UNIVERSIDAD DON BOSCO

VICERRECTORÍA ACADÉMICA

FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE

MAESTRO EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

PROYECTO

GUÍA PARA LA EVALUACIÓN DE LA CIBERSEGURIDAD EN INSTITUCIONES PRIVADAS

PRESENTADO POR:

Licda. Otilia Isabel Ramírez de Quezada

Ing. Douglas Rodrigo Orellana Aguilar

Ing. Erick Gerardo Pérez Marroquín

ASESOR:

Msc. Herson Miguel Serrano Chacón

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América

MAYO 2023

GUÍA PARA LA EVALUACIÓN DE LA CIBERSEGURIDAD EN INSTITUCIONES PRIVADA

Resumen– La ciberseguridad es una realidad para las organizaciones y para las personas en la actualidad, aunque el concepto no parece claro, en la práctica es más sencillo y necesario de entender, ya que ahora la ciberseguridad es tan requerida como la seguridad física en lugares de trabajo, en la sociedad o residencial.
Por lo tanto, surge la necesidad de informarse y obtener una guía de evaluación que determine el estado actual de la organización dentro del concepto de ciberseguridad y así mismo oriente a la organización sobre los aspectos a fortalecer y reforzar, considerando el apetito de riesgo, presupuesto y criterios que impacten en la aplicación de herramientas, políticas y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios.
Para ello se propone una guía para relacionar conceptos relevantes de las organizaciones en un contexto laboral, social, profesional y legal, con el único fin de proteger sus activos, que generan beneficios económicos, sociales, etc.

Palabras Clave– Guía de Ciberseguridad, Ciberseguridad, Controles de Seguridad, Evaluación, Seguridad.

I. INTRODUCCIÓN

La tecnología está inmersa en todos los aspectos de las personas naturales y jurídicas, tanto laboral, personal y social, que permite ejecutar actividades de la oficina, académicas o personales de forma remota; desde redactar un correo electrónico de la empresa donde se labora, hasta realizar un pedido en una tienda de conveniencia, pero dentro de esos procesos deben existir lineamientos de seguridad y medidas de seguridad que se requieren para completarse de manera correcta y segura.

Por lo tanto, existen responsabilidades por parte de la organización y los usuarios para resguardar documentos, respaldos de datos y todo tipo de archivos, los cuales deben ser resguardados bajo las normas de seguridad que cada uno de ellos requiere y que la regulación gubernamental de cada país exige.

La investigación propone una guía de criterios generales, técnicos, de seguridad y legales que las organizaciones deben considerar para aplicar y obtener un control idóneo de

ciberseguridad. Por ende, se debe contemplar las características propias de la organización, su aplicabilidad.

Como resultado de la investigación, se plantea una metodología de autoevaluación de ciberseguridad de las organizaciones, la cual consiste en una lista detallada de los criterios importantes, los criterios deberán ponderarse de acuerdo a la valoración que cada organización que aplique la metodología.

Se considera que la metodología puede ser de mucha utilidad para las organizaciones para autoevaluar sus niveles de seguridad de diferentes áreas y que facilite la comprensión de todos los aspectos que deben ser considerados.

II. JUSTIFICACIÓN

La ciberseguridad es un tema crítico para cualquier organización que maneje información sensible y la falta de medidas de seguridad adecuadas puede resultar en pérdida de datos, daño a la reputación y pérdida financiera. Además, una guía de evaluación de ciberseguridad puede ayudar a las instituciones privadas a identificar y mitigar los riesgos de seguridad cibernética y cumplir con las regulaciones y estándares de seguridad aplicables.

Las instituciones deben mantenerse vigilantes para lograr enfrentar las amenazas en el ciberespacio o tratar de disminuir o minimizar su impacto, contar con el servicio del internet se vuelve un área con riesgos a la seguridad.
En el entorno actual, las instituciones privadas se enfrentan a una creciente cantidad de amenazas cibernéticas que pueden comprometer la confidencialidad, integridad y disponibilidad de la información crítica y los sistemas que respaldan sus operaciones. Estas amenazas pueden provenir de actores malintencionados, como hackers, delincuentes cibernéticos, espías industriales o incluso empleados desleales.

La implementación de medidas de ciberseguridad adecuadas es fundamental para proteger los activos digitales y garantizar la continuidad del negocio. Sin embargo, muchas instituciones privadas carecen de una guía estructurada y práctica para evaluar su postura actual de ciberseguridad y tomar medidas correctivas necesarias.

Por lo tanto, la justificación para desarrollar una guía de evaluación de ciberseguridad en instituciones privadas se basa en los siguientes puntos:

- Identificación de vulnerabilidades: La guía proporcionará un marco sistemático para identificar y evaluar las vulnerabilidades y debilidades en los sistemas de información y las infraestructuras tecnológicas de las instituciones privadas. Esto permitirá un análisis exhaustivo de los riesgos a los que se enfrentan y una comprensión clara de las áreas que requieren atención inmediata.

- Protección de la información confidencial: Las instituciones privadas manejan grandes cantidades de información confidencial, incluyendo datos financieros, datos personales de los clientes y secretos comerciales. La guía de evaluación de ciberseguridad ayudará a establecer controles efectivos para proteger esta información contra accesos no autorizados, filtraciones y robo. Esto garantizará la confianza de los clientes y cumplirá con las regulaciones de protección de datos vigentes.

- Cumplimiento normativo: Muchas industrias están sujetas a regulaciones y estándares específicos relacionados con la seguridad de la información, como la Norma ISO 27001. La guía de evaluación de ciberseguridad proporcionará un enfoque estructurado para garantizar el cumplimiento de estos requisitos, ayudando a las instituciones privadas a evitar sanciones legales, pérdida de reputación y pérdida de clientes.

- Gestión proactiva de incidentes: La guía permitirá a las instituciones privadas desarrollar un enfoque proactivo para la gestión de incidentes de ciberseguridad. Al establecer procedimientos claros para la detección, respuesta y recuperación de incidentes, las organizaciones podrán minimizar el impacto de las brechas de seguridad y reducir los tiempos de inactividad.

- Mejora continua: La guía de evaluación de ciberseguridad fomentará una cultura de mejora continua en materia de ciberseguridad. Al realizar evaluaciones periódicas, las instituciones privadas podrán identificar áreas de mejora, implementar medidas correctivas y fortalecer constantemente su postura de seguridad, adaptándose a las nuevas amenazas y tecnologías emergentes.

En resumen, la guía de evaluación de ciberseguridad en instituciones privadas es esencial para proteger los activos digitales, garantizar la continuidad del negocio y cumplir con las regulaciones y estándares aplicables. Proporciona un enfoque estructurado y práctico para evaluar y mejorar la postura de ciberseguridad, lo que resulta en una mayor confianza de los

clientes, mitigación de riesgos y una respuesta eficaz ante las amenazas cibernéticas en constante evolución.

III. OBJETIVOS

3.1. OBJETIVO GENERAL

Desarrollar una metodología integral y práctica que permita evaluar la ciberseguridad en instituciones privadas, con el fin de fortalecer y proteger sus sistemas de información contra amenazas y ataques cibernéticos.

3.2. OBJETIVOS ESPECÍFICOS

1. Analizar el estado actual de la ciberseguridad en instituciones privadas, identificando las principales amenazas y vulnerabilidades a las que se enfrentan.

2. Revisar las normativas y estándares internacionales de ciberseguridad aplicables a instituciones privadas, para determinar los requisitos y mejores prácticas a considerar en la evaluación.

3. Diseñar una metodología de evaluación de ciberseguridad adaptada a las necesidades y características específicas de las instituciones privadas, teniendo en cuenta su tamaño, sector y tipo de datos manejados.

4. Desarrollar un conjunto de herramientas y técnicas de evaluación de ciberseguridad que permitan realizar un diagnóstico preciso y exhaustivo de los sistemas de información de las instituciones privadas.

5. Elaborar una guía práctica y completa que documente la metodología de evaluación de ciberseguridad, junto con recomendaciones y acciones específicas para fortalecer la seguridad en las instituciones privadas, con el objetivo de servir como referencia y apoyo en la implementación de medidas de ciberseguridad efectivas.

IV. DELIMITACIÓN

La guía de evaluación de ciberseguridad en instituciones privadas se enfocará en proporcionar un marco general para evaluar y fortalecer la ciberseguridad en instituciones privadas, abordando aspectos técnicos y organizativos, y basándose en estándares reconocidos. Sin embargo, no abordará aspectos legales específicos ni proporcionará una implementación detallada, dejando espacio para la adaptación y personalización por parte de cada institución.

Enfoque en instituciones privadas: La guía estará específicamente dirigida a instituciones privadas, incluyendo empresas, organizaciones sin fines de lucro y otras entidades del sector privado.
Cobertura de aspectos técnicos y organizativos: La guía abordará tanto los aspectos técnicos como los organizativos de la ciberseguridad. Esto incluye la evaluación de sistemas y redes, políticas de seguridad, gestión de identidad y acceso, concienciación del personal, respuesta a incidentes y otras áreas relacionadas.

Marco general: La guía proporcionará un marco general para la evaluación de ciberseguridad en instituciones privadas. No se profundizará en detalles específicos de cada sector o industria en particular. Se espera que las instituciones adapten y personalizan el marco según sus necesidades y características específicas.
Enfoque preventivo: La guía se centrará en la prevención y mitigación de riesgos en ciberseguridad. Si bien la respuesta a incidentes y la recuperación posterior son aspectos importantes, no serán el foco principal de la guía. Sin embargo, se proporcionarán directrices generales para establecer procesos de gestión de incidentes.

Orientación, no implementación: La guía proporcionará recomendaciones y directrices generales para la evaluación de ciberseguridad, pero no pretenderá ser un conjunto exhaustivo de procedimientos o soluciones específicas. Las instituciones deberán adaptar las recomendaciones según sus necesidades y recursos disponibles.

Basada en estándares y mejores prácticas reconocidas: La guía se basará en estándares y mejores prácticas reconocidas en el campo de la ciberseguridad, como la Norma ISO 27001, el Marco de Ciberseguridad del NIST, entre otros. Sin embargo, no se limitará únicamente a estos estándares y podrá incluir otras referencias relevantes.

No abarca aspectos legales y regulatorios específicos: Si bien la guía puede mencionar la importancia del cumplimiento normativo, no proporcionará una cobertura detallada de los

requisitos legales y regulatorios específicos de cada jurisdicción. Las instituciones deberán consultar y cumplir con las leyes y regulaciones aplicables en su ámbito de operación.

Es importante tener en cuenta estas delimitaciones al utilizar la guía de evaluación de ciberseguridad en instituciones privadas para asegurarse de que se aplique de manera adecuada y se complementen con otros conocimientos y recursos relevantes según las necesidades específicas de cada institución.

V. MARCO TEÓRICO

1. DETERMINAR ÁREA DE RIESGO.

Una evaluación de Ciberseguridad es un procedimiento que evalúa el nivel de seguridad de una empresa o entidad, analizando sus procesos y comprobando si sus políticas de seguridad se cumplen.

El principal objetivo de una evaluación de seguridad es el de detectar las vulnerabilidades y debilidades de seguridad que pueden ser utilizadas por terceros malintencionados para robar información, impedir el funcionamiento de sistemas, o en general, causar daños a la empresa.

Al momento de plantear una evaluación de ciberseguridad, uno de los primeros puntos es establecer el contexto:

Conocer información clave de la empresa y con base en esto poder determinar los aspectos a auditar, entre estos se deben considerar redes, servidores, equipos y personas. Debido al aumento en el número de dispositivos interconectados, se ha vuelto difícil desarrollar una solución de seguridad dinámica y confiable que pueda proteger la red contra todos los riesgos potenciales de seguridad.

