Enfoque metodológico para la gestión del riesgo asociado con las ciberamenazas

Ronal Enrique Hernández Cogollo

Facultad de Ciencias Económicas, Universidad Militar Nueva Granada

Especialización en Control Interno, II semestre

Iván Cortes Clopatofsky, director

Bogotá D.C. 2021

Nota autor

Este trabajo de investigación formativa fue elaborado de la asignatura de Investigación que hace parte del programa.

Tabla de Contenido

Lista de Ilustraciones

Lista de Tablas

Resumen

Uno de los efectos inmediatos de la pandemia de Covid 19 fue la repentina necesidad de muchas personas, en distintas edades y condición socioeconómica, de tener acceso rápido y seguro a la información y poder continuar ejecutando sus actividades laborales o académicas desde casa, apoyándose en herramientas tecnológicas. En consecuencia, en la medida que aumentó el uso y la disponibilidad de las tecnologías, las personas y las industrias en general, se exponen a mayores riesgos debido a la proliferación de delincuentes que buscan beneficiarse de las debilidades o vulnerabilidades existentes en la tecnología que utilizamos a diario. Es así como los delincuentes del ciberespacio han desarrollado y perfeccionado el secuestro de datos, las metodologías para la ingeniería social, con el objetivo de engañar, extorsionar, estafar a las personas y las organizaciones, para lograr beneficios económicos.

Palabras clave: Cibercriminales, herramientas tecnológicas, debilidades, ciberespacio.

Abstract

One of the immediate effects of the Covid 19 pandemic was the sudden need for many people, at different ages and socioeconomic status, to have quick and secure access to information and to be able to continue executing their work or academic activities from home, relying on technological tools. Consequently, as the use and availability of technologies increased, people and industries in general are exposed to greater risks due to the proliferation of criminals seeking for benefits from existing weaknesses or vulnerabilities in the technology we use daily. This is how cybercriminals have developed perfected data kidnapping, methodologies for social engineering, with the objective of deceiving, extorting and defrauding people and organizations, to achieve economic benefits.

Keywords: Cybercriminals, technological tools, weaknesses, cyberspace.

Introducción

Durante los dos últimos años, la sociedad en general vivió uno de los mayores retos de la última década enfrentándose a una pandemia que obligó a las personas a refugiarse en sus hogares y motivó a las empresas a implementar nuevos mecanismos para continuar produciendo, para ello se apoyó en las herramientas tecnológicas que permiten las conexiones remotas y la interacción simultánea a través de video llamadas.

Lo anterior aceleró el uso masivo de internet conectando los hogares a las empresas y extendiendo la redes corporativas hasta sitios impensados hace unos años atrás. En el ciberespacio las fronteras son imperceptibles y las distancias se hacen insignificantes, acercándonos a través de una pantalla.

En ese mismo sentido se incrementaron los incidentes de seguridad y las actividades delictivas como el secuestro de información, las suplantaciones y las actividades maliciosas en general, se masificaron y se perfeccionaron, al punto de convertirse en una amenaza que hace parte de nuestro día a día, tanto para las organizaciones como para las personas en su entorno familiar o académico.

Para poder enfrentar este tipo de amenazas, es imperativo que las empresas y las personas en general, evalúen su nivel de exposición ante los riesgos asociados con las ciberamenazas y que determinen su potencial afectación ante la materialización de los mismos. Para ello deben aplicar metodologías que consideren en lo posible todas, o por lo menos la mayoría de las causas que podrían originar este riesgo y asimismo, que se identifiquen de manera clara y precisa, los controles que evitan estas causas.

Definición del problema

Las Entidades del Sector Defensa de Colombia están sujetas a diversas normas a nivel nacional que la obligan a implementar controles para mitigar el riesgo de ciberataques, sin embargo, dicho sector no cuenta con una metodología que le permita medir el nivel de riesgo cibernético, identificar los controles necesarios para su mitigación y evaluar la eficacia de estos.

Esta situación involucra una entidad del Sector Defensa Nacional, más específicamente en las áreas encargadas de la administración la ciberseguridad. Se genera por la falta de una metodología específica para la medición de riesgo de ciberataques, se debe a que las múltiples causas que lo pueden generar son de alta complejidad técnica y esto dificulta el diseño de un enfoque semi-cuantitativo que permita la reducción de la subjetividad en la medición tanto del impacto como de la probabilidad de ocurrencia.

El riesgo de tener un ciberataque es permanente para las organizaciones cuyos procesos tanto misionales como administrativos, dependan de la tecnología, como es el caso de la Unidad Administrativa del Sector Defensa Nacional. En otras palabras, los controles para mitigar este riesgo deben operar 24 horas del día durante los 7 días a la semana.

Pregunta de investigación

¿Considerando las posibles causas y los controles que los mitigan, es posible reducir la posibilidad de materialización del riesgo de ciberataques?

Objetivos

Objetivo General

Brindar un enfoque metodológico para la gestión del riesgo de ciberataques y diseñar controles que permitan la mitigación de dicho riesgo en la Entidad.

Objetivos Específicos

Plantear un mecanismo dirigido a medir el riesgo de ciberataques, que permita aplicar las medidas pertinentes para reducir ese riesgo, mitigarlo y llevarlo a márgenes aceptables para la organización, fortaleciendo los mecanismos que permitan alcanzar los objetivos.

Priorizar los controles que eficaces, teniendo en consideración las normativas vigentes, las causas que mitiga, los activos en riesgo y la criticidad de los procesos o servicios que puedan afectar.

Identificar controles a implementar la organización asociados con la ciberseguridad, el propósito de mitigar los riesgos en la medida y características de la Entidad.

Marco teórico

En el marco de este trabajo, se han consultado fuentes externas, como: prácticas comunes en Entidades del Sector, marcos de referencia especializados en el riesgo a evaluar y normatividad vigente aplicable a organización en relación con dicho riesgo.

