video), aplicaciones software y bases de datos digitales.

1. **La Identificación de los activos**

Para la realización de este proceso se utilizará como referencia la norma ISO 27001:2017 en la cual en el anexo A incluye como control la correcta gestión de los activos de información.



Imágen : Procedimiento a Seguir en el Inventario de Activos: tomado de MINTIC Gestión y clasificación de activos

* 1. **Tipos de Activos**

Los activos los podemos separar en dos grandes grupos: tangibles e intangibles. Los activos tangibles son aquellos activos materiales que contienen información, y sobre los que tomaremos medidas preventivas para protegerlos principalmente de riesgos físicos: golpes, agua, fuego, etc. Los activos intangibles son aquellos que soportan la información dentro de un activo material, y pueden inutilizar la información, pese a que el activo físico no haya sufrido daño alguno.

* + 1. **Activos Tangibles o Materiales**

A continuación, se mencionarán algunos ejemplos de los tipos de activos considerados como

tangibles:

**Equipos informáticos**: Cada vez son más los equipos informáticos presentes en las empresas, y pese a no contener información crítica en su interior, sí que tienen acceso a servidores y redes que si la poseen.

**Servidores físicos**: Los servidores propios donde guardamos todos los documentos de la organización o donde se encuentran las aplicaciones informáticas compartidas (ERP, CRM...), y los externos donde alojamos nuestros servicios web y de correo electrónico, suelen ser los Activos más críticos dentro de un sistema de gestión de seguridad de la información.

**Equipos red local:** nuestros equipos informáticos están conectados entre sí por medio de redes inalámbricas o cableadas. Las cuales pueden ser cortadas, obstruidas o interceptadas por atacantes cibernéticos.

**Periféricos y pendrives**: Hay que tener un especial cuidado con escáneres e impresoras donde se deja información impresa olvidada con frecuencia. Los pendrives, CDs, DVDs... suelen perderse con facilidad o quedar olvidados por los cajones con información muy sensible.

**Portátiles, tabletas y móviles:** En esta categoría se incluyen todos aquellos dispositivos electrónicos que salen de nuestras instalaciones habitualmente. Sea por visitas comerciales, porque el trabajador se lo lleva a casa después del trabajo, o se ceden temporalmente a terceros.

**Oficinas e instalaciones**: Las oficinas, los edificios, casas, bodegas industriales, entre otros que contienen los ordenadores, los servidores físicos, los archivadores, la documentación en papel, Por lo que deben ser consideradas como un activo material más, que deberemos proteger.

**Personal propio:** Cada una de las personas que trabajan en la organización, tienen información del negocio en su cabeza: conocimientos del proceso productivo, salarios, contactos de proveedores y clientes., entre otro tipo de información, dependiendo del puesto que ocupe el trabajador, ésta será más o menos sensible.

**Oros contenedores:** Armarios RF, cajas fuertes, archivadores, estanterías, salas refrigeradas para servidores, cuartos de archivo, entre otros, son activos físicos que podemos tener en nuestra organización, y deberemos identificar.

* + 1. **Activos Intangibles**

Entre otros, los siguientes son ejemplos de activos intangibles que puede poseer cualquier organización:

**Aplicaciones informáticas:** cualquier software que contenga o gestione información del negocio, será un Activo: el ERP, aplicaciones de contabilidad, el CRM, Aplicaciones ofimáticas (Word, Excel, PowerPoint), software de control de calidad, aplicaciones de gestión de proyectos o producción, software de nómina, entre otros.

**Gestores de copias de seguridad:** las aplicaciones de creación y restauración de copias de seguridad se tratan como herramientas diferentes a las anteriores, dado que se debe garantizar su disponibilidad en el caso de caída grave del resto de sistemas.

**Sistemas operativos**: Dado que soportan el resto de aplicaciones informáticas y que son uno de los principales objetivos de los virus informáticos, los gestionaremos de manera especial al resto del software.

**Comunicaciones:** Las comunicaciones con el exterior también son críticas ante una situación de emergencia, por lo que se tratarán de forma diferente: los servicios telefónicos, el acceso a internet y los servidores de correo electrónico.

**Gestores de bases de datos:** el mal funcionamiento de una aplicación puede suponer una pérdida de accesibilidad de la información durante un tiempo determinado. Pero la caída del gestor de bases de datos que hay detrás, puede generar la perdida de una parte del contenido o su totalidad. Por lo que requiere de un cuidado más exigente y delicado.

**Suministros:** la perdida de suministro eléctrico durante un espacio de tiempo prolongado puede suponer la caída de los sistemas de información de la organización. Por lo que deberemos tener alternativas a nuestro proveedor habitual de estos servicios.