Por lo tanto, es importante analizar y comprender la conectividad de diferentes sistemas a diferentes niveles para identificar vulnerabilidades y mitigarlas. Estas vulnerabilidades incluyen el efecto en cascada, eliminación de nodos, enlaces vitales de identificación, capacidad de control de nodos, ataques de ruta iterativa y estrategias de cambio para

propagación a gran escala. Sin embargo, estas soluciones pueden no ser tan efectivas ya que se centran solo en la conectividad de red y sus características (centralizadas).

1.1. ÁREA DE RIESGO

Actualmente la mayoría de las organizaciones cuentan con áreas y personal especializado para la gestión del riesgo y control interno. Sin embargo, sus actividades están divididas y distribuidas dentro de la organización sin una adecuada coordinación y comunicación, por lo que pueden existir brechas o espacios en la cobertura de los controles internos y hasta generar duplicación o creación de actividades innecesarias.

- El modelo de las Tres Líneas de Defensa proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados.

- El modelo clasifica las áreas funcionales y de responsabilidad de la empresa y brinda una visión de las operaciones, garantizando una adecuada supervisión y gestión del riesgo, además de ser apropiado para cualquier organización independientemente de su tamaño o complejidad.

- El modelo distingue tres líneas de actividades que participan en una efectiva gestión y supervisión de riesgos. La alineación de las tres líneas de defensa permite mitigar de una forma integral los riesgos.

La primera línea está compuesta por el control de la gerencia, donde cada área operativa de la organización pone en práctica la gestión de sus propios riesgos y controles, para asegurar el cumplimiento de los objetivos de la organización a través de un adecuado sistema de control interno.

La segunda línea contempla las funciones de supervisión de riesgos, controles y cumplimiento de políticas y estándares establecidas por la administración, abordando riesgos transversales, complejos y específicos; ambas, primera y segunda línea, reportan a la Alta Dirección.

Y en la tercera línea está el aseguramiento independiente, la Evaluación Interna, la cual aporta supervisión objetiva sobre las dos primeras líneas de defensa, evalúa el sistema de control interno de la organización en su conjunto para identificar debilidades y recomendar mejoras.

La Evaluación Interna debe reportar a la Alta Dirección y a la Junta Directiva. Finalmente, y fuera del marco de la organización, se encuentran la Evaluación Externa y Organismos Reguladores, que no integran el sistema de control interno, sino que lo examinan independiente y externamente.

Se debe comprobar que el control y la gestión de la tecnología se encuentran segregados conforme al modelo de ciberseguridad, por ejemplo, el modelo Tres líneas de defensa:

Gráfico 1: MODELO DE LAS TRES LÍNEAS DE DEFENSA

Tomado del documento emitido por la IIA: IIA Declaración de posición: las tres líneas de defensa para una efectiva gestión de riesgos y control.

Cada una de las tres líneas juega un papel distinto dentro del marco de gobernabilidad de la organización.
Las tres líneas de defensa deben contar con un nivel de separación e independencia suficiente para no comprometer la efectividad del esquema general, y actuar coordinadamente con el fin de maximizar su eficiencia y potenciar su efectividad. El modelo tiene un grado elevado de sofisticación y complejidad. Por tanto, el IIA establece ciertos principios orientativos para determinar si el grado de madurez de la organización permite avanzar hacia un modelo de tres líneas de defensa, o no.
Estos requisitos son:

- Existencia de un comité de evaluación idóneo, capaz de monitorear el accionar de las diferentes funciones de aseguramiento y su integración.

- Formalización de las responsabilidades por el mantenimiento de un sistema de control interno y la gestión de riesgos.

- La evaluación interna debe ser profesional y eficaz, habiendo logrado demostrar su adhesión a las Normas Internacionales para el Ejercicio Profesional de la Evaluación Interna, y el director ejecutivo de Evaluación Interna debe contar con la necesaria independencia para ejercer sus funciones

Si se intenta avanzar en un modelo de tres líneas de defensa sin haber asegurado previamente estas condiciones, es posible que el control interno de la organización no mejore, sino que incluso se desmejore, al intentar confiar funciones más importantes a áreas que no son idóneas ni confiables

La implementación del modelo implica tanto ventajas como desventajas, que se derivan del uso de una metodología más racional para la gestión de riesgos y control, y que también significa ser más eficiente en los recursos y más confiable en los resultados, así como asumir ciertas desventajas para la organización y retos para la evaluación interna, que deben tomarse en consideración al momento de tomar la decisión de adoptar este modelo.

1.2. VENTAJAS DEL MODELO DE TRES LÍNEAS DE DEFENSA

- **Es un modelo sólido:**
  Sólido significa que no presenta grietas. En el estado actual de formulación de control interno existen grietas, porque no está explícito el alcance de las labores de cada una de las funciones de segunda línea de defensa, hasta dónde llega cada una de ellas. Esto produce ocasionalmente solapamientos en las tareas, contradicciones entre las opiniones de diversas áreas y zonas grises.

- **Es un modelo robusto:**
  Esta característica se percibe al advertir que la fuerza de las distintas funciones de aseguramiento es mayor cuando actúan coordinadamente que cuando cada una de ellas lo hace por separado.

- **Es un modelo resistente:** La resistencia deriva de su integralidad y de la confianza que provee a la Dirección Superior el saber que una diversidad de especialistas está actuando coordinadamente a su servicio. Esto reduce sustancialmente la probabilidad de que alguna o algunas de las tareas de aseguramiento resulten eliminadas o debilitadas por no percibirse claramente su contribución al éxito de la organización.

- **Se genera un crecimiento dentro de la organización**
  Que finalmente coloca a la Evaluación Interna en el nivel de Alta Gerencia a la cual siempre aspiró y nunca llegó. Debido a que la Evaluación Interna es actualmente una función de Gerencia media colocada en el más alto nivel del organigrama. El rol de evaluación de un marco de control interno amplio que salvaguarde el cumplimiento de las metas operativas y atienda a sus riesgos estratégicos puede, por fin, colocar a la Evaluación Interna en un nivel alto.

  Una vez implementado el modelo las operaciones se hacen más eficientes, al integrar y fluir la operación y el control como parte del mismo engranaje y sin oponerse el uno a la otra.

- **La información mejora y se integra.**
  Los diversos informes producidos por cada sector de la organización podrán ser consultados por el resto en forma oportuna para sus necesidades.

- **Se reducen los inconvenientes operacionales por riesgos imprevistos.** Dado que cada función atiende su responsabilidad sin omisiones, duplicidades ni contradicciones

1.3. DESVENTAJAS DEL MODELO DE TRES LÍNEAS DE DEFENSA

Es un modelo tan sofisticado y complejo que involucra diversas erogaciones:

- En personal, debe existir personal idóneo para atender las diversas funciones de la segunda línea de defensa.

- En capacitación, este personal debe mantenerse constantemente entrenado y motivado.

- En desarrollo de normativa. El desarrollo de las políticas y procedimientos para coordinar a este equipo de gente suponen un esfuerzo económico considerable.

- En software, no necesariamente, pero idealmente, debiera contarse con un software que integre una base de datos de conocimiento compartido por todas las áreas, de modo que cada uno disponga de información adecuada para el desarrollo de sus funciones, en primer lugar, y para supervisión del nivel superior, en segundo término.

Para lograr las sinergias entre las áreas de segunda línea de defensa, y una adecuada interrelación entre éstas y la gerencia de primera línea, se requiere un importante esfuerzo de coordinación y buena comunicación interdepartamental. En caso contrario, surge una burocracia que traba la operación y resta eficiencia a la organización.

Especialmente importante es delimitar las funciones a cumplir por cada área y persona, de modo de evitar zonas grises en las cuales exista un entendimiento generalizado de que alguien se está ocupando de algo, mientras en realidad no lo está haciendo. Lo inverso también es cierto, pues puede acontecer que varias áreas traten de abordar un tema al mismo tiempo, generando no solamente duplicación de esfuerzos sino también contradicciones entre las valoraciones y cursos de acción de las diferentes áreas respecto del mismo tema.

- Implica una dificultad para la Evaluación Interna porque en varias ocasiones los intereses del Directorio y Alta Gerencia no son exactamente coincidentes. Adicionalmente, el Directorio tiene como reportes a los Gerentes más poderosos de la organización, comenzando por el Gerente General. El director ejecutivo de Evaluación Interna dirige un departamento de tamaño normalmente modesto, y que no desarrolla funciones tan vitales para la organización como las de una Gerencia General.

  Al colocarlo en un pie de reporte equitativo, se le da cierto respaldo, por una parte. Pero, por otro lado, se corre el riesgo de que el Directorio no preste la debida atención a las necesidades de la Evaluación Interna, postergando siempre sus necesidades para atender las urgencias de vida o muerte de la Alta Gerencia. Y la Alta Gerencia puede percibir este factor y utilizarlo para anular a la Evaluación Interna.

- Se puede generar un angostamiento de las responsabilidades de la evaluación interna, en la medida que la creación de nuevas funciones de segunda línea le van restando labores que anteriormente desempeñaba. En adición a ello, la creación y potenciación de estas funciones de segunda línea de defensa puede generar una confianza creciente de la evaluación externa en el sistema de control interno de la organización, al punto de considerar y eventualmente sugerir al Directorio la supresión de la función de evaluación interna.

El equipo de evaluación interna deberá cambiar el alcance de sus tareas y comunicaciones con otras áreas, lo cual supone un reto a nivel colectivo, además los evaluadores internos deberán adquirir nuevas destrezas y potenciar las actuales.

La gestión de la ciberseguridad en una organización, y sus áreas encargadas dan cobertura a las funcionalidades siguientes:

- Elaborar, proponer y desarrollar las normas y metodologías de seguridad de TI, asegurando el cumplimiento del nivel de información de seguridad de los sistemas, de acuerdo con las definiciones de la política de seguridad informática.

- Realizar pruebas periódicas de seguridad lógica con el fin de verificar la eficacia de los controles instalados, identificar brechas de seguridad y proponer medidas correctivas.

- Analizar las fuentes de exposición al riesgo tecnológico utilizando, indicadores de riesgo y cuestionarios de autoevaluación, además de seguir las recomendaciones y sugerencias para mejorar la calidad, y además dar seguimiento a los proyectos de mitigación existentes en cada una de las áreas que estén ya establecidas como vulnerables en ciberseguridad.

- Colaborar para la definición de los requisitos para garantizar la seguridad, integridad y control de las áreas en las que operan con la tecnología.

1.4. ORGANIZACIÓN Y ESTRATEGIA

Son muchos los factores que una organización debe considerar para definir su estrategia de ciberseguridad, sin embargo, el simple hecho de que una organización se plantee esta pregunta, ya es un síntoma de madurez.

En primera instancia, la ciberseguridad es un “conjunto de medidas de protección de la información, a través del tratamiento de las amenazas que ponen en riesgo la información y que es tratada por los sistemas de información que se encuentran interconectados”. Según ISACA (Information Systems Audit and Control Association).
Es decir, de sistemas, redes y datos que se necesitan proteger. Y esta protección va a depender de la infraestructura que se tiene, los recursos de la organización para protegerlos, su madurez, etc.

La tecnología relacionada con la ciberseguridad no tiene sentido por sí misma, sino que tiene la obligación de dar soporte a los objetivos estratégicos de la organización. Por ejemplo, si la organización quiere abrir una nueva línea de negocio o digitalizar un área mediante la implantación de un nuevo software, la ciberseguridad debe ser el área encargada de proteger a la organización contra ataques que pongan en peligro la seguridad de la información de estos nuevos servicios.

Por esta razón, en algunos modelos, un rol como el CISO se encuentra dentro de la alta dirección para conocer de primera mano los objetivos estratégicos del negocio y protegerlos adecuadamente. Como en toda estrategia, la implicación de la alta dirección es una pieza clave.