Análisis Legal

El análisis normativo tiene especial relevancia, considerando que pueden existir requisitos de obligatorio complimiento para los cuales la organización no está preparada, lo que podría generar pérdidas de alto impacto para la organización. A continuación, se detallan algunas de las principales normativas aplicables, que podrían generar riesgos de tecnologías de información:

- Constitución Política de Colombia. El artículo 15 menciona “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos

de datos y en archivos de entidades públicas y privadas". (Colegio de Abogados Rosaristas Edición conmemorativa, 2016).

- Ley 1581 de 2012, Ley de protección de datos personales de Colombia, por la cual se dictan disposiciones generales para la protección de datos personales. (Universidad del Cauca, 2017).
- Ley 1273 de 2009, Ley de delitos informáticos de Colombia, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (Secretaria del Senado, 2009).

Análisis de marcos de referencia

Para este Ensayo se analizaron los principales marcos de referencia utilizados a nivel internacional y que tienen relación con la gestión de riesgos, la seguridad de la información y ciberseguridad. A continuación, se relacionan los marcos de referencia tenidos en cuenta para el presente Ensayo.

Norma ISO 27001

La norma ISO 27001 es considerada como una norma muy relevante en el entorno de la seguridad de la información. Es una norma certificable por las autoridades de acreditación autorizadas a nivel mundial como, por ejemplo: SGS, Icontec y Bureau Veritas. Utilizan como soporte los riesgos que tiene la organización relacionados con los pilares de la seguridad de la información, su objetivo es determinar, implantar, mantener y fortalecer la continuidad de la seguridad de la información. Los requerimientos de controles técnicos de la norma ISO 27001 están contenidos en la norma ISO 27002, la cual usaremos en este trabajo en la fase de

evaluación de riesgo ya que determina un listado de buenas prácticas que contiene un catálogo de objetivos de control y controles que se relacionan con los requisitos de la norma ISO 27001 relacionados con el tratamiento de los riesgos. (International Standart Organizations, 2013).

La norma ISO 27002 consta de 14 capítulos que relacionan las áreas a considerar para proveer la seguridad de la información con un total de 114 controles. A continuación, se resumen los 14 capítulos:

- Políticas de Seguridad de la Información: Es un elemento fundamental de un sistema de gestión de seguridad de la información, la cual debe estar autorizada por la alta dirección, informada a todos los miembros de la entidad, periódicamente revisada y actualizada en concordancia con los cambios que ocurren en la entidad.
- Organización de la Seguridad de la Información: contiene controles para armar un marco eficiente mediante los roles, actividades de aseguramiento, entre otros.
- Seguridad relativa a los recursos humanos: se deben adelantar campañas orientadas a sensibilizar y educar a todo el personal sobre las directrices del manejo adecuado de la información en la ejecución de sus funciones.
- Gestión de activos: resalta la gestión de la información como activo y detalla cómo se deben implementar las salvaguardas para prevenir incidentes cibernéticos que pongan en riesgo su seguridad.
- Control de acceso: explica cómo se deben controlar los accesos a la información y restringirlos para que se dé acceso al personal estrictamente necesario.
- Criptografía: cuando se trata de información sensible o crítica es relevante utilizar técnicas de cifrado con el objetivo de garantizar aspectos como la autenticidad, la confidencialidad e la integridad.

- Seguridad física y del entorno: es relevante contemplar aspectos de protección en el ambiente físico como por ejemplo, implementar mecanismos que permitan asegurar la información disponible en la pantallas, ubicar en sitios seguros las impresoras, controlar el acceso físicos a las áreas que manejan información clasificada, entre otros. Aspectos como los mencionados permiten cerrar las brechas y asegurar el entorno de seguridad.
- Seguridad de las operaciones: posee importantes elementos técnico relacionados con la protección del ante malware, respaldos, control de aplicativos en ambiente productivo, gestión de vulnerabilidad, entre otros.
- Seguridad de las comunicaciones: en la actualidad es un elemento fundamental teniendo en cuenta que el intercambio de información se realiza mediante las redes sociales. Proteger adecuadamente los mecanismos de transmisión de los datos es vital para las personas y las organizaciones.
- Adquisiciones, desarrollo y mantenimiento de los sistemas de información: la gestión de la seguridad debe está presente desde el momento en que los productos o servicios relacionados con la gestión de la información, inicien su evaluación para ser desarrollados internamente o adquiridos mediante proveedores externos.
- Relación de proveedores: en el momento en que se toma la decisión de establecer relacionados con proveedores, se deben determinar lineamiento de seguridad orientados a establecer reglas claras en el manejo de los activos de información.
- Gestión de incidentes de seguridad de la información: los incidentes en seguridad son un componente clave, ya que se debe tener total claridad del tratamiento que se les

aplicará cuando estos se presenten, con el propósito de dar una respuesta eficiente y efectiva, evitando a futuro su repetición.

- Aspectos de seguridad de la información para la gestión de la continuidad de negocio: en ocasiones no tenemos una idea clara del valor de la información hasta cuando se materializan escenarios de perdida parcial o total de la información. La continuidad del negocio nos brinda la oportunidad de reducir la posibilidad y el impacto causados por perdidas de información o disponibilidad de la infraestructura de TI para la ejecución de sus actividades.
- Cumplimiento: es importante conocer la legislación, los lineamientos, las políticas y las normas relacionadas con la seguridad de la información aplicables a las organizaciones. Es importante asegurar el cumplimiento normativo y mantenerse actualizado para evitar, incumplimientos que deriven en demandas, multas o investigaciones de carácter administrativo. (SGSI, 2017).

