21.1

FECHA	viernes, 11 de diciembre de 2020

Señores
UNIVERSIDAD DE CUNDINAMARCA
BIBLIOTECA
Ciudad

UNIDAD REGIONAL	Sede Fusagasugá
TIPO DE DOCUMENTO	Pasantía
FACULTAD	Ingeniería
NIVEL ACADÉMICO DE FORMACIÓN O PROCESO	Pregrado
PROGRAMA ACADÉMICO	**Ingeniería Electrónica**

El Autor(Es):

APELLIDOS COMPLETOS	NOMBRES COMPLETOS	No. DOCUMENTO DE IDENTIFICACIÓN
Rozo Jimenez	Juan Manuel	1069758635

Director(Es) y/o Asesor(Es) del documento:

APELLIDOS COMPLETOS	NOMBRES COMPLETOS
Gordillo Gaitán	Alexander

TÍTULO DEL DOCUMENTO
ACTUALIZACIÓN DE RIESGOS ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO/IEC 27001, 27005 E ISO 31000 BASADOS EN LA METODOLOGÍA DE LA COMPAÑÍA NEXA BPO.

SUBTÍTULO (Aplica solo para Tesis, Artículos Científicos, Disertaciones, Objetos Virtuales de Aprendizaje)

TRABAJO PARA OPTAR AL TÍTULO DE: Aplica para Tesis/Trabajo de Grado/Pasantía
Ingeniero Electrónico

AÑO DE EDICION DEL DOCUMENTO	NÚMERO DE PÀGINAS
08/12/2020	94

DESCRIPTORES O PALABRAS CLAVES EN ESPAÑOL E INGLÉS (Usar 6 descriptores o palabras claves)	
ESPAÑOL	**INGLÉS**
1.Actualización	Upgrade
2.Riesgos	Risks
3.Seguridad de la información (SDI)	Security of the information (SDI)
4. ISO/IEC 27001	ISO/IEC 27001
5.ISO/IEC 27005	ISO/IEC 27001
6.ISO 31000	ISO 31000

RESUMEN DEL CONTENIDO EN ESPAÑOL E INGLÉS

(Máximo 250 palabras – 1530 caracteres, aplica para resumen en español):

Resumen

La presente propuesta se basa en una actualización de riesgos asociados a la seguridad de la información para la compañía NEXA BPO; esto, haciendo uso de tres normas de la Organización Internacional de Estandarización (ISO), como lo son los estándar ISO/IEC 27001, 27005 e ISO 31000.Tomando como referencia estas tres normas se establecen los parámetros, directrices y requerimientos que deben permanecer actualizados para contribuir al fortalecimiento del sistema de gestión de seguridad de la información de la compañía Nexa BPO. Por esta razón, se realiza una identificación, análisis y valoración de riesgos comunes, que en escenarios reales pueden causar un impacto negativo a la compañía si se llegaran a materializar. Sin embargo, el correcto tratamiento de riesgos permite implementar controles y estrategias que previenen y facilitan la ejecución de planes de contingencia de manera más eficaz, con el fin de proteger los activos de información comprometidos.

Abstract

This proposal is based on an update of risks associated with information security for the company NEXA BPO; This, making use of three standards of the International Organization for Standardization (ISO), such as the ISO / IEC 27001, 27005 and ISO 31000 standards. Taking these three standards as a reference, the parameters, guidelines and requirements that must remain updated are established. to contribute to the strengthening of the information security management system of the Nexa BPO company. For this reason, an identification, analysis and assessment of common risks is carried out, which in real scenarios can have a negative impact on the company if they materialize. However, the correct treatment of risks allows the implementation of controls and strategies that prevent and facilitate the execution of contingency plans in a more effective way, in order to protect the information assets compromised.

AUTORIZACION DE PUBLICACIÒN

Por medio del presente escrito autorizo (Autorizamos) a la Universidad de Cundinamarca para que, en desarrollo de la presente licencia de uso parcial, pueda ejercer sobre mí (nuestra) obra las atribuciones que se indican a continuación, teniendo en cuenta que, en cualquier caso, la finalidad perseguida será facilitar, difundir y promover el aprendizaje, la enseñanza y la investigación.

En consecuencia, las atribuciones de usos temporales y parciales que por virtud de la presente licencia se autoriza a la Universidad de Cundinamarca, a los usuarios de la Biblioteca de la Universidad; así como a los usuarios de las redes, bases de datos y demás sitios web con los que la Universidad tenga perfeccionado una alianza, son:
Marque con una “X”:

AUTORIZO (AUTORIZAMOS)	SI	NO
1. La reproducción por cualquier formato conocido o por conocer.	x	
2. La comunicación pública por cualquier procedimiento o medio físico o electrónico, así como su puesta a disposición en Internet.	x	
3. La inclusión en bases de datos y en sitios web sean éstos onerosos o gratuitos, existiendo con ellos previa alianza perfeccionada con la Universidad de Cundinamarca para efectos de satisfacer los fines previstos. En este evento, tales sitios y sus usuarios tendrán las mismas facultades que las aquí concedidas con las mismas limitaciones y condiciones.	x	
4. La inclusión en el Repositorio Institucional.	x	

De acuerdo con la naturaleza del uso concedido, la presente licencia parcial se otorga a título gratuito por el máximo tiempo legal colombiano, con el propósito de que en dicho lapso mi (nuestra) obra sea explotada en las condiciones aquí estipuladas y para los fines indicados, respetando siempre la titularidad de los derechos patrimoniales y morales correspondientes, de acuerdo con los usos honrados, de manera proporcional y justificada a la finalidad perseguida, sin ánimo de lucro ni de comercialización.

Para el caso de las Tesis, Trabajo de Grado o Pasantía, de manera complementaria, garantizo(garantizamos) en mi(nuestra) calidad de estudiante(s) y por ende autor(es) exclusivo(s), que la Tesis, Trabajo de Grado o Pasantía en cuestión, es producto de mi(nuestra) plena autoría, de mi(nuestro) esfuerzo personal intelectual, como consecuencia de mi(nuestra) creación original particular y, por tanto, soy(somos) el(los) único(s) titular(es) de la misma. Además, aseguro (aseguramos) que no contiene citas, ni transcripciones de otras obras protegidas, por fuera de los límites autorizados por la ley, según los usos honrados, y en proporción a los fines previstos; ni tampoco contempla declaraciones difamatorias contra terceros; respetando el derecho a la imagen, intimidad, buen nombre y demás derechos constitucionales. Adicionalmente, manifiesto (manifestamos) que no se incluyeron expresiones contrarias al orden público ni a las buenas costumbres. En consecuencia, la responsabilidad directa en la elaboración, presentación, investigación y, en general, contenidos de la Tesis o Trabajo de Grado es de mí (nuestra) competencia exclusiva, eximiendo de toda responsabilidad a la Universidad de Cundinamarca por tales aspectos.

Sin perjuicio de los usos y atribuciones otorgadas en virtud de este documento, continuaré (continuaremos) conservando los correspondientes derechos patrimoniales sin modificación o restricción alguna, puesto que, de acuerdo con la legislación colombiana aplicable, el presente es un acuerdo jurídico que en ningún

caso conlleva la enajenación de los derechos patrimoniales derivados del régimen del Derecho de Autor.