Los factores que pueden determinar la estrategia de ciberseguridad dependerán de los objetivos estratégicos y de negocio de la organización, de los recursos y capacidades que esta posea y de los factores internos, un buen punto de partida para definir la estrategia de seguridad es responder las siguientes interrogantes:

- ¿Qué es crítico para la organización?
- ¿Cuáles son los activos de los que no se pueden prescindir?

Es conveniente realizar estas preguntas a las gerencias estratégicas de la organización, es muy común que un proceso de negocio importante dependa de un activo que únicamente conoce un área de compañía, sabiendo lo que se necesita proteger, se debe hacer el ejercicio de identificar los riesgos que podrían poner en peligro su integridad e identificar los controles que se tienen establecidos. Sin saber qué podría pasar y qué se tiene, sería un error ponernos directamente a implementar controles.

Este ejercicio permitirá identificar fortalezas y debilidades en materia de ciberseguridad en la compañía, identificar carencias y actuar sobre ellas. Además, ofrecerá una visión general de las diferentes capas y cómo proteger los activos más valiosos, siendo una estrategia que permite disminuir el avance del enemigo a través de los distintos métodos y controles (capas), en lugar de confiar en un único método de protección.

Esta estrategia permite que el atacante necesite más tiempo y conocimientos para lograr su objetivo, que es comprometer la seguridad de los activos críticos de la compañía. Además de permitir al defensor elaborar una respuesta más eficaz, la complejidad de la infraestructura hace necesario establecer un marco de gestión que permita implementar los procesos según las necesidades que tenga la organización o implementar un marco de seguridad de la información conocido en la industria. Existen algunos que, dependiendo de nuestro propósito

se podria implementar: ISO 27001, Controles de Seguridad CIS, Marco NIST, PCI-DSS, ENS, etc.

La estrategia que se defina en Ciberseguridad debe ser lo suficientemente flexible para adaptarse a los requisitos del mercado y nuevas tecnologías mantenerse en constante evolución, y ser capaces de adaptarse a los cambios, como los que se realizaron provocados por la pandemia de COVID-19, home office, cambió la estrategia de seguridad de la mayoría de las organizaciones y vulnero su estrategia de seguridad.

Dependiendo del tamaño de la compañía la evaluación en ciberseguridad externa puede ser una buena alternativa.

Para definir la estrategia de ciberseguridad es necesario lo siguiente:

- Decisiones Basadas en datos e información: conocer la organización cuáles son sus fortalezas y debilidades.

- La estrategia de ciberseguridad deberá ser apoyada por la alta dirección. Y al revés, la ciberseguridad debe apoyar y adaptarse a los objetivos de negocio.

- Implementar un marco de gestión de la ciberseguridad nos permitirá gestionar mejor los procesos. Ya sea ISO 27001, 27110, COBIT, marco NIST, etc. Es una buena estrategia escoger un estándar que defina y relacione los distintos procesos.

- La estrategia es consecuencia del contexto de la organización. Para definir una estrategia, se debe conocer la realidad de la organización. Los recursos siempre son limitados.

- Responsabilidades y roles de seguridad definidos. Es fundamental determinar quién se ocupa de qué para definir los diferentes procesos a implementar para llevar a cabo una buena gestión de la ciberseguridad.

1.5. MODELO DE GESTIÓN DE CIBERSEGURIDAD

Uno de los frameworks más importantes en relación con la ciberseguridad es el “Marco para la mejora de la seguridad cibernética en infraestructuras críticas”, publicado por el NIST el

cual propone cinco funciones que ayudan a una organización en la estructuración de su programa de gestión del riesgo cibernético, lo que facilita la toma de decisiones, identificando y abordando amenazas y mejorando la capacidad de aprendizaje de actividades previas.

Gráfico 2
Funciones definidas en el Cybersecurity Framework -NIST

Revisión de los marcos internacionales de ciberseguridad
Instituto Nacional de Estándares y Tecnología (Abril 2018). "Cibersecurity Framework".
Recuperado de: https://www.nist.gov/cyberframeworkframework

GUIA DE BUENAS PRÁCTICAS PARA AUDITAR LA CIBERSEGURIDAD

Con base en estas cinco funciones se pueden establecer objetivos de control y una serie de acciones para realizar evaluaciones de evaluación de ciberseguridad, apoyados en las categorías y subcategorías definidas en el Marco:

- **Identificar:**

Permite desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. Las actividades que engloban esta función son fundamentales para el uso efectivo del marco.

• Proteger:
Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento que atente a la ciberseguridad.

• Detectar:
Define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad, permitiendo su descubrimiento oportuno. Los ejemplos de categorías de resultados dentro de esta función incluyen: anomalías y eventos, monitoreo continuo de seguridad y procesos de detección.

• Responder:
incluye actividades necesarias para tomar medidas frente a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial ataque. Algunos ejemplos de categorías de esta función son: planificación de respuesta, comunicaciones, análisis, mitigación y mejoras.

• Recuperar:
Permite identificar las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado como consecuencia de un incidente de ciberseguridad.

Esta función es compatible con la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad.

1.6. ANÁLISIS Y EVALUACIÓN

La evaluación de riesgos de ciberseguridad no se ajusta a unas únicas directrices o procedimientos estándar. Cada organización enfrenta sus propias amenazas de seguridad de la información porque estas dependen de su contexto.
Por eso, antes de realizar la evaluación de riesgos de ciberseguridad, o de seguridad de la información en general, ISO/IEC 27001 solicita a las organizaciones que definan su contexto tanto interno como externo.

Este proceso permite a una organización identificar los riesgos a los que está expuesta la información que es tratada por medios digitales o informáticos, para evaluarlos, categorizarlos y priorizarlos.

La evaluación de riesgos de ciberseguridad permite optimizar el uso de recursos, emprender proyectos que impliquen tratamiento de datos y de información sobre un marco seguro, generar confianza y credibilidad en inversores, clientes y empleados, entre otras partes representativas.

Inicio Evaluación de riesgos de ciberseguridad: pasos para llevar a cabo la evaluación de riesgos de ciberseguridad no se ajusta a unas únicas directrices o procedimientos estándar. Cada organización enfrenta sus propias amenazas de seguridad de la información porque estas dependen de su contexto.

Realizar evaluaciones de riesgos de ciberseguridad es una tarea desafiante, pero indispensable. Por eso, a continuación, proponemos una guía para hacerlo en cinco pasos, empezando por definir lo que es exactamente una evaluación de riesgos de ciberseguridad.

1.7. EVALUACIÓN DE RIESGOS DE CIBERSEGURIDAD

Antes de iniciar la evaluación de riesgos de ciberseguridad conviene conformar un equipo de trabajo que integren profesionales en el área de TI, gestión de riesgos y seguridad de la información, este equipo debe ser avalado por la Alta Dirección, cuanto más diverso y multidisciplinario resulte el equipo, mejor.

Una vez conformado el equipo, la evaluación de riesgos de ciberseguridad se desarrolla en cinco pasos:

1. Hacer un inventario de los activos de información
2. Identificar y evaluar los riesgos
3. Analizar y priorizar los riesgos
4. Diseñar e implementar controles de seguridad
5. Monitorizar, revisar y corregir

1.8. POLÍTICAS Y PROCEDIMIENTOS

- **Política de Ciberseguridad:**

  Esta política debe ser aprobada por la Dirección de la organización o Junta Directiva y documentar las responsabilidades, procesos, etapas y gestión que se realiza frente al riesgo cibernético, se debe establecer las funciones de la unidad de seguridad de información y los principios y lineamientos.

- **Unidad de gestión de riesgos de seguridad de la información y ciberseguridad:**

  Esta Unidad debe considerar la estructura, el tamaño, el volumen transaccional, el riesgo y los servicios prestados por la entidad, para reportar a la alta dirección la evaluación de la información, la identificación de amenazas y los resultados de los programas de ciberseguridad.

  Debe actualizarse de forma permanente a las nuevas modalidades de ciberataques, capacitar regularmente a los encargados de la organización, monitorear y verificar el cumplimiento de las políticas y procedimientos de ciberseguridad y realizar un análisis de riesgo para determinar si es conveniente contratar un evaluador externo.

- **Sistema de gestión para la ciberseguridad:**

  Este puede tomar como referencia el estándar ISO 27032, NIST con sus publicaciones SP800 y SP1800, CIS Critical Security Controls (CSC) o COBIT 5, y sus respectivas actualizaciones.

Adicionalmente, las entidades deben:

a) Implementar controles para mitigar los riesgos que pudieran afectar la seguridad de la información confidencial, en reposo o en tránsito.

b) Emplear mecanismos para la adecuada autenticación y segregar las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad de la información.

c) Establecer procedimientos para la retención y destrucción final de la información.

d) Definir dentro del ciclo de vida del desarrollo del software, incluyendo servicios web y apps que procesan la información confidencial de la entidad o de los consumidores financieros, aspectos relativos con la seguridad de la información que permitan mitigar dicho riesgo.

e) Incluir en los contratos que se celebren con terceros críticos, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas para la gestión de los riesgos de seguridad de la información y ciberseguridad.

f) Verificar periódicamente el cumplimiento de las obligaciones y medidas establecidas en contratos con terceros.

g) Contar con indicadores para medir la eficacia y eficiencia de la gestión de la seguridad de la información y la ciberseguridad.

h) Gestionar la seguridad de la información y la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.

1.9. PREVENCIÓN

En esta etapa las entidades deben desarrollar e implementar los controles adecuados para velar por la seguridad de la información y la gestión de la ciberseguridad, llevando a cabo las siguientes acciones:

- Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales) y gestión de identidades.

- Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos e información.

- Gestionar y documentar la seguridad de la plataforma tecnológica.

- Garantizar que la unidad de gestión de riesgos de seguridad de la información y ciberseguridad cuente con los recursos necesarios para realizar una adecuada gestión del riesgo cibernético.

- Identificar, y en la medida de lo posible, medir, los riesgos cibernéticos emergentes y establecer controles para su mitigación.

Considerar la conveniencia de contar con un seguro que cubra los costos asociados a ataques cibernéticos y ciberseguridad:

- Considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos.

- Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques cibernéticos.

- Contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad.

- Monitorear diferentes fuentes de información tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la entidad.

- Colaborar con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad.

- Informar a los consumidores financieros de la entidad sobre las medidas de seguridad y recomendaciones que deberán adoptar para su ciberseguridad.

1.10. PROTECCIÓN Y DETECCIÓN

Las entidades deben desarrollar e implementar actividades apropiadas para detectar la ocurrencia de un evento de ciberseguridad y de adoptar medidas para protegerse ante los mismos.

En este sentido, es necesario:

- Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de ciberseguridad que se presenten.
- Gestionar las vulnerabilidades de aquellas plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.
- Realizar un monitoreo continuo a su plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad.

1.11. RESPUESTA Y COMUNICACIÓN

En esta etapa las entidades deben desarrollar e implementar actividades para responder de manera efectiva a los incidentes relacionados con ciberseguridad, para ello deben:

- Establecer procedimientos de respuesta a incidentes cibernéticos.
- Evaluar los elementos de la red para identificar otros dispositivos que pudieran haber resultado afectados.
- Establecer los procedimientos para reportar, cuando se considere pertinente, al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) o quien haga sus veces, directamente o a través de CSIRT sectoriales, los ataques cibernéticos que requieran de su gestión.
- Adoptar los mecanismos necesarios para recuperar los sistemas de información al estado en que se encontraban antes del ataque cibernético.
- Preservar las evidencias digitales para que las áreas de seguridad o las autoridades puedan realizar las investigaciones correspondientes.