NIST Cybersecurity Framework

Este marco de referencia del Instituto Nacional de Estándares Norteamericano (NIST), tiene como una de sus finalidades, guiar a las entidades en el entendimiento, la gestión y la reducción de los riesgos relacionados con la ciberseguridad. Está compuesto por un conjunto de actividades y referencias comunes de la infraestructura critica, contribuyendo a la priorización y el logro de los objetivos relacionados con la ciberseguridad.

Es importante tener presente que cada organización es diferente a las demás, por este motivo cada una debe gestionar el riesgo de ciberseguridad de acuerdo con su infraestructura.

A continuación, se anexa una imagen que ilustra las 5 funciones que se encuentran definidas en este framework. (Cybersecurity, 2016).

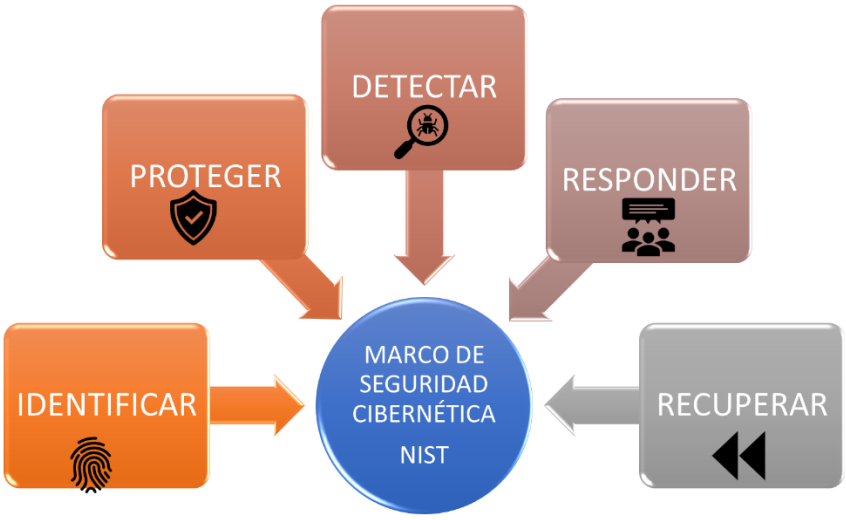

Ilustración 1 Marco de seguridad cibernética NIST

Nota. Tomado del Marco NIST, Elaboración propia.

Niveles de madurez COBIT

El marco de referencia COBIT, se puede definir como un compendio de elementos que le permiten a las organizaciones aumentar el nivel de concordancia entre los requisitos de control, los temas técnicos y los riesgos. Con el fin de gobernar efectivamente TI. Para ello es necesario establecer las actividades y los riesgos que requieren ser gestionados. En COBIT, se encuentra los dominios que se relacionan a continuación:

- Planear y Organizar (PO): brinda una dirección para proporcionar soluciones y la entrega de servicio.
- Adquirir e Implementar (AI): entrega soluciones hasta transformarlas en servicios.
- Entregar y Dar Soporte (DS): a partir de las resultados entrega soluciones a los usuarios finales.

- Monitorear y Evaluar (ME): supervisar que todos los procesos se encuentran en la ruta planeada.

COBIT le brinda a las organizaciones un vocabulario común y las referencias necesarias para la administración de las tecnologías de información, permitiendo establecer mecanismos para su medición y seguimiento del desempeño de cada uno de los procesos, integrando las mejores prácticas internacionales. (IT Governance Institute, 2007).

Para este proyecto se aplicará el objetivo de control correspondiente a entregar y dar soporte, el cual lo componen los siguientes objetivos de control que se detalla a continuación :

- DS5.1 Administración de la Seguridad de TI: gestionar la seguridad de las tecnologías de información desde el más alto nivel.
- DS5.2 Plan de Seguridad de TI: incorpora los riesgos y los requisitos a cumplir por la entidad.
- DS5.3 Administración de Identidad: Proporciona la seguridad necesaria para que los usuarios se identifiquen correctamente.
- DS5.4 Administración de Cuentas del Usuario: brindar el aseguramiento de las altas y bajas de los usuarios en los sistemas de información.
- DS5.5 Pruebas, Vigilancia y Monitoreo de seguridad: asegura que las modificaciones o nuevos desarrollos se realicen apropiadamente.
- DS5.6 Definición de Incidente de Seguridad: gestionar los incidentes y problemas de seguridad de TI que se presenten en la organización.
- DS5.7 Protección de la Tecnología de Seguridad: asegurar que los elementos de protección de la infraestructura de TI son eficaces y eficientes.

- DS5.8 Administración de Llaves Criptográficas: establecer que los mecanismos y procedimientos para el uso de llaves criptográficas estén implementados.
- DS5.9 Prevención, Detección y Corrección de Software Malicioso: contar con medidas que permitan proteger a la organización contra software malicioso.
- DS5.10 Seguridad de la Red: técnicas de seguridad documentados para la administración de equipos utilizados para las comunicaciones.
- DS5.11 Intercambio de Datos Sensitivos: transporte electrónico de datos sensibles con controles para proporcionar su autenticidad, durante el envío, la recepción y el no repudio del origen. (IT Governance Institute, 2007)

Data Management (DAMA)

Desde el marco de referencia Data Management (DAMA), se obtuvo un enfoque de riesgos que está en la Dimensión de Seguridad de la Información de dicho marco de referencia:

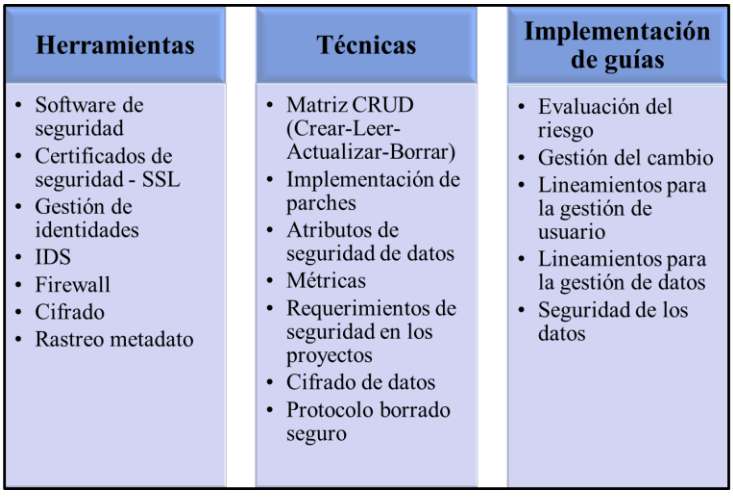

Ilustración 2 Dimensión de seguridad DAMA

Nota. Fuente DAMABOOK. elaboración propia

En la ilustración 2, se observan las diferentes herramientas propuestas en el marco de referencia DAMA, de igual manera se relacionan las técnicas propuestas y las guías de implementación sugeridas en la referencia.

Los elementos descritos en la ilustración 2, serán tenidos en cuenta durante el presente Ensayo. Servirán como insumo al momento de identificar y definir cada uno de los controles que serán utilizados para reducir la posibilidad de ocurrencia y la afectación que estos puedan tener sobre la entidad. (DAMA International, 2010).

Norma ISO 31000

En el presente proyecto se utilizará como base fundamental la norma ISO 31000, que pone a disposición de todas las organizaciones a nivel mundial los lineamientos, principios y directrices para gestionar los riesgos. A continuación, se anexa una imagen que ilustra las etapas presentes en la norma.

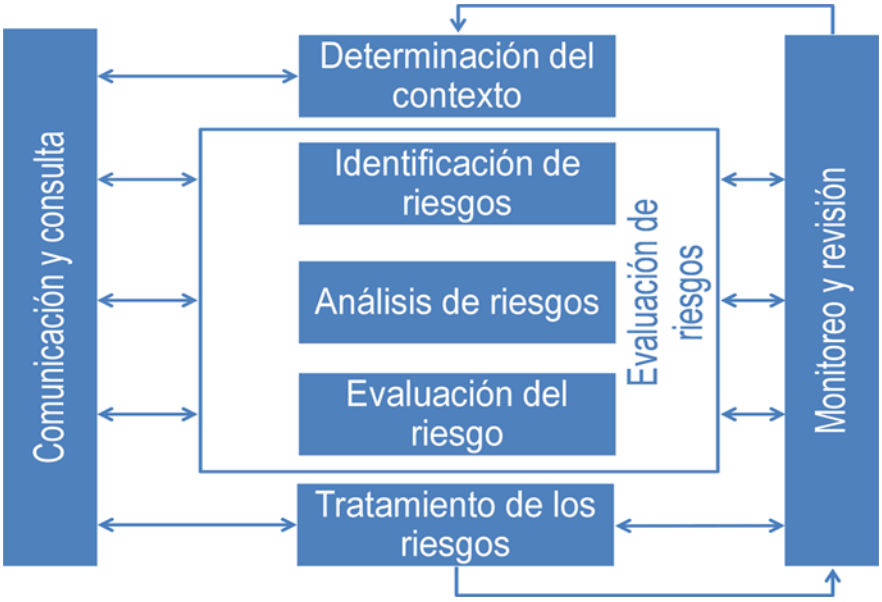

Ilustración 3 Gestión del riesgo de acuerdo con la norma ISO 31000

Nota. Tomado Pagina web OECD. (OECD, s.f.).

Los pasos dispuestos en la norma ISO31000, le permiten a cualquier organización contar con las etapas básicas como se observan en la ilustración 3, brindándoles las pautas generales para operar un sistema de gestión de riesgos.

Teniendo en cuenta lo anterior, para el presente Ensayo se tomará como base las definiciones existentes en la norma ISO 31000.

Contexto, análisis y desarrollo del enfoque metodológico

Este enfoque metodológico tiene como propósito desarrollar una herramienta que le permita a la entidad evaluar su nivel de riesgo inherente de ataques cibernéticos, identificar controles, priorizarlo y realizar el diseño de este, permitiendo reducir el riesgo llevándolo a los niveles aceptables para la entidad.

La organización hace parte del sector público nacional de Colombia y tiene como propósito la formulación, diseño, desarrollo y la ejecución de las políticas relacionadas con la seguridad nacional

Tomando como referencia la norma ISO 31000 y para efecto del presente Ensayo, se plantea el siguiente gráfico que ilustra los elementos que serán definidos como productos del Ensayo.