De conformidad con lo establecido en el artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, *"Los derechos morales sobre el trabajo son propiedad de los autores"*, los cuales son irrenunciables, imprescriptibles, inembargables e inalienables. En consecuencia, la Universidad de Cundinamarca está en la obligación de RESPETARLOS Y HACERLOS RESPETAR, para lo cual tomará las medidas correspondientes para garantizar su observancia.

NOTA: (Para Tesis, Trabajo de Grado o Pasantía):

Información Confidencial:

Esta Tesis, Trabajo de Grado o Pasantía, contiene información privilegiada, estratégica, secreta, confidencial y demás similar, o hace parte de la investigación que se adelanta y cuyos resultados finales no se han publicado. **SI** _x_ **NO** ___.
En caso afirmativo expresamente indicaré (indicaremos), en carta adjunta tal situación con el fin de que se mantenga la restricción de acceso.

LICENCIA DE PUBLICACIÒN

Como titular(es) del derecho de autor, confiero(erimos) a la Universidad de Cundinamarca una licencia no exclusiva, limitada y gratuita sobre la obra que se integrará en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha de inclusión en el repositorio, por un plazo de 5 años, que serán prorrogables indefinidamente por el tiempo que dure el derecho patrimonial del autor. El autor podrá dar por terminada la licencia solicitándolo a la Universidad por escrito. (Para el caso de los Recursos Educativos Digitales, la Licencia de Publicación será permanente).

b) Autoriza a la Universidad de Cundinamarca a publicar la obra en formato y/o soporte digital, conociendo que, dado que se publica en Internet, por este hecho circula con un alcance mundial.

c) Los titulares aceptan que la autorización se hace a título gratuito, por lo tanto, renuncian a recibir beneficio alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente licencia y de la licencia de uso con que se publica.

d) El(Los) Autor(es), garantizo(amos) que el documento en cuestión, es producto de mi(nuestra) plena autoría, de mi(nuestro) esfuerzo personal intelectual, como consecuencia de mi (nuestra) creación original particular y, por tanto, soy(somos) el(los) único(s) titular(es) de la misma. Además, aseguro(aseguramos) que no contiene citas, ni transcripciones de otras obras protegidas, por fuera de los límites autorizados por la ley, según los usos honrados, y en proporción a los fines previstos; ni tampoco contempla declaraciones difamatorias contra terceros; respetando el derecho a la imagen, intimidad, buen nombre y demás derechos constitucionales. Adicionalmente, manifiesto (manifestamos) que no se incluyeron expresiones contrarias al orden público ni a las buenas costumbres. En consecuencia, la responsabilidad directa en la elaboración, presentación, investigación y, en general, contenidos es de mí (nuestro) competencia exclusiva, eximiendo de toda responsabilidad a la Universidad de Cundinamarca por tales aspectos.

e) En todo caso la Universidad de Cundinamarca se compromete a indicar siempre la autoría incluyendo el nombre del autor y la fecha de publicación.

f) Los titulares autorizan a la Universidad para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión.

g) Los titulares aceptan que la Universidad de Cundinamarca pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

h) Los titulares autorizan que la obra sea puesta a disposición del público en los términos autorizados en los literales anteriores bajo los límites definidos por la universidad en el “Manual del Repositorio Institucional AAAM003”

i) Para el caso de los Recursos Educativos Digitales producidos por la Oficina de Educación Virtual, sus contenidos de publicación se rigen bajo la Licencia Creative Commons: Atribución- No comercial- Compartir Igual.

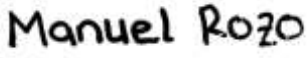
j) Para el caso de los Artículos Científicos y Revistas, sus contenidos se rigen bajo la Licencia Creative Commons Atribución- No comercial- Sin derivar.

Nota:
Si el documento se basa en un trabajo que ha sido patrocinado o apoyado por una entidad, con excepción de Universidad de Cundinamarca, los autores garantizan que se ha cumplido con los derechos y obligaciones requeridos por el respectivo contrato o acuerdo.

La obra que se integrará en el Repositorio Institucional, está en el(los) siguiente(s) archivo(s).

Nombre completo del Archivo Incluida su Extensión (Ej. PerezJuan2017.pdf)	Tipo de documento (ej. Texto, imagen, video, etc.)
1. ACTUALIZACIÓN DE RIESGOS ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO-IEC 27001, 27005 E ISO 31000 BASADOS EN LA METODOLOGÍA DE LA COMPAÑÍA NEXA BPO.pdf	TEXTO E IMÁGENES

En constancia de lo anterior, Firmo (amos) el presente documento:

APELLIDOS Y NOMBRES COMPLETOS	FIRMA (autógrafa)
Rozo Jimenez Juan Manuel	 Firma del Estudiante

21.1-40

ACTUALIZACIÓN DE RIESGOS ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO/IEC 27001, 27005 E ISO 31000 BASADOS EN LA METODOLOGÍA DE LA COMPAÑÍA NEXA BPO

JUAN MANUEL ROZO JIMENEZ

Universidad de Cundinamarca
Ingeniería Electrónica
Facultad de ingeniería
Fusagasugá, Colombia
2020

ACTUALIZACIÓN DE RIESGOS ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO/IEC 27001, 27005 E ISO 31000 BASADOS EN LA METODOLOGÍA DE LA COMPAÑÍA NEXA BPO

Trabajo de grado presentado como requisito parcial para optar por el título de ingeniero electrónico

JUAN MANUEL ROZO JIMENEZ

Director externo:
José Manuel Chávez Gonzales

Director interno:
Ing. Alexander Gordillo Gaitán, MSc

Línea de investigación:
Software, Sistemas Emergentes y Nuevas Tecnologías

Universidad de Cundinamarca
Ingeniería Electrónica
Facultad de ingeniería
Fusagasugá, Colombia
2020

Resumen

La presente propuesta se basa en una actualización de riesgos asociados a la seguridad de la información para la compañía NEXA BPO; esto, haciendo uso de tres normas de la Organización Internacional de Estandarización (ISO), como lo son el estándar ISO/IEC 27001:2013, cuyo objetivo principal es proporcionar la metodología adecuada para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para una organización (Norma ISO 27001, 2013). Además, de la norma ISO/IEC 27005:2018 que fue diseñada como soporte para emplear correctamente un SGSI estableciendo las directrices generales enfocadas en la gestión de riesgo que puede sufrir el activo de información de una compañía (Norma ISO 27005, 2018) y la norma ISO 31000:2018 que proporciona los principios para la gestión de riesgos y describe el proceso de implementación en los niveles operativos y estratégicos de las compañías (Norma ISO 31000, 2018).

Tomando como referencia estas tres normas se establecen los parámetros, directrices y requerimientos que deben permanecer actualizados para contribuir al fortalecimiento del sistema de gestión de seguridad de la información de la compañía Nexa BPO. Por esta razón, se realiza una identificación, análisis y valoración de riesgos comunes, que en escenarios reales pueden causar un impacto negativo a la compañía si se llegaran a materializar. Sin embargo, el correcto tratamiento de riesgos permite implementar controles y estrategias que previenen y facilitan la ejecución de planes de contingencia de manera más eficaz, con el fin de proteger los activos de información comprometidos.