VI. MARCO DE EVALUACIÓN

1. SEGURIDAD EN BASE DE DATOS

La seguridad de base de datos se refiere al conjunto de procesos, herramientas, y controles que protegen las bases de datos frente a cualquier tipo de amenaza, ya sea accidental o intencional. El objetivo principal de la seguridad de base de datos es proteger los datos almacenados y mantener la confidencialidad, disponibilidad e integridad de la base de datos. La seguridad de bases de datos trata y protege lo siguiente:

- Los datos de la base de datos
- El sistema de gestión de bases de datos (DBMS)
- Cualquier aplicación asociada
- El servidor de base de datos físico y/o el servidor de base de datos virtual, y el hardware subyacente
- La infraestructura informática y/o de red utilizada para acceder a la base de datos

1.1. TIPOS DE INYECCIÓN SQL

Los atacantes usan varios trucos y tecnologías para ver, manipular, insertar y eliminar datos del base de datos de aplicaciones. Dependiendo de la técnica usada, existen varios tipos de ataques de inyección de SQL. En un ataque de este tipo, los atacantes inyectan código

malicioso a través de una consulta SQL que puede leer información sensitiva o hasta podría manipularla.

Estos son los principales tipos de inyección de SQL:

- **Inyección SQL en banda (In-band SQL Injection):** un atacante usa el mismo canal de comunicación para realizar el ataque y obtener resultados. Este tipo de ataques son frecuentemente usados y fáciles de realizar. El ataque más común de este tipo se llama inyección de SQL basado en error e inyección de SQL UNION.
- **Inyección SQL ciega (Blind SQL Injection):** este ataque no tiene un mensaje desde el sistema con el cual se pueda trabajar, el atacante simplemente envía la consulta SQL maliciosa a la base de datos. Este ataque requiere más tiempo de ejecución porque el resultado retorna generalmente en formato booleano. Se usa los resultados False o True para determinar la estructura de la base de datos y los datos
- **Inyección SQl fuera de banda (Out-of-band SQL Injection):** se utilizan diferentes canales de comunicación (como la funcionalidad de correo electrónico de la base de datos o las funciones de escritura y carga de archivos) para realizar el ataque y obtener los resultados. Este tipo de ataque es difícil de realizar porque el atacante necesita comunicarse con el servidor y determinar las características del servidor de base de datos utilizado por la aplicación web.

Se puede tomar como referencia el **ANEXO A** que corresponde a listado de elementos para realizar la evaluación de la seguridad de los motores de base de datos

1.2. SEGURIDAD EN REDES Y TELECOMUNICACIONES

Las redes y telecomunicaciones son la columna vertebral de la tecnología moderna. Permiten la comunicación, el acceso a información y el intercambio de datos en tiempo real. Sin embargo, también son un objetivo primario de los ciberataques. Por lo tanto, evaluar la ciberseguridad en las redes y telecomunicaciones es esencial para garantizar la protección de los datos y la privacidad de los usuarios.

- **Identificación de activos críticos:** es necesario identificar los activos críticos, como los servidores, routers, switches y aplicaciones. Además, se deben conocer las

interdependencias entre estos activos y cómo se utilizan para mantener la integridad y confidencialidad de los datos.

- **Evaluación de las políticas de seguridad:** es necesario evaluar las políticas de seguridad en las redes y telecomunicaciones, como las políticas de contraseñas, autenticación, encriptación y control de acceso. También se deben revisar las políticas de gestión de parches y actualizaciones de software.
- **Análisis de vulnerabilidades:** se debe realizar un análisis de vulnerabilidades para identificar posibles vulnerabilidades en las redes y telecomunicaciones. También es importante realizar una evaluación de riesgos para identificar los riesgos asociados con cada vulnerabilidad.
- **Evaluación de las medidas de prevención y detección de intrusiones:** es necesario evaluar las medidas de prevención y detección de intrusiones, como los firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS). También es importante revisar los registros de eventos y las alertas de seguridad.
- **Evaluación de la gestión de incidentes de seguridad:** es necesario evaluar el proceso de gestión de incidentes de seguridad para determinar si se está respondiendo de manera efectiva a los incidentes de seguridad. También es importante realizar simulaciones de incidentes para medir la eficacia de los procesos de respuesta.
- **Evaluación de la seguridad de los dispositivos móviles:** es importante evaluar la seguridad de los dispositivos móviles, como los teléfonos inteligentes y las tabletas, que se utilizan para acceder a las redes y telecomunicaciones. Se deben revisar las políticas de seguridad móvil y las medidas de seguridad implementadas.
- **Evaluación de la seguridad de los proveedores:** es necesario evaluar la seguridad de los proveedores de servicios y de los proveedores de equipos de red y telecomunicaciones. Se deben revisar los acuerdos de nivel de servicio (SLA) y las políticas de seguridad implementadas.
- **Evaluación de la formación y concienciación del personal:** es importante evaluar la formación y concienciación del personal sobre la seguridad en las redes y telecomunicaciones. Se deben revisar las políticas de formación y concienciación y medir su eficacia.
- **Evaluación de la continuidad del negocio y la recuperación ante desastres:** es necesario evaluar la capacidad de las redes y telecomunicaciones para recuperarse después de un desastre. Se deben revisar los planes de continuidad del negocio y los planes de recuperación ante desastres.

- **Evaluación de la seguridad física:** es importante evaluar la seguridad física de los equipos y dispositivos que se utilizan en las redes y telecomunicaciones. Se deben revisar las políticas de seguridad física y las medidas de protección implementadas, como las cámaras de seguridad y los controles de acceso.
- **Evaluación de la gestión de la identidad y el acceso:** es necesario evaluar la gestión de la identidad y el acceso a los recursos de red y telecomunicaciones. Se deben revisar las políticas de control de acceso y las medidas de autenticación implementadas.
- **Evaluación de la gestión de los registros:** es importante evaluar la gestión de los registros de las redes y telecomunicaciones. Se deben revisar las políticas de registro y las medidas de protección implementadas para asegurar la integridad y confidencialidad de los registros.
- **Evaluación de la gestión de la configuración:** es necesario evaluar la gestión de la configuración de los dispositivos y equipos de las redes y telecomunicaciones. Se deben revisar las políticas de gestión de la configuración y las medidas de protección implementadas.
- **Evaluación de la seguridad de las aplicaciones:** es importante evaluar la seguridad de las aplicaciones que se utilizan en las redes y telecomunicaciones. Se deben revisar las políticas de seguridad de las aplicaciones y las medidas de protección implementadas, como la validación de entrada y la gestión de errores.
- **Evaluación de la seguridad en la nube:** es necesario evaluar la seguridad en la nube de los servicios y recursos que se utilizan en las redes y telecomunicaciones. Se deben revisar las políticas de seguridad en la nube y las medidas de protección implementadas.
- **Evaluación de la privacidad de los datos:** es importante evaluar la privacidad de los datos que se transmiten y almacenan en las redes y telecomunicaciones. Se deben revisar las políticas de privacidad de los datos y las medidas de protección implementadas, como la encriptación y la anonimización.
- **Evaluación de la gestión de la red:** es necesario evaluar la gestión de la red para garantizar la disponibilidad y el rendimiento de los servicios y recursos de la red y telecomunicaciones. Se deben revisar las políticas de gestión de la red y las medidas de protección implementadas.
- **Evaluación de la gestión de la capacidad:** es importante evaluar la gestión de la capacidad de las redes y telecomunicaciones para garantizar que se pueda satisfacer la demanda de los usuarios. Se deben revisar las políticas de gestión de la capacidad y las medidas de protección implementadas.

- **Evaluación de la gestión de cambios:** es necesario evaluar la gestión de cambios de los equipos y dispositivos de las redes y telecomunicaciones. Se deben revisar las políticas de gestión de cambios y las medidas de protección implementadas para garantizar que los cambios se realicen de manera segura y controlada.
- **Evaluación de la gestión de los proveedores de servicios de red:** es importante evaluar la gestión de los proveedores de servicios de red para garantizar que se cumplan los requisitos de seguridad y privacidad. Se deben revisar las políticas de gestión de los proveedores de servicios de red y las medidas de protección implementadas.

Se puede tomar como referencia el **ANEXO B** que corresponde a listado de elementos listado para realizar la evaluación de la seguridad de Red y Telecomunicaciones

1.3. USUARIOS

Con la creciente cantidad de amenazas cibernéticas y la creciente cantidad de datos personales que se almacenan en línea, es vital que los usuarios comprendan los riesgos y tomen medidas para protegerse. Se proporcionará una visión general de los principales riesgos de seguridad para los usuarios y las medidas que pueden tomar para reducir estos riesgos.

Riesgos de seguridad comunes para los usuarios:

- Contraseñas débiles: Las contraseñas débiles son una de las principales vulnerabilidades de seguridad para los usuarios. Las contraseñas comunes y fáciles de adivinar pueden ser descifradas por hackers en segundos.
- Phishing: El phishing es una técnica común utilizada por los ciberdelincuentes para obtener información confidencial de los usuarios. Los ataques de phishing se realizan a menudo a través de correos electrónicos falsos que parecen legítimos.
- Malware: el malware, como los virus y los troyanos, puede infectar un dispositivo sin que el usuario lo sepa. Una vez infectado, el malware puede robar información personal, destruir archivos y dañar el dispositivo.
- Redes Wi-Fi públicas: las redes Wi-Fi públicas pueden ser muy convenientes, pero también pueden ser peligrosas. Los ciberdelincuentes pueden interceptar el tráfico de datos y robar información confidencial de los usuarios.
- Ingeniería social: la ingeniería social es una técnica utilizada por los ciberdelincuentes para engañar a los usuarios y obtener información confidencial. Esta técnica puede involucrar llamadas telefónicas falsas, correos electrónicos falsos y mensajes de texto.

Medidas de seguridad para los usuarios:

- Contraseñas seguras: es importante crear contraseñas fuertes que incluyen letras, números y caracteres especiales. Las contraseñas deben ser diferentes para cada cuenta y deben cambiarse regularmente.
- Verificación de correo electrónico: antes de hacer clic en un enlace en un correo electrónico, asegúrese de que el remitente sea legítimo y que el correo electrónico no sea sospechoso.
- Actualizaciones de software: es importante mantener el software actualizado para evitar vulnerabilidades de seguridad. Las actualizaciones de software a menudo incluyen correcciones de seguridad que protegen al usuario de las últimas amenazas cibernéticas.
- Redes Wi-Fi seguras: cuando se utiliza una red Wi-Fi pública, es importante utilizar una conexión segura. Una VPN (Red privada virtual) puede proporcionar una conexión cifrada que protege la información del usuario.
- Sensibilización sobre la ingeniería social: los usuarios deben estar al tanto de la ingeniería social y estar alerta a las llamadas telefónicas falsas, correos electrónicos falsos y mensajes de texto que solicitan información confidencial.

Se puede tomar como referencia el **ANEXO C** que corresponde al listado de elementos listado para realizar la evaluación de la seguridad de los usuarios en las aplicaciones.

1.4. CUMPLIMIENTO

La norma ISO 27001 es una norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) efectivo. La norma se basa en un enfoque de gestión de riesgos para identificar, evaluar y gestionar los riesgos de seguridad de la información de una organización. El cumplimiento de la norma ISO 27001 puede ayudar a una organización a proteger su información confidencial y cumplir con los requisitos legales y normativos.

El cumplimiento de la norma ISO 27001 puede proporcionar numerosos beneficios para una organización, incluyendo:

- Mejora de la seguridad de la información: el cumplimiento de la norma ISO 27001 puede ayudar a una organización a identificar y gestionar los riesgos de seguridad de la información de manera efectiva.

- Cumplimiento legal y normativo: el cumplimiento de la norma ISO 27001 puede ayudar a una organización a cumplir con los requisitos legales y normativos relacionados con la seguridad de la información.
- Aumento de la confianza de los clientes: el cumplimiento de la norma ISO 27001 puede mejorar la confianza de los clientes en la capacidad de una organización para proteger su información confidencial.
- Reducción de los costos: el cumplimiento de la norma ISO 27001 puede ayudar a una organización a identificar y gestionar los riesgos de seguridad de la información de manera efectiva, lo que puede reducir los costos relacionados con la violación de la seguridad de la información.