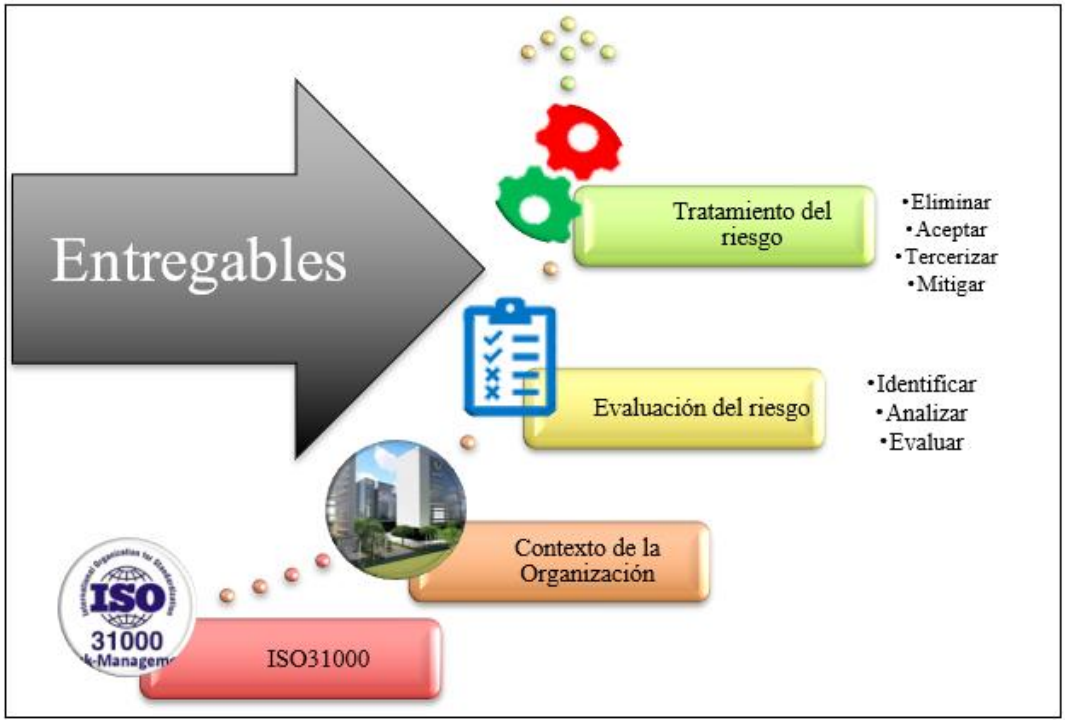

Ilustración 4 Relación ISO 31000 enfoque metodológico propuesto

Nota. Fuente Norma ISO31000. Elaboración propia

Para el presente Ensayo se tomará como punto de partida, la norma ISO31000. Inicialmente se realizará un análisis de contexto, posteriormente se evaluarán los riesgos mediante la identificación, análisis y evaluación de los riesgos.

En la etapa de tratamiento del riesgo, se aplicarán las opciones planteadas en el presente Ensayo, como son eliminar, aceptar, tercerizar o mitigar el riesgo.

Análisis del Contexto

Inicialmente se debe establecer el contexto de la organización. Para el caso de la entidad del orden nacional, cuyo objetivo fundamental es el de ejercer como máxima autoridad en materia de seguridad y entre sus funciones están las de elaborar, desarrollar, controlar y propender por el cumplimiento de los lineamientos nacionales en materia de seguridad.

Posteriormente se debe establecer el contexto del riesgo a evaluar, según la necesidad de la entidad. Para esto se deben consultar fuentes externas, como: prácticas de industria, marcos de referencia especializados en el riesgo a evaluar, normatividad vigente aplicable.

El análisis normativo tiene especial relevancia, considerando que pueden existir requisitos de obligatorio complimiento para los cuales la entidad no está preparada, lo que podría derivar en multas, demandas y afectación a la reputación de la entidad.

Riesgo

La norma ISO 31000 define el riesgo como "El efecto de la incertidumbre sobre los objetivos". (Organización Internacional de Normalización, 2018) . El efecto es la desviación de lo que sucederá y puede ser positivo, negativo o la combinación de los dos aspectos. Los objetivos corresponden a diversos ámbitos como son financieros, seguridad, entre otros. Es común encontrar que los riesgos están caracterizados por la relación que existe entre los eventos, las consecuencias y la posibilidad de ocurrencia. La incertidumbre corresponde al nivel de deficiencia de información asociada con el entendimiento de un evento, la posibilidad de ocurrencia y su impacto.

Control

El estado colombiano viene adelantando un trabajo importante en la generación de lineamientos que tienen como propósito desarrollar adecuadamente la gestión de las tecnologías de la información. Un producto de ese esfuerzo generó entre otros valiosos documentos, la Guía Metodológica de Pruebas de Efectividad donde se define el control como los "Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, practicas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal". (MINTIC, 2016).

Teniendo como marco de referencia la norma ISO 31000 sobre gestión del Riesgo, a continuación, se describe la organización gestiona el riesgo de ciberataque.

Ciberseguridad

El Consejo Nacional de Política Económica y Social CNPES, como máxima autoridad de planeación estableció los lineamientos de política para ciberseguridad y ciberdefensa , es así como define la ciberseguridad "Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.". (Consejo Nacional de Política Económica y Social República de Colombia, 2011).

La seguridad de la información

Define que "Es el conjunto de medidas y técnicas utilizadas para controlar y salvaguardar todos los datos que se manejan dentro de la organización y asegurar que los datos no salgan del sistema que ha establecido la organización." (Isotools Excellence, 2021).

A continuación, se ilustra gráficamente los conceptos relacionados.

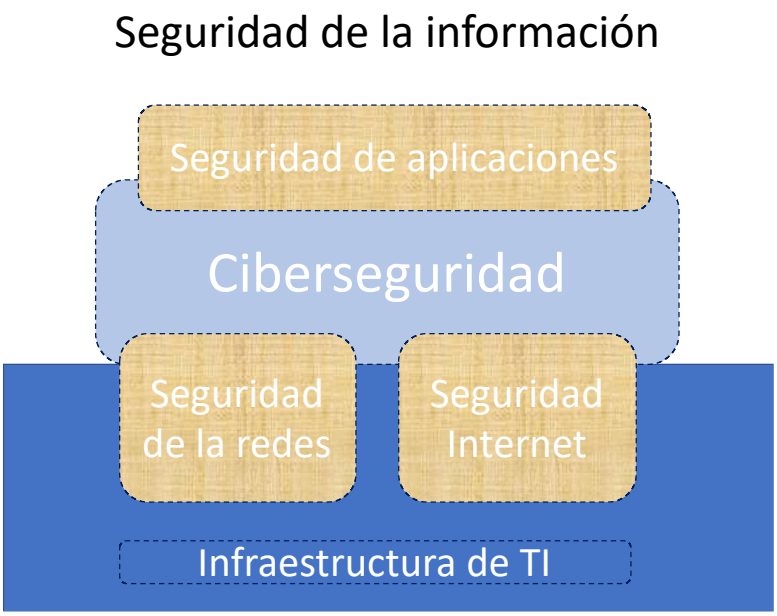

Ilustración 5 Relación seguridad de la información – Ciberseguridad

Nota. Elaboración propia

Identificación del riesgo

La entidad viene gestionando los riesgos de acuerdo con los lineamientos internos, los cuales están referenciados con las guías emitidas por el Departamento Administrativo de la función Pública (DAFP), es así como tiene identificados diez (10) riesgos.