Adicionalmente, es importante aclarar que la información que contiene este documento es de carácter sensible y dando cumplimiento al contrato de confidencialidad con la compañía NEXA BPO, se limita la divulgación de cierta información que se debe mantener reservada al público y únicamente se publica la información autorizada por el CISO (*Chief Information Security Officer:* u oficial principal de seguridad de la información).

Contenido

Resumen....3
1. Contexto....8
2. Actividades....9
2.1. Revisiones técnicas de equipos de cómputo....10
2.2. Validación de eventos e incidentes de seguridad y ciberseguridad....12
2.3. Actas de borrado seguro....14
2.4. Custodia de activos de información....16
2.5. Control de gestión de usuarios....17
2.6. Herramientas....19
2.6.1. Symantec Endpoint Protection....19
2.6.2. Aranda Software....23
2.6.3. NETSCAN....29
2.6.4. NEXAPLUS....30
3. Marco de referencia....33
3.1. Marco conceptual....33
3.2. Marco legal....36
4. Plan de trabajo....38
4.1. Activos....38
4.1.1. Identificación de activos....38
4.1.2. Propiedad de los activos....39
4.1.3. Clasificación de activos....40
4.1.4. Etiquetado de activos de información....42
4.2. Principios y directrices....44
4.3. Marco de referencia....44
4.4. Gestión del riesgo....45
4.4.1. Componentes del riesgo de seguridad de la información....45
4.4.2. Proceso de gestión del riesgo en seguridad de la información....46
4.5. Análisis y valoración de riesgos....48
4.5.1. Amenazas....50
4.5.2. Vulnerabilidades....53
4.5.3. Riesgos asociados a la seguridad de la información....55

4.5.4. Identificación, análisis y valoración de riesgos 56
4.5.5. Matriz de valoración de riesgos en la seguridad de la información.....71
4.6. Tratamiento de riesgos 73
4.6.1. Opciones de tratamiento del riesgo 73
4.6.2. Selección de las opciones para el tratamiento del riesgo 74
5. Análisis de resultados 80
6. Conclusiones.....81
7. Glosario.....82
8. Referencias.....84
Apéndice 1. Documentos adjuntos.....87

Índice de figuras

Figura 1. Resumen de actividades en el área de seguridad de la información. 9
Figura 2. Borrado seguro de información con la herramienta DBAN.....15
Figura 3. Interfaz principal del directorio activo de Windows.....18
Figura 4. Ventana de búsqueda de usuarios en el directorio activo. 19
Figura 5. Capas de protección de Symantec Endpoint Protection. 20
Figura 6. Interfaz de Symantec Endpoint Protection 21
Figura 7. Interfaz de Aranda Asset Management (AAM). 24
Figura 8. Interfaz de Aranda Software Delivery (ASD) 25
Figura 9. Interfaz de Aranda Software Metrix (ASM).....26
Figura 10. Interfaz de Aranda Power Management (APWM) 27
Figura 11. Interfaz de Aranda Patch Management (APM).....28
Figura 12. Ventana Principal de la herramienta NETSCAN. 30
Figura 13. Interfaz para solicitudes de la plataforma NEXAPLUS. 31
Figura 14. Ejemplo de un ID generado al solicitar un requerimiento. 32
Figura 15. Estampilla de seguridad para archivos restringidos. 43
Figura 16. Etiqueta de confidencialidad de correos electrónicos.....44
Figura 17. Cadena de detección y tratamiento de amenazas. 45
Figura 18. Proceso de gestión del riesgo en la seguridad de la información. 47
Figura 19. Elementos del análisis de riesgos potenciales. 48
Figura 20. El riesgo en función del impacto y la probabilidad.....52
Figura 21. Registro de vulnerabilidades identificadas hasta septiembre de 2020. 54
Figura 22. Impacto potencial de la vulnerabilidad CVE-2020-1508.....57
Figura 23. Impacto potencial de la vulnerabilidad CVE-2020-25826.....59
Figura 24. Impacto potencial de la vulnerabilidad CVE-2020-1338.....60
Figura 25. Impacto potencial de la vulnerabilidad CVE-2020-1581.....62
Figura 26. Impacto potencial de la vulnerabilidad CVE-2020-25776.....64
Figura 27. Impacto potencial de la vulnerabilidad CVE-2020-5839.....65
Figura 28. Impacto potencial de la vulnerabilidad CVE-2020-12107.....67
Figura 29. Impacto potencial de la vulnerabilidad CVE-2020-17365.....68
Figura 30. Impacto potencial de la vulnerabilidad CVE-2020-15663.....69
Figura 31. Impacto potencial de la vulnerabilidad CVE-2020-15963.....70

Índice de tablas

Tabla 1. Fases de protección contra ataques.....22
Tabla 2 Datos visualizados en la consola (SEP) al conectar un dispositivo. 23
Tabla 3. Demostración de la clasificación de activos de información. 40
Tabla 4. Clasificación por criterios de integridad. 42
Tabla 5. Clasificación por criterios de disponibilidad. 43
Tabla 6. Clasificación por criterios de confidencialidad. 43
Tabla 7. Amenazas que pueden afectar los activos de la compañía. 50
Tabla 8. Niveles de degradación del valor de un activo. 51
Tabla 9. Probabilidad de ocurrencia de la materialización de una amenaza. 51
Tabla 10. Vulnerabilidades identificadas para el sistema operativo Windows. 56
Tabla 11. Vulnerabilidades identificadas en Microsoft office. 59
Tabla 12. Vulnerabilidades identificadas para antivirus. 63
Tabla 13. Vulnerabilidades identificadas para VPN. 66
Tabla 14. Vulnerabilidades identificadas para navegadores. 68
Tabla 15. Matriz de valoración del riesgo. 72
Tabla 16. Matriz de valoración del riesgo para las vulnerabilidades identificadas. 72
Tabla 17. Matriz para el tratamiento de riesgos. 74
Tabla 18. Plan de tratamiento para los riesgos identificados. 76

1. Contexto

La compañía nace en el año 1976 bajo el nombre de Ventas y Servicios S.A como sociedad limitada formando parte del grupo financiero más grande de Colombia, el Grupo Aval, conformado por cinco bancos (Banco de Bogotá, Banco de Occidente, Banco Popular, Banco AV Villas y Banco BAC). En el año 1991 se constituye como la primera Sociedad Anónima Colombiana en ser pionera en el mercado de *Outsourcing* operativo, Administrativo y comercial.

En 2019 se reinventa bajo el nombre de NEXA BPO, como una compañía experta en la gestión de la experiencia al cliente en el sector de BPO (*Business Process Outsourcing*) en la tercerización de procesos y *Contact Center* brindando soluciones y creando modelos ajustados a las necesidades de sus clientes y fundamentados en la satisfacción, seguridad y eficacia que generan beneficios a sus negocios. Actualmente cuenta con más de 8.000 colaboradores y presencia nacional en más de 21 oficinas en 94 ciudades y municipios.