Para lograr la certificación ISO 27001, una organización debe seguir varios pasos clave:

- Establecer un SGSI: la organización debe establecer un SGSI que cumpla con los requisitos de la norma ISO 27001. Esto incluye la identificación de los activos de información, la evaluación de los riesgos de seguridad y la implementación de medidas de seguridad adecuadas.
- Realizar una evaluación interna: la organización debe realizar una evaluación interna para asegurarse de que su SGSI cumple con los requisitos de la norma ISO 27001.
- Obtener una evaluación externa: la organización debe obtener una evaluación externa de un organismo de certificación acreditado para verificar que cumple con los requisitos de la norma ISO 27001.
- Mantener el SGSI: la organización debe mantener y mejorar continuamente su SGSI para garantizar que siga cumpliendo con los requisitos de la norma ISO 27001.

La norma ISO 27001 establece los siguientes requisitos para un SGSI efectivo:

- Política de seguridad de la información: la organización debe establecer y mantener una política de seguridad de la información que refleje sus objetivos de seguridad de la información.

- Gestión de riesgos: la organización debe llevar a cabo una evaluación de riesgos de seguridad de la información y establecer medidas de seguridad para gestionar los riesgos identificados.
- Gestión de activos de información: la organización debe identificar y clasificar sus activos de información y establecer medidas de seguridad para protegerlos.
- Control de acceso: la organización debe establecer medidas de seguridad para controlar el acceso a sus activos de información.
- Criptografía: la organización debe implementar medidas de criptografía para proteger su información confidencial.
- Seguridad física y ambiental: la organización debe establecer medidas de seguridad física y ambiental para proteger sus activos de información.
- Gestión de incidentes de seguridad: la organización debe establecer un proceso de gestión de incidentes de seguridad para detectar, investigar y responder a los incidentes de seguridad de la información.
- Continuidad del negocio: la organización debe establecer medidas de seguridad para garantizar la continuidad del negocio en caso de interrupciones de seguridad.
- Conformidad: la organización debe cumplir con los requisitos legales y normativos relacionados con la seguridad de la información.
- Se puede tomar como ejemplo el siguiente listado para realizar las evaluaciones de la ISO 27001
- Política de seguridad de la información: ¿Se cuenta con una política que defina los objetivos de seguridad de la información y las responsabilidades para su implementación?
- Análisis de riesgos: ¿Se ha realizado una evaluación de riesgos para identificar los activos de información, las amenazas y las vulnerabilidades?
- Plan de tratamiento de riesgos: ¿Se ha desarrollado un plan de tratamiento de riesgos que incluya la implementación de controles para reducir o eliminar los riesgos?
- Asignación de roles y responsabilidades: ¿Están claramente definidos los roles y responsabilidades del personal involucrado en la seguridad de la información?
- Control de acceso: ¿Se han establecido políticas y procedimientos para controlar el acceso a los recursos de información?
- Gestión de activos de información: ¿Se han identificado los activos de información y se han establecido controles para su protección?
- Seguridad física y ambiental: ¿Se han implementado medidas para garantizar la seguridad física y ambiental de los activos de información?

- Gestión de la comunicación y operación: ¿Se han establecido controles para garantizar la integridad, confidencialidad y disponibilidad de la información en los procesos de comunicación y operación?
- Adquisición, desarrollo y mantenimiento de sistemas de información: ¿Se han establecido políticas y procedimientos para garantizar la seguridad de la información en los sistemas de información adquiridos, desarrollados y mantenidos?
- Gestión de incidentes de seguridad de la información: ¿Se han establecido procedimientos para la detección, registro, análisis y gestión de incidentes de seguridad de la información?
- Gestión de la continuidad del negocio: ¿Se han establecido medidas para garantizar la continuidad del negocio en caso de interrupciones en la operación?
- Conformidad legal: ¿Se han establecido controles para garantizar el cumplimiento de los requisitos legales y contractuales relacionados con la seguridad de la información?
- Evaluación de la seguridad de la información: ¿Se han establecido procedimientos para la revisión y evaluación periódica de la eficacia de los controles de seguridad de la información?
- Mejora continua: ¿Se han establecido mecanismos para la mejora continua de la gestión de la seguridad de la información?

1.5. SEGURIDAD EN DIRECTORIO ACTIVO

El Directorio Activo de Windows (AD) es una base de datos que contiene información sobre los recursos y los usuarios de una red. Es esencial para el funcionamiento de la mayoría de las redes empresariales y gubernamentales. La evaluación de la ciberseguridad en el Directorio Activo es importante para garantizar que los datos estén protegidos y que la información no sea accesible para usuarios no autorizados.

Evaluación de la seguridad del Directorio Activo

La evaluación de la seguridad del Directorio Activo debe ser una tarea constante y periódica. La evaluación puede comenzar con una revisión de los permisos y la seguridad de la cuenta. Esto incluye la revisión de las políticas de contraseñas, el bloqueo de cuentas y la autenticación. La autenticación debe ser fuerte y segura, con una longitud mínima de contraseña y una política de bloqueo después de varios intentos de inicio de sesión fallidos.

También se debe revisar la estructura de la unidad organizativa y los permisos de los grupos. Se debe asegurar que los grupos no tengan permisos excesivos y que los usuarios no tengan acceso a recursos que no necesitan. La revisión también debe incluir la eliminación de cuentas inactivas y la revisión de las políticas de retención de contraseñas.

Otro aspecto importante de la evaluación de la seguridad del Directorio Activo es la revisión de los registros de eventos. Los registros de eventos deben ser revisados para detectar cualquier actividad sospechosa o inusual. Se deben monitorear los eventos de inicio de sesión, cambio de contraseña y creación de cuentas nuevas. También se deben monitorear los eventos relacionados con el acceso no autorizado a recursos y la eliminación de cuentas.

Se debe asegurar que las políticas de seguridad del sistema operativo se hayan aplicado correctamente en los controladores de dominio. Esto incluye la revisión de los permisos y los derechos del usuario en los controladores de dominio. Los controladores de dominio deben ser monitoreados para detectar cualquier actividad sospechosa o inusual.

La siguiente lista de verificación se puede utilizar como ejemplo para evaluar la ciberseguridad del Directorio Activo de Windows:

Se puede tomar como ejemplo el siguiente listado para evaluar la seguridad del Directorio Activo de Windows

- Revisar la política de contraseñas: la política de contraseñas debe ser lo suficientemente fuerte para evitar contraseñas fáciles de adivinar. Se debe revisar la longitud mínima de la contraseña y la política de bloqueo después de varios intentos fallidos de inicio de sesión.
- Revisar los permisos de los grupos: se debe revisar la estructura de la unidad organizativa y los permisos de los grupos. Los grupos no deben tener permisos excesivos y los usuarios no deben tener acceso a recursos que no necesiten.
- Revisar la autenticación: La autenticación debe ser fuerte y segura. se deben desactivar los protocolos de autenticación obsoletos y se deben implementar métodos de autenticación de dos factores.
- Revisar los registros de eventos: los registros de eventos deben ser revisados para detectar cualquier actividad sospechosa o inusual. Se deben monitorear los eventos de inicio de sesión, cambio de contraseña y creación de cuentas nuevas. También se deben monitorear los eventos relacionados con el acceso no autorizado a recursos y la eliminación de cuentas.

- Revisar las políticas de retención de contraseñas: se deben revisar las políticas de retención de contraseñas para garantizar que los usuarios cambien sus contraseñas periódicamente.
- Revisar la eliminación de cuentas inactivas: las cuentas inactivas deben eliminarse para reducir el riesgo de que se utilicen cuentas no autorizadas.
- Revisar la seguridad del sistema operativo en los controladores de dominio: se debe revisar que las políticas de seguridad del sistema operativo se hayan aplicado correctamente en los controladores de dominio. Los controladores de dominio deben ser monitoreados para detectar cualquier actividad sospechosa o inusual.
- Revisar los permisos y los derechos del usuario: se deben revisar los permisos y los derechos del usuario en los controladores de dominio.
- Revisar la política de bloqueo de cuentas: se debe revisar la política de bloqueo de cuentas para garantizar que se bloqueen las cuentas después de un número determinado de intentos de inicio de sesión fallidos.
- Revisar la política de contraseñas para cuentas de servicio: las cuentas de servicio deben tener contraseñas fuertes y se debe revisar la política de contraseñas para garantizar que se cumpla con las normas de seguridad.
- Revisar la autenticación de red: la autenticación de red debe ser segura y se deben desactivar los protocolos de autenticación obsoletos.
- Revisar las directivas de seguridad del sistema operativo: las directivas de seguridad del sistema operativo deben ser revisadas para garantizar que se hayan aplicado correctamente y que no haya brechas de seguridad.
- Revisar las políticas de acceso remoto: las políticas de acceso remoto deben ser revisadas para garantizar que sean seguras y que solo se permita el acceso a los usuarios autorizados.
- Revisar las políticas de evaluación: las políticas de evaluación deben ser revisadas para garantizar que se estén registrando los eventos importantes de seguridad.
- Revisar las políticas de grupo de seguridad
- Revisar la integridad del Directorio Activo: se deben revisar regularmente la integridad del Directorio Activo para detectar posibles errores de configuración o problemas de seguridad.
- Revisar las directivas de encriptación: las directivas de encriptación deben ser revisadas para garantizar que se estén utilizando protocolos de encriptación fuertes y actualizados.
- Revisar la configuración de permisos de los objetos: se debe revisar la configuración de permisos de los objetos para garantizar que los usuarios solo tengan acceso a los objetos que necesitan.

- Revisar las políticas de parches y actualizaciones: las políticas de parches y actualizaciones deben ser revisadas para garantizar que se estén aplicando regularmente las actualizaciones de seguridad y los parches críticos.
- Revisar la configuración de firewall: la configuración de firewall debe ser revisada para garantizar que se estén bloqueando las conexiones no autorizadas y se están permitiendo solo las conexiones necesarias

1.6. RESPUESTAS A INCIDENTES

- Revisión de la política de respuesta a incidentes:

El primer paso en la evaluación de un proceso de respuesta a incidentes es la revisión de la política de respuesta a incidentes de la organización. Se deben evaluar las políticas y procedimientos de respuesta a incidentes para asegurarse de que estén documentados y actualizados de acuerdo con las mejores prácticas de la industria. La política de respuesta a incidentes debe cubrir aspectos como la clasificación de incidentes, los roles y responsabilidades de los equipos de respuesta a incidentes, la notificación y comunicación de incidentes y la gestión de incidentes de seguridad.

- Evaluación de la preparación del personal:

Es importante evaluar la preparación del personal para responder a incidentes de seguridad. El personal debe estar capacitado y preparado para identificar, notificar y documentar incidentes de seguridad de manera efectiva. Además, se deben realizar simulaciones y ejercicios regulares de respuesta a incidentes para evaluar la preparación del personal para enfrentar situaciones de crisis.

- Evaluación de la detección y análisis de incidentes:

Es importante evaluar la capacidad de la organización para detectar e identificar incidentes de seguridad. La organización debe contar con herramientas y tecnologías de detección efectivas y contar con un equipo de analistas de seguridad experimentados para analizar y comprender el alcance de los incidentes de seguridad.

- Evaluación de la respuesta y recuperación de incidentes:

Es importante evaluar la capacidad de la organización para responder y recuperarse de los incidentes de seguridad. La organización debe contar con un plan de respuesta a incidentes sólido que incluya medidas para mitigar el daño y recuperar los sistemas y datos afectados.