1. **Actividades para realizar el inventario de activos**

De acuerdo con la norma ISO 27001 sobre la cual basamos el desarrollo de este componente formativo las siguientes son las actividades que deben de ejecutarse en el proceso de control de los activos informáticos.

* 1. **Inventario de Activos**

todos los activos deben estar claramente identificados y la entidad debe elaborar y mantener un inventario de estos, las siguientes son algunas pautas que podemos aplicar para la realización de esta actividad.

* Identifique los servicios tanto internos como externos de la organización
* ¿Qué información necesita para desarrollar los servicios?
* ¿Qué infraestructura está involucrada en la prestación de los servicios?
* Hardware, por ejemplo, computadoras portátiles, servidores, impresoras, pero también teléfonos móviles o memorias USB.
* Infraestructura: oficinas, electricidad, aire acondicionado etc.
* ¿Aplicaciones Software están involucradas en la prestación de los servicios? No solo el software comprado, sino también el software gratuito y el software desarrollado in house.
* Identifique las actividades subcontratadas
  + Servicios legales
  + Servicios de limpieza
  + Servicios en la nube
  + Servicios de correo
  + Entre otros
* Identifique las personas de las que dependen los servicios. Considere que tipo de información relevante para el negocio se puede encontrar solo en “las cabezas” de ciertas personas y que a menudo no está disponible en otras formas.
* Determine los medios por los que se transmite la información
* Identifique los soportes en los que se encuentra la información: no solo en soportes electrónicos como bases de datos, archivos en PDF, Word, Excel y otros formatos, sino también en papel y otras formas.
  1. **Propiedad de los activos**

Los activos de información del inventario deben tener un propietario o responsable. Se recomienda establecer una tabla que permita determinar claramente la siguiente información:

* Nombre del Proceso
* Dueño o propietario del proceso
* Nombre del Activo
* Descripción del Activo
  1. **Clasificación de la Información**

La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada, El sistema de clasificación definido se basa en la confidencialidad como principio rector en la selección e incluye el tratamiento de la información en cuanto a la Confidencialidad, la Integridad y la Disponibilidad de cada activo.

En esta parte se debe agregar a la tabla ya existente de propiedad de los activos la siguiente información:

* Tipo de activo de información / Medio
  + Copia impresa, archivo electrónico: (especificar tipo)
  + Medio / dispositivo extraíble: (especificar tipo)
* ¿Contiene Datos personales?
* ¿Contiene Datos personales Sensibles?
* Confidencialidad (Alta – Media – Baja)
* Disponibilidad (Alta – Media – Baja)
* Integridad (Alta – Media – Baja)

En esta parte para realizar una correcta clasificación de activos según la confidencialidad, integridad y disponibilidad se recomienda la utilización de las siguientes tablas:

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, Esta se debe definir de acuerdo con las características de los activos que se manejan en cada entidad.

Tabla : Clasificación de acuerdo con la confidencialidad

|  |  |
| --- | --- |
| Confidencial | acceso restringido a la alta dirección |
| Restringido | directores de área y empleados clave tienen acceso. |
| Interno | relativo a la información accesible solo los miembros de la organización, pero en cualquier nivel. |
| Público | todas las personas, dentro y fuera de la organización, tienen acceso. |

Para la integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. Se recomienda el siguiente esquema de clasificación de tres (3) niveles:

Tabla : Clasificación de acuerdo a la Integridad

|  |  |
| --- | --- |
| A  (Alta) | Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad. |
| M  (Media) | Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad. |
| B  (Baja) | Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos |
| No Clasificado | Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser  tratados como activos de información de integridad ALTA. |

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

Tabla : Clasificación de acuerdo a la Disponibilidad

|  |  |
| --- | --- |
| A  (Alta) | Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad. |
| M  (Media) | Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad. |
| B  (Baja) | Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos |
| No Clasificado | Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser  tratados como activos de información de integridad ALTA. |

La clasificación de los activos de información se basa en los tres criterios de seguridad, Confidencialidad Integridad y Disponibilidad, asimismo contempla el impacto que causaría la perdida de alguna de estas propiedades, por lo tanto, se definen 3 niveles que permiten determinar la criticidad o el valor general del activo de información.

|  |  |
| --- | --- |
| A  (Alta) | Activos de información en los cuales la clasificación de la  información en dos o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta. |
| M  (Media) | Activos de información en los cuales la clasificación de la  información es alta en una de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel medio |
| B  (Baja) | Activos de información en los cuales la clasificación de la  información en todos sus niveles es baja |

