PLAN DE RIESGOS

PRESENTADO POR:

JUAN MANUEL CUELLAR BAHAMÓN

JHON ALEXANDER SUAREZ OSSA

PRESENTADO

A: LUIS ANGEL VARGAS NARVAES

SOFTWARE VIII

NEIVA – RIVERA

FUNDACIÓN ESCUELA TECNOLÓGICA DE NEIVA "JESÚS OVIEDO PEREZ"

TABLA DE CONTENIDO

1. INTRODUCCION

Los riesgos iniciales se refieren principalmente a emergencias de carácter natural y tecnológico, cuyas consecuencias vienen determinadas por eventos posteriores y relevantes como terrorismo, disturbios políticos, epidemias y normativa de malware, etc. señalan la necesidad de incorporar nuevas amenazas no solo en el mundo físico sino también en el entorno digital. Trate de comprender los principales riesgos de los recursos de información. El análisis de riesgo de activos de información nos permite comprender un riesgo efectivo de pérdida de confidencialidad, integridad y disponibilidad. Uno de los activos definidos como parte del alcance del análisis

Gestionar eficazmente los riesgos de seguridad de la información y seguridad digital del sistema de información de la entidad, así como participar en sus procesos y activos expuestos, para asegurar la confidencialidad, integridad y disponibilidad de la información de las siguientes formas, teniendo en cuenta la evaluación de los resultados de la evaluación de riesgos del sistema de gestión de seguridad de la información y Se evaluó la aplicación de opciones de manejo de riesgos de seguridad de la información y seguridad digital de acuerdo con las regulaciones aplicables.

Por lo anterior, la entidad implementó el desafío SGSI siguiendo los principios rectores de la estrategia de gobierno en línea MSPI, que a su vez aprobó el Decreto N ° 1078 de 2015 sobre el Reglamento de la Industria de Tecnologías de la Información y las Comunicaciones Decreto N ° 2573 de 2014 , Estableció pautas generales para las estrategias de gobierno en línea.

La defensa y protección de los activos de información es una tarea importante para asegurar la continuidad y desarrollo de los objetivos de la organización y mantener las normas y cumplimiento normativo aplicable a la entidad, además de transferir confianza a la empresa.

Cuanto mayor sea el valor de la información, mayor será el riesgo asociado a su pérdida, deterioro, manipulación indebida o maliciosa. Por tanto, la reorganización del SGSI de Eiatec sas adopta un método de identificación y evaluación de activos de información, y un método de evaluación y tratamiento de riesgos; teniendo en cuenta el impacto de los riesgos en las entidades y sus

grupos de interés, esto es para tratar, gestionar y minimizar. El método de riesgo más eficaz.

De manera similar, el SGSI reorganizado por Eiatec SAS define políticas y procedimientos efectivos consistentes con la estrategia corporativa, como la formulación de medidas de control para el tratamiento de riesgos, y el establecimiento de indicadores de monitoreo y medición continua para asegurar la efectividad del control; en planes de auditoría y revisiones de gestión Con el apoyo de, finalmente se determinan las oportunidades de mejora que pueden mantener la mejora continua del SGSI. El contenido anterior se complementa con el plan de formación y transferencia de conocimientos relacionados con la seguridad de la información y las campañas de sensibilización que lidera la entidad.

Por lo tanto, la entidad introdujo el modelo SGSI adoptado por la entidad según el ciclo PDCA (planificar, ejecutar, verificar y tomar acción) con el fin de cumplir con el marco regulatorio, misión establecida y seguimiento de visión. De este modo Describe las disposiciones aceptadas por la entidad para establecer los antecedentes, políticas, objetivos, alcance, procedimientos, métodos, roles, responsabilidades y autoridad del SGSI; en el marco de la seguridad de la información de acuerdo con las leyes, contratos y requisitos regulatorios aplicables a la entidad.

Para ello, las empresas han adoptado los siguientes lineamientos normativos: NTC / ISO 27001: 2013, que establece los requisitos para la implementación del SGSI, NTC / ISO 31000: 2011, que brinda las mejores prácticas para la gestión de riesgos y planes de gestión de riesgos, como ISO 27002: 2015, ISO 27005: 2009, etc..; buscan mejorar el desempeño y brindar servicios que puedan satisfacer las necesidades y expectativas de las partes interesadas.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

1. Presentar un plan de Riesgo y privacidad de la información, que oriente la implementación de controles de seguridad con base en el modelo de sistema de gestión de seguridad de la información adoptado por Eiatec SAS En Reorganización.

