Universitat Autònoma de Barcelona

UOC www.uoc.edu

Universitat Rovira i Virgili

Máster Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Final de Máster

Plan de Seguridad de la Información

Compañía XYZ Soluciones

Luis Alejandro Bautista Torres
DNI: 79520578

Tabla de Contenido

Tabla de ilustraciones

0 DESCRIPCIÓN

El presente documento suministra detalles del contexto general de la compañía ***XYZ Soluciones*** (nombre ficticio), metodología requerida para la elaboración del Plan de Seguridad de la Información, resultados de las diferentes fases de recolección y análisis de información y sugerencias de proyectos y planes de tratamiento en seguridad de la información y consolidados en un solo documento como proyecto final del programa oficial Máster en Seguridad de las TIC de las universidades UOC-URV-UAB.

1 FASE 1: CONTEXTUALIZACIÓN Y DOCUMENTACIÓN

1.1 XYZ SOLUCIONES

XYZ Soluciones es una compañía de servicios, que cuenta con 60 funcionarios a nivel nacional y cinco dependencias conocidas como: Área de Seguridad Informática, Bases de Datos, Redes, Procesamiento de Información, y Help. Todas ellas con personal especializado para suministra servicios de almacenamiento y procesamiento básico de información para pequeñas empresas a través de ambientes Windows y bases de datos SQL Server. Adicionalmente provee a través de su mesa de ayuda, servicios como alistamiento y puesta en producción de equipos de escritorio, instalación de software ofimático y soporte básico de PC para todos sus clientes.

Algunas responsabilidades asignadas a las dependencias existentes en XYZ Soluciones son:

Área de Seguridad Informática: Gestión de antivirus, administración de firewall, control de contenido perimetral, administración de circuito cerrado de televisión, etc.

Bases de Datos: Mantenimiento de las bases de datos, gestión y administración de capacidad de bases de datos, etc.
Redes: Administración de enlaces, configuración y monitoreo de dispositivos de red, etc.

Procesamiento de información: Administración de servidores, administración de licenciamiento, respaldos, almacenamiento, etc.

Help: Soporte y Atención de usuarios

1.2 DOCUMENTACIÓN Y RECOLECCIÓN DE INFORMACIÓN

Para los propósitos del presente análisis y documentación, se emplean normas, técnicas y sugerencias referenciadas en publicaciones reconocidos internacionalmente como:

- International Standards Organization, ISO/IEC 27001: Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la seguridad de la Información (SGSI) – Requisitos.

- International Standards Organization, ISO/IEC 27002: Tecnología de la Información – Técnicas de Seguridad – Código de práctica para la gestión de la seguridad de la información.

- International Standards Organization, ISO/IEC 27005: Tecnología de la Información – Técnicas de Seguridad – Gestión del Riesgo en la seguridad de la información.

- NIST: Computer Security Division of the National Institute of Standards and Technology, NIST 800-30: Risk Management Guide for Information Technology Systems
- MAGERIT: Metodología de Análisis y Gestión de riesgos de lossistemas de información.
- ISACA: Control Objectives For Information And Related Technology COBIT 4.0
- ISACA: Gobierno de seguridad de la Información. CISM.
- ISC2: Information Security Governance. CISSP

1.3 GLOSARIO DE TÉRMINOS

Los términos y principios establecidos en el presente documento tienen por base definiciones constituidas en las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005 con exactitudes como:

- Aceptación del riesgo: Admisión de la pérdida o ganancia proveniente de un riesgo particular.
- Activo: bienes o recursos de información que tienen valor para la compañía.
- Amenaza: Origen, fuente potencial de afectación que causa un incidente no deseado y puede resultar en un daño a un sistema u organización y/o a sus activos.
- Análisis de riesgo: Uso sistemático de una metodología para la identificación fuentes o amenazas a las cuales están expuestos los activos, bienes o recursos de la compañía y estimar el riesgo.
- Comunicación del riesgo: Compartir la información acerca del riesgo entre las personas o área responsable que toma la decisión y otras partes interesadas.
- Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- Control: Es una forma de mitigar el impacto generado por la materialización de los riesgos existentes. Un control incluye entre otras: la definición de políticas, la puesta en marcha de procedimientos, la definición de guías, la definición de cambios en una estructura organizacional, o la ejecución de buenas prácticas que pueden ser de carácter administrativo, técnico o legal.
- Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad de la información de la compañía.
- Disponibilidad. Propiedad que determina que la información sea accesible y utilizable bajo solicitud por individuos, entidades o procesos autorizados.
- Estimación del riesgo: Proceso de asignación de valores a la probabilidad y consecuencias de un riesgo.
- Evaluación del riesgo: Proceso para determinar la importancia del riesgo con base en la comparación del mismo contra unos criterios dados.
- Evento de seguridad de la información: Presencia identificada de una condición de un bien o recurso (sistema, servicio, red, etc.), asociada a una posible violación de la política

de seguridad de la información, falla en controles y contramedidas, o que implica una situación desconocida que puede ser pertinente a la seguridad.

- Evitar el riesgo: Decisión de la organización de no involucrarse en una situación de riesgo o tomar acciones para retirarse de dicha situación.

- Gestión del riesgo: Actividades coordinadas para dirigir y controlar los aspectos asociados al Riesgo dentro de una organización.

- Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo asociados a la seguridad de la información.

- Impacto: Se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo generando cambios adversos en los objetivos del negocio.

- Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

- Reducción del riesgo: Acciones que se toman para disminuir la probabilidad y/o el impacto negativo asociado a un riesgo.

- Riesgo en la seguridad de la información: Es la probabilidad de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando daño a la organización.

- Riesgo inherente: Es aquel riesgo que por su naturaleza no se puede separar de la situación donde se presenta. Es propio de las actividades que conlleva el proceso relacionado.

- Riesgo residual: Nivel restante de riesgo después de su tratamiento.

- Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

- Sistema de gestión de seguridad de la información SGSI: Parte del sistema de gestión global cuyo fin es establecer, implementar, operar, monitorear y mejorar la seguridad de la información.

- Transferencia del riesgo: Compartir con otra de las partes la pérdida (consecuencias negativas) de un riesgo.

- Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

- Valoración del riesgo: Proceso global de análisis y evaluación del riesgo.

- Vulnerabilidad: Debilidad asociada con los procesos, recursos o infraestructura de una organización. Una vulnerabilidad frecuentemente aumenta la probabilidad de que se materialice una amenaza.

Para el logro de objetivos del Plan de seguridad, se acordó con la organización realizar una reunión de inicio en la cual con apoyo del gerente asignado por parte de XYZ soluciones, se conocieran detalles de los procesos involucrados por cada área, los perfiles y roles relacionados, las entradas y salidas de cada proceso y los productos o servicios misionales entregados por cada unidad.

Una vez finalizada esta reunión, se acuerda la directriz de análisis de riesgo a ser empleada (ISO 27005) y los criterios de evaluación a ser utilizados, además de definir el personal idóneo frente a la identificación de activos y análisis de riesgos contemplando los límites de tiempo de cada entrevista bajo un cronograma que vislumbre las fechas de entrega aceptables para cada fase.

1.4 METODOLOGÍA DE VALORACIÓN Y ANÁLISIS

La valoración de riesgos es el primer proceso de la metodología de administración de riesgos. Esta valoración de riesgos permite determinar la extensión de amenazas potenciales y riesgos asociados con los activos. La salida de este proceso permite la identificación de controles que reducen o eliminan riesgos durante el proceso de mitigación.

Riesgo es una función de la probabilidad de que una fuente de amenaza dada explote una vulnerabilidad potencial, y que el impacto resultante sea un evento adverso para la organización.

Para determinar la probabilidad de un evento adverso, las amenazas de los recursos deben ser analizadas en conjunto con las vulnerabilidades potenciales y los controles existentes en los mismos.

El impacto se refiere a la magnitud del daño que podría ser causado porque las amenazas exploten una vulnerabilidad. El nivel de impacto es determinado por el impacto potencial en el logro de la misión y el valor relativo de los activos de información que resultaren afectados (por ejemplo, la criticidad y sensibilidad de componentes de procesamiento y los datos).

La Metodología de valoración de riesgos está compuesta por nueve (10) pasos primarios, que son:

- Paso 1 – Caracterización del Contexto Evaluado
- Paso 2 - Identificación de activos y sus amenazas
- Paso 3 - Identificación de vulnerabilidades
- Paso 4 - Análisis de controles
- Paso 5 - Determinación de probabilidades
- Paso 6 - Análisis de impacto
- Paso 7 - Determinación de riesgos
- Paso 8 - Recomendaciones de control
- Paso 9 – Otros factores de evaluación
- Paso 10 – Resultados Documentados

Ilustración 1. Metodología de Valoración y Análisis

Paso 1 - Caracterización del Contexto Evaluado: En este paso se define principalmente el alcance de los esfuerzos requeridos y los límites de ejercicio para su ejecución.
Para este paso es importante contar con la identificación de elementos involucrados como Hardware, software, interfaces de sistemas, datos de información, personas involucradas y para conocer finalmente los límites del contexto evaluado, sus funciones principales, la criticidad de sus datos y recursos además de identificar la sensibilidad de su información.

Paso 2 – Identificación de Activos y sus Amenazas: Una fuente de amenaza se define como cualquier circunstancia o evento con el potencial para causar daños en la información. Las fuentes comunes de amenazas son las personas, la naturaleza y el ambiente. Sin embargo según la norma ISO/IEC 27005 y el anexo C los ejemplos de amenazas comunes se pueden tipificar en varias clases como:

- Causantes de daño físico (Fuego, daño por agua, contaminación, destrucción de equipos o medios, polvo corrosión, congelamiento, etc.),
- Eventos naturales,
- Perdida de servicios esenciales,
- Perturbación por radiación,
- Compromiso de la información,
- Fallas técnicas,
- Acciones no autorizadas,
- Compromiso de las funciones,
- Intrusiones, terrorismo, etc

Los activos de información de cada proceso o actividad analizada son identificados y clasificados de acuerdo a su criticidad (integridad, confidencialidad y disponibilidad) y a su vez los recursos críticos son agrupados de acuerdo a sus funciones dentro de los procesos, para posteriormente ser revisados a través de un ciclo continuo de valoración de riesgos para determinar las amenazas relevantes, las consecuencias de su materialización y la existencia y efectividad de controles implementados que disminuyen el impacto o la probabilidad de concretar la amenaza.

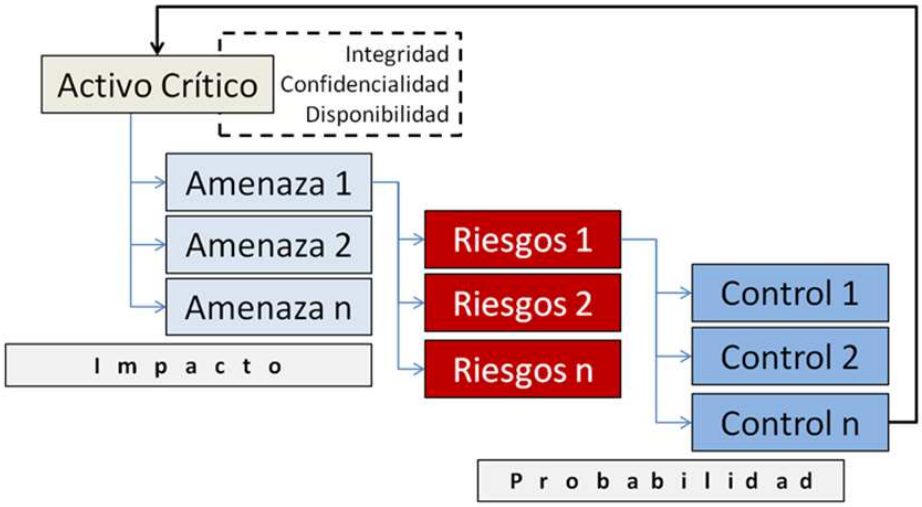

Ilustración 2. Ciclo de Estimación y Valoración de Riesgos

Para efectos del presente ejercicio y con la idea de apoyar a XYZ Soluciones en la tipificación inicial de amenazas existentes se establece que: con base en la norma ISO/IEC 27005 la lista de amenazas aplicables al contexto mediante una declaración formal de peligros a ser contemplados, facilitando así el proceso de levantamiento de información durante las entrevistas.