* 1. **Etiquetado y manipulación de la información**

Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

A continuación, se proponen una seria de ítems que podrían ser tenidos en cuenta para realizar este proceso y se deberían tener en cuenta las siguientes pautas generales:

* Se etiquetarán todos los Activos de Información que estén clasificados según el esquema clasificación en Confidencialidad, Integridad y disponibilidad.
* Se etiquetará el nivel de clasificación en relación a Confidencialidad, Integridad y Disponibilidad.
* Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como NO CLASIFICADA.
* Cada Activo de Información debe ser etiquetado teniendo en cuenta el esquema de clasificación, y en el campo correspondiente diligenciar la clasificación de la siguiente forma: {Clasif.Confidencialidad} - {Clasif.Integridad} - { Clasif.Disponibilidad}.
* Para los activos clasificados en confidencialidad se podría utilizar la etiqueta IC, IR, IP, ISC
* Para los activos clasificados en integridad como ALTA se utilizará la etiqueta A, MEDIA, M y BAJA, B.
* Para los activos clasificados en disponibilidad como ALTA se utilizará la etiqueta 1, MEDIA, 2 y BAJA, 3.

De esta manera se realizarían las combinaciones de acuerdo con los criterios de clasificación de la información.

Nota: Para desarrollar el proceso de identificación y clasificación de los activos utilizar el formato adjunto denominado: Formato de Categorización de Activos.xlsx

1. **Modelos y estándares de Referencia en Ciberseguridad** 
   1. **¿Qué es un estándar?**

La normalización o estandarización tiene como función la elaboración de una serie de especificaciones técnicas – NORMAS – que son adoptadas de manera voluntaria. La legislación (Artículo 8 de la Ley 21/1992 de Industria) define el concepto de norma como “la especificación técnica de aplicación repetitiva o continuada cuya observancia no es obligatoria, establecida con participación de todas las partes interesadas, que aprueba un Organismo reconocido, a nivel nacional o internacional, por su actividad normativa.”

* 1. **Clases**

Existen varios estándares de seguridad informática, incluido el grupo de estándares ISO/IEC 27000 que hacen parte de un sistema de administración de seguridad de la información (information security management system ISMS) el cual va dirigido a la seguridad de la información bajo un detallado control administrativo de la misma, está el grupo de estándares NIST en el cual encontramos el Marco para la mejora de la seguridad cibernética en infraestructuras críticas, El SOC2 o controles de servicio y organización 2 el cual es un estándar internacional creado por el Instituto Americano de Contables Públicos Certificados (AICPA) el cual es un estándar de informes sobre los sistemas de gestión de los riesgos de ciberseguridad de las organizaciones.

Finalmente podemos mencionar el modelo COSO (Committee of Sponsoring Organizations of the Tradeway Commission) este modelo es propuesto por varias empresas y compañías privadas en los estados unidos buscando estandarizar las orientaciones a las entidades sobre aspectos fundamentales de gestión ejecutiva y de gobierno, ética empresarial, control interno, gestión del riesgo empresarial, control de fraude y prestación de informes financieros.

COBIT (Control Objectives for Information and related Technology) el cual proporciona un marco de trabajo con buenas practicas para la gestión se los sistemas de información de las compañías.

El ISO 15408 permite que diferentes aplicaciones de software puedan ser integradas y probadas de forma o manera segura.

El RFC 2196 es memorándum publicado por el Internet Engineering Task Force para el desarrollo de políticas y procedimientos de seguridad para sistemas de información conectados a Internet

Para el campo industrial, se inició en el año 2007, con el grupo de trabajo de la International Society for Automation (ISA), el estándar ISA-99 denominado Security for Industrial Automation and Control Systems con la publicación del estándar ANSI/ISA-99.00.01-2007 Security for Industrial Automation and Control Systems: Concepts, Terminology and Models, en conjunto con el reporte técnico ANSI/ISA-TR99.00.01-2007, Security Technologies for Manufacturing and Control Systems. A principios de 2009, fue aprobado por ANSI el estándar ANSI/ISA-99.02.01-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program. Y finalmente en el año 2010, se cambió por el estándar ISA/IEC 62443 para alinear la numeración de la documentación del estándar con los estándares correspondientes de la International Electrotechnical Commission (IEC).

* 1. **Familia ISO**
     1. **ISO/IEC 27001:2022**

Teniendo en cuenta el enfoque que se le ha dado al proyecto es importante adoptar aspectos y lineamientos de la ISO 27001:2022,ISO 27002, ISO 27032 perteneciente a la familia ISO 27000 y NISTSP 800 perteneciente a la familia NIST.