2.2 OBJETIVOS ESPECIFICOS

1. Comunicar e implementar estrategias de seguridad de la información.
2. Mejorar la madurez de la gestión de la seguridad de la información.
3. Implementar y adoptar un modelo de seguridad y privacidad de la información: MSPI Proteger la información y los sistemas de información, acceso, uso, Divulgación, destrucción o destrucción no autorizadas.

3. MARCO NORMATIVO

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019
Modelo de Seguridad y privacidad de la información - MSPI	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC/ISO 31000:2009	Gestión del Riesgo. Principios y directrices.
Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

4. DEFINICIONES

Activo: Cualquier elemento que tenga valor para la organización.

Análisis del riesgo: Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.

Causa: Elemento específico que origina el evento.

Controles: Procesos, políticas y/o actividades que pueden modificar el riesgo.

Criterios de riesgos: Términos de referencia frente a los cuales se evaluará la importancia del riesgo.

Evaluación del riesgo: Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.

Fuente: Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Identificación del riesgo: Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.

Riesgo: Posibilidad o probabilidad de que un evento pueda afectar las funciones de la entidad e impactar el logro de sus objetivos.

Riesgo de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. incluye aspectos relacionados con el ambiente físico, digital y las personas.

Factores externos: Situaciones generadas por agentes externos, las cuales no son controlables por la entidad y que afectan de manera directa o indirecta el proceso

Infraestructura: Conjunto de recursos físicos que apoyan el funcionamiento de la organización y de manera específica el proceso

5. DESARROLLO DEL PLAN

5.1 IDENTIFICACION Y VALORACION DE RIESGOS:

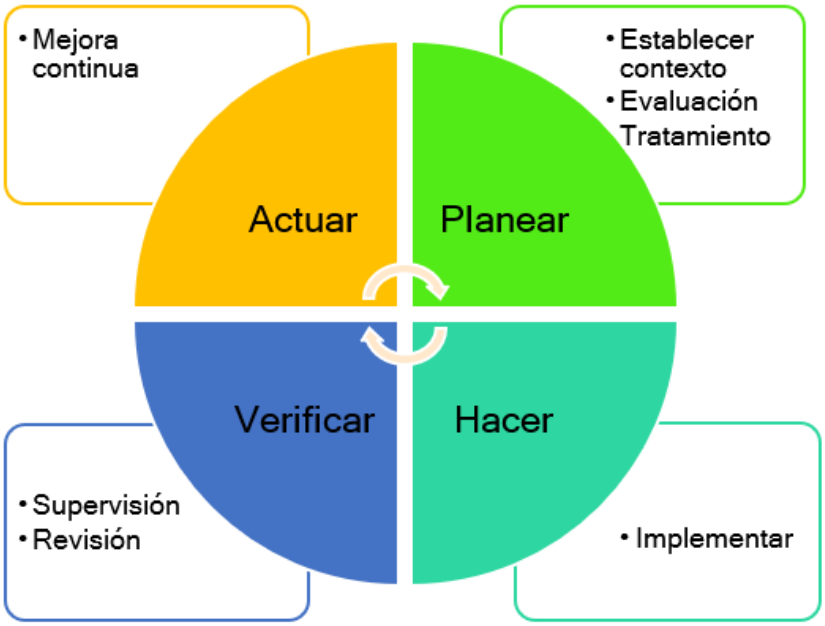
La tecnología de análisis de riesgos de los activos de información nos permite comprender claramente los riesgos de los activos de información que ESAP puede enfrentar desde una perspectiva sistémica y orientada al negocio. Se recomienda utilizar técnicas tradicionales para identificar riesgos específicos asociados con los activos y complementar este proceso tanto como sea posible mediante la identificación de puntos clave de falla, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de fallas.

La información en EIATEC SAS RE ORGANIZACIÓN debe ser determinante para el desarrollo de sus procesos, la correcta implementación de las políticas y la relación con la ciudadanía, por lo que debe estar protegida de cualquier evento de riesgo. Seguridad de la información, que parece ser perjudicial, Tendrá un impacto negativo en el desarrollo normal de las actividades físicas.