Las amenazas aplicables al contexto de XYZ Soluciones y finalmente acordadas con la organización para la fase de entrevistas se registran a continuación:

- A01. Fuego
- A02. Accidentes Laborales
- A03. Fallas de hardware
- A04. Acceso físico no autorizado
- A05. Causas naturales (terremoto, inundación, huracán, tormenta eléctrica, etc.)
- A06. Fallas en suministro de servicios públicos (energía, agua, gas, etc.)
- A07. Causas ambientales (Clima, Temperatura,
- Contaminación, Polvo, Corrosión, Congelamiento, humedad extrema)
- A08. Señales de interferencia (Electromagnética, Térmica)
- A09. Espionaje
- A10. Intrusión
- A11. Escucha encubierta
- A12. Hurto de información, medios o documentos (negocio, clientes, personal o privada)
- A13. Hurto de equipos
- A14. Recuperación de medios reciclados o desechados
- A15. Divulgación
- A16. Datos Provenientes de fuentes no confiables
- A17. Manipulación del Hardware
- A18. Manipulación del Software
- A19. Detección de posiciones
- A20. Deterioro de equipos
- A21. Obsolescencia tecnológica
- A22. Fallas de software
- A23. Saturación del sistema de información
- A24. Incumplimiento en el mantenimiento del SI
- A25. Uso no automatizado del equipo
- A26. Copia fraudulenta del software
- A27. Uso de software no licenciado o copiado
- A28. Corrupción de los datos
- A29. Procesamiento ilegal de los datos
- A30. Errores humanos/operación
- A31. Abuso de Derechos
- A32. Falsificación de Derechos
- A33. Negación de acciones
- A34. Dependencia de funcionarios críticos
- A35. Dependencia de terceras partes
- A36. Actos malintencionados
- A37. Asonada/Conmoción civil/terrorismo

Paso 3 – Identificación de Vulnerabilidades: las vulnerabilidades son movidas por un defecto o debilidad en los procedimientos de seguridad, diseño, implementación o de controles y que podrían ser explotadas (activadas accidentalmente o explotadas intencionalmente) generando una brecha de seguridad.

La meta de este paso es identificar la lista de vulnerabilidades (defectos o debilidades) que permiten la materialización de amenazas potenciales y diferenciadas en el paso anterior.

Paso 4 – Análisis de Controles: Los controles de seguridad reúnen controles técnicos y no técnicos. Los controles técnicos son las protecciones incorporadas en el hardware, software o firmware (por ejemplo, mecanismos de control de acceso, mecanismos de identificación y autenticación, métodos de encripción, software de detección de intrusos).

Los controles no técnicos son controles administrativos y operacionales, tales como políticas de seguridad, procedimientos operacionales y seguridad del personal, física y ambiental.

La meta de este paso es identificar con los entrevistados los controles que se encuentran implementados en XYZ Soluciones, o cuya implementación es viable para minimizar la probabilidad de que las amenazas exploten vulnerabilidades.

Paso 5 - Determinación de probabilidades: Se deben tener en cuenta los siguientes factores a la hora de construir una escala de probabilidad que mida el grado en que pueden ser explotadas las vulnerabilidades existentes:

- Motivos de las fuentes de amenazas y su dimensión (capacidad de hacer daño)
- Naturaleza de las vulnerabilidades
- Existencia y efectividad de los controles existentes

Los grados de medición establecidos para la probabilidad de que una vulnerabilidad pueda ser explotada por una fuente de amenaza se acuerdan con XYZ Soluciones, mediante la siguiente Ilustración.

PROBABILIDAD		
Calificación		**Explicación**
A	1	100%, Alta, certera, siempre ocurre
M+	0,75	75%, Mayor, probable, se espera que ocurra
M	0,5	50%, se espera que no ocurra regularmente
M-	0,25	25%, No esperado, pero podría ocurrir algunas veces
B	0,1	10%, Remoto, puede ocurrir en circunstancias excepcionales

Ilustración 3. Valoración de la Probabilidad

Paso 6 - Análisis de Impacto: El impacto adverso de un evento de seguridad se puede describir en términos de la degradación de una o varias de las metas de seguridad (Integridad, Disponibilidad y Confidencialidad)

Pérdida de Integridad: Se pierde integridad cuando se presentan modificaciones no autorizadas sobre los datos y sistemas, bien sea de manera accidental o intencional.

Pérdida de Disponibilidad: Si un sistema de misión crítica no está disponible para sus usuarios finales, se afecta el logro de la misión de la organización.

Pérdida de Confidencialidad: La confidencialidad de los datos y sistemas se refiere a la protección contra divulgación no autorizada.

IMPACTO	
Calificación	**Explicación**
A	Muy Alto. La explotación de la vulnerabilidad puede resultar en altas pérdidas financieras por: daño de activos o recursos tangibles, impedimento del logro de los objetivos de la organización, deterioro de la reputación e intereses.
M+	Alto. Pérdida financiera significativa, amenaza con pérdida de imagen de la Organización.
M	Medio. Pérdida financiera moderada, no amenaza la imagen y confianza de la Organización
M-	Bajo. Pérdida financiera menor.
B	Menor, Si perjuicios, costos asociados bajos.

Ilustración 4. Valoración del Impacto

Es necesario tener en cuenta que una valoración cuantitativa exige del personal entrevistado contar con la siguiente información:

- Un costo aproximado de cada ocurrencia
- Una ponderación del impacto de cada ocurrencia
- Una estimación del valor de los activos

Por lo cual se suministra la siguiente ilustración de referencia

IMPACTO	
Calificación	**Explicación**
A	Mas de US$500.000 mensuales
M+	De U$ 250.001 - U$ 500.000
M	De US$ 100.001 - US$ 250.000
M-	Hasta US$100.000
B	Hasta US$ 50.000

Ilustración 5. Impacto Cuantificado

Paso 7 - Determinación de Riesgos: El propósito de este paso es determinar el nivel de riesgo que tienen los activos de información evaluados. La determinación del riesgo para una amenaza/vulnerabilidad en particular se expresa en función de:

- La probabilidad que una fuente de amenaza intente explotar una vulnerabilidad
- La magnitud del impacto resultante de la explotación exitosa de una vulnerabilidad
- La efectividad de los controles existentes o planeados para reducir o mitigar los riesgos.

Para determinar el nivel de riesgo inherente se multiplican los valores asignados a la probabilidad de una amenaza por los valores asignados a la magnitud del impacto, como se muestra en la siguiente matriz:

Impacto							
	A	5	M	M+	M+	A	A
	M+	4	M	M	M+	M+	A
	M	3	M-	M-	M	M	M+
	M-	2	B	B	M-	M-	M
	B	1	B	B	B	B	M
			0-20%	21-40%	41-60%	61-80%	81-100%
			B	M-	M	M+	A
			Probabilidad de ocurrencia				

Ilustración 6. Mapa de Riesgo

La escala de riesgo, con los niveles Alto, Medio Alto, Medio, Medio Bajo y Bajo, representa el grado o nivel a que se encuentra expuesto el activo de información evaluado, cuando una vulnerabilidad es explotada exitosamente. También presenta las acciones que deben tomar la gerencia ejecutiva y los responsables del logro de la misión, en cada uno de los niveles como se indica en la siguiente ilustración

Nivel de Riesgo	Descripción del Riesgo y Acciones Necesarias
ALTO	Requiere fuertes medidas correctivas. Planes de Tratamiento implementados en corto tiempo, reportados y controlados con atención directa de la alta dirección.
MEDIO ALTO	Requiere vigilancia de la alta dirección con planes de tratamiento implementados y reportados a los Gerentes de Unidades
MEDIO	Se requieren acciones correctivas controladas por grupos de manejo de incidentes en periodo de tiempo razonable.
MEDIO BAJO	Riesgo aceptable – Administrado por los grupos de incidentes bajo procedimientos normales de control
BAJO	El Propietario del activo lo administra con procedimientos rutinarios o decide aceptar el riesgo.

Ilustración 7. Descripción de Escalas de Riesgo

Los criterios de aceptación de riesgo demandados por XYZ soluciones, establece que riesgos de niveles “Extremo” y “Alto” se consideran inaceptables y deben ser tratados de forma inmediata con los recursos necesarios requeridos. Así mismo, para los niveles “Medio” y “Bajo” su tratamiento depende del aporte del control para mitigar riesgos, la relación coste/beneficio y la contribución que éste aporte al cumplimiento de objetivos del negocio.

Mejor esfuerzo	Inaceptables
Bajo	Alto
Medio	Extremo

Ilustración 8. Criterios de Aceptación

Paso 8 – Recomendaciones de Control: Las recomendaciones de control son los resultados del proceso de valoración de riesgos y proveen una entrada al proceso de mitigación de riesgos, durante el cual los controles técnicos y procedimientos recomendados se evalúan, priorizan e implementan teniendo en cuenta los siguientes factores:

- Efectividad de las opciones recomendadas (compatibilidad de sistemas, por ejemplo)
- Legislación y regulaciones
- Política organizacional
- Impacto operacional
- Seguridad y confiabilidad

Es posible que no todos los controles recomendados se implementen, esto depende del resultado del análisis costo/beneficio, el cual debe demostrar que la implementación se justifica porque hay una reducción en el nivel de riesgo.

Paso 9 – Otros factores de evaluación Otros factores de evaluación suelen ser relacionados con la identificación de umbrales de seguridad alcanzados frente a los requeridos por la organización a nivel de confidencialidad, integridad y disponibilidad, para con los activos evaluados.

CONFIDENCIALIDAD	
Calificación	**Explicación**
Pública	Cuya divulgación no afecte a la Empresa en términos de pérdida de imagen y/o económica.
Uso Interno	La información debe mantenerse dentro de la Empresa y no debe estar disponible externamente
Restringida	Información sensible, interna a áreas o proyectos a los que deben tener acceso controlado por seguridad e intereses de la compañía.
Reservada	Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidad de negocio, potencial de fraude o requisitos legales.

Ilustración 9 Evaluación Niveles de Confidencialidad

INTEGRIDAD	
Calificación	**Explicación**
Baja	Si tras el daño, la información se puede recuperar fácilmente con la misma calidad
Normal	Recuperación fácil con una calidad semejante
Alta	Si la calidad necesaria se reconstruye de forma difícil y costosa.
Crítica	No puede volver a reconstruir

Ilustración 10. Evaluación Niveles de Integridad

DISPONIBILIDAD	
Calificación	**Explicación**
De 0 a 1 hora	Se puede estar sin el activo en funcionamiento máximo 1 hora
De 1 a 2 horas	Se puede estar sin el activo en funcionamiento máximo 2 horas
De 2 a 4 horas	Se puede estar sin el activo en funcionamiento máximo 4 horas
De 4 a 8 horas	Se puede estar sin el activo en funcionamiento máximo 8 horas
De 8 a 24 Días	Se puede estar sin el activo en funcionamiento máximo 1 día
24H +	Se puede estar sin el activo en funcionamiento más de un día

Ilustración 11. Evaluación Niveles de Disponibilidad

AUTENTICIDAD Y TRAZABILIDAD	
Calificación	**Explicación**
ALTO	Requiere fuertes medidas de control para autenticidad y trazabilidad del manejo de la información.
MEDIO ALTO	Requiere Vigilancia constante con planes de tratamiento y manejo de incidentes apoyados por el área de seguridad y Directores
NORMAL	Requiere monitoreo básico de autenticidad y trazabilidad con el manejo de la información.

Ilustración 12. Evaluación Niveles de Autenticidad y Trazabilidad

Otro criterio de evaluación es identificar los niveles de madurez alcanzados con los controles implementados empleando mediciones como las sugeridas por CMM de COBIT bajo las siguientes convenciones:

- “0” No Existente: No hay procesos de control reconocidos.

- “1” Inicial / Ad hoc: La Dirección reconoce un problema que debe ser tratado, Sin embargo, no existen procesos estandarizados sino procedimientos particulares aplicados.

- “2” Repetible pero intuitivo: Se desarrollan procesos por diferentes personas entendiendo las mismas tareas. No hay una comunicación ni entrenamiento formal y la responsabilidad recae sobre los individuos.

- “3” Procesos definidos: Los procesos se definen, documentan y se comunican a través de entrenamiento formal.

- “4” Administrados y medibles: Existen mediciones y monitoreo sobre el cumplimiento de los procedimientos.

- “5” Optimizado: Los procesos se refinan a nivel de buenas prácticas con base en los resultados del mejoramiento continuo y los modelos de madurez.

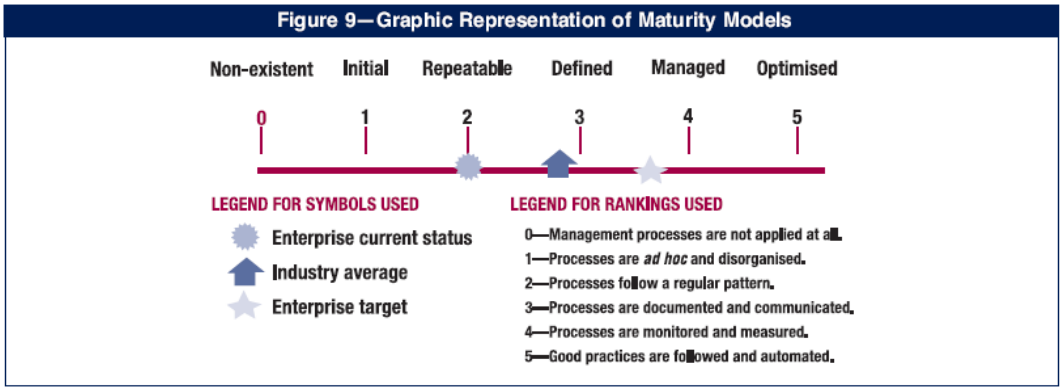

Ilustración 13. Nivel de Madurez de los Controles

Paso 10 – Resultados Documentados: El informe final de los resultados permite a la alta dirección y los diferentes grupos y funcionarios responsables de gestionar la seguridad, tomar decisiones, calcular presupuestos y gestionar los cambios administrativos y operacionales.