ISO 27000 es un estándar Internacional que ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos y sus sistemas de apoyo cambien a lo largo del tiempo. Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple.

Los requerimientos establecidos en este Estándar Internacional son genéricos y están diseñados para ser aplicables a todas las organizaciones, sin importar el tipo, tamaño y naturaleza. No es aceptable laexclusión de ninguno de los requerimientos especificados en las Cláusulas 4, 5, 6, y 8 cuando una organización asegura su conformidad con este Estándar Internacional.

* + - 1. **El Anexo A**

Es un documento normativo que sirve como guía para implementar los controles de seguridad específicos de ISO 27001. Todos estos controles están dirigidos a mejorar la Seguridad de la información, probablemente, el anexo más nombrado de todas las normas de gestión.

Dicho anexo está compuesto de 114 controles de seguridad, sin embargo, como hemos dicho anteriormente, solo se aplicarán aquellos que sean necesarios para este componente. Está compuesto por 93 controles de seguridad agrupados en 4 dominios o grandes grupos de controles que son los siguientes:

* Controles Organizacionales: 37 controles de los cuales 3 son nuevos.
* Controles al Personal: 8 controles, sin cambios respecto a la versión anterior.
* Controles Físicos: 14 controles de los cuales 1 es nuevo.
* Controles Tecnológicos: 34 controles de los cuales 7 son nuevos.

A continuación, mencionaremos los controles de seguridad de la norma actual para ISO 27001:

1. **Controles Organizacionales**

5.11 Devolución de activos

Control: El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo.

5.12 Clasificación de la información

Control: La información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la organización sobre la base de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.

5.13 Etiquetado de la información

Control: Se debe elaborar y implementar un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el sistema de clasificación de la información adoptado por la organización.

5.14 Transferencia de información

Control: Las reglas, procedimientos o acuerdos de transferencia de información deben estar vigentes para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.

5.15 Control de acceso

Control: Las normas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar sobre la base de los requisitos de seguridad empresarial y de la información.

5.16 Gestión de identidades

Control: Se debe gestionar el ciclo de vida completo de las identidades.

5.17 Información de autenticación

Control: La asignación y gestión de la información de autenticación se debe controlar mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.

5.18 Derechos de acceso

Control: Los derechos de acceso a la información y otros activos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política y reglas específicas de la organización para el control de acceso.

5.19 Seguridad de la información en las relaciones con proveedores

Control: Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.

5.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores

Control: Los requisitos pertinentes de seguridad de la información se deben establecer y acordar con cada proveedor en función del tipo de relación con el proveedor.

5.21 Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las

telecomunicaciones (TIC)

Control: Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.

5.22 Seguimiento, revisión y gestión del cambio de los servicios de los proveedores

Control: La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información de los proveedores y la prestación de servicios

5.23 Seguridad de la información para el uso de servicios en la nube

Control: Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer, de acuerdo con los requisitos de seguridad de la información de la organización.

5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

Control: La organización debe planificar y preparar la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de

incidentes de seguridad de la información.

5.25 Evaluación y decisión sobre eventos de seguridad de la información

Control: La organización debe evaluar los eventos de seguridad de la información y debe decidir si clasificarse como incidentes de seguridad de la información.

5.26 Respuesta a incidentes de seguridad de la información

Control: Los incidentes de seguridad de la información se deben responder de conformidad con los procedimientos documentados.

5.27 Aprender de los incidentes de seguridad de la información

Control: Los conocimientos adquiridos a partir de incidentes de seguridad de la información se deben utilizar para reforzar y mejorar los controles de seguridad de la información.

5.28 Recopilación de evidencias

Control: La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.

5.29 Seguridad de la información durante una interrupción

Control: La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.

5.30 Preparación de las TIC para la continuidad de negocio

Control: La preparación para las TIC se debe planificar, implementar, mantener y probar basado en los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.

5.31 Requisitos legales, legales, reglamentarios y contractuales

Control: Los requisitos legales, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos se deben identificar, documentar y mantener actualizados.

5.32 Derechos de propiedad intelectual

Control: La organización debe implementar procedimientos apropiados para proteger derechos de propiedad intelectual.

5.33 Protección de registros

Control: Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso y liberación no autorizados

5.34 Privacidad y protección de la información de identificación personal (PII, por sus siglas en ingles)

Control: La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.

5.35 Revisión independiente de la seguridad de la información

Control: El enfoque de la organización para administrar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se debe revisar de forma independiente a intervalos planificados o cuando ocurran cambios significativos.