- Evaluación de la mejora continua:

La evaluación de la mejora continua es un aspecto crítico de la evaluación de un proceso de respuesta a incidentes. La organización debe llevar a cabo una revisión periódica del proceso de respuesta a incidentes y realizar mejoras continuas para garantizar la efectividad del proceso.

Se puede tomar como referencia el **ANEXO D** que corresponde al listado de elementos listado para realizar la evaluación del proceso de Respuesta a Incidentes.

VII. METODOLOGÍA

1. DETERMINAR DOCUMENTACIÓN REQUERIDA PARA RESPALDAR LOS HALLAZGOS ENCONTRADOS

En este Apartado se dan a conocer las herramientas y funciones principales que se utilizan, el tipo de formato a utilizar para evaluar el nivel de madurez de la seguridad en la organización, donde se analizan las políticas, procedimientos de seguridad definidos y su grado de cumplimiento.

Se necesita registrar formalmente la información que obtuvo al realizar la evaluación de forma ordenada en el desarrollo de su trabajo, que sea útil como evidencia y pruebas de las situaciones relevantes encontradas y reportadas.

El soporte fundamental, aparentemente muy simple en una evaluación, es el registro de la información recopilada en los formatos de trabajo, y estos pueden ser, desde documentos, gráficos, fotos y videos, en los cuales se registran los hechos y acontecimientos. También se utilizan para transcribir y concentrar los resultados de entrevistas, cuestionarios, pruebas, investigaciones observaciones y opiniones del personal auditado.

Son utilizados como memoria para asentar la evaluación de los documentos formales resultados de las pruebas realizadas en cada una de las áreas auditadas, sirven de apoyo al evaluador para emitir una opinión y para evidenciar los hallazgos encontrados en una evaluación.

Objetivos de los formatos de trabajo

- Respaldar la opinión del evaluador en todas las etapas del proceso de evaluación, demostrando que el trabajo fue planeado eficazmente.

- Proporcionar la información básica y fundamental necesaria para facilitar la planeación, organización y desarrollo de las etapas de evaluación

Los formatos de trabajo son documentos que describen detalles clave de la evaluación como el alcance, el cronograma, las áreas, los métodos, los hallazgos, las conclusiones y las recomendaciones

Los formatos de trabajo son el aspecto fundamental para elaborar el informe de evaluación, estos se deben diseñar y formular cuidadosamente para que sirvan de herramienta y soporte en la planeación, organización y coordinación del examen de evaluación y a la vez para que brinde un respaldo al informe.

Los formatos de trabajo se definen así: “comprende el conjunto de cédulas preparadas por el evaluador y/o personal colaborador, con motivo del desarrollo del programa de evaluación para obtener evidencia comprobatoria suficiente y competente, que sirva como base objetiva para emitir una opinión independiente sobre el objeto auditado”. Estas cédulas o formatos son registros que mantiene el evaluador de los procedimientos aplicados, pruebas desarrolladas, información obtenida y conclusiones pertinentes a que se llegó en el trabajo.

Contenido de los formatos de Trabajo

Los formatos de trabajo por su naturaleza y contenido, es el aspecto fundamental para elaborar el informe de evaluación y su uso es confidencial y exclusivo del evaluador debido que este va integrando en estos formatos de trabajo los documentos reservados y exclusivos de la empresa mismos que va recopilando a medida se avanza con la evaluación.

Archivo de formatos de trabajo

Estos pueden variar de acuerdo con las circunstancias y criterio del evaluador y el tipo de evaluación ya que en cada trabajo existen procedimientos, técnicas y métodos de evaluación especiales que forzosamente harán la diferencia en la recolección de evidencia, para una mejor comprensión dividiremos el archivo de formatos de trabajo en:

- **Archivo Permanente**

  Contiene información general que puede ser de utilidad en cualquier etapa, de la evaluación, por ejemplo:

  - El plan de trabajo
  - Propuesta de servicios
  - Organigrama de la compañía
  - Diccionario de datos, programas y menús
  - Diagramas de flujo, de programación y de desarrollo de sistemas
  - Descripción y evaluación de procedimientos
  - Carta de recomendaciones
  - Informe

- **Archivo Corriente**

  Se elabora para examinar cada fase de la evaluación a realizar constituyéndose en evidencia del trabajo desarrollado, mostrando todas sus fases y sirviendo como respaldo para presentar el informe respectivo, el archivo contiene:

  - Programa de trabajo
  - Analítica
  - Sumarias
  - Pruebas sustantivas
  - Hojas de trabajo para aplicaciones en funcionamiento
  - Hoja de aplicaciones para aplicaciones en desarrollo

2. DISEÑO DE LOS FORMATOS DE TRABAJO

Los formatos de trabajo deben estar identificados correctamente en la parte frontal de cada archivo de formatos de trabajo de evaluación y el primer documento formal que se identifica es la carátula que sirve para identificar la documentación contenida y debe contener como mínimo los siguientes datos:

- Empresa responsable de la evaluación
- Identificación del archivo (Archivo Permanente)
- Nombre de la empresa auditada
- Periodo de evaluación
- Responsable de la integración de la documentación

- ❖ Fecha de presentación del informe

- **Nombre de la empresa responsable de llevar a cabo la evaluación de sistemas**
  En esta parte se anota el logo y nombre de la empresa que está a cargo de realizar la evaluación si es externa y si es evaluación interna el nombre del responsable de llevar a cabo dicha evaluación.

- **Identificación el archivo de formatos de trabajo**
  Se identifica como archivo permanente o archivo corriente y sirve para identificar qué se trata de la concentración de los documentos que avalan la realización de la evaluación en sistemas

- **Nombre de la empresa o área de sistema auditada**
  Se anota el nombre completo de la empresa auditada, junto con el nombre del área de sistemas en donde se lleva a cabo la evaluación

- **Periodo en que se realizó la evaluación**
  Se anota la fecha de inicio de la evaluación y la fecha de finalización

- **Puesto y cargo del responsable de realizar la evaluación**
  Se anota el nombre completo del encargado o responsable de la evaluación. En caso de ser un grupo se anotan a todos los participantes, pero se debe destacar al responsable de la evaluación.

- **Fecha de presentación del informe**
  Es la fecha en la que se presenta por escrito el informe final de evaluación a la dirección de la empresa.

La importancia de este punto es que sirve para identificar a quién pertenecen los formatos de trabajo, el periodo en que se realizó la evaluación y quien fue el responsable de llevarla a cabo.

Los formatos de Trabajo: Deben ser sencillos, completos, legibles y ordenados fáciles de aplicar, no se deben prestar para ambigüedades y deben contener:

- ❖ Nombre y logo de la empresa auditada
- ❖ Nombre de la empresa evaluadora o responsable de la evaluación
- ❖ Nombre de la persona entrevistada
- ❖ Persona que diligencia el papel de trabajo
- ❖ Fecha del papel de trabajo

[LOGO]

Empresa XXX
Auditoría XXX

Fecha:

COD	PAPEL DE TRABAJO	VER.
AI-PT-SV		1.0

AUDITORIA	PROGRAMA DE SEGURIDAD INFORMATICA		
PROCESO AUDITADO	Riesgos de perdida de información y datos.		
RESPONSABLE			
DOCUMENTOS DE REFERENCIA			
DOMINIO	COBIT	PROCESO	Gestión de Seguridad

RIESGO: Bajo
Probabilidad de ocurrencia: Bajo
Impacto: Bajo

DESCRIPCIÓN

2.1. CONTENIDO DE LOS FORMATOS DE TRABAJO

El plan de trabajo o planeación

Este documento contiene el desarrollo del trabajo de evaluación, definiendo las pautas a seguir para lograr su desarrollo, paso a paso y determinar el tiempo que se invertirá en el encargo, cuando se tratan de evaluaciones de sistemas externas, son la base para determinar el costo económico de esta evaluación y está fase está integrada de la siguiente manera:

- **Fase de planeación:**

- ❖ Conocimiento de la empresa
- ❖ Se deben realizar visitas a la empresa para conocer a detalle, se elaboran cuestionarios, se realizan requerimientos de políticas, reglamentos, manuales y se realizan entrevistas.
- ❖ Objetivos de la empresa
- ❖ Enfoque de la evaluación
- ❖ Fechas claves
- ❖ Cronograma de actividades
- ❖ Presupuesto de horas y costo

Es necesario recordar que el proceso de planeación es continuo y se debe realizar durante el desarrollo de la evaluación de forma permanente.

- **Fase de ejecución**

Esta fase se realiza el análisis, de las áreas que serán auditadas, se verifica cada una de ellas y se obtienen la evidencia necesaria por cada una de las áreas auditadas o que según la planificación se determinó auditar

Ejecución

- ❖ Programa de evaluación
  En este programa se detallan cómo se realizará la revisión, evaluación y control de seguridad, se detalla además el examen que se efectuará a cada una de las áreas críticas encontradas.
- ❖ Procedimientos y técnicas
  Este procedimiento y las técnicas se establecerán de acuerdo con las áreas críticas encontradas y se hará un examen exhaustivo de cada una de ellas

- **Fase evidencia de evaluación**

La evidencia de evaluación o pruebas de cumplimiento, la conforman todos los documentos que soportan la información obtenida en el proceso de evaluación y en cada una de las áreas analizadas, y estas pueden ser grabaciones, fotos, imágenes, reportes, memorándum, manuales, etc., documentos que soporten como se encuentra el área auditada.

Evidencia de Evaluación

- ❖ Formatos de trabajo
  Los formatos de trabajo son todos los documentos que representa la evidencia de evaluación y el soporte de los análisis realizados a cada una de las áreas que han sido

revisadas y van desde cuestionarios, elaborados por el evaluador, evaluaciones de seguridad y documentos de la empresa que sirven para respaldar los hallazgos encontrados en cada una de las áreas auditadas.

- ❖ Conclusiones

  Con la cédula de hallazgos encontrados, se elabora una carta de recomendaciones informando por orden de importancia del más importantes al menos importantes, detallando la condición encontrada, el riesgo encontrado, detallando si, se está transgrediendo alguna normativa legal o existe algún castigo o sanción y la recomendación para subsanar, y se presenta a la dirección de la compañía con copia al encargado del área

- **Fase de recomendaciones**

La carta de recomendación es el pre cierre de la evaluación, y se solicita sea respondida por escrito para dejar evidencia de sus respuestas y si es necesario se programa una reunión con todas las partes involucradas incluyendo la dirección de la empresa

Recomendaciones

- ❖ Recomendaciones para la dirección de la empresa
- ❖ La carta de recomendación es el documento de carácter formal en el cual se presenta los incumplimientos encontrados y una vez se entregue a la alta dirección y los encargados de las áreas auditadas es necesario discutir con ellos cada uno de los puntos encontrados, si en algún punto difieren de lo encontrado es necesario conocer el punto de vista de la parte auditada y explicar la base técnica y la normativa aplicada del porque se está calificando como incumplimiento así mismo si pueden demostrar que están en lo correcto el punto se puede retirar de la carta de recomendaciones y no llega a mencionarse en el informe.

- **Informe de evaluación**

  El informe de evaluación es la conclusión de todo el trabajo y es donde se plasma la opinión del profesional y es un documento formal.