Identificación de Controles para Mitigación de Riesgos

En la implementación de controles para mitigar riesgos, una organización debe considerar controles técnicos, operativos y administrativos para maximizar la efectividad de los controles a ser implementados en la empresa en general.

Para ubicar los recursos e implementar los controles efectivos, es también necesario llevar a cabo un análisis costo beneficio determinando cuáles controles son requeridos y apropiados según las circunstancias.

Una vez implementados los controles, el riesgo remanente con los nuevos controles es el riesgo residual. Sin embargo, es importante tener siempre presente que no hay activos de información libres de riesgos, y no todos los controles implementados eliminan los riesgos

Implementación de Buenas Prácticas

Los sistemas de gestión de seguridad de la información (SGSI) se inician con los procesos de valoración y mitigación de riesgos, pues las medidas de seguridad deben apuntar hacia los riesgos más importantes para el negocio.

La norma ISO 27001, exige compresión de requerimiento (integridad, disponibilidad y confidencialidad), implantación y gestión adecuada de controles que ayuden a mitigar riesgos, monitoreo constante del adecuado desempeño del SGSI y mejoramiento continuo para las organizaciones que deseen emplear buenas prácticas y aplicar a una posible certificación.

El objetivo final de este trabajo y la implantación de la presente metodología es suministrar finalmente un plan director de Seguridad para la compañía XYZ Soluciones que le permita alcanzar las prácticas requeridas para manejar niveles de seguridad adecuados en el suministro de sus servicios y servir de pedestal para una futura certificación en ISO 27001

2 FASE 2: OBJETIVOS DEL PLAN DIRECTOR

2.1 INTRODUCCIÓN

La identificación y valoración de riesgos asociados a la gente, los procesos, las tecnologías, arquitecturas, aplicaciones, y todos los recursos que soportan y procesan información de XYZ Soluciones, será la forma de establecer medidas de tratamiento y protección que gestionadas oportunamente permitan mitigar impactos negativos y mantener niveles tolerables de riesgos así como aumentar los umbrales de seguridad requeridos por la Organización.

XYZ Soluciones busca particularmente con ésta actividad, promover la ejecución de prácticas de seguridad adecuadas y la posible implementación un Sistema de Gestión de Seguridad de la Información (SGSI) con base en la norma ISO/IEC 27001:2005 para cubrir los servicios de Soporte y Servicios Especializados, disponibles para clientes interno y externos a través de su Centro de Operaciones.

Como parte del análisis, se establecieron diferentes frentes de trabajo y etapas de registro de información (contextualización, identificación de activos, análisis de impacto, análisis de riesgo) que posteriormente se consolidan y registran en el presente documento, detectando escenarios de riesgo que pudieran atentar contra la operación y manejo adecuado de los recursos o activos de información críticos de XYZ Soluciones.

2.2 MECANISMOS DE EJECUCIÓN

Los mecanismos con los que contará el Plan Director para hacer viable su ejecución son:

Sensibilizar a la Alta Dirección, de la necesidad de optimizar las relaciones de confianza con sus clientes y convertirse en una alternativa más confiable y competitiva frente a otras empresas del mercado con actividades como:

- El uso de estadísticas financieras, donde las proyecciones se vean afectadas con pérdida de negocios por inadecuados manejo de la información.

- Por otra parte, identificando un Retorno de Inversión en transformaciones alcanzadas con la implementación de mejores controles de seguridad, frente a perdidas de imagen o costos por incidentes no controlados o manejados a tiempo y daños colaterales con clientes y propietarios de la información.

En segundo lugar, promover en la organización una metodología estándar con fundamentos lógicos soportados en normatividad reconocida internacionalmente para el desarrollo de un programa de administración de riesgos efectivo y trasversal a toda la organización con ventajas como:

- Unificación de criterios de evaluación y valoración
- Lenguaje común entre las áreas o unidades de negocio
- Cuadros de mando unificados con métricas e indicadores claros
- Toma de decisiones rápidas y objetivas

Por otra parte, fomentar el uso de técnicas de recolección de información para consolidación de la información sobre las áreas operacionales de la organización con:

- **Cuestionarios:** El personal responsable por la valoración de riesgos desarrolla cuestionarios para recoger información sobre los controles administrativos y operacionales planeados o utilizados por las diferentes dependencias de la organización.

- **Entrevistas en sitio:** Las entrevistas en sitio con personal idóneo (con experiencia y conocimiento de sus funciones y contratiempos manejados) de los procesos con el objeto de obtener información útil para la valoración de riesgos. Las visitas en sitio también son contempladas para valorar áreas y ambientes de trabajo.

- **Revisión de documentos:** La documentación de ejercicios anteriores, procesos, normas, directrices, formatos, plantillas de control, bitácoras, informes de auditorías previas, proveen excelente información acerca de los controles usados y planeados por la organización.

- **Herramientas de escaneo:** Mediante el uso de herramientas técnicas, y proactivas se recolecta información complementaria y validan perfiles y configuraciones individuales sobre recursos tecnológicos.

Finalmente, Auxiliar a XYZ Soluciones en el desarrollo y manejo de una técnica de selección de controles y medidas de seguridad efectivas con el objeto de instaurar un RoadMap que proporcione mejoras a los niveles de seguridad involucrados en los procesos de almacenamiento y transporte seguro de la información mediante un Sistema de Gestión de la Seguridad de la Información formalmente establecido.

2.3 OBJETIVOS

Objetivos Generales

XYZ Soluciones desea principalmente mejorar los niveles de seguridad incluidos en sus servicios, con el objeto de optimizar las relaciones de confianza con sus clientes y convertirse en una alternativa más confiable y competitiva frente a otras empresas del mercado.

En segundo lugar XYZ Soluciones, se ha propuesto encauzar sus procesos con practicas adecuadas a nivel de seguridad y solicita de la consultoría: identificar los activos de información relevantes de sus actuales servicios, conocer los riesgos relacionados, los niveles de madurez alcanzados con los controles actualmente implementados y finamente identificar un plan de acción que le permita en un tiempo no mayor a dos años acercarse a un marco de referencia certificable en temas de seguridad de la información.

Objetivos Específicos

Consolidar en el presente documento los resultados, conclusiones, y recomendaciones de la identificación de activos, evaluación y valoración de riesgos, así como determinar las bases para el tratamiento de riesgos y establecer el mapa de ruta o Plan Director de Seguridad de la Información para XYZ Soluciones.

Definir y estructurar lineamientos, procesos y directrices en seguridad de la información y soportar la posible construcción de un Sistema de Gestión de Seguridad de la Información (SGSI).

En general, mitigar riesgos, impacto o consecuencia que podrían materializarse al infringir los niveles de confidencialidad, integridad y disponibilidad además de registrar y documentar:

- La Identificación de recursos críticos dentro de la operación de Soporte y Servicios Especializados de XYZ Soluciones.
- La identificación de las amenazas y vulnerabilidades a las que están supeditados los procesos y activos críticos durante su operación.
- La estimación de la probabilidad de materialización de cada una de las amenazas identificadas al explotar vulnerabilidades existentes.
- La estimación del impacto de comprometer las operaciones del negocio y amenazar la seguridad de la información con la materialización de amenazas
- La identificación de consecuencias por afectación interna o externa de las operaciones del negocio y la seguridad de la información de la compañía.
- La identificación de los controles que actualmente se tienen implementados, y que permiten la mitigación en mayor o menor medida de las fuentes de riesgo.
- La estimación de los niveles de efectividad de los controles existentes.
- La estimación de los niveles de riesgo residual a los cuales aún se encuentra expuesta la operación.
- La identificación de hallazgos y recomendaciones de mejora.

Facilitar los instrumentos suficientes para refinar compromisos a nivel de seguridad de la información a través de los diferentes roles y perfiles con metas como:

- Operadores y usuarios: Garantizar que el uso de los activos de XYZ Soluciones y su información por parte de Operadores y Usuarios, es congruente con las órdenes administrativas, políticas, guías y reglas de la organización para mitigar los riesgos y proteger adecuadamente los recursos. Adicionalmente, conocer los programas de entrenamiento y concientización requeridos para estos perfiles.

- Propietarios o Dueños de la información: Lograr que los propietarios (existentes dentro y fuera de las áreas) sean responsables por definir, aprobar y autorizar los lineamientos de seguridad y cambios en sus sistemas, razón por la cual deben entender el rol que juegan en la administración de riesgos.

- Administradores y Coordinadores de áreas o dependencias**:** Como responsables de la infraestructura y servicios de XYZ Soluciones (administradores Bases de Datos, Redes,
- Procesamiento de la Información, Help, Seguridad Informática) o custodios comprometidos con la apropiada implementación y monitoreo de los requerimientos de seguridad demandados por la alta dirección y los dueños de la información.

- Analista de monitoreo e incidentes: **C**ontar con un grupo responsable de consolidar log´s y pistas de auditoría y definir los procedimientos para monitorear los comportamientos anormales o posibles incidentes y escalar en tiempos adecuados para tomar las medidas de contención necesarias o realizar investigaciones especiales bajo un procedimiento de recolección de evidencia confiable sin afectar los derechos fundamentales de las personas.

- Oficial de Seguridad de la Información: Jugando un rol líder en la introducción de una apropiada y estructurada metodología para ayudar a identificar, evaluar y minimizar los

riesgos de los sistemas que soportan la misión de la organización y cumpliendo funciones como:

  - Liderar y coordinar la implementación de políticas de seguridad de la información.
  - Evaluar y coordinar la implementación de controles.
  - Monitorear cambios significativos en los riesgos que afecten los activos de información.
  - Identificar las necesidades y recursos necesarios para el mantenimiento de los niveles de seguridad adecuados.
  - Identificar las necesidades de formación, capacitación o concienciación.
  - Actuar como asesor de la seguridad de la información.
  - Responder al comité de seguridad de la información sobre el estado de la investigación y monitoreo de incidentes de seguridad.
  - Presentar al comité informes periódicos del estado de la seguridad de la información dentro de las áreas y la organización en general.

- Comité de Seguridad de la Información: Para que pueda estar conformado por los líderes o responsables de las diferentes áreas de la organización y determine, apruebe y de seguimiento a políticas, planes y proyectos que requiera la entidad en materia de seguridad de la información y responda por actividades como:

  - Proponer cambios en mejora de los niveles de seguridad de la información.
  - Mantener informada a la alta dirección sobre el estado general de la seguridad de la información.
  - Conocer, vigilar y apoyar las actividades del oficial de seguridad de la información.
  - Proponer iniciativas de inversión a nivel de seguridad de la información.
  - Evaluar y aprobar metodologías y procesos específicos relativos a seguridad de la información.
  - Adoptar indicadores de gestión para seguridad de la información.
  - Promover la difusión y apoyo en campañas de sensibilización o concienciación.

- Alta Dirección: Lograr que la Alta dirección, pueda mantener y apoyar formalmente los proyectos y directrices a nivel de seguridad de la información a fin de garantizar la participación de todas las partes interesadas y sancionar los incumplimiento.

Adicionalmente, ayudar a XYZ Soluciones, a emplazar sus esfuerzos en fines como:

- Disponer de las bases suficientes para establecer y mantener una política y estándares de seguridad de información que cubra toda la organización.
- Tener una metodología estándar de evaluación a procesos y actividades relacionados con la seguridad de Información.
- Establecer un programa de evaluación periódica de vulnerabilidades sobre los activos de la Organización.
- Administrar conscientemente el programa de identificación y clasificación de activos de información.
- Establecer y documentar las responsabilidades de la organización en cuanto a seguridad de información.
- Identificar y Monitorear vulnerabilidades reconocidas sobre funciones de los proveedores.
- Mejorar los procesos de control de incidentes de seguridad o violaciones de seguridad.
- Coordinar todas las funciones relacionadas a seguridad, como seguridad física, seguridad de personal y seguridad de información, etc.
- Desarrollar y administrar con fundamento el presupuesto de seguridad de información.
- Generar y ejecutar programas periódicos de concientización para comunicar aspectos básicos de seguridad de información y lineamientos.

3 FASE 3: ESTADO DEL RIESGO: IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS Y AMENAZAS

3.1 INTRODUCCIÓN

La presente sección informa los resultados obtenidos del levantamiento de información de activos críticos de XYZ Soluciones. La principal meta es caracterizar los elementos de infraestructura por el tipo de activo, sus relaciones con otros activos y determinar en qué dimensiones de seguridad son importantes y valorados.