5.36 Cumplimiento de políticas, reglas y estándares de seguridad de la información

Control: El cumplimiento de la política de seguridad de la información, el tema, las políticas específicas, las reglas y los estándares de la organización se debe revisar periódicamente.

5.37 Procedimientos operativos documentados

Control: Los procedimientos operativos de las instalaciones de procesamiento de la información se debe documentar y poner a disposición del personal que los necesite

**6 Controles de personas**

6.1 Selección

Control: Las verificaciones de antecedentes de todos los candidatos para convertirse en personal se deben llevar a cabo antes de unirse a la organización y de forma continúa teniendo en cuenta las leyes, regulaciones y ética aplicables y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.

6.2 Términos y condiciones de empleo

Control: Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información.

6.3 Conciencia de seguridad de la información, educación y formación

Control: El personal de la organización y las partes interesadas pertinentes deben recibir información, educación y capacitación adecuadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea pertinente para su función laboral.

6.4 Proceso disciplinario

Control: Se debe formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información.

6.5 Responsabilidades después de la terminación o cambio de empleo

Control: Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se debe definir, hacer cumplir y comunicar al personal pertinente y a otras partes interesadas.

6.6 Acuerdos de confidencialidad o no divulgación

Control: Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados y firmados periódicamente por

el personal y otras partes interesadas pertinentes.

6.7 Trabajo remoto

Control: Las medidas de seguridad se deben implementar cuando el personal trabaje de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización.

6.8 Informes de eventos de seguridad de la información

Control: La organización debe proporcionar un mecanismo para que el personal informe oportunamente sobre los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados.

**7 controles físicos**

7.1 Perímetros de seguridad física

Control: Los perímetros de seguridad se deben definir y utilizar para proteger las zonas que contengan información y otros activos asociados.

7.2 Entrada física

Control: Las zonas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.

7.3 Asegurar oficinas, habitaciones e instalaciones

Control: Se debe diseñar e implementar la seguridad física de las oficinas, salas e instalaciones.

7.4 Monitoreo de la seguridad física

Control: Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.

7.5 Protección contra amenazas físicas y ambientales

Control: Se debe diseñar e implementar la protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas a las infraestructuras.

7.6 Trabajar en áreas seguras

Control: Se deben diseñar e implementar medidas de seguridad para trabajar en zonas seguras.

7.7 Escritorio y pantalla limpios

Control: Se deben definir e implementar adecuadamente normas claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas claras para las instalaciones de tratamiento de la

información.

7.8 Emplazamiento y protección de equipos

Control: El equipo debe estar situado de forma segura y protegida

7.9 Seguridad de los activos fuera de las instalaciones

Control: Los activos externos deben estar protegidos.

7.10 Medios de almacenamiento

Control: Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y disposición de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.

7.11 Servicios públicos de apoyo

Control: Las instalaciones de procesamiento de la información deben estar protegidas contra los cortes de energía y otras interrupciones causadas por fallos en los servicios públicos de apoyo.

7.12 Seguridad del cableado

Control: Los cables que transporten energía, datos o servicios de información de apoyo deben estar protegidos contra la interceptación, las interferencias o los daños.

7.13 Mantenimiento de equipos

Control: El equipo se debe mantener correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información.

7.14 Disposición o reutilización segura de los equipos

Control: Los elementos de los equipos que contengan medios de almacenamiento se deben verificar para asegurarse de que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura

antes de su disposición o reutilización.

**8 Controles Tecnológicos**

8.1 Dispositivos de punto final de usuario

Control: Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario.

8.2 Derechos de acceso privilegiado

Control: La asignación y el uso de los derechos de acceso privilegiado deben estar restringidos y gestionados.

8.3 Restricción de acceso a la información

Control: El acceso a la información y a otros activos asociados se debe restringir de acuerdo con la política específica establecida sobre el control de acceso.

8.4 Acceso al código fuente

Control: El acceso para leer o escribir sobre un código fuente, las herramientas de desarrollo, y las librerías de software se deben gestionar apropiadamente.

8.5 Autenticación segura

Control: Se deben implementar tecnologías y procedimientos de autenticación seguros basados en restricciones de acceso a la información y en la política específica del tema sobre control de acceso.

8.6 Gestión de la capacidad

Control: El uso de los recursos se debe monitorear y ajustar en función de las necesidades de capacidad actuales y previstas.

8.7 Protección contra malware

Control: La protección contra el malware se debe implementar y respaldar mediante la conciencia adecuada del usuario.

8.8 Gestión de vulnerabilidades técnicas

Control: Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se deben adoptar las medidas apropiadas.