Nexa BPO Cuenta con certificaciones de control de calidad que aseguran los más altos estándares en gestión de procesos con la certificación ISO 9001:2008 en Sistemas de Gestión de Calidad y la certificación ISO/IEC 27001:2013 en Sistemas de Gestión de seguridad de la información, este último tiene un alto valor en las compañía debido a que la vulneración de datos es un daño casi incalculable que no solo afecta los clientes sino que también la reputación de la empresa, por esto la reglamentación de ética y respeto por los datos personales es indispensable fortalecerla con un adecuado sistema de gestión de la seguridad de la información que garantice el correcto tratamiento de activos de información.

2. Actividades

Las actividades desarrolladas durante la practica universitaria en la compañía NEXA BPO específicamente en el área de seguridad de la información se pueden observar en la figura 1; donde las actividades fueron administrativas y prácticas, iniciando con una ***revisión técnica de equipos***, basada en la verificación del cumplimiento de controles aplicados a la seguridad de la información. También se realizó la ***custodia de activos de información*** para garantizar la actualización de credenciales de usuarios del área administrativa. Así mismo se realiza un ***control de gestión de usuarios*** para validar y gestionar los permisos y actividades del personal operativo. Por otro lado, se ***elaboraban actas de borrado seguro*** con el fin de evidenciar la correcta eliminación de datos en dispositivos y bases de datos. Por otra parte, la ***validación de eventos e incidentes de seguridad*** permitían registrar precedentes del incumplimiento de políticas de seguridad en el área administrativa y operativa de la compañía. Finalmente, el uso de herramientas mediante ***consola facilitaba el monitoreo, gestión y seguimiento de controles*** que respaldaban el sistema de gestión de seguridad de la información.

Como resultado de las actividades realizadas a lo largo de la práctica se determina la recopilación de información, que permite establecer vulnerabilidades en los activos de información de la compañía, lo que deriva en una actualización de riesgos asociados a la seguridad de la información, bajo las directrices de las normas ISO 27001, 27005 y 31000.

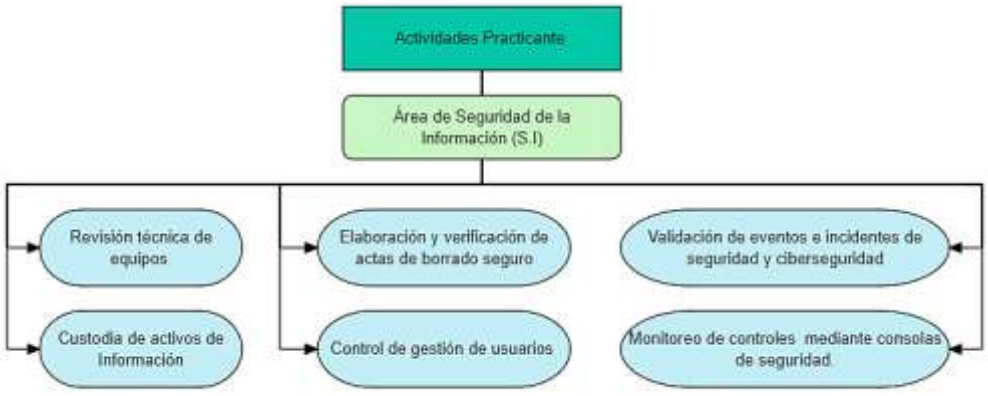


Figura 1. Resumen de actividades en el área de seguridad de la información.

A continuación, se describen cada una de las actividades desarrolladas durante la practica en el área de seguridad de la información con su respectivo soporte que da constancia del aprendizaje obtenido a lo largo de cada actividad desarrollada.

2.1. Revisiones técnicas de equipos de cómputo

El objetivo principal de realizar una revisión técnica es dar cumplimiento a una lista de parámetros creados por el área de seguridad de la información, donde se establecen los requerimientos mínimos del sistema de gestión de seguridad de la información (SGSI) que deben cumplir los diferentes dispositivos asociados al sector operativo y administrativo de la compañía.

Estas revisiones deben garantizar el adecuado uso y manejo de los activos físicos y de información, basándose en los pilares de la seguridad de la información: integridad, disponibilidad y confidencialidad. Fundamentados en los controles aplicados y las políticas de seguridad de la compañía.

Los dispositivos inspeccionados son:

- Equipos portátiles *(Laptop)*: Son de uso exclusivo del personal administrativo de la compañía y para uso únicamente laboral, son proporcionados por la compañía.
- Computadores de escritorio: Utilizados principalmente en la operación por los asesores de las diferentes campañas, pueden ser propiedad de la compañía o alquilados por terceros.

La información obtenida a través del "Formato auditoria de estándar de seguridad en equipos de cómputo" y "Estándar de revisión de equipos portátiles" es responsabilidad del coordinador de seguridad de la información, hace parte del proceso de administración de seguridad de la información y cuenta con clasificación restringida de la información que se contiene en dichos formatos.

El ***Formato de auditoria de estándar de seguridad en equipos de cómputo (ANEXO_1)*** contiene los siguientes parámetros:

1. *Campaña o área*: Se utiliza el nombre completo de la campaña o área que se va a auditar.
2. *Nombre del equipo*: Se localiza en una etiqueta que contiene un identificar basado en el inventario de activos de la compañía.
3. *Ip del equipo*: Es la asignación que permite identificar el equipo en una red y se obtiene por medio de un aplicativo de la intranet.
4. *Sistema operativo del equipo:* Se utilizan las abreviaturas (W-U-A) para referirse a Windows, Ubuntu y Apple respectivamente, seguido del número de la versión del sistema operativo.
5. *Sistema operativo Licenciado*: Se identifica que el sistema operativo cuente con la activación de su respectiva licencia.

6. Internet: Basados en las autorización y permisos que poseen los usuarios, se hace la elección más apropiada dentro de las siguientes categorías:
    - Restringido (R): Se encuentra inhabilitado el uso de internet.
    - Consulta (C): Solo permite hacer búsquedas específicas y permitidas.
    - Libre (L): Se tiene acceso general a internet.
7. Eliminar historial bloqueado: Se verifica la eliminación de archivos temporales, historial, cookies y datos del sitio web.
8. Navegador: Se identifican los navegadores utilizados en el equipo: Chrome (CH), Microsoft Edge (ME), Explorer (E), Firefox (F), Opera (O).
9. Antivirus instalado: Se comprueba la instalación de Symantec Endpoint Security.
10. Fecha última actualización del antivirus: En caso de que se cuente con el antivirus instalado, se registra la última fecha de actualización.
11. Usuarios locales eliminados: A través de la administración de equipos, se verifican los usuarios y grupos locales visibles.
12. Unidades de disco duro: Se examinan que las unidades de disco duro se encuentren ocultas.
13. Panel de control bloqueado: No debe permitir la ejecución de la herramienta panel de control.
14. DLP Endpoint: La administración de tareas debe mostrar el proceso edpa.exe (*software de Agent Install* o *AgentInstall64* de Symantec) ejecutándose.
15. Aplicaciones de soporte inventario: Comprobar la Instalación y ejecución del software Aranda que permite realizar eficientemente la gestión de la infraestructura tecnología.
16. Juegos bloqueados: La carpeta de juegos debe estar vacía.
17. Gadgets bloqueados: Está prohibido el uso de gadgets.
18. Unidad de cd bloqueada: Las unidades de cd deben estar deshabilitadas.
19. Puertos USB bloqueadas: Se utiliza una USB autorizada por seguridad de la información para realizar el bloqueo de puertos para dispositivos de almacenamiento masivo.
20. Hora sincronizada: Se comprueba que la fecha y hora del dispositivo sean las correctas.
21. Bloqueo símbolo del sistema: No debe estar permitido la ejecución del CMD.
22. Bloqueo menú ejecutar: No se debe iniciar la herramienta EJECUTAR.
23. Bloqueo recortes: Está prohibido el uso de la herramienta recortes.
24. Bloqueo impresiones pantalla: Se comprueba que no se puedan tomar capturas de pantalla desde el teclado físico.
25. Teclado en pantalla: No se permite el uso del teclado digital.
26. Ofimática: Se registra el uso de aplicaciones como *Microsoft office* (M.O) y *Libre office* (L.O), según corresponda.
27. Escritorio limpio: El escritorio no debe contener archivos ni accesos directos.