3.2 CRITERIOS DE IDENTIFICACIÓN DE ACTIVOS

Se denominan activos los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección. El activo esencial es la información; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes como:

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

Dependiendo del tipo de activo, las amenazas y requerimiento de los controles pueden variar. Cuando un sistema maneja datos de carácter misional, estos suelen ser importantes por sí mismos y requieren de controles minuciosos o regulados con mayor frecuencia.

Por otra parte, se debe tener presente que los activos que manejen datos de carácter misional, siempre trascienden su importancia a todos los demás activos involucrados exigiendo de la organización y sus responsables el mismo tratamiento y conservación.

3.3 CARACTERIZACIÓN Y TIPIFICACIÓN DE LOS ACTIVOS

Para cada activo es necesario determinar las características que lo definen:

- Código o nombre, típicamente procedente del inventario
- Tipo de activo (Qué caracterizan el activo)
- Servicios soportados
- Datos o Información comprendida
- Unidad responsable. (Custodia y Propiedad o explotación).
- Ubicación geográfica (en activos materiales)
- Otras características específicas del tipo de activo.

Una vez identificadas las características que componen los activos estos pueden ser representados bajo la siguiente clasificación:

- Equipos Informáticos (Servicios / Información)
- Redes de Comunicaciones
- Soportes de Información
- Instalaciones

- Personal

Equipos informáticos: son bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesamiento y transporte de datos (Equipos de macro-procesamiento de datos, Servidores, Microcomputadores, Equipo Móvil, Switch, Router, Firewall, IDS, IPS, etc.)

Redes de comunicaciones: incluye instalaciones dedicadas a servicios de comunicaciones propios o contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro (Canales de comunicación, interfaces de comunicación, antenas, etc.) Soportes de Información: se consideran otros equipos que sirven de soporte a los sistemas de información como: dispositivos de almacenar datos de forma permanente o, al menos, durante largos periodos de tiempo, fuentes de alimentación, equipos de climatización, cableados, mobiliarios, etc.

Instalaciones: Identifica los lugares físicos donde se hospedan los sistemas de información y comunicaciones (Edificaciones, Establecimientos, Oficinas, Centros de procesamiento de datos, Zonas, etc.)

Personal y Funciones: En este nivel aparecen las personas y sus funciones relacionadas con los sistemas de información (Desarrolladores, Operadores, Usuarios, etc.) Los servicios: aparecen como las funciones que satisfacen las necesidades de los usuarios y tienen múltiples denominaciones (Software, Sistemas Operativos, programas, aplicativos, desarrollos, etc.) y han sido automatizadas para su desempeño.

Los Datos / Información: se muestran como elementos de información que, de forma singular o agrupada, representan el conocimiento que se tiene de algo (Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.)

Cabe resaltar que los activos más llamativos suelen ser los datos y los servicios; pero estos activos dependen de otros activos base como pueden ser los equipos, las comunicaciones o las personas que trabajan con aquellos.

Se dice que un “activo superior” depende de otro “activo inferior” cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior.

Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores. Por esta razón, la estructura general del conjunto de activos de la organización puede verse en capas de soporte a la información, donde las capas superiores dependen de las inferiores:

- Capa 1: Son activos que se precisan para garantizar las siguientes capas como el entorno físico, suministros de energía, climatización, edificios, mobiliarios, personal, etc.

- Capa 2 y 3: el sistema de información propiamente dicho como los equipos informáticos hardware), aplicaciones (software), dispositivos de comunicaciones, soportes de información (discos, cintas, etc.) y la información, los datos, meta-datos, índices, claves de cifra, etc.

- Capa 4: las funciones misionales de la Organización, que justifican la existencia del sistema de información y le dan finalidad

- Capa 5: otros activos como credibilidad o buena imagen.

Normalmente los activos inferiores acumulan el valor de los activos que se apoyan en ellos. Es decir, el valor nuclear suele estar en la información (o datos) que el sistema maneja, quedando los demás activos subordinados a las necesidades de explotación y protección de la información

3.4 VALORACIÓN DE LOS ACTIVOS

La valoración de los activos depende de los atributos que hacen valioso el activo (Ej.: Autenticidad, integridad, confidencialidad, disponibilidad, trazabilidad). Una dimensión es una faceta o aspecto en particular (confidencialidad) y puede ser usada para valorar el activo de forma independiente de lo que ocurra con otras dimensiones.

Para valorar los activos es muy importante usar una escala común o criterio homogéneo que permita comparar análisis realizados en ejercicios previos. Para nuestro caso, la valoración es por aproximación cuantitativa para confidencialidad, integridad, disponibilidad y trazabilidad como se establece en las ilustraciones 8 a 10 del presente documento y tomado en consideración:

- Obligaciones regulatorias y contractuales.
- Intereses comerciales y económicos
- Afectación financiera
- Interrupción del servicio

Los interrogantes a resolver con estos criterios de evaluación son: “¿Qué daño causaría a la Organización, el que la Información fuese conocida por quien no debe?”. “¿Qué perjuicio causaría que el activo valorado estuviera dañado o suministrara información corrupta?”. “¿Qué perjuicio causaría el no tener o poder usar el activo valorado?”. “¿Qué niveles de Autenticidad y trazabilidad son requeridos para el manejo adecuado de la información?”

3.5 INVENTARIO DE ACTIVOS

La estructura general del conjunto de activos críticos identificados en XYZ Soluciones es:

Capa 1: Activos que se precisan para garantizar las siguientes capas de soporte a la información como el entorno físico, suministros de energía, climatización, edificios, mobiliarios, personal, etc.

NOMBRE ACTIVO	TIPIFICACION	JERARQUIAS
EIXYZSOL17	Instalaciones	CAPA 1
EIXYZSOL19	Soporte	CAPA 1
EIXYZSOL73	Red	CAPA 1

Ilustración 14. Activos Capa 1

- **Instalaciones:** Identifica el Centro de computo, lugar físicos donde se hospedan los sistemas de información y comunicaciones.

- **Soporte:** son equipos de relacionados con aire acondicionado, UPS, alarmas de fuego, etc. Vitales para garantizar el ambiente de funcionamiento adecuado para el centro de cómputo y los sistemas de comunicación e información hospedados.

- **Red de comunicaciones:** incluye las instalaciones dedicadas a servicios de comunicaciones contratados a terceros para el transporte de datos de XYZ soluciones sus oficinas, instalaciones y clientes

Capa 2 y 3: el sistema de información propiamente dicho como los equipos informáticos, servidores, Microcomputadores, dispositivos de comunicaciones, dispositivos de seguridad,

soportes de información (discos, cintas, etc.) con información de directrices de seguridad, configuraciones comunicación y acceso, aplicaciones, bases de datos y servicios suministrados por XYZ Soluciones.

NOMBRE ACTIVO	TIPIFICACION	JERARQUIAS
EIXYZSOL08	Hardware	CAPA 2
EIXYZSOL12	Hardware	CAPA 2
EIXYZSOL14	Hardware	CAPA 2
EIXYZSOL15	Hardware	CAPA 2
EIXYZSOL16	Hardware	CAPA 2
EIXYZSOL18	Hardware	CAPA 2
EIXYZSOL04	Aplicación	CAPA 3
EIXYZSOL05	Aplicación	CAPA 3
EIXYZSOL21	Aplicación	CAPA 3
EIXYZSOL25	Aplicación	CAPA 3
EIXYZSOL28	Hardware	CAPA 3
EIXYZSOL32	Hardware	CAPA 3
EIXYZSOL34	Aplicación	CAPA 3
EIXYZSOL35	Hardware	CAPA 3
EIXYZSOL36	Hardware	CAPA 3
EIXYZSOL45	Aplicación	CAPA 3
EIXYZSOL46	Aplicación	CAPA 3

Ilustración 15. Activos Capa 2 y 3

- Un Dispositivo de Seguridad

  Firewall - EIXYZSOL08

- Tres equipos encargados de filtrar el acceso y navegación en Internet y el correo electrónico.

  Proxy EIXYZSOL12
  Internet EIXYZSOL35
  Correo Electrónico EIXYZSOL36

- Cuatro Equipos de Comunicaciones (Switches)

  Switch EIXYZSOL14
  Switch EIXYZSOL15
  Switch EIXYZSOL16
  Switch EIXYZSOL18

- Dos Servidores: depositarios temporales o permanentes de datos y ejecución de las aplicaciones informáticas de los clientes

  WebServices - EIXYZSOL34
  Servidor clientes Corporativos - EIXYZSOL32

- Siete Aplicaciones que soportan servicios internos o de soporte a clientes de la organización

  Antivirus - EIXYZSOL04
  AntiSpam - EIXYZSOL05
  Help - EIXYZSOL21
  Domain Controller - EIXYZSOL25
  Financieras - EIXYZSOL45
  Servicios en línea - EIXYZSOL46

Capa 4: Información o datos de las funciones misionales de la Organización, que justifican la existencia del sistema de información o le dan finalidad

NOMBRE ACTIVO	TIPIFICACION	JERARQUIAS
EIXYZSOL33	Datos	CAPA 4
EIXYZSOL48	Datos	CAPA 4
EIXYZSOL22	Datos	CAPA 4
EIXYZSOL49	Datos	CAPA 4
EIXYZSOL50	Datos	CAPA 4
EIXYZSOL53	Datos	CAPA 4
EIXYZSOL40	Personal	CAPA 4
EIXYZSOL70	Personal	CAPA 4

Ilustración 16. Activos Capa 4

3.6 HERENCIAS

Es necesario resaltar que los activos más importantes suelen ser los datos; por lo cual activos base como aplicaciones y servidores (de los que dependen para el procesamiento adecuado de la información) heredan la criticidad y niveles de valoración dados a los activos clasificados como información.

La siguiente Ilustración muestra un resumen del código identificador de los activos que heredan su valoración e importancia a otros activos de capas inferiores.

HERENCIAS				
ACTIVOS	CAPA 1	CAPA 2 Y 3	CAPA 4	CAPA 5
CAPA 1	1,2,3	N/A	N/A	N/A
CAPA 2 Y 3	4 al 20	4 al 20	N/A	N/A
CAPA 4	21,22,24 y 26 al 29	21,22,24 y 26 al 29	21,22,24 y 26 al 29	N/A
CAPA 5	N/A	N/A	N/A	N/A

Ilustración 17. Herencia de los Activos

El anexo “Act_Consolidado.pdf” ADICIONALMENTE suministra detalles de la identificación y valoración de activos, con base en la peso de la información bajo los umbrales de Autenticidad, Confidencialidad, Integridad, Disponibilidad y Trazabilidad.

3.7 ANÁLISIS DE AMENAZAS

Las amenazas son eventos inesperados con el potencial para causar daños. Las amenazas explotan las vulnerabilidades presentes en las tecnologías, las personas o los procesos. Las amenazas se conocen como causas de riesgos, esto es, si la amenaza no explota una vulnerabilidad el riesgo no acontece. Algunas vulnerabilidades más notorias y registradas durante las entrevistas son la falta de selección y validación de zonas críticas, la falta de buenas prácticas para administración y operación de las dependencias, La falta de lineamientos básicos de seguridad, la falta de procedimientos documentados y manuales, información no clasificada, y ausencia de planes de continuidad.

A continuación se registra la estadística de vulnerabilidades más referenciadas por los entrevistados o identificadas durante las visitas a sitio.