A continuación, las actividades que se desarrollan en cada una de las fases de la evaluación de sistemas:

Fases y Actividades de una evaluación de sistemas

FASES O ETAPAS	ACTIVIDADES PARA DESARROLLAR
Fase de Conocimiento	1. Realizar visitas a la empresa u organización. 2. Realizar observaciones de cada uno de los procesos que se lleva a cabo. 3. Establecer los recursos de TI involucrados en el manejo de la información. 4. Determinar las entradas y salidas de la información. 5. Revisar la documentación existente. 6. Identificar las vulnerabilidades y amenazas a que está expuesta la organización. 7. Identificar los riesgos iniciales. 8. Hacer el análisis y evaluación de riesgos preliminar
Fase de Planeación de la Evaluación	1. identificar el origen de la evaluación. 2. Determinar el estándar que será aplicado para la evaluación. 3. Elaborar plan de evaluación: establecer los objetivos, alcances, metodología, recursos y cronograma de actividades de la evaluación. 4. Elaborar el programa de evaluación: grupo evaluador, definir responsabilidades y actividades a desarrollar. 5. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la evaluación. 6. Diseñar los formatos de trabajo: entrevistas, listas de chequeo, cuestionarios, otros. 7. Elaborar el plan de pruebas de análisis y ejecución
Fase de Ejecución de la Evaluación	1. Realizar las acciones programadas para la evaluación. 2. Aplicar los instrumentos diseñados para la evaluación. 3. Aplicar las pruebas diseñadas. 4. Aplicar el proceso de análisis y evaluación de riesgos aplicando una metodología. 5. Elaborar la matriz de riesgos. 6. Identificar los controles definidos para cada dominio y proceso. 7. Elaborar los formatos de hallazgos: identificar procesos, describir riesgos, identificar las causas, identificar los recursos afectados, identificar posibles soluciones en el contexto.
Fase de Resultados de la Evaluación	1. Definir tratamiento de los riesgos. 2. Determinar los controles y tipos de control: preventivos, correctivos, recuperación. 3. Elaborar el Dictamen de la evaluación para cada dominio y procesos evaluado

	4. Elaborar el informe preliminar y presentarlo a discusión. 5. Elaborar el informe final de evaluación. 6. Integrar el legajo de formatos de trabajo de la evaluación. 7. Presentar el informe final de Evaluación y documentación

2.2. PROPIEDAD DE LOS FORMATOS DE TRABAJO

Los formatos de trabajo son propiedad del evaluador y deben ser conservados por un periodo no inferior a 5 años, la información que allí se consigna es considerada confidencial y se debe garantizar su integridad, y no se puede dar a conocer a terceros salvo por disposición legal. Y se pueden poner a disposición del cliente según el criterio del evaluador.

Se realiza un programa para evaluar cada una de las áreas a ser auditada y que componentes de ella serán revisados, y las herramientas que se utilizarán para ello, dejando constancia de cada uno de los procesos realizados como evidencia de papel de trabajo.

Se realiza un programa para evaluar cual de los riesgos es el que necesita prioridad, se hacen una lista de riesgos y se revisa con el administrador de los sistemas y se define cuál es el más importante para ellos en nivel de prioridad.

Documentos Adjuntos
Los documentos adjuntos son todos los anexos necesarios para documentar, los cuales se encuentran en **Anexo E**.

VIII. REVISIÓN DE RESULTADOS FINAL

1. RESULTADOS DE LA EVALUACIÓN

El objetivo de la evaluación es ayudar a la organización en el desarrollo de una estrategia para la gestión de la ciberseguridad.

Se realiza un resumen de las recomendaciones realizadas durante la evaluación de ciberseguridad y las recomendaciones se pueden categorizar como no técnicas y técnicas y físicas, también se agrega en **Anexo F** un formato de carta de recomendación formal:

1.1. Recomendaciones de gobernanza

Asignar la rendición de cuentas y la responsabilidad de la seguridad a un individuo.

1.2. Recomendaciones de activos

Crear un registro de activos con secciones para hardware, software, datos, personas, procesos, bienes intangibles y terceros.

Implementar una política de clasificación y etiquetado de la información.

1.3. Recomendaciones para la gestión de riesgos

Llevar a cabo una evaluación de riesgos a intervalos regulares, las organizaciones, activos y aplicar los controles aplicados en su caso.

1.4. Recomendaciones de capacitación y concientización

Brindar capacitación sobre seguridad a todo el personal en inducción y comunicar actualizaciones de seguridad en forma regular intervalos

1.5. Recomendaciones sobre políticas y procedimientos

Documentar políticas de seguridad, procedimientos, procesos internos e instrucciones técnicas de trabajo.

1.6. Recomendaciones de seguridad física

Proteja las oficinas desatendidas, las salas de servidores y los archivadores.

Implementar una política de escritorio despejado y pantalla despejada.

1.7. Recomendaciones de gestión de respuesta a incidentes

Documentar un proceso de gestión de respuesta a incidentes.

1.8. Recomendaciones para la Gestión de la Continuidad del Negocio

Probar el plan o los arreglos de continuidad del negocio.

1.9. Recomendaciones de terceros

Llevar a cabo evaluaciones de riesgo de proveedores de terceros.

1.10. Recomendaciones legales, reglamentarias y contractuales

Prepárese para las regulaciones

1.11. Seguridad de la red

Implemente un escaneo y monitoreo regular de vulnerabilidades.

1.12. Acceso de usuario y privilegios de usuario

Documentar una política de control de acceso.

1.13. Almacenamiento de datos

Introducir una política de retención de datos.

Cifrar todos los datos en almacenamiento y tránsito.

Introducir una política de eliminación de datos y dispositivos

1.14. Desarrollo

Evite el uso de datos en vivo para pruebas de desarrollo. Documentar el proceso de desarrollo.

2. INFORME FINAL

Las organizaciones son cada vez más vulnerables a las amenazas debido al aumento de las tecnologías en las organizaciones en general. Las vulnerabilidades de seguridad pueden afectar a las organizaciones y a sus consumidores, en aspecto económico y de imagen.

Por esta razón, se desarrolla una guía cuya metodología está diseñada para que miembros de cualquier empresa que posean un serie de conocimientos que se detallarán más adelante, puedan evaluar de una manera sistemática diversos aspectos de uno o más proveedores de servicios de almacenamiento en la nube, a fin de poder elegir el que más se adecúe a las necesidades de su organización y que cumpla con los requisitos mínimos para asegurar la integridad, confidencialidad y disponibilidad de los datos que se necesitan almacenar en la nube del mismo.

Para este fin, se define una guía de autoevaluación que sirve de ayuda como autodescubrimiento de los factores antes mencionados, a fin de que haya una mejor comprensión del contexto actual de la organización, sus capacidades y necesidades.

También se debe presentar un resumen de los asuntos críticos identificados en la revisión del control interno a la fecha realizado:

- ASUNTOS DE CARÁCTER URGENTE
- ASUNTOS DE CARÁCTER IMPORTANTE
- OTROS ASUNTOS DE CONTROL INTERNO

A continuación, se detalla la serie de aspectos considerados en la guía de autoevaluación, y que se recomienda conocer sobre la empresa objeto de estudio:

Guía de autoevaluación de ciberseguridad

- Madurez de la empresa.
- Rubro/Sector que opera la empresa.
- Tipo de empresa.
- Reglas y lógica del negocio.

- Cantidad y tipo de usuarios que usarán el servicio.
- Valor y tipo de información a migrar.
- Manejo de acuerdos de nivel de servicio con
- proveedores.
- Tipo de almacenamiento que necesita la empresa.
- Presupuesto destinado para invertir en el servicio.
- Leyes y regulaciones que rigen el manejo de los datos de la empresa.
- Necesidades de seguridad, uso, acceso y tratamiento de la información de la empresa.
- Retorno de la inversión en seguridad de la información: tomando en cuenta el presupuesto asignado, el tipo de información a almacenar en la nube y su valor, y las necesidades de seguridad de la empresa se debe calcular el ROSI del proyecto para determinar su viabilidad y defenderlo ante los directivos que lo aprobarán.

Se han establecido criterios clasificados en categorías para detallar los lineamientos de la guía de evaluación dentro de las organizacion, siendo las siguientes:

- Norma generales.
- Norma técnica.
- Norma de seguridad.
- Norma legal.

Para su definición, cada norma se debe detallar utilizando la siguiente estructura:

- Nombre.
- Descripción de la norma.
- Ponderación de la norma.
- Obligatoriedad: Describe al usuario cómo identificar si un criterio puede ser considerado obligatorio para efectos de realizar un filtro más detallado de los proveedores que se evaluarán.
- Evaluación: Describe al usuario las técnicas que pueden ser usadas para evaluar los criterios de forma que se tenga una representación cuantitativa de los mismos y poder identificar su posición en la escala de la matriz de evaluación.

IX. CONCLUSIONES

1. CONCLUSIONES

1.1.1. OBTENIDAS DE LA PROBLEMÁTICA

- Con la guía de evaluación de ciberseguridad se observa la necesidad de contar con un diagnóstico de la organización privada para trabajar en las áreas de riesgos más urgentes para asegurar los activos de la organización.

1.1.2. OBTENIDAS DE LOS OBJETIVOS

- Los resultados de la autoevaluación permiten a la organización extraer conclusiones del estado actual con el objetivo de implementar medidas de seguridad ante los riesgos identificados y establecer estrategias de control, considerando la capacitación del personal y así concienciar a la organización.

- La guía de autoevaluación permite visualizar el cumplimiento de las normativas y regulaciones aplicadas en la organización privada.

- Se observa que el resultado de autoevaluar la ciberseguridad en organizaciones privadas identifica principales amenazas y vulnerabilidades brindando recomendaciones en la toma decisiones para fortalecer las políticas, estándares y medidas de seguridad definidas dentro de la organización.

X. BIBLIOGRAFÍA

Messier, R. (2021). *CEH v11 Certified Ethical Hacker Study Guide*. Sybex.

Gibson, D. (2017). *CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide*. Ycda, LLC.

Staff, B. S. I., Institution, B. S., Standardization, I. O. F., & Commission, I. E. (2013). *Information Technology. Security Techniques. Information Security Management Systems. Requirements*.

Alonso Tamayo Álzate. (1998). Sistemas de Información. 03/04/2023, de https://unal.edu.co/. Sitio web: https://repositorio.unal.edu.co/bitstream/handle/unal/60024/lospapaelesdetrabajoenauditoriadesistemas.pdf?sequence=1&isAllowed=y

Francisco Nicolás Javier Solarte Solarte. (2017). Metodología Práctica para Auditoría de Sistemas Aplicando el Estándar de Mejores Prácticas Cobit 4.1. 05/04/2023, de https://revista.jdc.edu.co/. Sitio web: https://revista.jdc.edu.co/index.php/rciyt/article/view/78/76

Carlos Muñoz Razo, Auditoría en sistemas computacionales. México D.C., Editorial Pearson, 2002, p. 818.[6] https://books.google.com.sv/books?id=3hVDQuxTvxwC&pg=PR12&lpg=PR11&ots=3gSjolwVgg&focus=viewport&dq=papeles+de+trabajo+auditoria+de+sistemas&lr=&hl=es#v=onepage&q=papeles%20de%20trabajo%20auditoria%20de%20sistemas&f=false

XI. ANEXOS

1. DETALLE DE ANEXOS

1.1. ANEXO A

Se puede tomar como ejemplo el listado para realizar la evaluación de la seguridad de los motores de base de datos:

1. ¿La base de datos está debidamente instalada, configurada y actualizada?
2. ¿La base de datos está protegida con autenticación y autorización adecuadas?
3. ¿Los usuarios y roles de la base de datos tienen permisos asignados de forma apropiada?
4. ¿Los datos almacenados en la base de datos están encriptados y protegidos contra accesos no autorizados?
5. ¿Las contraseñas de la base de datos son lo suficientemente fuertes y están protegidas mediante una política de contraseñas sólida?
6. ¿La base de datos cuenta con un plan de recuperación ante desastres y se realizan pruebas periódicas de recuperación?
7. ¿La base de datos cuenta con registros de evaluación activados y configurados adecuadamente?
8. ¿Los registros de evaluación se almacenan en un lugar seguro y no son modificados?
9. ¿La base de datos está actualizada con los parches de seguridad más recientes?
10. ¿La base de datos cuenta con un proceso de respaldo y recuperación de datos, y se realizan pruebas periódicas para asegurar su efectividad?
11. ¿Los procesos y servicios de la base de datos se ejecutan con privilegios mínimos necesarios?
12. ¿La configuración de la base de datos cumple con las mejores prácticas de seguridad?
13. ¿La base de datos está protegida contra vulnerabilidades conocidas y desconocidas?
14. ¿La base de datos se encuentra detrás de un firewall y es monitoreada de forma continua?
15. ¿Se han establecido políticas de seguridad para la gestión de la base de datos?
16. ¿La base de datos cumple con las regulaciones y normativas aplicables, como PCI DSS, HIPAA, GDPR, entre otras?
17. ¿Se realiza una revisión regular de los permisos de usuario y se eliminan los usuarios inactivos o no autorizados?