28. Observaciones: Se utiliza para hacer descripciones breves. Además de registrar los nombres y usuarios que hacen uso del equipo.

El Formato ***Estándar de revisión de equipos portátiles***, es similar al anterior, pero modifica algunos parámetros como:

1. Responsable: Son los nombres completos de la persona que hará uso del equipo.
2. Actualizaciones: Se verifican que contenga todas las actualizaciones disponibles hasta la fecha.
3. Particiones: No deben existir particiones del disco duro.
4. Cifrado de disco: Debe existir una protección para la información almacenada.
5. Guaya de seguridad: Se debe garantizar una protección física antirrobo.
6. Inventario: Es el registro con el que se relaciona el dispositivo con el inventario de la compañía.
7. Sello de seguridad: Es una etiqueta con un serial y código de barras con el cual se identifica y autoriza la salida y entrada del dispositivo portátil.

Una vez que se identifican todos los parámetros establecidos anteriormente para cada caso, se procede a establecer los equipos que no cumplen con al menos uno de los atributos y se realiza una petición tipo requerimiento de cumplimiento de políticas de seguridad al área de tecnología, donde deben resolver el problema lo más pronto posible para obtener la autorización de operación nuevamente del equipo.

2.2. Validación de eventos e incidentes de seguridad y ciberseguridad

Los activos de información son de vital importancia para NEXA BPO, por lo que deben ser protegidos. El incumplimiento de una política interna del SGSI ocasiona un incidente. El área de seguridad de la información es la encargada de hacer cumplir las políticas de seguridad validando los eventos e incidentes de seguridad como:

- Control y administración del acceso a la información: El objetivo principal es prevenir el acceso no autorizado a los recursos de información. Esto, controlando los privilegios de accesibilidad de cada usuario y limitando el acceso a solo lo requerido según los permisos de su perfil.
- Uso de recursos informáticos: Todos los recursos físicos son exclusivos del negocio y de manejo propio del encargado para fines laborales, no deben ser manipulados por terceros sin autorización.

- Identificación y autenticación: Todo el personal operativo y administrativo debe contar con medios de identificación y de acceso, controlados por medio de la autenticación personal como lo es el carnet y *passpoint*. El acceso a la red es únicamente para el desarrollo de labores estrictamente especificadas, por lo que no se puede realizar ningún otro tipo de actividades que no hayan sido asignadas.
- Administración de alertas: Cualquier violación a las políticas de seguridad establecidas por la compañía debe ser informada inmediatamente.

Los incidentes de seguridad más comunes son:

- Préstamo o abandono de credenciales: Todos los accesos al área operativa y administrativa en la compañía Nexa BPO, cuentan con autenticación para permitir el acceso a las diferentes áreas según el nivel de permisos que se posean. Por lo que está completamente prohibido el prestamos de credenciales para permitir el ingreso de personas a zonas no autorizadas. Adicionalmente, todo el personal debe transportar su carnet de identificación en una zona visible y por ningún motivo debe desatender o perderlo, debido a que esto conlleva a sanciones, suspensiones o en casos extremos perdida de integridad por uso indebidos por parte de terceros. Igualmente está prohibido el préstamo de usuarios de red para iniciar sesión.

- Uso de dispositivos móviles, USB y papeleo: Los colaboradores tienen prohibido el ingreso y uso del celular, dispositivos de almacenamiento masivo y papelería (hojas, agendas, esferos entre otros) en las zonas de operación. Debido a que estos implementos representan una amenaza de fuga de información.

Otros de los incidentes más recurrentes son el uso de los celulares corporativos por fuera de las áreas designadas para su empleo, la desatención de los equipos de cómputo con la sesión y aplicativos abiertos, el ingreso de maletas y bolsos en los puestos de trabajo.

En el ***Formato Reporte de Incidentes (ANEXO_2),*** se puede evidenciar que es un proceso correspondiente al área de seguridad de la información, donde el responsable es el coordinador de seguridad de la información y cuenta con clasificación restringida. Todo incidente de seguridad debe contar con material probatorio que de constancia del incidente cometido. Algunos de los datos que se deben contemplar son:
Nombres y apellido de la persona que cometió el incidente, el cargo en el que se encuentra matriculado, la campaña o área a la cual pertenece, la fecha y hora en la que se cometió y se registró el incidente. Adicionalmente, se realiza una breve descripción del evento o incidente de seguridad que fue cometido.

En el espacio denominado “Firma de quien reporta”, se diligencian los campos de: nombre, firma y la cedula de ciudadanía de quien reporta o levanta el incidente.
El implicado tiene disponible el espacio de “observaciones colaborador”, para justificar la falta cometida y debe diligenciar el espacio colaborador con su nombre, firma y cedula de ciudadanía. Finalmente, el espacio de testigo es completado por el supervisor o jefe inmediato del implicado.

Una vez diligenciado en su totalidad el formato, se procede a reportar el incidente de seguridad a través de la plataforma digital, donde es estudiado por los expertos que toman la decisión en base al grado de la falta o reincidencia del evento.
Cuando es por primera vez y no tiene mayor gravedad, se realizan retroalimentaciones que son compromisos por parte del implicado para no volver a cometer la falta.
Cuando es reincidente o una falta grave, se exponen desde sanciones hasta la terminación del contrato laboral.

2.3. Actas de borrado seguro

Cuando termina el tiempo de operación de una campaña, el área de soporte técnico de tecnología informática se encarga de realizar el borrado seguro de discos duros con herramientas como DBAN (*Darik’s Boot and Nuke*), el cual consiste en la escritura de datos de manera prolongada sobre el disco duro, permitiendo la eliminación de archivos, aplicaciones, carpetas y cualquier rastro de información almacenada en las unidades de disco duro en computadoras de escritorio, portátiles o servidores. Esto, con el fin de garantizar la confidencialidad y privacidad de la información que paso por el dispositivo.

Algunos de los equipos utilizados en operación, son propiedad de la compañía y otros son alquilados por empresas dedicadas a este tipo de actividades como *Milenio Pc*, por lo que antes de asignarles un nuevo uso o hacer la devolución de los dispositivos, se debe garantizar el correcto borrado de datos con el fin de prevenir que alguien con experiencia en el análisis de volcado de memoria logre recuperar y extraer archivos, fotografías, bases de datos, contraseñas o datos bancarios, en la figura 2 se muestra un ejemplo del resultado obtenido después del borrado seguro de información con la herramienta DBAN.