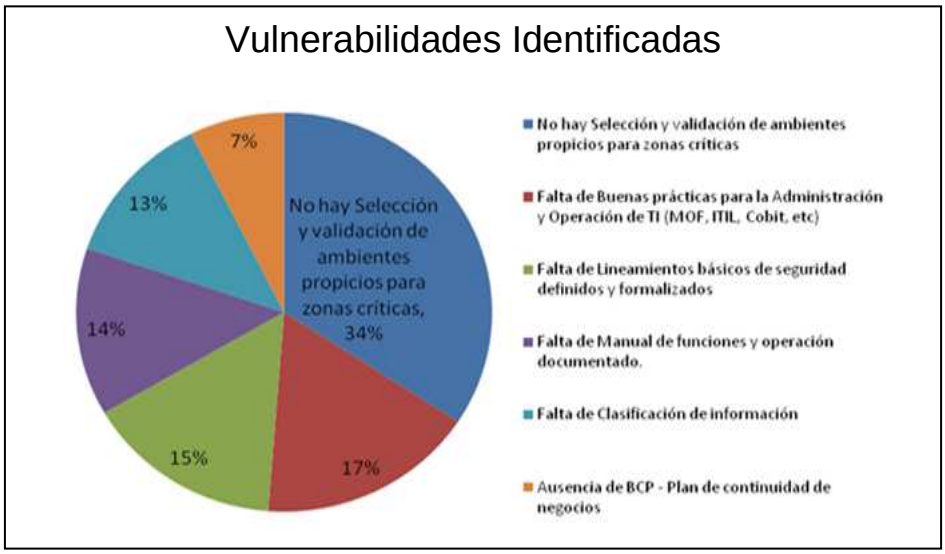

Ilustración 18. Vulnerabilidades

De acuerdo con el Anexo C de la norma NTC-ISO/IEC 27005 las categorías de amenazas o fuentes de amenazas se pueden clasificar en:

- A_ Daño Físico
- B_ Eventos Naturales
- C_ Pérdida de servicios esenciales
- D_ Perturbación por radiación
- E_ Compromiso de la información
- F_ Fallas Técnicas
- G_ Acciones no Autorizadas
- H_ Compromiso de la Funciones
- I_ Errores Humanos
- J_ Fallas en la gestión y operación del servicio

Para la elaboración del presente informe, por cada activo de información se indagó a los responsables de atender las entrevistas, acerca de las posibles amenazas potenciales (pueden suceder) y reales (han sucedido). Esta información se consolido en tablas de Excel y a continuación se presentan estadísticas de análisis a los resultados obtenidos agrupando las amenazas por su categoría:

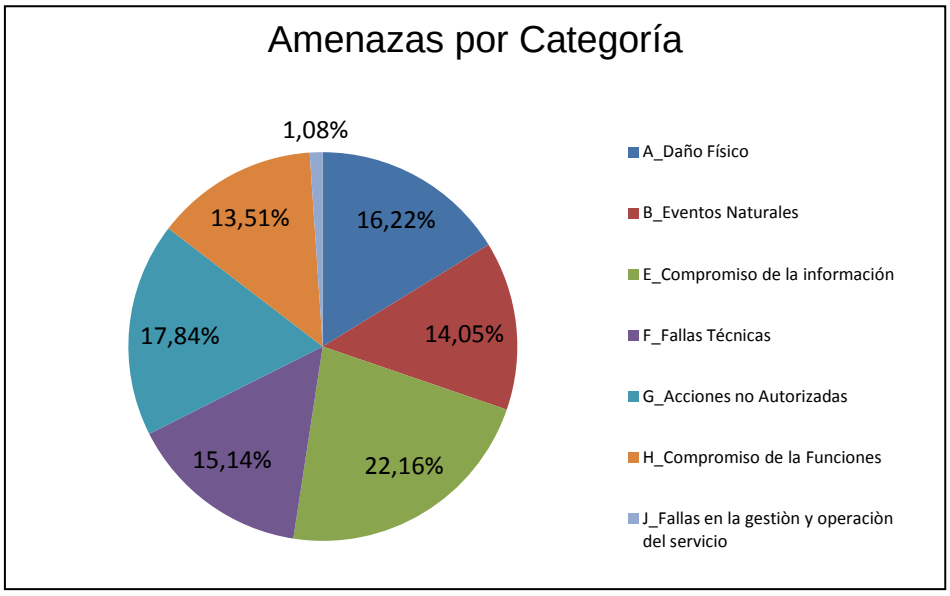

Ilustración 19. Amenazas por Categoría

La categoría más representativa y que más debe preocupar a XYZ Soluciones es la correspondiente a “COMPROMISO DE LA INFORMACION” que comprende amenazas como Errores humanos, Accidentes Laborales, Divulgación, Interceptación, Escucha encubierta o Espionaje, manipulación del hardware, manipulación del software, entre otros. Dichos actos afectan principalmente a los recursos de la Organización, puesto que son las barreras a vencer por posibles atacantes internos y externos. Hay varias circunstancias particulares que explican el por qué en esta categoría es la que más se concentran las amenazas y son:

- Insuficiencia de personal a nivel de seguridad de la información.
- Carencias en la generación y distribución de Políticas de Seguridad.
- Carencias en la generación de lineamientos de seguridad plenamente definidos.
- Deficiencia en la capacitación y concienciación en temas de seguridad de la información.
- Deficiencias en la asignación formal de funciones y responsabilidades
- Deficiencia en la segregación de funciones y acuerdos de confidencialidad

La categoría de “ACCIONES NO AUTORIZADAS” se ubica en segundo lugar principalmente por accesos no autorizados y la ausencia de esquemas fuertes de control de acceso (físico y lógico). También afecta de manera importante la falta de asignación formal de responsabilidades, segregación de funciones, acuerdos de confidencialidad y acuerdos de niveles de servicio.

La categoría de " DAÑO FISICO” concentra amenazas como Contaminación, Polvo, Corrosión, congelamiento y Temperatura o humedad extremas y se ubica en tercer lugar debido a que las condiciones físicas del Centro de Cómputo.

Dicho activo no cuentan con esquemas confiables para soportar el apropiado funcionamiento y operación de los recursos críticos de la Organización.

Las amenazas presentes por “FALLAS TECNICAS” se deben principalmente a que XYZ Soluciones mantiene un nivel alto de dependencia de software sobrellevado en plataformas antiguas y no estandarizadas, que requieren de migración y unificación inmediata con niveles de seguridad adecuados.

La categoría de “EVENTOS NATURALES” se deben a que son elementos externos que pueden ocurrir en cualquier lugar y a cualquier organización, para los cuales no se cuenta con un proceso de continuidad con el nivel apropiado En la siguiente gráfica se presenta la distribución de las amenazas identificadas:

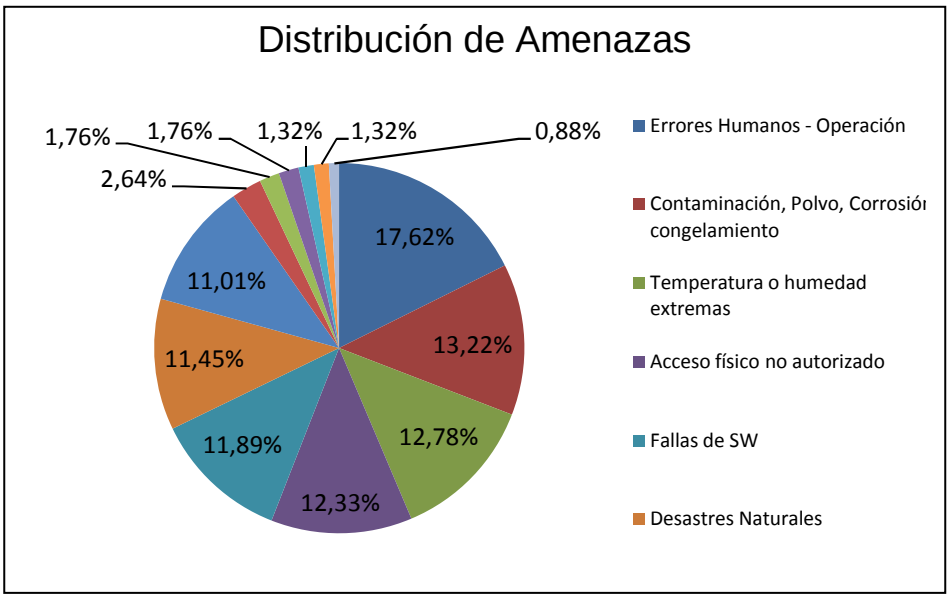

Ilustración 20. Distribución de Amenazas

Las principales amenazas identificadas son:

Errores humanos: Esta amenaza se presenta en mayor medida siempre que la organización no realice programas de conciencia y capacitación a nivel de seguridad de la información, genere y monitoree lineamientos y directrices de seguridad o realice auditorías internas de desempeño, seguridad y clima organizacional de manera periódica.

Contaminación, polvo, corrosión, temperatura y humedad extrema: Por las deficiencias en las condiciones físicas localizadas sobre puntos críticos o únicos de falla como el centro de cómputo e instalación de soporte a equipos de comunicación y procesamiento de datos que salvaguardan los activos de información de todo XYZ Soluciones.

Acceso físico no autorizado: Se encuentran identificados de igual forma sobre puntos únicos de falla (principalmente sobre el centro de cómputo). Un incidente por acceso no autorizado sobre este recurso se convierte en una gran amenaza para la continuidad de los servicios.

Fallas de software: Las múltiples aplicaciones de software no estandarizadas y soportadas por fabricantes, se convierten en espacios críticos de falla, que afectan en todo momento la prestación de los servicios.

Desastres Naturales: Dentro de las amenazas principales se encuentra la posibilidad de un desastre natural que exige de la Organización se cuente con un proceso de continuidad con el nivel apropiado.

3.8 ESTIMACIÓN DEL RIESGO, PROBABILIDAD E IMPACTO

Los resultados de las entrevistas también permitieron establecer que las amenazas identificadas como relevantes conducen a los siguientes impactos tipificados según la norma ISO 27005:

AMENAZA	IMPACTO
Errores Humanos - Operación	Alteración / perdida o Fuga de Información
	Costos Excesivos
	Daño / Pérdida de activos o Indisponibilidad colateral de otros servicios

AMENAZA	IMPACTO
	Información para la toma de decisiones errada o inoportuna
	Interrupción del servicio o del negocio
	Pérdida de credibilidad, competitividad o imagen de la entidad
	Pérdida de productividad de los empleados
	Sanciones económicas o legales
Contaminación, Polvo, Corrosión, congelamiento	Alteración / perdida o Fuga de Información
	Costos Excesivos
	Daño / Pérdida de activos o Indisponibilidad colateral de otros servicios
	Información para la toma de decisiones errada o inoportuna
	Ingresos Deficientes
	Interrupción del servicio o del negocio
	Pérdida de credibilidad, competitividad o imagen de la entidad
	Pérdida de productividad de los empleados
Temperatura o humedad extremas	Alteración / perdida o Fuga de Información
	Costos Excesivos
	Daño / Pérdida de activos o Indisponibilidad colateral de otros servicios
	Información para la toma de decisiones errada o inoportuna
	Ingresos Deficientes
	Interrupción del servicio o del negocio
	Pérdida de credibilidad, competitividad o imagen de la entidad
	Pérdida de productividad de los empleados
Acceso físico /lógicos no autorizado	Alteración / perdida o Fuga de Información
	Daño / Pérdida de activos o Indisponibilidad colateral de otros servicios
	Fraude/Robo o malversación de fondos
	Interrupción del servicio o del negocio
Fallas de SW	Alteración / perdida o Fuga de Información
	Información para la toma de decisiones errada o inoportuna
	Interrupción del servicio o del negocio
	Pérdida de credibilidad, competitividad o imagen de la entidad
	Pérdida de productividad de los empleados
Desastres Naturales	Interrupción del servicio o del negocio
	Pérdida de credibilidad, competitividad o imagen de la entidad

Ilustración 21. . Impactos o consecuencias por materialización de amenazas

Para cada una de las amenazas identificadas también se indagó por la probabilidad de ocurrencia y el impacto con base en los niveles definidos en las ilustraciones 3 y 4 del presente documento y estableciendo las consecuencias que puede producir la materialización de dichas amenazas.

A continuación se presenta de forma gráfica los principales impactos que enfrenta la Organización. Las escalas numéricas que aparecen indican la frecuencia con que un impacto fue asociado por los entrevistados a los diferentes recursos de infraestructura.

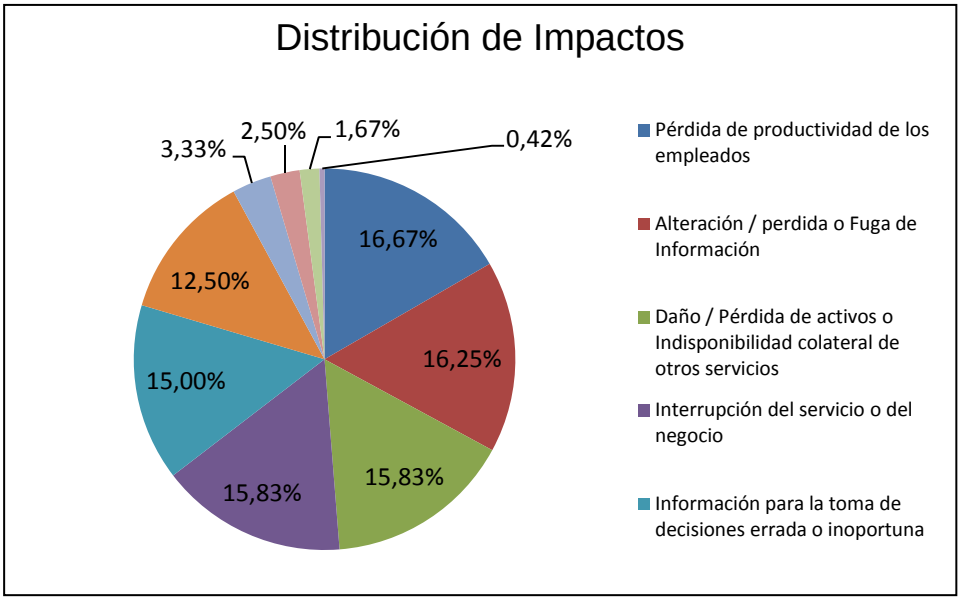

Ilustración 22. Distribución de impactos

En la gráfica se puede apreciar que los riesgos más mencionados son:

Pérdida de Productividad de los Empleados: La principal preocupación es por la dependencia generalizada de los clientes de XYZ Soluciones por el uso de recursos tecnológicos y activos de información que allí se manejan.