El plan propuesto en este documento incluye las siguientes actividades principales: establecer antecedentes, identificación de riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgos y aceptación de riesgos, y de conformidad con las "Directrices de gestión".

La importancia de realizar este tipo de prácticas permite estabilizar a la empresa o entidad, con el fin del poder identificar y evaluar el riesgo de tener un dispositivo físico “confiable”, evaluar si el riesgo es mínimo o leve, y con ello poder analizar las causas y consecuencias para la propia entidad

La gestión de riesgos dentro del alcance de la seguridad de la información también se puede planificar en el ciclo de planificar, ejecutar, verificar y tomar medidas (PDCA), como se muestra en la siguiente figura (ISO 27001: 2013):



5.1.1 RIESGOS DE SEGURIDAD DIGITAL:

Los riesgos provocados por la combinación de amenazas y vulnerabilidades en el entorno digital, y dado su carácter dinámico, también incluyen aspectos relacionados con el entorno físico

5.1.2 RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:

Riesgos que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.

De acuerdo con lo descrito en la norma GTC-ISO/IEC 27035, un incidente de seguridad de la información está definido como “Evento o serie de eventos no deseados o inesperados, que tienen probabilidad significativa de comprometer Las actividades y vulnerar la seguridad”; por consiguiente, se representarían en Riesgos de Seguridad y Privacidad de la Información.

5.1.3 ANÁLISIS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA EMPRESA:

Se identifican los activos de información, con el objetivo de valorarlos e identificar los riesgos de seguridad y privacidad de la información asociada a los factores. En la gestión de valoración del activo, se consideran los siguientes aspectos:

ACTIVOS	DESCRIPCIÓN
Activos Esenciales	**Datos importantes o vitales para la Administración de la Entidad:** Aquellos que son esenciales, imprescindibles para la continuidad de la entidad; es decir que su carencia o daño afectaría directamente a la entidad, permitiría reconstruir las misiones críticas o que sustancian la naturaleza legal de la organización o de sus usuarios. **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012). **Datos Clasificados o Calificados:** Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014).
Datos / Información	**Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.** Ejemplo: Copias de Respaldo, , Datos de Configuración, Contraseñas, Datos de Control de Acceso, Registros de Actividad, Código Fuente,
Hardware / Infraestructura	**Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.** Ejemplo: Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Equipos de Respaldo, Periféricos, Dispositivos Biométricos, Impresoras, Escáneres, Equipos Soporte de la Red , IP interconectados con tecnología Grandstream, IP y 4 NVR para los registros y administración, Lector de huellas biométrico IP para control de acceso, arquitectura Ethernet Router Board Mikrotic RB1100Ahx2.
Software / Aplicaciones Informáticas	**Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.** Ejemplo: Estándar, Navegador, Servidor, Correo Electrónico, Servidor de Correo Electrónico, Sistemas de Gestión de Bases de Datos, Software SOUL GT, Ofimática, Antivirus, Sistema Operativo, Backup o Respaldo,
Servicios	**Funciones que permiten suplir una necesidad de los usuarios (del servicio).** Ejemplo: Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, Gestión de Identidades (altas y bajas de usuarios del sistema)
Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Contratistas, Proveedores.

Soportes de Información	**Dispositivos físicos electrónicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo.** Ejemplo: Discos, Discos Virtuales, Almacenamiento en Red, Memorias USB, CDROM, DVD, Cinta Magnética, Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso.

ACTIVOS	DESCRIPCIÓN
Redes de Comunicaciones	**Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro.** Ejemplo: Red Telefónica, Red Inalámbrica,
Equipos Auxiliares	**Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.** Ejemplo: Fuentes de alimentación, generadores eléctricos, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, paneles solares fibra óptica,
Instalaciones	Lugares donde residen los sistemas de información y comunicaciones.

Determinar el nivel de riesgo según la propia clasificación de la empresa.

Dimensión del Riesgo de Seguridad y Privacidad de la Información	Acción Requerida
Riesgo Extremo	Evadir el riesgo empleando controles que busquen reducir el nivel de probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Alto	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.
Riesgo Moderado	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor. Compartir el riesgo.
Riesgo Bajo	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones defectivas y preventivas.

5.1.4 PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN:

Apoyar el modelo de seguridad de la información dentro de la entidad.
Evidencia de cumplimiento legal y debida diligencia.