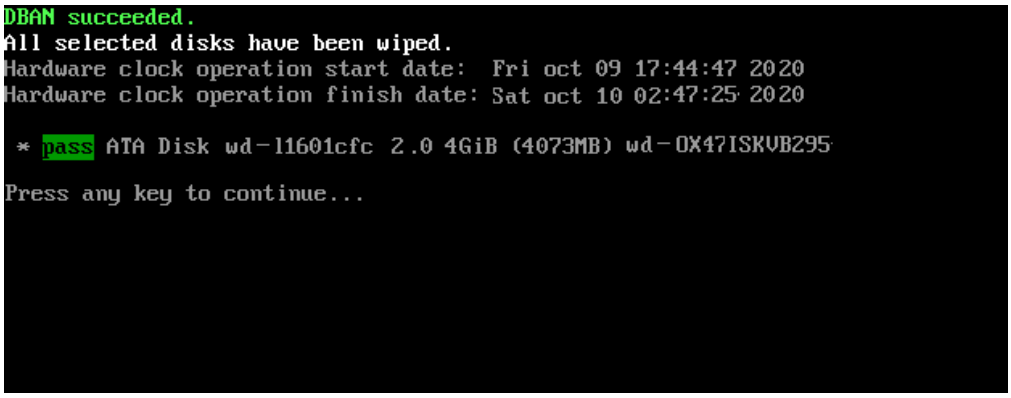


Figura 2. Borrado seguro de información con la herramienta DBAN.

El uso de la herramienta DBAN para organizaciones empresariales requiere de un certificado de borrado seguro para fines de cumplimiento legal, donde se asegura la destrucción permanente de datos, sectores reasignados y discos ocultos bajo estándares de seguridad de la información.

En el formato de ***Revisión borrado seguro de la información en equipos (ANEXO_3)***, Se puede evidenciar que es un proceso correspondiente a la administración de seguridad de la información, donde el responsable es el director de riesgos y cuenta con clasificación de la información de uso interno. Este formato cuenta con los siguientes parámetros:

1. *Fecha de revisión:* Se indica el día, mes y año en el que se registró la revisión.
2. *Sede de origen:* Es la ubicación física donde se localiza el equipo.
3. *Cantidad de equipos:* Especifica el número total de equipos registrados.
4. *Ubicación:* Hace referencia a la campaña o área donde se encuentra el equipo.
5. *Destino:* Es el lugar donde será almacenado (Bodega administrativa) o transferido (Nueva campaña).
6. *Fecha del borrado:* Detalla la fecha en la que se efectuó el borrado.
7. *Marca:* Se especifica la marca industrial de origen, ejemplo: Lenovo, Samsung, Asus, Toshiba, Hewlett-Packard, etc.
8. *Modelo:* Se detalla la versión que corresponde al equipo de cómputo.

Una vez concluida la ejecución de la herramienta DBAN se extraen los siguientes datos:

9. *Serial:* Es una serie de caracteres únicos que permiten identificar el equipo.
10. *Milenio ID/VYS ID:* Cada equipo posee una etiqueta con el identificador asignado en la lista de activos de la compañía.

11. *Hora de inicio:* Se especifica el día/mes/año y hora en la que se inició el borrado seguro.
12. *Hora final:* Detalla la hora, día, mes y año en la que finalizo con éxito el proceso de borrado de la información.
13. *Log:* Es una serie alfanumérica que contiene el registro de los cambios efectuados en el disco.

Una vez diligenciados todos los datos anteriormente nombrados, el acta de borrado seguro de información en equipos, debe ser firmada por el coordinador de soporte técnico de tecnología informática, el encargado de la elaboración del acta (testigo) y finalmente por el responsable de seguridad de la información. Si el borrado es de equipos propios de la compañía, se entrega una copia al área de soporte técnico y la otra se archiva en los documentos del área de seguridad de la información, si los equipos pertenecen a una empresa prestadora del servicio de alquiler, se hace entrega de una copia adicional del acta que certifica la entrega de equipos en óptimas condiciones y sin rastros de información.

2.4. Custodia de activos de información

La información de carácter confidencial debe tener un tratamiento más riguroso, donde se pueda garantizar la protección en todo momento de la confidencialidad, integridad, disponibilidad y privacidad de los activos de información que se encuentren bajo custodia del personal de seguridad de la información.
La entrega de usuarios y contraseñas del personal con permisos privilegiados (administración y gerencia), deben ser renovadas constantemente, con el fin de dar cumplimiento a las políticas de seguridad. Para ello se solicitan los nuevos usuarios y/o contraseñas, se agenda una fecha y hora especifica en la cual se hace la recepción de las credenciales vencidas y se entregaran las nuevas.

El objetivo principal de esta actividad es garantizar que los activos transportados se encuentren íntegros y disponibles de principio a fin, de manera que solamente el personal autorizado tenga acceso a la información.

Este procedimiento se desarrolla de la siguiente manera:

1. Verificar las credenciales que están próximas a vencer.
2. Solicitud de nuevos usuarios y/o contraseñas para el personal identificado.
3. Notificación para efectuar la renovación:

"*Con el fin de dar cumplimiento a lo establecido en el procedimiento P-AN-ASI-001 para la custodia de credenciales que hacen parten de los controles asociados al área de seguridad de la información. Se hará la recepción de las actas que por revisión se encuentran desactualizadas por vencimiento de usuario y/o contraseña y se otorgaran las credenciales renovadas en la fecha y hora indicadas*".

4. Descarga e impresión de los documentos solicitados.
5. Archivamiento de la información anterior.
6. Sellado y etiquetado de los documentos de carácter confidencial.
7. Custodia desde el área de seguridad de la información hasta su destino.
8. Recepción de credenciales vencidas.
9. Entrega de credenciales nuevas.
10. Firma de recibido por parte del personal de seguridad de la información y el destinatario.
11. Destrucción de las credenciales vencidas por confidencialidad.

2.5. Control de gestión de usuarios

En la compañía NEXA BPO el modo de interconectar todos los equipos que conforman la red de la sede norte, es de tipo Intranet. Debido a que es un entorno de trabajo donde existen más de 4.000 equipos interconectados mediante una red LAN, que a su vez está dividida en subredes donde no solamente se comparten archivos e impresoras, sino que además se debe hacer un monitoreo de los usuarios y los permisos de acceso.

El software que ayuda a cumplir con esta tarea es: *Active Directory* o Directorio Activo de Microsoft. Esta herramienta es un directorio que proporciona servicios capaces de crear usuarios, equipos o grupos para ser administrados en cuanto se conectan a la red. Además, permite la gestión de los permisos de acceso de usuarios, control de actualizaciones, instalación de programas, creación o modificación de carpetas centralizadas desde donde se permite acceder a los recursos de manera remota a la estación de trabajo.

Con el uso de protocolos como LDAP (Protocolo ligero de acceso a directorios), DHCP (Protocolo de configuración dinámica de host), DNS (Sistema de nombres de dominio), KERBEROS (autenticación de redes de ordenador).