Alteración pérdida o fuga de Información, Daño de Activos e Interrupción del servicio: Son riesgos inherentes favorecido por vulnerabilidades como ausencia de lineamientos de seguridad, software no estandarizado, especificaciones incompletas o no claras para administradores y operadores, puntos únicos de falla (redes y comunicaciones), procedimientos inadecuados de contratación, uso inadecuado del hardware o software y falta de conciencia y entrenamiento a nivel de seguridad entre otros.

Información para la toma de decisiones errada o inoportuna: La mayor preocupación es generada por el promedio máximo de recuperación de los servicios para los clientes que debe ser inferior a 4 horas.

3.9 EFECTIVIDAD DE LOS CONTROLES.

Los controles identificados durante el proceso de entrevistas son categorizados de la siguiente forma:

.

Tipo	Explicación	Ejemplos de controles
Preventivo	Evitan que la amenaza se materialice	Acceso por contraseñas
		Cifrado de mensajes
		Autenticación fuerte
Detectivo	Alertan sobre violaciones o intentos de violación de la política de seguridad	Pistas de auditoría
		Sistemas de detección de intrusos – IDS
		Dígitos de chequeo
Correctivo	Se utilizan para restaurar recursos de computación perdidos o	Restauración de sistemas y datos
		Plan de recuperación de desastres

Tipo	Explicación	Ejemplos de controles
	dañados	Sistemas automáticos de extinción de incendios
Automático	El control se ejecuta sin intervención humana	Control de acceso biométrico
		Acceso por contraseñas
Manual	Es requerida la intervención humana para la ejecución del control	Inspección física de paquetes, bolsos, etc.
		Entrevistas de selección
		Procedimientos de aprobación
Mandatorio	El control se ejecuta siempre	Acceso por contraseñas
		Verificación de antecedentes
Discrecional	La ejecución del control es potestativa de una persona o grupo de personas	Aseguramiento de plataformas (actualización de parches, desactivación de puertos y servicios)
		Revisión de logs de acceso

Ilustración 23. Categorías de los controles

A continuación se identifican los controles más mencionados o difundidos para mitigación de riesgos relacionados con los activos de información.

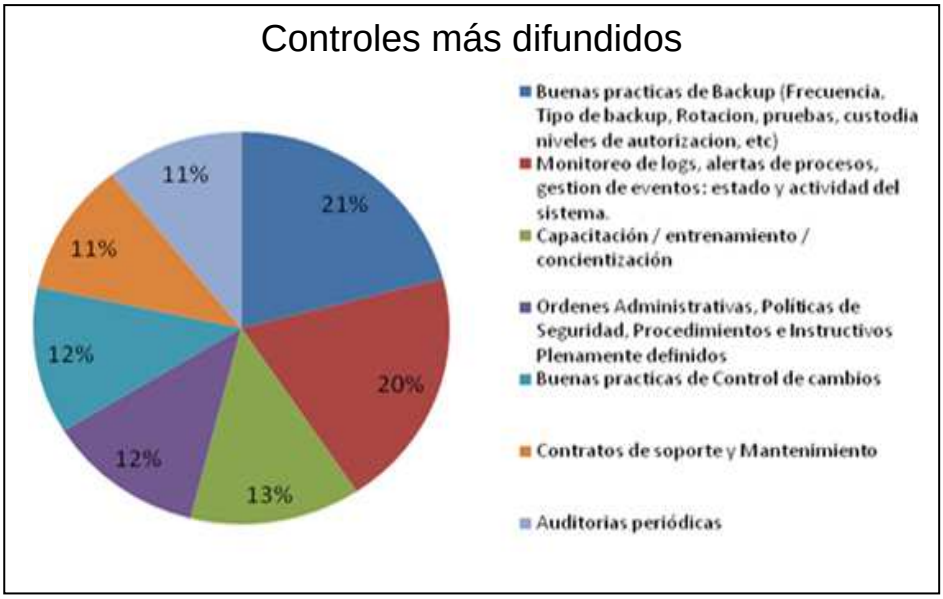

Ilustración 24. Controles difundidos

4 FASE 4: AUDITORÍA DE CUMPLIMIENTO DE LA ISO:IEC 27002:2005

4.1 INTRODUCCIÓN

La presente sección registra un GAP_Analysis (análisis de brecha) de seguridad para XYZ Soluciones el cual consiste en identificar el nivel de eficiencia y eficacia de los controles existentes en la organización para proteger la integridad, confidencialidad y disponibilidad de sus activos de información.

4.2 METODOLOGÍA

Dentro de las diferentes metodologías para establecer el nivel de madurez alcanzado por controles implementados para una organización, la valoración propuesta por el Engineering Institute's Capability Maturity Model (CMM) y adoptada en el presente ejercicio, requiere las siguientes métricas de comprobación:

0 No Existente: No hay procesos de control reconocidos. La organización no reconoce el problema y por ende la necesidad de su tratamiento.

1 Inicial / Ad hoc: La organización reconoce un problema que debe ser tratado. No existen procesos estandarizados sino procedimientos particulares aplicados a casos individuales.

2 Repetible pero intuitivo: Se desarrollan procesos para ser aplicados por personas diferentes entendiendo las mismas tareas. No hay una comunicación ni entrenamiento formal y la responsabilidad recae sobre los individuos. Excesiva confianza en el conocimiento de los individuos, por tanto, los errores son comunes.

3 Procesos definidos: Los procesos se definen, documentan y se comunican a través de entrenamiento formal. Es obligatorio el cumplimiento de los procesos y por tanto la posibilidad de detectar desviaciones es alta. Los procedimientos por si mismos no son sofisticados pero se formalizan las prácticas existentes.

4 Administrados y medibles: Existen mediciones y monitoreo sobre el cumplimiento de los procedimientos. Los procedimientos están bajo constante mejoramiento y proveen buenas prácticas. Normalmente requiere de herramientas automatizadas para la medición.

5 Optimizado: Los procesos se refinan a nivel de buenas prácticas con base en los resultados del mejoramiento continuo y los modelos de madurez de otras empresas.

4.3 EVALUACIÓN DE LA MADUREZ

Actualmente XYZ soluciones no cuenta con un SGSI o prácticas alineadas con la normatividad requerida para certificación en temas de seguridad de la información.

De acuerdo a los datos aportados por los funcionarios entrevistados, en XYZ Soluciones el compromiso de seguridad de información solo se concentra sobre el área de "seguridad Informática", donde se realizan bajo función y aprobación de un Analista de Seguridad, actividades de administración técnica o a nivel de maquinas con gestión de dispositivos como firewall, IPS y antivirus entre otras.

Las áreas de Bases de Datos, Redes, Procesamiento de la Información cuentan con Administradores o Coordinadores. Todos ellos, encargados de labores administrativas y

operativas que ajustan sus actividades con prácticas básicas a nivel de seguridad de la información como uso de usuarios y contraseñas seguras.

El área de Help cumple con labores de soporte básico (primer nivel) a solicitudes de pre-configuración de equipos, instalación y soporte a sistemas operativos y aplicaciones de software avalando lineamientos funcionales como la creación de perfiles básicos de usuario para operación básica de funciones y servicios en los sistemas.

Es importante reconocer que concluidas las entrevistas, se pudo observar la existencia de directivas administrativas que cubren distintos aspectos de la seguridad de la información de forma aislada. Sin embargo, la Organización en general necesita adoptar mayor cantidad de prácticas que permitan gestionar la seguridad de la información y establecer mayor número de responsabilidades.

Haciendo una validación frete a los objetivos de control de la norma ISO 27001 y con ayuda de la métrica CMM de COBIT, se pudo establecer que los niveles de madurez alcanzados son de grado cero"0 - No Existente" en algunos dominios y el máximo nivel de madurez encontrado es de "3 Procesos definidos"

4.4 PRESENTACIÓN DE RESULTADOS

A continuación se emiten las principales conclusiones del análisis gap ISO 27002 por cada dominio:

Política de seguridad de la información: La existencia, revisión y cumplimiento de Políticas de Seguridad de la Información es solo una idea / no existe. Se requiere definir, documentar e implementar las directrices con un alcance definido y procurando el compromiso de la Alta Dirección.

POLÍTICA DE SEGURIDAD			
CTROL - ISO	**Aplica**	**CMM**	**% CMM**
5.1			
5.1.1	**S**	**1**	20,00%
5.1.2	**S**	**0**	0,00%
Total	**2**	**0**	0,10%

Ilustración 25. Cumplimiento Dominio A5 / ISO 27001

Organización de la seguridad de la información: La implementación de controles de este Dominio también se encuentra prácticamente en nivel 0 (inexistente). Se requiere trabajar en controles básicos como, lograr mayor compromiso de la Alta Dirección con la seguridad de la información, depuración de roles y perfiles con asignación formal de responsabilidades y renovación de acuerdos de confidencialidad

ORGANIZACIÓN DE LA SEGURIDAD			
CTROL - ISO	**Aplica**	**CMM**	**% CMM**
6.1			
6.1.1	**S**	**0**	0,00%
6.1.2	**S**	**0**	0,00%
6.1.3	**S**	**0**	0,00%
6.1.4	**S**	**0**	0,00%
6.1.5	**S**	**0**	0,00%

ORGANIZACIÓN DE LA SEGURIDAD			
6.1.6	S	1	20,00%
6.1.7	S	0	0,00%
6.1.8	S	0	0,00%
6.2			
6.2.1	S	0	0,00%
6.2.2	S	0	0,00%
6.2.3	S	0	0,00%
	11	0	1,82%

Ilustración 26. Cumplimiento Dominio A6 / ISO 27001

Gestión de Activos: En general este Dominio se encuentra en nivel de madurez 1 (Inicial/Ad hoc). Dada la relevancia de la información que se gestiona de los clientes, es primordial desarrollar e implementar un apropiado conjunto de procedimientos para clasificar y manejar la información.

GESTION DE ACTIVOS			
CTROL	Aplica	CMM	% CMM
7.1			
7.1.1	S	1	20,00%
7.1.2	S	1	20,00%
7.1.3	S	2	40,00%
7.2			
7.2.1	S	1	20,00%
7.2.2	S	0	0,00%
	5	1	0,20%

Ilustración 27. Cumplimiento Dominio A7 / ISO 27001

Seguridad de los recursos humanos: Este dominio tiene un nivel de madurez 3 debido a las directrices fuertemente vigiladas por el estado y por normatividad interna. Sin embargo a través de auditorías periódicas se deben escudriñar mejoras, ya que un incidente de seguridad relacionado con este tema podría poner en riesgo la confidencialidad de información.

RECURSOS HUMANOS			
CTROL	Aplica	CMM	% CMM
8.1			
8.1.1	S	3	60,00%
8.1.2	S	3	60,00%
8.1.3	S	3	60,00%
8.2			
8.2.1	S	3	60,00%
8.2.2	S	3	60,00%
8.2.3	S	3	60,00%
8.3			
8.3.1	S	3	60,00%
8.3.2	S	3	60,00%
8.3.3	S	3	60,00%
	9	3	0,60%

Ilustración 28. Cumplimiento Dominio A8 / ISO 27001

Seguridad física y del entorno: Este dominio se encuentra en nivel de madurez 1 (Inicial/Ad hoc), y es necesario fortalecer la implementación de controles como sistemas de tarjetas de acceso inteligente, bitácoras de ingreso a zonas restringidas, CCTV, alarmas y equipos de detección de incendios, entre otros

SEGURIDAD FISICA Y DEL ENTORNO			
CTROL	**Aplica**	**CMM**	**% CMM**
9.1			
9.1.1	**S**	**2**	40,00%
9.1.2	**S**	**2**	40,00%
9.1.3	**S**	**3**	60,00%
9.1.4	**S**	**1**	20,00%
9.1.5	**S**	**1**	20,00%
9.1.6	**S**	**1**	20,00%
9.2			
9.2.1	**S**	**3**	60,00%
9.2.2	**S**	**3**	60,00%
9.2.3	**S**	**3**	60,00%
9.2.4	**S**	**3**	60,00%
9.2.5	**S**	**0**	0,00%
9.2.6	**S**	**0**	0,00%
9.2.7	**S**	**3**	60,00%
	13	**1**	0,38%

Ilustración 29. Cumplimiento Dominio A9 / ISO 27001

Gestión de operaciones y comunicaciones: Este dominio se encuentra en nivel de madurez 1 (Inicial/Ad hoc) y concentra la mayoría de controles en soluciones de nivel técnico olvidando procedimientos y intervenciones administrativas.