18. ¿La base de datos cuenta con medidas de seguridad adicionales, como monitoreo de actividad de usuario, detección de intrusiones y protección contra malware?
19. ¿Se realizan pruebas regulares de seguridad de la base de datos para identificar posibles vulnerabilidades?
20. ¿La organización tiene un plan de gestión de incidentes de seguridad que incluye la respuesta a posibles incidentes de seguridad relacionados con la base de datos?

1.2. ANEXO B

Se puede tomar como referencia el listado de elementos listado para realizar la evaluación de la seguridad de Red y Telecomunicaciones:

1. ¿Se utilizan contraseñas seguras y se cambian regularmente?
2. ¿Se han implementado políticas de seguridad para la gestión de contraseñas?
3. ¿Se utilizan políticas de bloqueo de cuentas después de varios intentos fallidos de inicio de sesión?
4. ¿Se utiliza la autenticación de dos factores para acceder a los sistemas críticos?
5. ¿Se han implementado políticas de control de acceso para limitar el acceso solo a los usuarios necesarios?
6. ¿Se utilizan firewalls y se han configurado adecuadamente?
7. ¿Se han implementado políticas de detección y prevención de intrusiones?
8. ¿Se utilizan sistemas de detección y prevención de intrusiones para monitorear la red y detectar actividad maliciosa?
9. ¿Se utilizan soluciones de cifrado para proteger la información confidencial que se transmite a través de la red?
10. ¿Se realizan pruebas regulares de vulnerabilidades y se corrigen las brechas encontradas?
11. ¿Se han implementado políticas de gestión de parches para garantizar que los sistemas estén actualizados con las últimas correcciones de seguridad?
12. ¿Se utilizan soluciones de protección contra malware, como antivirus y antimalware?
13. ¿Se utilizan políticas de protección de datos para garantizar que la información confidencial se maneje adecuadamente?
14. ¿Se ha establecido un plan de continuidad del negocio en caso de una interrupción de servicio?
15. ¿Se utilizan soluciones de respaldo y recuperación de desastres para garantizar la disponibilidad de datos importantes?

16. ¿Se han implementado políticas de monitoreo de red para detectar actividad sospechosa?
17. ¿Se han establecido procesos para la gestión de incidentes de seguridad?
18. ¿Se realizan evaluaciones regulares de riesgos y se actualizan los controles de seguridad en consecuencia?
19. ¿Se han implementado políticas de gestión de dispositivos móviles para garantizar que los dispositivos personales no comprometan la seguridad de la red?
20. ¿Se realizan evaluaciones regulares para evaluar la efectividad de las medidas de seguridad implementadas?

1.3. ANEXO C

Se puede tomar como referencia el ANEXO C que corresponde a listado de elementos listado para realizar la evaluación de la seguridad de los usuarios en las aplicaciones:

1. ¿Las contraseñas son lo suficientemente fuertes y se actualizan regularmente?
2. ¿La autenticación multifactor está disponible y se utiliza cuando sea necesario?
3. ¿Se utilizan protocolos de cifrado adecuados para proteger la información del usuario en tránsito?
4. ¿Las sesiones de usuario están controladas adecuadamente para prevenir ataques de sesión?
5. ¿La política de seguridad de contraseñas se comunica adecuadamente a los usuarios?
6. ¿El sistema tiene un mecanismo de bloqueo de cuenta después de varios intentos fallidos de inicio de sesión?
7. ¿Se tienen en cuenta las pautas de seguridad al implementar la recuperación de cuenta?
8. ¿Se tiene un sistema para detectar y alertar sobre actividades sospechosas de los usuarios?
9. ¿Los usuarios pueden ver y editar solo la información necesaria?
10. ¿Los usuarios tienen los permisos apropiados para realizar sus tareas diarias?
11. ¿Se utilizan mecanismos de autenticación adicionales para actividades sensibles?
12. ¿Los usuarios pueden ver y descargar solo los archivos que necesitan?
13. ¿Los usuarios son informados adecuadamente sobre los riesgos de seguridad al compartir información?
14. ¿Los usuarios tienen una forma de informar sobre vulnerabilidades o sospechas de actividad maliciosa?

15. ¿Los archivos y datos de usuario son destruidos adecuadamente al final de su ciclo de vida?
16. ¿Se controla el acceso a los datos de usuario desde dispositivos personales no autorizados?
17. ¿La seguridad de la información se ha integrado en el ciclo de vida del desarrollo de software?
18. ¿Los usuarios reciben formación adecuada sobre la seguridad de la información?
19. ¿Se realizan pruebas regulares de penetración para identificar y solucionar vulnerabilidades?
20. ¿Se lleva a cabo una evaluación de riesgos de seguridad de manera regular y se toman medidas para abordar los riesgos identificados?

1.4. ANEXO D

Se puede tomar como referencia el listado de elementos listado para realizar la evaluación del proceso de Respuesta a Incidentes:

1. ¿Existe una política de respuesta a incidentes escrita y actualizada?
2. ¿La política cubre todos los aspectos importantes de un proceso de respuesta a incidentes?
3. ¿Se ha comunicado la política de respuesta a incidentes a todo el personal relevante?
4. ¿El equipo de respuesta a incidentes está debidamente capacitado y preparado para responder a situaciones de crisis?
5. ¿Se han realizado simulaciones y ejercicios de respuesta a incidentes para evaluar la preparación del personal?
6. ¿La organización tiene un proceso efectivo para detectar y analizar incidentes de seguridad?
7. ¿Se utilizan herramientas y tecnologías efectivas para la detección de incidentes?
8. ¿La organización cuenta con un equipo de analistas de seguridad experimentado para analizar y comprender el alcance de los incidentes de seguridad?
9. ¿La organización tiene un plan de respuesta a incidentes sólidos?
10. ¿El plan de respuesta a incidentes incluye medidas para mitigar el daño y recuperar los sistemas y datos afectados?
11. ¿La organización cuenta con un equipo de respuesta a incidentes dedicado y disponible en todo momento?
12. ¿Se han definido claramente los roles y responsabilidades de los miembros del equipo de respuesta a incidentes?

13. ¿Existe un proceso de notificación y comunicación de incidentes de seguridad?
14. ¿Se realizan revisiones periódicas del proceso de respuesta a incidentes para identificar posibles mejoras?
15. ¿Se documentan y registran todos los incidentes de seguridad?
16. ¿La documentación incluye información detallada sobre el incidente, incluyendo la fecha, hora, duración, tipo de incidente y las acciones tomadas para responder?
17. ¿Se han implementado medidas de seguridad adicionales para prevenir futuros incidentes?
18. ¿Se han implementado medidas para mejorar la eficacia del proceso de respuesta a incidentes?
19. ¿Se han definido métricas y objetivos claros para evaluar la efectividad del proceso de respuesta a incidentes?
20. ¿La organización está en cumplimiento con las regulaciones y normativas aplicables en cuanto a la gestión de incidentes de seguridad?

1.5. ANEXO E

Se puede tomar como referencia el listado de elementos listado para realizar la evaluación del proceso de Respuesta a Incidentes:

Formato de Plan de Evaluación

LOGO	PLAN DE AUDITORIA EN SISTEMAS					
Auditoría No.		Fecha programada				
Información de la empresa a auditar						
Objetivo de la Auditoria				Alcance de auditoría:		
Auditor Líder / Equipo Auditor:				Criterio de auditoría:		
Ubicación /Área	Proceso	Procedimiento	Responsable Procedimiento	Fecha / Hora	Auditor(es)	Criterios a auditar
Riesgos identificados y estrategias para su atención						
Riesgo	Efecto	Causas	(I) Impacto	(P) Probabilidad	Nivel de riesgo (I X P)	Plan de Acción
Leyes reglamentos y otras normas aplicables.						
Tiempo estimado según cronograma de actividades						

Formato de Programa de evaluación de riesgo

PROGRAMA DE AUDITORÍA
EVALUACIÓN DE LOS SISTEMAS DE RIESGO

OBJETIVO

Evaluar la conformación y el cumplimiento de las funciones, para tener el control de la seguridad de la informcion manejada en un sistema.

No.	PROCEDIMIENTO	PROCEDIMIENTO DE AUDITORÍA	CUMPLE		REVISIÓN DETALLADA		
			SI	NO	HECHO POR	Ref. P/T	OBSERVACIONES
1	Planificacion	Planficacion de la Seguridad Informatica					
1.1	Como primer punto seria de indagar con el encargado de TI sobre los siguientes puntos.	De que manera tiene protegidos los sistemas de Seguridad lógicos, Físicos, de usuarios finales, y con la seguridad de Red.	X	X			
1.2	Seguridad Logica	Lógica con Acceso a Sistemas. Indagar si todo el personal de tiene acceso a toda la información de los sistemas de la empresa.					
1.3	Seguridad de Contraseñas	Indagar sobre si el tipo de restricciones de contraseñas lo manejan mayor a una cantidad de caracteres y con un rango menor de caracteres, incluyendo mayúsculas, minúsculas, números, y caracteres.					
1.4	Certificación de Cuentas de Usuario	se Indaga con el encargado de TI, para ver si manejan una cuenta de empresa para manejar solo información confidencial de la empresa y que no haya fuga de información a terceros.					

Formato de programa de Evaluación

[LOGO]

Empresa XXX
Auditoría XXX

Fecha:

COD	PROGRAMA DE AUDITORIA EN SISTEMAS	VER.
AI-PT-SV		1.0

AUDITORIA	En Ciberseguridad		
PROCESO AUDITADO	Riesgos de pérdida de información y datos.		
RESPONSABLE			
DOCUMENTOS DE REFERENCIA			
DOMINIO	COBIT/ISO27001	**PROCESO**	Gestión de Seguridad

RIESGO: Bajo
Probabilidad de ocurrencia: Bajo
Impacto: Bajo

No.	Procedimiento	Referencia P.T.	Hecho Por	Fecha
1	Coteje la última copia de seguridad realizada			

1.6. ANEXO F

Modelo de carta formal de recomendaciones.

San Salvador, xx de mayo de 2023

Señores
Sociedad Anónima, S.A.
Presente

Atención: director o R.L.

Hemos efectuado la revisión de evaluación de ciberseguridad, en el periodo establecido del 01 de mayo al 31 de mayo de dos mil veintitrés a su empresa Sociedad Anónima, S.A., como parte de nuestro examen hemos evaluado el sistema de control interno que posee la empresa en el área informática, a la fecha antes mencionada. Durante el desarrollo de nuestro trabajo hemos considerado ciertas situaciones que consideramos necesario hacerlas de su conocimiento.

Las observaciones y recomendaciones que se adjuntan son el resultado de la evaluación del control interno que posee la sociedad

Esta carta está destinada únicamente para uso de Sociedad Anónima, S.A., y de sus accionistas. Agradecemos la cooperación y disposición mostrada por el personal asignado por la compañía durante el desarrollo de nuestro trabajo. Con gusto ampliaremos el contenido de estas recomendaciones, si así lo estiman conveniente.

Esperamos una respuesta por escrito del compromiso tomado para subsanar las recomendaciones señaladas en la presente

_____

Firma y nombre del Auditor