1. Desarrolle un plan de respuesta a incidentes.
2. Descripción de los requisitos de seguridad de la información del producto, servicio o mecanismo.
3. El alcance, los límites y la organización del proceso de gestión de riesgos de seguridad de la información.

5.1.5 ANALISIS DE VULNERABILIDADES:

Con base en los resultados obtenidos en el diagnóstico, se pueden identificar las vulnerabilidades de seguridad de la empresa, indicando que existen amenazas reales que pueden afectar los activos físicos.

• A partir del diagnóstico de toda la infraestructura técnica de la empresa, se pueden identificar las vulnerabilidades que presentan riesgos para los activos de información y TI.

• Para evitar pérdidas de información, daños a los equipos por diversos voltajes y servicios deficientes a la comunidad, la operación de las plantas de energía de la empresa es fundamental.

• Determinar el riesgo total en los recursos de red de la entidad, sistemas informáticos, manipulación de información y sistemas de seguridad.

• Se debe crear un plan de gestión de riesgos y un manual de normas y políticas de seguridad informática para evitar que se descubran posibles amenazas en la infraestructura técnica de la entidad.

• De acuerdo con los cambios en la estructura organizacional e infraestructura física y técnica, es necesario actualizar y mejorar las políticas de seguridad en la entidad para enfrentar los riesgos de manera continua.

• Es fundamental diseñar e implementar un modelo de seguridad que permita la continuidad del negocio y el almacenamiento de copias de seguridad dentro y fuera de las instalaciones de la empresa.

• Dado que no existe reporte, reporte o medidas de control que constituyan una mejora al plan de gestión de riesgos de seguridad de la información, es necesario registrar todos los procesos relacionados con la seguridad de la información llevados a cabo por el personal del sistema en la entidad.

• Apoyando esta investigación está la herramienta de evaluación, que se encuentra en un archivo Excel adjunto a la carpeta digital entregada al jefe de la oficina de TIC.

5.1.6 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:

Con base en los resultados del análisis de riesgos de seguridad y privacidad de la información, se proponen medidas de mejora que se pueden implementar mediante acciones o planes de procesamiento para que la información mantenga siempre su confidencialidad. , Integridad y disponibilidad son lo mismo, este es el proceso de selección e implementación de medidas para modificar el nivel de riesgo.

La formulación de actividades de tratamiento de riesgos de seguridad de la información y su aplicación de acuerdo con la valoración del riesgo inherente documentado.

5.1.7 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN:

la empresa Eiatec "evaluará el plan de tratamiento de riesgos de seguridad y privacidad de la información mediante el monitoreo necesario" para verificar si el comportamiento se está realizando y evaluar su eficiencia de ejecución, y verificarlo al menos una vez. Un año o cuando sea necesario, resalte todas las situaciones o factores que puedan afectar la implementación de las medidas de tratamiento.

El responsable del proceso, el responsable de control interno y coordinación de las TIC, quien debe encargarse del seguimiento anual o en un momento determinado, aplicar y proponer las correcciones y ajustes necesarios para promover una gestión eficaz de los riesgos de seguridad. Y privacidad de la información.

6. CONCLUSIONES

El tratamiento seguro a la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la entidad. Este proceso es el que constituye un Sistema de seguridad que brindará un sistema de calidad para la seguridad de la información, La evaluación de los sistemas de información y las características de los equipos arrojó un análisis positivo, pero las conexiones están en su mayoría expuestas a riesgos y no cumplen estándares de seguridad para los equipos informáticos. El análisis de seguridad en la estructura de la red no satisface los requerimientos de funcionalidad en la entidad, por lo que se dejó planteada una implementación de red estructurada. Es importante resaltar que el diagnóstico permite al personal directivo de la entidad tomar las medidas necesarias para garantizar la protección e integridad de toda su información

GUIA PLAN DE RIESGO SOFTWARE PILAR

Resumen - Este documento trata de cómo realizar un plan de riesgos para la propia entidad EIATEC para la seguridad de su sistema de información con el fin de defender y proteger los activos vigentes haciendo el uso correcto del sistema para asegurar la continuidad y desarrollo de los objetivos de la organización. La entidad esta utilizado el modelo SGSI adoptado por la entidad según el ciclo PDCA (planificar, ejecutar, verificar y tomar acción) con el fin de cumplir con el marco regulatorio, misión establecida, etc. y haciendo uso de las normas ISO tomando en cuenta las buenas prácticas.