Para el presente proyecto se tomará como muestra para efectos académicos, el riesgo que hace parte de los tecnológicos y que se encuentra definido como: La fuga, manipulación o perdida de la información a través de cualquier medio de ataque cibernético.

Tabla 1

Tipos de riesgos identificados en la entidad

Tipo	Cantidad
Riesgos estratégicos	2
Riesgos operativos	3
Riesgos financieros	3
Riesgos de tecnología	2

Nota. Datos obtenidos de la entidad, elaboración propia

Análisis de riesgos

Para llevar a cabo el análisis se tendrá en cuenta el impacto y la probabilidad de ocurrencia, de acuerdo con los lineamientos actuales utilizados por la entidad, A continuación, se anexa un gráfico que ilustra la posición actual del riesgo mencionado.

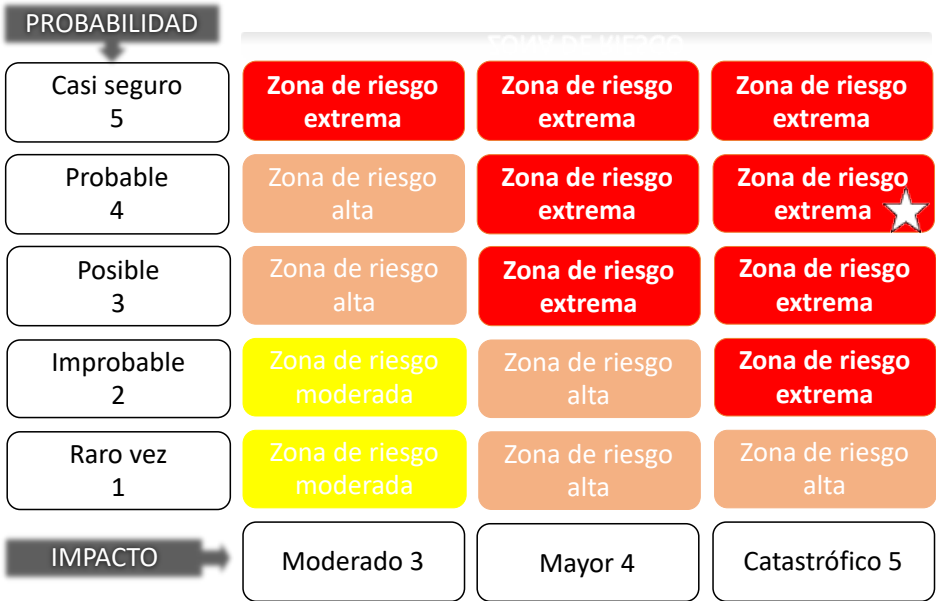

Ilustración 6 Matriz de calor del riesgo

Nota. Tomada de la Entidad. Elaboración propia.

En la ilustración se puede observar que el riesgo de fuga, manipulación o perdida de la información a través de cualquier medio de ataque cibernético. Se encuentra ubicado en la zona de riesgo extremo y la entidad presenta como opciones para su tratamiento evitar, reducir o compartir el riesgo. (Ministerio de Defensa Nacional de Colombia, 2008).

Como alternativa y producto de la evaluación realizada se plantea que para gestionar la probabilidad, se debe ejecutar la siguiente metodología:

Identificación de causas: se obtendrán de las siguientes fuentes:

- Base de datos de eventos materializados en los últimos 3 años
- Eventos materializados en el sector
- Eventos materializados a nivel global

Identificación de controles:

- Requisitos normativos mencionados para este proyecto.
- Marcos de referencia mencionados en el alcance de este trabajo.
- Asesoramiento de proveedor de seguridad de información.

Evaluación de riesgos

Considerando las causas y controles identificados para cada riesgo, según el paso anterior, se debe ejecutar utilizando una matriz que permita comparar los controles y las causas mediante un arreglo multidimensional. Para ello se deben relacionar los controles en las columnas y las causas en la fila superior para la medición de la probabilidad.

RIESGO						
CONTROLES	**DESCRIPCIÓN**	**RESPONSABLE**	**PERIODICIDAD**	**TIPO DE CONTROL**	**CALIFICACIÓN AUT: 75% COM: 50% MAN: 25%**	**CAUSA**

Ilustración 7 Matriz de calificación de controles y causas

Nota. Elaboración propia.

De acuerdo con el control planteado se asocia el marco de referencia abordado con su respectiva descripción, así mismo, se incluye el responsable por parte de la entidad y dependiendo del tipo de control se asocia el valor porcentual asignado, de acuerdo con la tabla 2 que se anexa a continuación.

Los controles deben ser calificados respecto a su nivel de automatización así:

Tabla 2

Valor porcentual por tipo de control

Descripción	Porcentaje
AUTOMÁTICO	75%
COMBINADO	50%
MANUAL	25%

Nota. Elaboración propia

Para la valoración de los controles se plantea una calificación porcentual, como se observa en la tabla 2. Los controles con acciones que se ejecutan manualmente recibirán una calificación de 25%, aquellos que presenten la combinación de acciones manuales y automáticas recibirán una calificación de 50%, aquellos relacionados con acciones automáticas recibirán un mayor valor 75%.