GEST. DE COMUNICACIONES Y OPER.			
CTROL	**Aplica**	**CMM**	**% CMM**
10.1			
10.1.1	**S**	**2**	40,00%
10.1.2	**S**	**2**	40,00%
10.1.3	**S**	**2**	40,00%
10.1.4	**S**	**2**	40,00%
10.2			
10.2.1	**S**	**0**	0,00%
10.2.2	**S**	**0**	0,00%
10.2.3	**S**	**0**	0,00%
10.3			
10.3.1	**S**	**2**	40,00%
10.3.2	**S**	**2**	40,00%
10.4			
10.4.1	**S**	**3**	60,00%
10.4.2	**S**	**0**	0,00%
10.5			
10.5.1	**S**	**2**	40,00%
10.6			
10.6.1	**S**	**0**	0,00%
10.6.2	**S**	**3**	60,00%
10.7			
10.7.1	**S**	**0**	0,00%
10.7.2	**S**	**0**	0,00%
10.7.3	**S**	**0**	0,00%
10.7.4	**S**	**1**	20,00%
10.8			

GEST. DE COMUNICACIONES Y OPER.			
10.8.1	S	3	60,00%
10.8.2	S	3	60,00%
10.8.3	S	1	20,00%
10.8.4	S	1	20,00%
10.8.5	S	3	60,00%
10.9			
10.9.1	N		
10.9.2	N		
10.9.3	S	3	60,00%
10.10			
10.10.1	S	0	0,00%
10.10.2	S	0	0,00%
10.10.3	S	0	0,00%
10.10.4	S	2	40,00%
10.10.5	S	2	40,00%
10.10.6	S	2	40,00%
	30	1	31,54%

Ilustración 30. Cumplimiento Dominio A10 / ISO 27001

Control de acceso: La implementación de controles de este Dominio se encuentra en un nivel de madurez 2 (Repetible pero intuitivo). Los puntos más importantes por trabajar son:
Revisión de los derechos de acceso de los usuarios Políticas de escritorios limpios y estaciones desatendidas, tiempo de inactividad de sesión, limitación del tiempo de conexión, entre otras.

CONTROL DE ACCESO			
CTROL	Aplica	CMM	% CMM
11.1			
11.1.1	S	2	40,00%
11.2			
11.2.1	S	2	40,00%
11.2.2	S	1	20,00%
11.2.3	S	3	60,00%
11.2.4	S	0	0,00%
11.3			
11.3.1	S	3	60,00%
11.3.2	S	1	20,00%
11.3.3	S	1	20,00%
11.4			
11.4.1	S	3	60,00%
11.4.2	S	3	60,00%
11.4.3	S	3	60,00%
11.4.4	S	3	60,00%
11.4.5	S	3	60,00%
11.4.6	S	3	60,00%
11.4.7	S	3	60,00%
11.5			
11.5.1	S	3	60,00%
11.5.2	S	3	60,00%
11.5.3	S	3	60,00%
11.5.4	S	3	60,00%
11.5.5	S	2	0,00%
11.5.6	S	2	0,00%
11.6			

CONTROL DE ACCESO			
11.6.1	S	3	60,00%
11.6.2	S	2	40,00%
11.7			
11.7.1	S	2	40,00%
11.7.2	N		
	24	2	44,17%

Ilustración 31. Cumplimiento Dominio A11 / ISO 27001

Adquisición, desarrollo y mantenimiento de software: Este dominio se encuentra en nivel de madurez 2 (Repetible pero intuitivo). Sin embargo se requiere implementar procesos de control de cambios y separación de ambientes para minimizar los riesgos por acceso no autorizado a datos de producción o activación de cambios sin previa verificación de alcances.

DESARROLLO Y MANT. DE SISTEMAS			
CTROL	Aplica	CMM	% CMM
12.1			
12.1.1	S	2	40,00%
12.2			
12.2.1	S	2	40,00%
12.2.2	S	2	40,00%
12.2.3	S	3	60,00%
12.2.4	S	3	60,00%
12.3			
12.3.1	S	2	0,00%
12.3.2	S	1	0,00%
12.4			
12.4.1	S	2	40,00%
12.4.2	S	2	0,00%
12.4.3	S	2	0,00%
12.5			
12.5.1	S	2	40,00%
12.5.2	S	2	40,00%
12.5.3	S	3	60,00%
12.5.4	S	2	40,00%
12.5.5	S	1	0,00%
12.6			
12.6.1	S	2	20,00%
	16	2	0,30%

Ilustración 32. Cumplimiento Dominio A12 / ISO 27001

Gestión de incidentes de seguridad: Este dominio se encuentra en nivel de madurez 2 (Repetible pero intuitivo). Es necesario documentar con mayor detalle los procedimientos relacionados con reporte de incidentes, y determinar los responsables por la evaluación y seguimiento de los mismos.

GESTION DE INCIDENTES			
CTROL	Aplica	CMM	% CMM
13.1			
13.1.1	S	2	40,00%
13.1.2	S	2	40,00%
13.2			
13.2.1	S	2	40,00%
13.2.2	S	2	40,00%

GESTION DE INCIDENTES			
13.2.3	S	2	40,00%
	5	2	0,40%

Ilustración 33. Cumplimiento Dominio A13 / ISO 27001

Gestión de la continuidad del negocio: Este dominio, el cual se encuentra en nivel de madurez 0 arriesga la subsistencia de la organización y varios clientes ya que no se dispone de infraestructura, conciencia, ni procedimientos relacionados para superar eventos catastróficos que afecten la operación y normal funcionamiento de la Organización.

CONTINUIDAD DEL NEGOCIO			
CTROL	Aplica	CMM	% CMM
14.1			
14.1.1	S	0	0,00%
14.1.2	S	0	0,00%
14.1.3	S	1	20,00%
14.1.4	S	0	0,00%
14.1.5	S	0	0,00%
	5	0	0,04%

Ilustración 34. Cumplimiento Dominio A14 / ISO 27001

Cumplimiento: Este dominio se encuentra en nivel de madurez 0 (inexistente), por lo cual es necesario trabajar esencialmente en todo lo relacionado con:

- Protección de los registros de la DNIE
- Protección de los Datos y privacidad de la información personal
- Prevención del uso inadecuado de los servicios de procesamiento de información.

CUMPLIMIENTO			
CTROL	Aplica	CMM	% CMM
15.1			
15.1.1	S	1	20,00%
15.1.2	S	1	20,00%
15.1.3	S	1	20,00%
15.1.4	S	1	20,00%
15.1.5	S	0	0,00%
15.1.6	S	0	0,00%
15.2			
15.2.1	S	0	0,00%
15.2.2	S	0	0,00%
15.3			
15.3.1	S	1	20,00%
15.3.2	S	1	20,00%
	10	0	0,12%

Ilustración 35. Cumplimiento Dominio A15 / ISO 27001

Consolidando los niveles de madurez alcanzados sobre los 130 controles aplicables podemos encontrar que:

- 30,83% están en nivel 0
- 16,54% están en nivel 1
- 21,80% están en nivel 2
- 28,57% están en nivel 3
- 0,00% están en nivel 4
- 0,00% están en nivel 5
- 2,26% No aplican para la Organización

A continuación se comparan los niveles de madurez alcanzados con cada dominio de la norma ISO 27002 frente a las prácticas recomendadas.

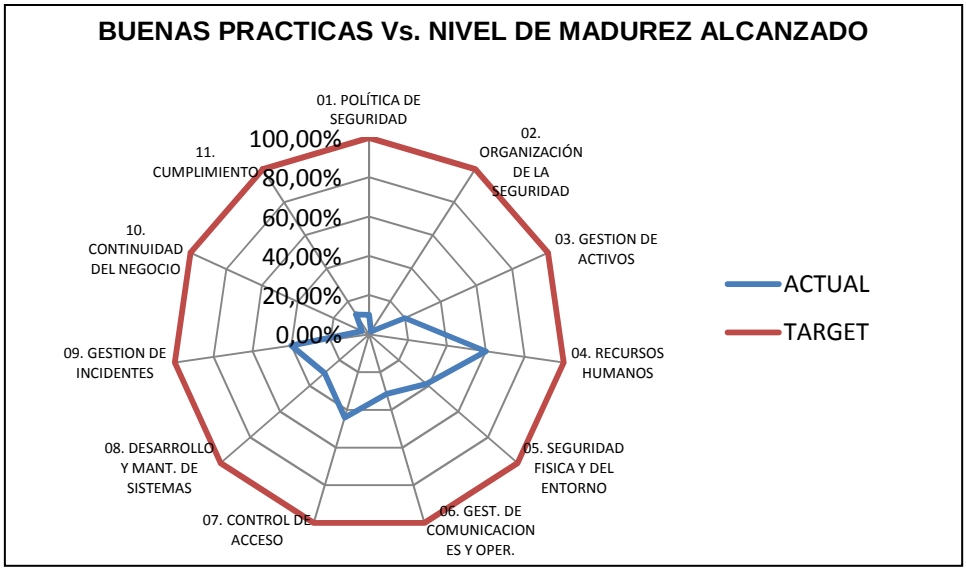

Ilustración 36. Madurez de los Controles

4.5 CONCLUSIONES

La organización requiere implementar mayor número de controles y mejorar la eficacia de los existentes con jornadas de sensibilización y divulgación de directrices en seguridad de la información.

Los controles y procesos manejados por la organización deben ser conocidos por todos los funcionarios de la organización además de controlados y mejorados.

Es importante concientizar a todos los funcionarios que la seguridad de la información es responsabilidad de todos.

5 FASE 5: PROPUESTAS DE PROYECTOS

5.1 INTRODUCCIÓN

La presente sección identifica planes de tratamiento de riesgos que incorporan proyectos de seguridad de la información, acciones rápidas y/o de contingencia para mitigar riesgos identificados en la fase de análisis sobre activos de información de XYZ Soluciones.

La principal meta es suministrar un documento base que permita establecer las medidas de seguridad demandadas para mitigar los riesgos identificados

5.2 PROPUESTAS PROYECTOS

Diseño e Implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

Propósito del Plan:
Diseñar y adoptar un modelo de gestión de seguridad de la información que facilite establecer, revisar, mantener y mejorar los niveles de seguridad demandados por el estado, los clientes y toda la Organización.

Situación actual:
Se realizan esfuerzos aislados por mantener niveles de seguridad adecuados sobre sus plataformas y servicios de la Organización.

Requerimientos Legales:
Las organizaciones requiere dar uso adecuado de la Información para cumplir con requerimientos hechos por disposiciones dadas a través de: La Constitución Española CE, LOPD, Código Penal CP , LEC, estándares Internacionales de Seguridad de la Información como ISO27001:2005, entre otras.

Identificación de recursos y actividades:
El apoyo de la alta dirección, seguido de la formalización del cargo de Oficial de Seguridad de la Información y la vinculación de un especialista en gestión de incidentes.

Posteriormente la capacitación de líderes de las diferentes áreas en temas de seguridad y la conformación de un comité de seguridad encargado de ejecutar, apoyar y monitorear los cambios requeridos sobre toda la Organización.

El desarrollo de Políticas, Normas y Procedimientos de seguridad de la Información que den respuesta a los objetivos de control y controles establecidos por ISO27001 es el principal entregable de esta actividad.

Campaña de sensibilización difundiendo la importancia de las buenas prácticas de seguridad que tienen aprobación de la Alta Dirección y serán exigidas en toda la Organización.

Prioridad: Alta - Corto Plazo

Tempos Estimados:
La dimensión de los cambios y ajustes requeridos sobre todas las dependencias son un factor decisivo, pero se puede estimar avances significativos al término de un año contando con el apoyo de un comité de Seguridad.

Implementación de un Plan de Continuidad del Negocio

Propósito del Plan:

Tratar de reducir los riesgos relacionados situaciones poco probables y difícil de evitar como: desastres naturales, incendios, fallos eléctricos prolongados, conmoción o atentados terroristas por nombrar algunos.

Situación actual:
Se mantienen los servicios core del negocio con operación básica y sin opción de respuesta oportuna ante situaciones de desastre.

Identificación de recursos:

El análisis de impactos sobre procesos implicados en la misión del negocio son el eje principal de todo Plan de Continuidad del Negocio, Este proceso es conocido formalmente como BIA (Business Impact Analisys) y se sugiere contar inicialmente con asistencia o consultoría de personal experto para la valoración y análisis de consecuencias económicas.

Adicionalmente y por ser un elemento estratégico, requiere del apoyo continuo de la alta dirección y participación activa de líderes administrativos de las diferentes áreas de la Organización.

Prioridad: Alta - Corto Plazo

Tempos Estimados:
Cuatro meses para superar la etapa inicial (BIA y Definición de estrategias de continuidad) y 6 meses en documentación y probas los planes.

Marco de trabajo para Control de Operaciones

Propósito del Plan:
Contar con un marco de trabajo ampliamente aceptado (Ej: ITIL) para el gobierno y control de operaciones.

Situación actual:
Hay diversificación de razonamientos, métodos implantados, términos manejados, criterios de evaluación adoptados que dificultan y generan contratiempos en la operación diaria de las diferentes dependencias.