I. INTRODUCCION

Si los factores de riesgo iniciales están relacionados principalmente con emergencias de naturaleza natural y tecnológica, cuyas consecuencias están determinadas por hechos posteriores y Relevante, como terrorismo, disturbios políticos, epidemias y regulaciones Malware, etc. señalan la necesidad de incorporar nuevas amenazas, No solo en el mundo físico, sino también en el entorno digital Trate de comprender los riesgos más importantes de los activos de información. Análisis El riesgo de los activos de información nos permite comprender y Riesgo efectivo de pérdida de confidencialidad, integridad y disponibilidad. Uno de los activos definidos como parte del alcance de análisis.

Gestionar eficazmente los riesgos de seguridad de la información y seguridad digital del sistema de información de la entidad, así como participar en sus procesos y activos expuestos, para asegurar la confidencialidad, integridad y disponibilidad de la información de las siguientes formas, teniendo en cuenta la evaluación de los resultados de la evaluación de riesgos del sistema de gestión de seguridad de la información y Se evaluó la aplicación de opciones de manejo de riesgos de seguridad de la información y seguridad digital de acuerdo con las regulaciones aplicables.

siguiendo los principios rectores de la estrategia de gobierno en línea MSPI, que a su vez aprobó el Decreto N ° 1078 de 2015 sobre el Reglamento de la Industria de Tecnologías de la Información y las Comunicaciones Decreto N ° 2573 de 2014 ,

Estableció pautas generales para las estrategias de gobierno en línea.

La defensa y protección de los activos de información es una tarea importante para asegurar la continuidad y desarrollo de los objetivos de la organización y mantener las normas y cumplimiento normativo aplicable a la entidad, además de transferir confianza a la empresa.

Cuanto mayor sea el valor de la información, mayor será el riesgo asociado a su pérdida, deterioro, manipulación indebida o maliciosa. Por tanto, la reorganización del SGSI de Eiatec sas adopta un método de identificación y evaluación de activos de información, y un método de evaluación y tratamiento de riesgos; teniendo en cuenta el impacto de los riesgos en las entidades y sus grupos de interés, esto es para tratar, gestionar y minimizar. El método de riesgo más eficaz.

De manera similar, el SGSI reorganizado por Eiatec SAS define políticas y procedimientos efectivos consistentes con la estrategia corporativa, como la formulación de medidas de control para el tratamiento de riesgos, y el establecimiento de indicadores de monitoreo y medición continua para asegurar la efectividad del control; en planes de auditoría y revisiones de gestión Con el apoyo de, finalmente se determinan las oportunidades de mejora que pueden mantener la mejora continua del SGSI. El contenido anterior se complementa con el plan de formación y transferencia de conocimientos relacionados con la seguridad de la información y las campañas de sensibilización que lidera la entidad.

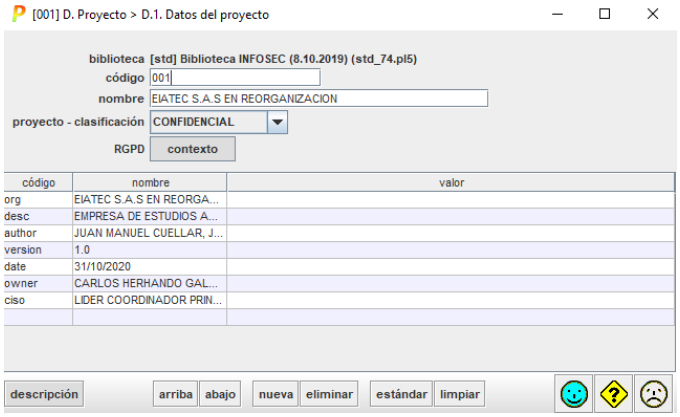
Por lo tanto, la entidad introdujo el modelo SGSI adoptado

por la entidad según el ciclo PDCA (planificar, ejecutar, verificar y tomar acción) con el fin de cumplir con el marco regulatorio, misión establecida y seguimiento de visión. De este modo Describe las disposiciones aceptadas por la entidad para establecer los antecedentes, políticas, objetivos, alcance, procedimientos, métodos, roles, responsabilidades y autoridad del SGSI; en el marco de la seguridad de la información de acuerdo con las leyes, contratos y requisitos regulatorios aplicables a la entidad.