La información recolectada por cada uno de estos protocolos, estructuran una base de datos que almacena información, por ejemplo, las credenciales de autenticación de los

usuarios en tiempo real al ingresar a la red, lo que permite una sincronización de todos los equipos bajo un elemento central. En la figura 3 se visualiza la interfaz principal del directorio activo de Windows que a su vez es un controlador de dominio, donde se pueden gestionar los permisos e interacciones de cada usuario.

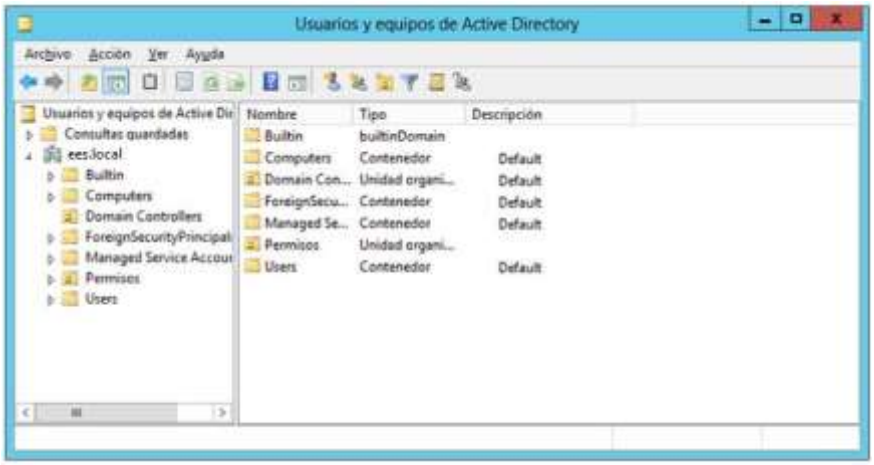


Figura 3. Interfaz principal del directorio activo de Windows.

Los elementos que componen el directorio activo son:

- *Dominio:* Grupo de ordenadores conectados a la red que son administrados por un equipo servidor.
- *Objeto*: Es cualquier componente que existe dentro de un directorio, como:
  - *Usuario:* Comprende las credenciales de acceso (usuario y contraseña).
  - *Recurso:* Son los elementos a los que los usuarios tienen acceso (Carpetas compartidas, impresoras etc.)
  - *Servicio:* Se basan en las funcionalidades permitidas para el usuario (Correo electrónico, crear o modificar carpetas, impresoras etc.)
- *Unidad organizativa*: Es el contendor de los objetos que permite asignar permisos y observar la jerarquía del dominio.
- *Árbol:* Es un conjunto de dominios que, al ser divididos en partes, permiten una mejor gestión de los recursos.
- *Bosque:* Son todos los árboles y dominios existentes en el directorio.

Para el área de seguridad de la información el uso del directorio activo es indispensable cuando de administración, validación y búsqueda de usuarios se trata; debido a que proporciona información detallada de los usuarios, sus direcciones IP asociadas, área y procesos a los que pertenecen, ubicación física del activo en la compañía y otro tipo de información proporcionada por la matriz de perfiles en la cual se determinan las funciones, actividades y accesos que posee cada usuario, según su perfil actual.

Al tratarse de una compañía grande, es normal encontrar mensualmente una gran cantidad de desvinculación de personal, por lo que se debe comprobar si los usuarios se encuentran en algunos de los dos siguientes casos:

Desvinculación temporal: Por suspensión o vacaciones, por lo que no deben registrarse actividades recientes del usuario durante el tiempo de ausencia.
Desvinculación Permanente: Despido o renuncia, se debe solicitar la eliminación del perfil del usuario.

En la figura 4 se puede observar un ejemplo del uso del directorio activo, para comprobar el estado del usuario ZEUS, que se encuentra suspendido temporalmente de la compañía.

Figura 4. Ventana de búsqueda de usuarios en el directorio activo.

2.6. Herramientas

En el área de seguridad de la información se hace uso de una variedad de herramientas que permiten el monitoreo, gestión, administración y seguimiento de controles aplicados, entre las más destacadas se encuentran:

2.6.1. Symantec Endpoint Protection

Es una herramienta que proporciona una solución cliente servidor que protege dispositivos informáticos de punto final como equipos portátiles, equipos de escritorio y servidores en red, contra software maliciosos, vulnerabilidades, amenazas y riesgos. *Symantec Endpoint Protection* es capaz de ofrecer seguridad contra los ataques más

sofisticados, como los que evaden medidas de seguridad (Symantec Corporation, 2007). Utilizando tres capas de protección contra amenazas de red, protección proactiva contra amenazas conocidas y desconocidas, protección de antivirus y software espía (gusanos, troyanos, *keyloggers, botnets, adware*, *ransomware* entre otros).

Figura 5. Capas de protección de Symantec Endpoint Protection.

El objetivo principal de Symantec es la seguridad y defensa de los activos de información. En la figura 5, se pueden observar las capas de protección que brinda esta herramienta, en la capa superior se encuentra la protección contra amenazas de red, donde mediante el uso de normas y firmas se bloquea el acceso sospechoso al equipo. Se utiliza una inspección completa del estado de trafico de red, por medio de *firewall* que permite protocolos como TCP, UDP, ICMP y otros protocolos de IP. Además, reconoce el tráfico legítimo de DNS y DHCP automáticamente, con lo que prevé intrusiones configurando el tráfico de red indicado para clientes, por lo que solo es necesario crear una regla que admita este tráfico y su retorno será permitido e inspeccionado automáticamente (Symantec Corporation, 2007). Estos parámetros permiten la protección contra ataques de negación de servicio, desbordamiento de buffer, bloqueo automático de tráfico maliciosos entre otros.

La segunda capa brinda protección proactiva contra amenazas conocidas y desconocidas basándose en sus acciones y características, lo que permite esta capa es identificar amenazas, analizar su comportamiento y compararlo con módulos de detección que permiten determinar cuándo un proceso activo es seguro o malicioso.

En algunos sistemas operativos, permite controlar el acceso a los atributos de lectura, escritura y ejecución de archivos y claves de registro (Symantec Corporation, 2007).

Finalmente, la última capa se encarga de la protección contra software espía y la detección de todo tipo de *malware*, previniendo infecciones en los equipos de cómputo. Esto mediante un análisis en el arranque, memoria y archivos en busca de virus. *Symantec* incluye *Auto-Protect* que es capaz de detectar virus y riesgos a la seguridad del sistema cuando estos, intentan acceder de manera irregular a la memoria o instalarse (Symantec Corporation, 2007).

Las definiciones de virus permiten una rápida detección de estos y según su categoría los archivos infectados son puestos en cuarentena, reparados o quitados del sistema. Adicionalmente se incluye la protección de correo electrónico de internet, analizando los mensajes de entrada y salida en busca de amenazas y heurística conocida (Broadcom, 2020). En la figura 6, se muestra la interfaz del antivirus *Symantec Endpoint Protection* donde los usuarios pueden consultar el estado de protección de sus equipos de cómputo.

Figura 6. Interfaz de *Symantec Endpoint Protection.*

En la tabla 1 se definen las cuatro fases de protección contra ataques, de acuerdo con el enfoque de seguridad utilizado para proteger todo el entorno.

Tabla 1. Fases de protección contra ataques.