8.9 Gestión de la configuración

Control: Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes se deben establecer, documentar, implementar, monitorear y revisar.

8.10 Eliminación de información

Control: La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se debe eliminar cuando ya no sea necesario.

8.11 Enmascaramiento de datos

Control: El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre control de acceso y otras políticas relacionadas con temas específicos, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.

8.12 Prevención de fugas de datos

Control: Las medidas de prevención de fugas de datos se deben implementar a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.

8.13 Copia de seguridad de la información

Control: Las copias de seguridad de la información, el software y los sistemas se deben mantener y probar periódicamente de conformidad con la política específica sobre copias de seguridad sobre temas específicos.

8.14 Redundancia de las instalaciones de procesamiento de información

Control: Las instalaciones de procesamiento de la información se deben implantar con redundancia suficiente para cumplir los requisitos de disponibilidad.

8.15 Registro

Control: Los registros que guarden actividades, excepciones, fallas y otros eventos pertinentes se deben producir, almacenar, proteger y analizar.

8.16 Actividades de seguimiento

Control: Se debe monitorear el comportamiento anómalo de las redes, los sistemas y las aplicaciones y se deben adoptar las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.

8.17 Sincronización de reloj

Control: Los relojes de los sistemas de procesamiento de información utilizados por la organización se deben sincronizar con las fuentes de tiempo aprobadas.

8.18 Uso de programas de utilidad privilegiados

Control: El uso de programas de utilidad que puedan ser capaces de anular los controles del sistema y de la aplicación debe restringirse y controlarse estrictamente

8.19 Instalación de software en sistemas operativos

Control: Se deben implementar procedimientos y medidas para gestionar de forma segura la instalación de programas informáticos en los sistemas operativos.

8.20 Seguridad de redes

Control: Las redes y los dispositivos de red deben estar asegurados, gestionados y controlados para proteger la información de los sistemas y las aplicaciones.

8.21 Seguridad de los servicios de red

Control: Se deben identificar, implementar y monitorear los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.

8.22 Segregación de redes

Control: Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en las redes de la organización.

8.23 Filtrado web

Control: El acceso a sitios web externos se debe gestionar para reducir la exposición a contenido malicioso.

8.24 Uso de la criptografía

Control: Se debe definir e implementar normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.

8.25 Ciclo de vida de desarrollo seguro

Control: Se deben establecer e implementar normas para el desarrollo seguro de software y sistemas.

8.26 Requisitos de seguridad de las aplicaciones

Control: Los requisitos de seguridad de la información se deben identificar, especificar y aprobar al desarrollar o adquirir aplicaciones.

8.27 Arquitectura de sistemas seguros y principios de ingeniería

Control: Los principios para la ingeniería de sistemas seguros se deben establecer, documentar, mantener y implementar a cualquier actividad de desarrollo de sistemas de información.

8.28 Codificación segura

Control: Los principios de codificación segura se deben implementar al desarrollo de programas informáticos.

8.29 Pruebas de seguridad en el desarrollo y aceptación

Control: Los procesos de ensayo de seguridad se deben definir y implementar en el ciclo de vida del desarrollo.

8.30 Desarrollo externalizado

Control: La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.

8.31 Separación de entornos de desarrollo, evidencia y producción

Control: Los entornos de desarrollo, ensayo y producción deben estar separados y protegidos.

8.32 Gestión del cambio

Control: Los cambios en las instalaciones de procesamiento de la información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.

8.33 Información de las pruebas

Control: La información de las pruebas se debe seleccionar, proteger y gestionar adecuadamente.

8.34 Protección de los sistemas de información durante las pruebas de auditoría

Control: Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de los sistemas operativos se deben planificar y acordar conjuntamente entre el probador y la dirección adecuada.

* + 1. **ISO 27002**

Establece un parámetro para las buenas prácticas, que determinan una serie de objetivos y controles que se integran con la ISO 27001 con relación en el tratamiento de los riesgos.

* + 1. **Familia NIST**

Al igual de la serie de normas ISO 27000, la serie SP 800 proporciona información que cubre la gestión y las prácticas operativas de seguridad de la información, pero en un mayor número de documentos. Para facilitar una guía específica para realizar la integración de la gestión de riesgos de seguridad de la información con las operaciones de la empresa, la serie SP NIST 800 tiene el documento SP 800-39- Gestión de Riesgos de Seguridad.