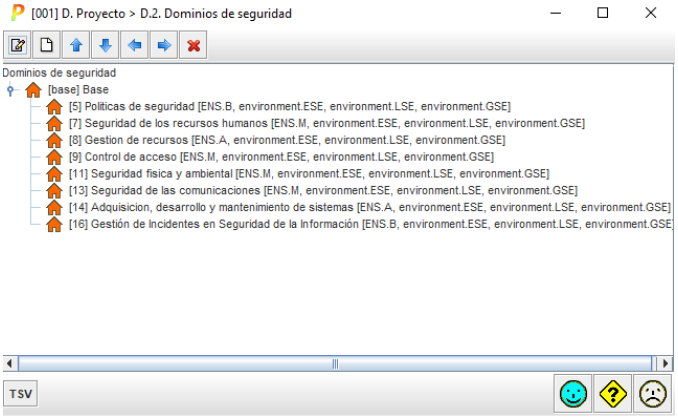
Para ello, las empresas han adoptado los siguientes lineamientos normativos: NTC / ISO 27001: 2013, que establece los requisitos para la implementación del SGSI, NTC / ISO 31000: 2011, que brinda las mejores prácticas para la gestión de riesgos y planes de gestión de riesgos, como ISO 27002: 2015, ISO 27005: 2009, etc..; buscan mejorar el desempeño y brindar servicios que puedan satisfacer las necesidades y expectativas de las partes interesadas.

II. PROCEDIMIENTO PARA EL ENVIÓ DEL TRABAJO

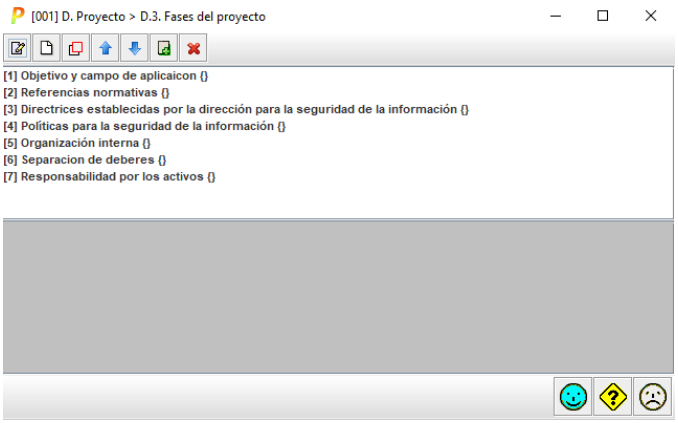
Se creo un nuevo proyecto con los datos respectivos



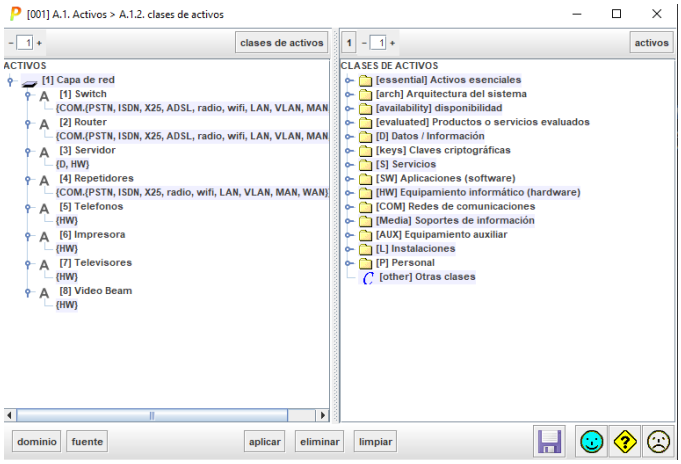
Se agrego los dominios de seguridad correspondientes a la empresa