La adopción de un marco de trabajo estándar permite:

- Facilitar el gobierno de las áreas, protegiendo los intereses de los stakeholders (clientes, accionistas, empleados, etc.)
- Optimizar la eficacia y eficiencia de los procesos y actividades de la organización
- Mejorar los niveles de confidencialidad, integridad y disponibilidad de la información
- Responder al cumplimiento normativo del sector al que pertenezca la organización

Identificación de recursos:
Apoyo de la alta dirección, seguido de la adquisición de asesoría o consultoría para implantar el marco de trabajo seleccionado. Posteriormente capacitación de líderes y usuarios de las diferentes dependencias de XYZ Soluciones

Prioridad: Moderada - Largo Plazo

Tiempos Estimados:
Contando con la disposición requerida se estima un período de **doce meses** para vislumbrar cambios significativos.

Clasificación de la Información

Propósito del Plan:

La información tratada por la Organización necesita identificar prioridades de manejo y grado de protección esperado.

Situación actual:
La información de las diferentes dependencias de la Organización tiene desiguales grados de sensibilidad e importancia. Sin embargo, la Organización no tiene definido niveles de clasificación, ocasionando exposición por errores humanos, uso inadecuado de la información o actos mal intencionados.

Identificación de recursos:
Apoyo en marcos de referencia como ISO 900l, ISO 27001 y líderes de las diferentes dependencias para la implantación, concienciación y exigencia de los procesos.

Prioridad: Mediano Plazo

Tiempo estimado de ejecución: 1 a 6 meses

Entregables: Niveles de protección y categorización de la información, procesos de clasificación de la información y concienciación al interior de la Organización.

Concienciación en Seguridad de la Información

Propósito del Plan:
Diseñar y ejecutar un plan de concientización en seguridad de la información que permita agrupar esfuerzos para mantener y mejorar los niveles de seguridad de toda la Organización.

Situación actual:
No hay cultura de manejo seguro y responsable de la información

Identificación de recursos:

El objetivo principal de la campaña es difundir la importancia de las buenas prácticas a nivel de seguridad de la información contando para ello con el apoyo de la Alta Dirección

Prioridad: Actividad Permanente

5.3 PROPUESTAS ACCIONES RÁPIDAS Y PERMANENTES

Acuerdos de Confidencialidad

Se recomienda formalizar los acuerdos de confidencialidad con personal directo y subcontratado y a la vez con empresas prestadoras de servicios.

Prioridad: Actividad Permanente

Tiempo estimado de ejecución: 1 mes

Controlar acceso a recursos tecnológicos

Establecer e implantar directrices de configuración y control acceso a los diferentes activos tecnológicos de la organización.

Prioridad: Actividad Permanente

Tiempo estimado de ejecución: 3 meses

5.4 PROPUESTA DE CONTROLES

La selección de controles o medidas viables para reducir la probabilidad de ocurrencia de eventos negativos en seguridad de la información e impactos nocivos de los mismos a la organización y sus clientes es factor clave de todo plan de tratamiento. Las siguientes listas sugieren controles específicos a ser mantenidos, mejorados o aplicados en XYZ Soluciones de acuerdo con la evaluación de riesgos previamente identificada.

Monitorear y mantener los siguientes controles y prácticas identificadas en los procesos de valorados.

- Buenas prácticas de Backups (Frecuencia, Tipo de Backups, Rotación, pruebas, custodia, niveles de autorización, etc.)
- La generación de "Backups" o copias de seguridad, registro de bitácoras gestión y etiquetados y envíos correspondientes.
- Garantizar la existencias de medio magnéticos suficientes para el almacenamiento de respaldos, considerando periodos de vida útil.
- Mantener hardware de respaldo por convenio con proveedores para el suministro de equipos de contingencia con características similares o mejores y disponibilidad 7*24 bajo tiempos de respuesta acordados.

Actualizar, comunicar, monitorear y exigir mayor cumplimiento de controles existentes como:

- Políticas de seguridad definidas, documentadas, aprobadas y socializadas
- Concientización y participación activa en temas de seguridad de la información.
- Concientización en temas Clasificación de información
- Reporte y manejo de incidentes "Empresariales"
- Mantener una política de escritorios y áreas limpias
- Almacenamiento de datos en sitios seguros y restringidos según la clasificación de la información.
- Bloqueos de sesión por inactivación
- Identificación permanente del personal(portar documento)
- Procedimiento de autorización y acompañamiento de ingreso de visitantes o personal de soporte.
- Asignación de permisos por roles y perfiles acordes con las funciones (menor privilegio)
- Esquemas de selección y contratación del personal
- Actualización periódica de acuerdos de confidencialidad
- Mediciones de desempeño (capacity planning)
- Manual de funciones y/o operaciones documentado
- Documentación de los procedimientos de Administración y Operación
- Proceso formal de solicitud, autorización y asignación de cuentas (especialmente las asignadas a terceros o contratistas)
- Custodia de contraseñas administradoras (especialmente contratistas con acceso a recursos críticos)
- Mantener y actualizar los inventario de activos críticos
- Selección y validación de ambientes propicios para zonas críticas
- Control de acceso físico (tarjetas de aproximación, zonas restringidas, anunciar visitantes, etc.).
- Acuerdos de nivel de servicio (ANS) con responsabilidades claramente definidas e indicadores de gestión para evaluar cumplimiento
- Validación de riesgos asociados con la dependencia de proveedores de servicios y tecnologías rentadas.

Analizar la viabilidad de implementación de nuevos controles como:

- Implementar el sistema de control de activos de información clasificados y documentados.
- Implementar el sistema de control de ingreso y retiro de elementos administrados por personal de XYZ Soluciones
- Bandas detectoras / detectores de metales
- La adquisición de seguro contra robo de equipos y portátiles.
- Ejecución periódica de pruebas de penetración internas y externas
- Ejecución periódica de pruebas de ingeniería social
- Estudios periódicos de análisis de vulnerabilidades de los sistemas de información
- Definición de OLAs o acuerdos de nivel de operación internos entre las unidades de negocio
- Ejecutar mediciones de desempeño y cumplimiento a empleado o contratista
- Promover la disponibilidad de Funcionario Backup
- Incorporación de firmas digital sobre archivos relevantes en el origen
- Ambientes independientes de Producción, Desarrollo y Pruebas
- Auditorías periódicas en seguridad de la información internas/externas
- Establecer y comunicar los procesos disciplinarios por faltas a seguridad de la información.
- Configuración de servidores y equipos de comunicación con lineamientos básicos de seguridad.
- Para casos de daños físicos mayores y/o desastre naturales, contar con directivas de evaluación de daños, procesos de traslado y reactivación de servicios, secuencias de reactivación de servicios críticos y un centro de operaciones alterno
- Plan de contingencias, Plan de recuperación de desastres DRP y Sitio Alterno

5.5 ROADMAP DE PROPUESTAS

Las siguientes tablas muestra el mapa de ruta establecido para encarar de manera acertada la prioridad de actividades que conforman los planes estratégicos y acciones rápidas del presente informe.

PROYECTOS Y ACTIVIDADES SUGERIDAS.	
01	Implementación del SGSI (1 año)
02	Implementación del PCN (1 año)
03	Clasificación de la Información. (1 - 6 meses)
04	Implementación Marco de Trabajo Estándar (1 año)
05	Concienciación en Seguridad de la Información
06	Renovación Acuerdos de Confidencialidad
07	Control de acceso a recursos

Ilustración 37. Proyectos Sugeridos

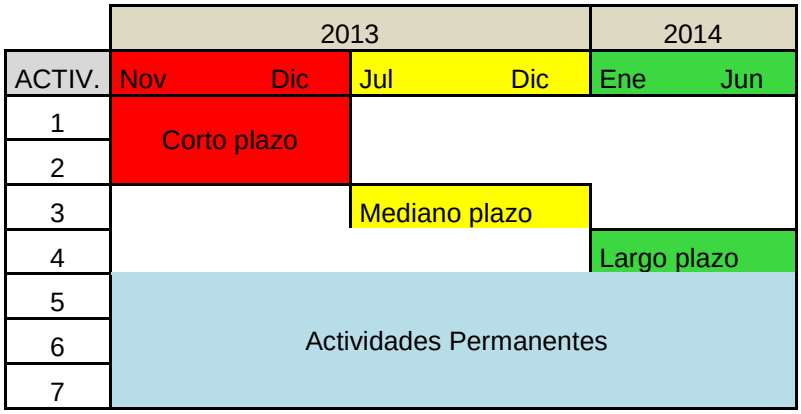

Ilustración 38. Roadmap de implementación

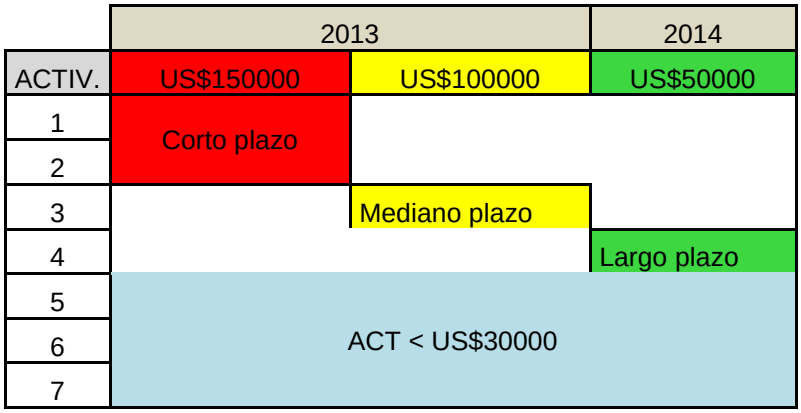

Ilustración 39. Costos de implementación

La primacía es para Jornadas de implementación del SGSI y los planes de Continuidad debido a la criticidad de los servicios de la Organización para con sus clientes. Todas estas actividades manejan una prelación alta con necesidad de ejecución en el corto plazo.

Una vez terminada las actividades previas se sugiere depurar los niveles identificación, clasificación y tratamiento de la información. Estas actividades tienen una prelación media y se sugiere su ejecución en un mediano plazo.

Seguido por la implementación de un marco de trabajo que permita unificar criterios de operación, control e indicadores de servicio de todas las dependencias de la Organización. Estas actividades tienen una prelación de largo plazo.

Finalmente y bajo la etiqueta de actividades permanentes se debe promover actividades de concienciación, renovación de acuerdos de confidencialidad y activación y monitoreo contante a controles de acceso sobre recursos críticos de la organización.

6 FASE 6: PRESENTACIÓN DE RESULTADOS Y ENTREGA DE INFORMES

6.1 INTRODUCCIÓN

La siguiente sección resume los hallazgos que tienen mayor afectación o relevancia en los niveles de seguridad de XYZ Soluciones.

Para la presentación y publicación de resultados del presente ejercicio, la consultoría acude a la creación de un archivo en PowerPoint el cual se anexa y abrevia todo el proceso de identificación y valoración de activos así como la valoración de riesgos, planes de tratamiento recomendado y mapa de ruta sugerido.

6.2 HALLAZGOS RELEVANTES

XYZ Soluciones realiza esfuerzos aislados por mantener niveles de seguridad mínimos sobre sus plataformas y servicios. Sin embargo, para lograr armonía y un perspectiva clara a nivel de seguridad, es necesario coincidir en el logro de metas y objetivos que apoyados a nivel estratégico y administrados apropiadamente permitan a la Organización implementar prácticas de seguridad de la información en todas las áreas funcionales con un tratamiento responsable de la Información.

La organización no cuenta con ciclos constantes de monitoreo y seguimiento a los controles de seguridad para ratificar el compromiso, concientización de alcances, caracterización de necesidades puntuales, identificación del valor de los mismos, condición que hace difícil canalizar inversiones y unificar esfuerzos para mejorar de los niveles de seguridad requeridos.

De acuerdo a las entrevistas realizadas, la información de las diferentes procesos de XYZ Soluciones tiene desiguales criterios de evaluación de sensibilidad e importancia, ocasionando exposición por errores humanos, uso inadecuado de la información o actos mal intencionados, por lo cual se recomienda identificar un esquema de categorización consolidado, instituyendo el conjunto apropiado de niveles de protección demandados para toda la Organización.

XYZ Soluciones carece de una solución de software apropiada para identificar, estimar, analizar, evaluar, monitorear y revisar periódicamente los riesgos de modo consecuente al tamaño y necesidades de la organización, razón por la cual se recomienda implementar un sistema de gestión basado en un conjunto apropiado de reglas de protección, normas y prácticas reconocidas internacionalmente para gestión del riesgo y seguridad de la información

XYZ Soluciones mantiene los servicios con procesos de operación básica pero carece de disposiciones concertadas que le permitan una recuperación ante eventos mayores o desastres con procesos y fases debidamente documentados, informados y probados.

XYZ Soluciones no cuenta con oficial o líder en seguridad de la información para soportar toda la carga estratégica y operativa de un Sistema de Gestión de Seguridad de la Información (SGSI) el cual demanda recursos de tiempo completo para monitorear, controlar, tratar y mejorar todas las medidas de control requeridas por la norma ISO/IEC 27001 y mitigar riesgos asociados a la seguridad de la información