Para el riesgo tomado como ejemplo se observa que el nivel de riesgo inherente se encuentra ubicado como probable y en la zona de impacto catastrófica.

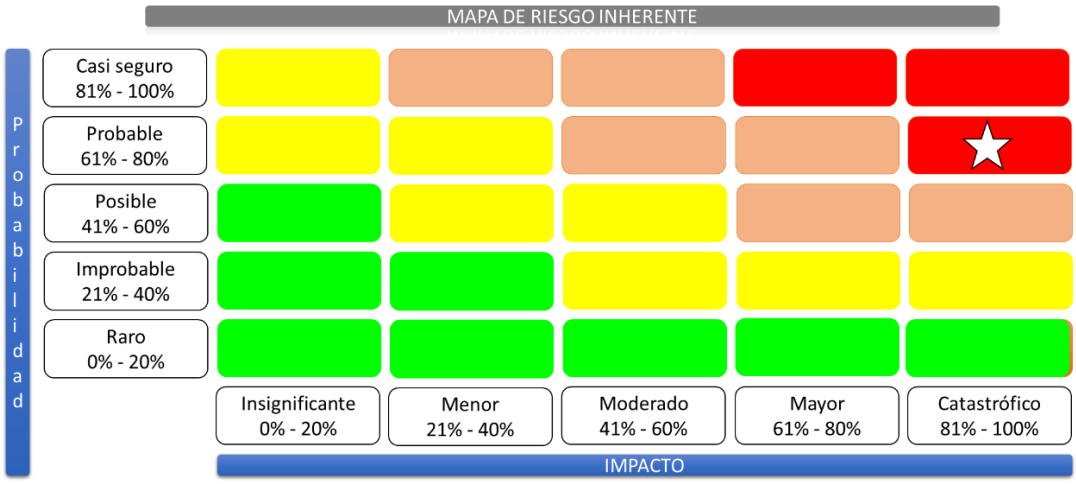

Ilustración 8 Mapa de riesgo inherente

Nota. Elaboración propia

Para evaluar el riesgo de fuga, manipulación o perdida de la información a través de cualquier medio de ataque cibernético, se identificaron controles relacionados con las mejores prácticas internacionales y se vincularon con las causas presentes en la entidad.

De acuerdo con el resultado, la entidad requerirá diseñar un plan de trabajo para la mitigación de este riesgo llevándolo a un nivel residual medio, según el siguiente mapa.

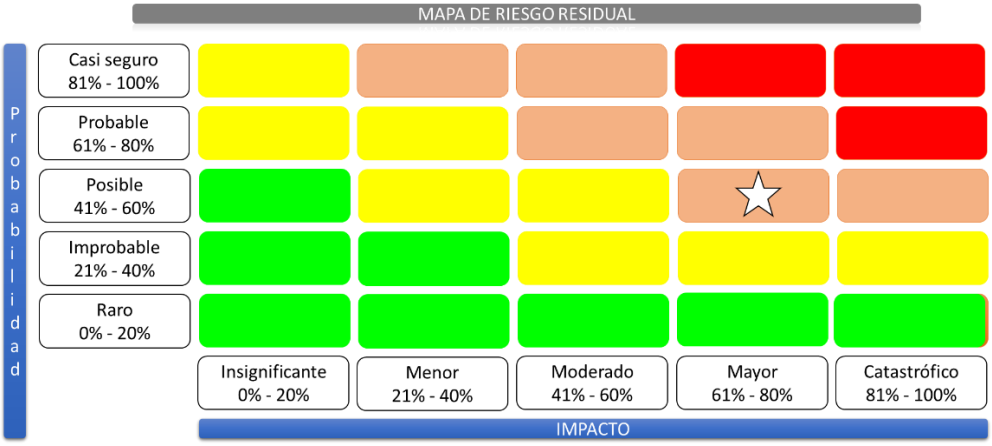

Ilustración 9 Mapa de riesgo residual

Nota. Elaboración propia

Tratamiento del Riesgo

Acorde con la metodología de gestión de riesgos planteada por los diferentes estándares tenidos en cuenta para este proyecto, las opciones para el tratamiento del riesgo son los siguientes.

Aceptar: No adelantar acciones y asumir el riesgo.

Transferir: Tercerización.

Mitigar: Implementar controles.

Es importante tener presente los siguientes criterios para seleccionar la opción de tratamiento:

Eliminar el riesgo, cuando se posible prescindir de los procesos o elementos que lo causan.

Aceptar el riesgo, cuando el monto de la materialización de este es más bajo que la implementación de controles para mitigarlo.

Transferir el riesgo, cuando el proceso es susceptible de ser ejecutado completamente por un tercero y este tercero puede asumir los costos de la materialización del riesgo.

Mitigar el riesgo, el impacto para el negocio de la materialización de este es intolerable y los costos de la materialización son considerantemente más altos que la implementación de los controles.

Para los casos donde la opción de tratamiento viable para la entidad sea la de mitigar el riesgo a través de la implementación de controles, es importante ejecutar la priorización de dichos controles con el objetivo de hacer un plan de trabajo organizado, con tiempos y recursos claramente definidos para ser implementados por la entidad, en la medida de sus posibilidades.

Conclusiones

Para mitigar el riesgo de ciber ataques y garantizar el cumplimiento legal, se ejecutó una evaluación, identificando que su nivel de riesgo inherente en MUY ALTO de acuerdo con los niveles de riesgo que la organización ha definido, lo cual puso en la mira de la alta dirección, este riesgo cibernético que suele ser poco valorado en organizaciones como las que componen el sector defensa, cuya razón social y procesos misionales no incluyen la prestación de servicios tecnológicos, pero si soportan el logro de sus objetivos en las tecnologías de información.