Para realizar la evaluación de los riesgos, la serie SP 800 tiene un conjunto de documentos que han sido creados utilizando la metodología de riesgo en seis pasos:

* Categorizar: se debe dar prioridad a los sistemas de información que se basan en la evaluación del impacto. El detalle se encuentra en el documento SP 800-60.
* Seleccionar: se deben definir los controles que se deben aplicar, en base a la evaluación del impacto y las bases de SP 800-53, siendo un documento de referencia para este paso.
* Poner en práctica: implementar los controles y la elaboración de los documentos. El detalle se encuentra en el documento SP 800-160.
* Evaluar: la confirmación de que los controles se implantan de forma correcta, operar según lo previsto, y producir los resultados deseados. El detalle lo podemos encontrar en el documento SP 800-53.
* Autorizar: la aceptación del escenario de riesgo, y la autorización para la operación de los sistemas de información y utilización. El detalle se encuentra en el documento SP 800-37.
* Monitorear: se acompaña de forma continua de los sistemas de información y el entorno operativo para establecer la eficiencia y el cumplimiento de los controles. El detalle se encuentra en el documento SP 800-137.
  + - 1. **Objetivos**
* Brindar directrices de referencia para la buena gestión de riesgos de la seguridad de la información y ciberseguridad.
* Propiciar cultura de la seguridad de la información a partir de la concienciación y capacitación del talento humano.
* Ayudar a la protección de los pilares de la seguridad de la información digital (confidencialidad, integridad y disponibilidad)
  + - 1. **Alcance**

La adopción de Normatividad y estándares de seguridad de la información y ciberseguridad es adecuada para implementarse en cualquier organización, sin importar las dimensiones, ya sean pequeñas empresas o grandes empresas esto permite a las mismas la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

* + - 1. **Características**
* La adopción de Normatividad y estándares de seguridad de la información y ciberseguridad otorga una serie de características entre ellas:
* Énfasis y continuo proceso de mejora de su sistema de gestión de seguridad de la información.
* Aclaración de requisitos para la documentación y archivos.
* Valoración de riesgos y procesos de gestión utilizando un modelo de proceso Plan, PHVA (Planificar, Hacer, Verificar, Actuar).
* Sensibilización
  + - 1. **Aplicación.**

Basada en las fases del ciclo planear, hacer, verificar y actuar (PHVA) del SGSI:

* Planear: Establecer el Sistema de gestión de seguridad de la información (SGSI).
* Hacer: Operar el SGSI.
* Verificar: Monitorear y revisar el SGSI.
* Actuar: Mantener y mejorar el SGSI**.**
  + 1. **Controles de Servicio y Organización 2 (SOC 2)**

SOC 2: este modelo de seguridad busca garantizar la seguridad de los datos, La SOC 2 es una certificación creada por el AICPA (American Institute of Certified Public Accountants), en los últimos años sobre todo en europa ha venido creciendo su uso en empresas que ofrecen sistemas y servicios de cloud computing a sus clientes, como SaaS o PaaS.

* + - 1. Objetivo

El SOC 2 tiene por objetivos

* Revisar los servicios prestados por una empresa para que los usuarios puedan evaluar y abordar los riesgos asociados a un servicio externalizado.
* La organización cliente puede pedir al proveedor de servicios que le proporcione un informe de auditoría, especialmente si se le confía información confidencial.
  + - 1. Los principios de la norma SOC 2

La norma SOC 2 define criterios de gestión de datos basados en los Criterios de Servicios Fiduciarios (TSC) de la AICPA. En términos más generales, se basa en los tres principios fundamentales de la ciberseguridad.

* + Disponibilidad. El sistema está operativo y listo para ser utilizado según lo acordado.
  + Integridad. Los datos sólo deben ser modificados por personas autorizadas y según un procedimiento definido.
  + Confidencialidad. La información considerada confidencial se protege de acuerdo con los compromisos y la normativa vigente.

Hay dos tipos de informes SOC 2.

* El "Tipo 1", basado en un informe del primer año de la auditoría, cubre el diseño teórico de los controles.
* El "Tipo 2", basado en la práctica, se produce en los años siguientes y certifica que los controles realizados fueron eficaces durante un periodo completo.
  + 1. **Modelos COSO**

El modelo COSO es un documento guía que contiene las principales directivas y recomendaciones para la implantación, gestión y control de un sistema de control. Debido a su gran nivel de aceptación en los últimos años se ha convertido en un estándar de referencia, en la actualidad existen dos versiones la generada en el año 1992 y la última generada en el año 2004 que agrega al modelo las exigencias de la ley Sarbanes Oxley.