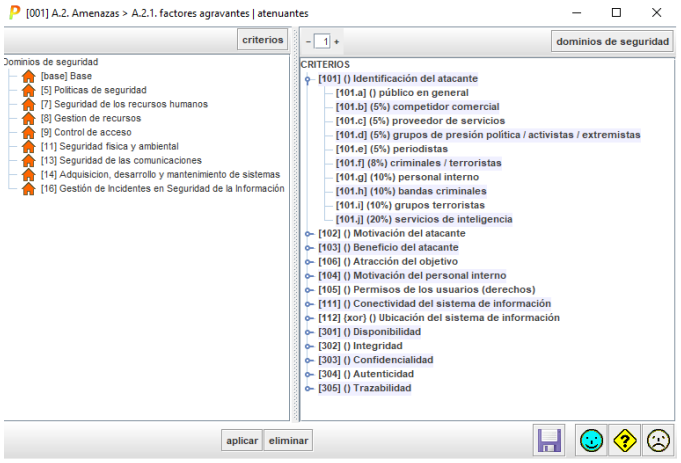
Aca podemos ver las fases de proyecto para realizar la practica de plan de riesgos



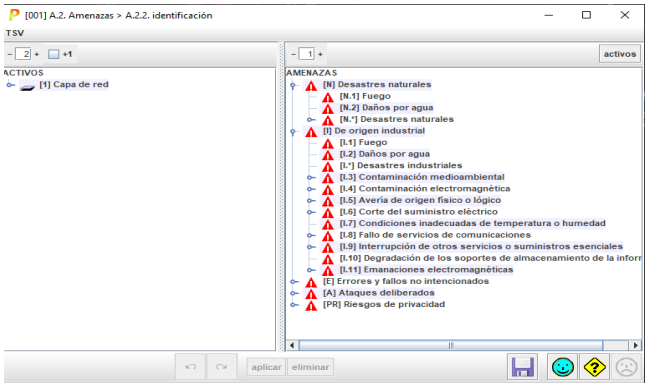
Se muestra de una forma mas detallada acerca de los activos de la empresa



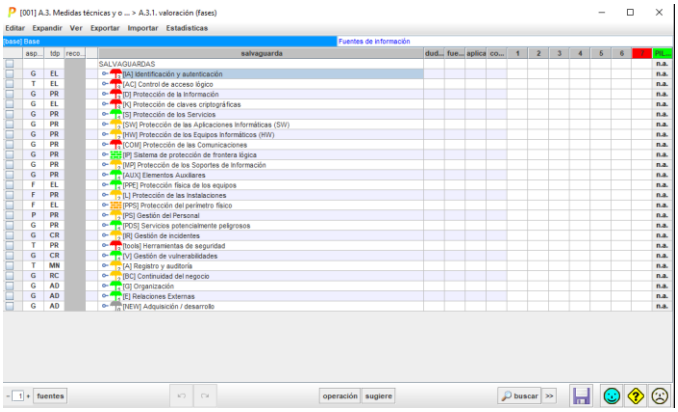
Se muestra las amenazas correspondientes a los dominios de seguridad, incluyendo el porcentaje de problabilidad



Se muestra de como podemos identificar de que tipo de amenaza se esta enfrentado la empresa y sus causas



Toma un registro completo de como se puede valorar con las circustancias que tiene la empresa



III. CONCLUSIÓN

El tratamiento seguro a la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la entidad. Este proceso es el que constituye un sistema de seguridad que brindara un sistema de calidad para la seguridad de la información, la evaluación de los sistemas de información y las características de los equipos arrojo un análisis positivo, pero la conexiones están en su mayoría expuestas a riesgos y no cumplen estándares de seguridad para los equipos informáticos. El análisis de seguridad en la estructura de la red no satisface los requerimientos de funcionalidad en la entidad, por lo que se dejo planteada una implementación de red estructurada. Es importante resaltar que el diagnostico permite al personal directivo de la entidad tomar las medidas necesarias para garantizar la protección e integridad de toda su información

Neiva, 14 de Noviembre de 2015

Señores:
Eiatec s.a.s en
Reoganizacion
Bogota D.C

Asunto: Solicitud del permiso de Estudio de plan de riesgo

Cordial Saludo:

Por medio de la presente, solicitamos al área encargada de control y seguridad de sistemas, de la Empresa Eiatec; a que nos conceda el permiso de Hacer un estudio de Registrar y Verificar el estado de seguridad que tiene el sistema de integración TIC en un la sede principal , con el plan de encontrar vulnerabilidad y poder entregar dicho informe para un mejoramiento de recursos y sistemático.

Gracias por la atención prestada.

Atentamente.
Fundación Escuela Tecnológica Del Huila

Estudiantes:

JHON ALEXANDER SUAREZ OSSA

MANUEL CUELLAR BAHAMON