Considerando el tipo de riesgo, objeto de este estudio y su impacto en la organización, la opción de tratamiento adecuada es la MITIGACIÓN, mediante la implementación de controles que logren reducir su impacto y de ser posible su probabilidad de ocurrencia y llevándolo a niveles de riesgo aceptables por la entidad.

Para efectos del análisis realizado, se consideró que el control priorizado, según los criterios definidos, es diseñar y mantener un adecuado proceso de gestión de accesos a las plataformas que manejan información secreta, privada o que ponga en riesgo la seguridad nacional, considerando la regulación aplicable, la cual ha sido ampliamente descrita en este Ensayo.

Para que el control de gestión de accesos sea efectivo y eficiente, es indispensable que la entidad cuente con las herramientas tecnológicas que permitan la integración de las fuentes autoritativas como sistemas de gestión humana o sistemas de gestión de terceros, con las demás aplicaciones de negocio, garantizando que se podrán gestionar (crear, modificar o eliminar) los acceso de cada persona a los diferentes sistemas utilizados en la organización para cumplir con el propósito de la entidad.

En la actualidad la pérdida de información por causales como el secuestro informático y la fuga de información por las debilidades presentes en la infraestructura tecnológica, son una realidad que en ocasiones es tomada a la ligera en algunas organizaciones, hasta cuando son víctima de los delincuentes informáticos o cuando los funcionarios se prestan para extraer información clasificada de la entidad. Es allí cuando la identificación e implementación de acciones que permitan cerrar las brechas de seguridad se hacen importantes para la organización.

Recomendaciones

Mantener un nivel adecuado de objetividad en la ejecución de este análisis, a través de herramientas que permitan reducir la subjetividad de la medición, utilizando hechos y datos históricos o estadísticos (internos o externos), para obtener un resultado semi cuantitativo que proporcione mayor nivel de certeza en la calificación final del riesgo.

Considerando que las organizaciones del sector pueden tener limitaciones, bien sea financieras, de tiempo o de recursos humanos, se pueden presentar retos a la hora de implementar los controles identificados en este estudio. Por tal razón, se recomienda adoptar un mecanismo que permita la priorización de los controles, según su nivel de impacto sobre los riesgos, implementado en el menor tiempo aquellos que mitiguen la mayor cantidad de causas y cuya implementación sea más rápida. Esto se traduce en una gestión efectiva del riesgo, generando victorias tempranas en el plan de trabajo que se deba definir para la implementación de controles.

Evaluar la posibilidad de adquirir las herramientas tecnológicas que permitan correlacionar los eventos que se presenten en los dispositivos utilizados por la entidad para proteger la infraestructura de TI, con el propósito de identificar preventivamente las situaciones de riesgos que se puedan presentar a partir de las alertas generadas por cada uno de los elementos de la infraestructura.

Paralelamente a la ejecución de la metodología desarrollada en este estudio, es recomendable desarrollar campañas de capacitación y sensibilización sobre el riesgo de ataque cibernético, orientadas a la prevención de incidentes que puedan ser causadas por los usuarios

internos o externos, como es al caso de los correos maliciosos que contengan enlaces o archivos adjuntos que comprometen a la seguridad de los equipos y de la red de datos.

Finalmente, se recomienda extender el enfoque metodológico definido en este estudio, para la gestión de otros riesgos, además del riesgo de ciberataques, con el fin de aplicar una única metodología estandarizada para el manejo de los distintos riesgos del sector defensa, mitigando de manera eficiente los riesgos de la organización.

Referencias

CONPES 3701. (2011, 14 julio). LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA. https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

CONPES 3854. (2016, 11 abril). DNP. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Crowdstrike. (2020). Crowdstrike: Global Security Attitude Survey. *Computer Fraud & Security*, *2020*(1), 4. https://www.crowdstrike.com/resources/reports/global-threat-report-latam/

Cybersecurity. (2021, 24 septiembre). NIST. https://www.nist.gov/cybersecurity

DAMA-DMBOOK. (2008, noviembre). TECHNICS PIBLICATIONS. https://technicspub.com/dmbok/

Guía para la administración del riesgo y el diseño de controles en entidades públicas. (s. f.). Ministerio de Comercio. Recuperado 1 de octubre de 2018, de https://www.mincit.gov.co/temas-interes/documentos/guia-para-la-administracion-del-riesgo-y-el-diseno.aspx

ISACA. (2012). *COBIT 5*. COTANA. http://cotana.informatica.edu.bo/downloads/COBIT5-Framework-Spanish.pdf

ISO ORG. (2018). *Figura 1 — Principios, marco de referencia y proceso* [Grafico]. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

ISO/IEC 27001 — Information security management. (2021, 16 febrero). ISO. https://www.iso.org/isoiec-27001-information-security.html

LEY 1273 DE 2009. (2009, 5 enero). SIC. https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1581_2012]. (2012, 18 octubre). SECRETARIA DEL SENADO. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

MINTIC. (2016, 6 mayo). *Guía Metodológica de Pruebas de Efectividad*. mintic.gov.co. https://mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

MINTIC. (2016, 29 julio). *Modelo de Seguridad y Privacidad de la Información*. https://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Sayavedra, A. (2021, 1 marzo). *Amenazas de ciberseguridad en 2021: ¿Dónde están nuestras vulnerabilidades ahora?*Rackspace. https://www.rackspace.com/es-co/blog/cybersecurity-threats-2021

Toro, R. (2021, 11 marzo). *¿Qué es la seguridad de la información y cuantos tipos hay?* PMG SSI - ISO 27001. https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

UNIDAD DE GESTION GENERAL. (2005, enero). *Guía Administración riesgos UGG*. MINDEFENSA. https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Sobre_el_Ministerio/Control_Interno/GPA/Guia_Administracion_riesgos.pdf