* + - 1. Ventajas de Coso
* Permite a la dirección de la empresa poseer una visión global del riesgo y accionar los planes para su correcta gestión.
* Posibilita la priorización de los objetivos, riesgos clave del negocio, y de los controles implantados, lo que permite su adecuada gestión. toma de decisiones más segura, facilitando la asignación del capital.
* Alinea los objetivos del grupo con los objetivos de las diferentes unidades de negocio, así como los riesgos asumidos y los controles puestos en acción.
* Permite dar soporte a las actividades de planificación estratégica y control interno.
* Permite cumplir con los nuevos marcos regulatorios y demanda de nuevas prácticas de gobierno corporativo.
* Fomenta que la gestión de riesgos pase a formar parte de la cultura del grupo.
  + 1. **COBIT (Modelo para la auditoría y control de sistemas de información)**

Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control Objectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association).

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

* + - 1. Principios de COBIT

Los principios compilados en la nueva guía son:

* **Satisfacer las necesidades de los colaboradores**. Es crítico definir y vincular los objetivos empresariales y los objetivos relacionados con TI.
* **Cubrir la empresa de extremo a extremo**. Las compañías deben cambiar de visión, con el objetivo de considerar el área de TI como un activo y no un costo. Los directivos deben tomar la responsabilidad de gobernar y gestionar los activos relacionados con TI dentro de sus propias funciones.
* **Aplicar un solo marco integrado**. Usar un solo marco de gobierno integrado puede ayudar a las organizaciones a brindar valor óptimo de sus activos y recursos de TI.
* **Habilitar un enfoque holístico.** El gobierno de TI empresarial (GEIT) requiere de un enfoque holístico que tome en cuenta muchos componentes, también conocidos como habilitadores. Los habilitadores influyen en si algo va a funcionar o no. COBIT 5 incluye siete habilitadores para mejorar el GEIT, como los principios, las políticas y marcos; los procesos; la cultura; la información y la gente.
* **Separar al gobierno de la administración.** Los procesos de gobierno aseguran que los objetivos se alcancen mediante la evaluación de las necesidades de los interesados, el establecimiento de la dirección a través de la priorización y la toma de decisiones; y el monitoreo del desempeño, el cumplimiento y el progreso. De acuerdo con los resultados de las actividades de gobierno, la administración de la empresa y de TI entonces debe planear, crear, realizar y monitorear las actividades para asegurar el alineamiento con la dirección que se estableció.

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** |
| Clasificación de la Información | Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado. |
| Propietario de la Información | Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. |
| 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. |
| ISO 27001 | Estándar de Organización de estándares internacionales relacionado con la seguridad de la información. |
| Activo Informático | Todo elemento tecnológico o relacionado con la tecnología necesario para que la organización cumpla con su misión y logre sus objetivos empresariales. |
| Información | Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. |
| Custodio | Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado |
| Usuario | Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información. |
| Estándar | la especificación técnica de aplicación repetitiva o continuada cuya observancia no es obligatoria, establecida con participación de todas las partes interesadas, que aprueba un Organismo reconocido, a nivel nacional o internacional, por su actividad normativa |
| COBIT | Objetivos de Control para Tecnología de Información y Tecnologías relacionadas |
| COSO | Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO) |
| SOC | Controles de Servicio y Organización 2 |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

* ISO 27001. 2020. Implantando ISO 27001 Paso A Paso - La Planificación Del SGSI. [online] Disponible en: <https://normaiso27001.es/fase-4-planificacion-del-sgsi>.
* ISO 27001. 2020. Implantando ISO 27001 Paso A Paso - La Planificación Del SGSI. [online] Available at: <https://normaiso27001.es/fase-4-planificacion-del-sgsi>.
* 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
* Magerit v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Disponible en: https://www.ccn-cert.cni.es/publico/ herramientas/Pilar-5.4.1/web/magerit/Libro\_I\_metodo.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
* Registro de Activos de Información - Registro de Activos de Información. (2023, September 12). Retrieved from <https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-ciudadania/Transparencia/135888:Registro-de-Activos-de-Informacion>
* Osores, M. (2014). Principios de COBIT 5 para el gobierno efectivo de TI. ComputerWeekly.es. Retrieved from <https://www.computerweekly.com/es/cronica/Principios-de-COBIT-5-para-el-gobierno-efectivo-de-TI>
* SOC 2: la auditoría para los controles de ciberseguridad – Instituto Nacional de Contadores Públicos de Colombia. (2023, September 15). Retrieved from <https://incp.org.co/soc-2-la-auditoria-para-los-controles-de-ciberseguridad>

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 1 de 2023 |
|  |  |  |  |

1. **CONTROL DE CAMBIOS**

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

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