FASE		DESCRIPCIÓN	MEDIDAS DE PROTECCIÓN
1	*Intromisión*	La infiltración en la red de una organización está basada en ataques de ingeniería social, inyección de código SQL, software malicioso, vulnerabilidades de día cero entre otros.	• Uso de *firewall* que analice el tráfico de red, bloqueando amenazas antes de ser ejecutadas en el equipo. • Control de acceso a archivos y registros. • Restricción de carga y descarga de información.
2	*Infección*	Ataques dirigidos.	• Análisis de sitios web y archivos para detectar software malicioso a través del uso de los antivirus basados en firmas y heurística de archivos. • Ejecución de archivos sospechosos en máquinas virtuales para revelar amenazas automáticamente.
3	*Invasión y extracción*	Transferencia de datos confidenciales de manera no autorizada.	• Supervisión del comportamiento anormal de procesos o servicios. • Prevención de intrusiones.
4	*Reparación e inoculación*	Alternativas de protección en diferentes sistemas operativos y plataformas.	• Uso de herramientas como *Power eraser* para resolver amenazas avanzadas y reparar software de manera remota. • Integración de APIS con el fin de detener la propagación de infecciones. • *Symantec endpoint detection and response*, se encarga de responder y bloquear ataques dirigidos y asignar prioridad a ataques automáticamente.

Uno de los principales objetivos del área de seguridad de la información es garantizar la protección de los datos alojados en los equipos, por lo que una de las políticas de seguridad de la compañía prohíbe la conexión de dispositivos de almacenamiento masivo como: celulares, discos duros, memorias USB o cualquier otro dispositivo con la capacidad de extraer información de los equipos de cómputo.

La consola del antivirus *Symantec Endpoint Protection* permite recibir alertas de seguridad cuando un dispositivo es conectado a cualquiera de los equipos de la compañía. Adicionalmente proporciona información detallada del dispositivo que fue conectado. La tabla 2 es un claro ejemplo de la información obtenida en la consola de *Symantec Endpoint Protection* cuando un usuario conecta un dispositivo de

almacenamiento masivo a un equipo de la compañía. Se logra evidenciar la fecha y hora en la que ocurrió la conexión, el nombre y la IP del equipo que se vio involucrado, el nombre de usuario del propietario del activo y otro tipo de información que permite identificar la ubicación del dispositivo y el responsable directo del incidente.

Tabla 2 Datos visualizados en la consola (SEP) al conectar un dispositivo.

Dirección IP	Equipo	Tipo de Dispositivo	Usuario	Fecha	Hora	Ubicación
192.168.0.10	PC-G400	M1908C3JH-Android-V3.0	jmrozo	10/11/20	10:35:24	Área de S.I

2.6.2. Aranda Software

El software encargado de integrar un conjunto de herramientas que permitan la gestión de los activos de hardware y software, la asignación y conservación del software actualizado y licenciado (Aranda Software, 2020). Para evitar riesgos de seguridad en la compañía es: Aranda *Device Management* (Gestión de dispositivos Aranda), una *suite* integrada por cinco herramientas que son:

Aranda Asset Management o Gestión de activos Aranda (AAM)

Se encarga de integrar soluciones para efectuar inventarios actualizados del software y hardware de la compañía, proporcionando el acceso remoto en las estaciones de trabajo, evitando desplazamientos del personal de soporte técnico y ahorrando tiempos de restauración del sistema, mediante un único agente instalado que brinda información relevante de los activos gestionados (Aranda Software, 2017).

En la figura 7, se puede observar la interfaz de *Aranda asset management,* la cual permite controlar el licenciamiento y los niveles de uso de los recursos informáticos de la compañía en tiempo real.

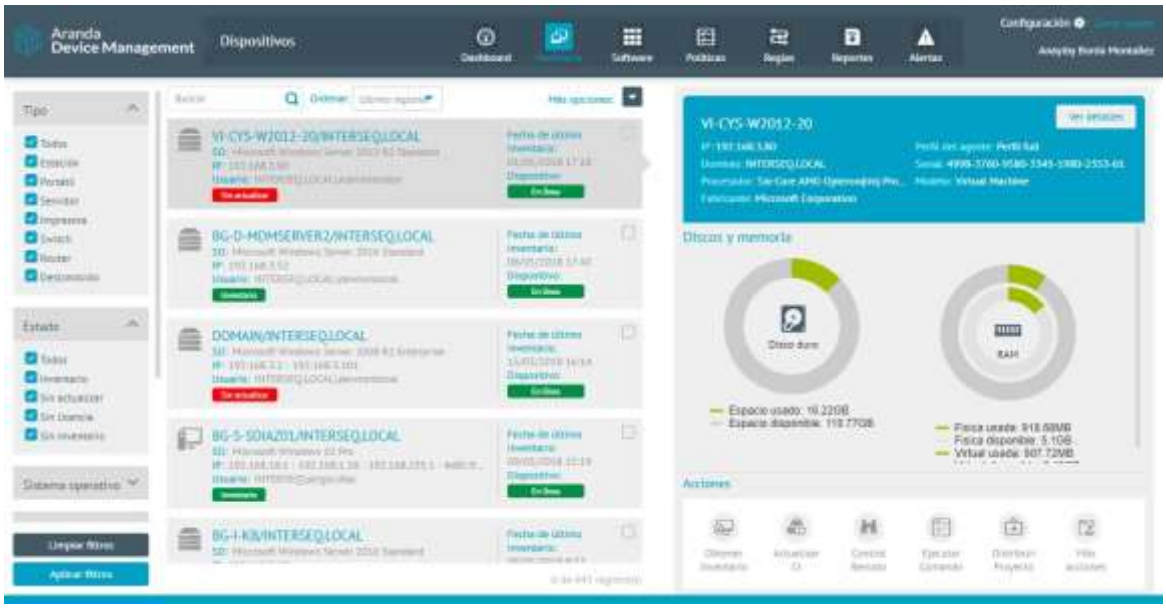


Figura 7. Interfaz de *Aranda Asset Management* (AAM).
Obtenido de arandasoft.com.

Aranda Software Delivery o Entrega de software Aranda (ASD)

Esta herramienta se destaca por permitir la distribución e instalación de software sin interrumpir la ejecución de las actividades laborales de los usuarios y posibilita la desinstalación de software no autorizado. Además, proporciona la planificación de distribución e instalación automática de aplicativos, mediante paquetes autoajustables y estandarizados, basándose en un catálogo con las ultimas actualizaciones de software del mercado (Aranda Software, 2017).

La figura 8, muestra la interfaz de *Aranda Software Delivery* que es capaz de distribuir la instalación de software y archivos sin interferir con el trabajo de los usuarios.

Figura 8. *Interfaz de* Aranda Software Delivery *(ASD).*
Obtenido de arandasoft.com.

Aranda Software Metrix o Software de Licenciamiento de Aranda (ASM)

Es la herramienta autorizada para administrar la instalación de licencias, basándose en el inventario de activos y determina el software que se encuentra licenciado y no licenciado, para posteriormente realizar las correcciones pertinentes. Además, permite auditar el nivel de uso del software por parte de los usuarios para mantener el control centralizado en los equipos de cómputo (Aranda Software, 2017).

En la figura 9, se presenta la interfaz de Aranda Software Metrix, la cual ofrece un diagnostico apropiado de los recursos tecnológicos de la compañía.

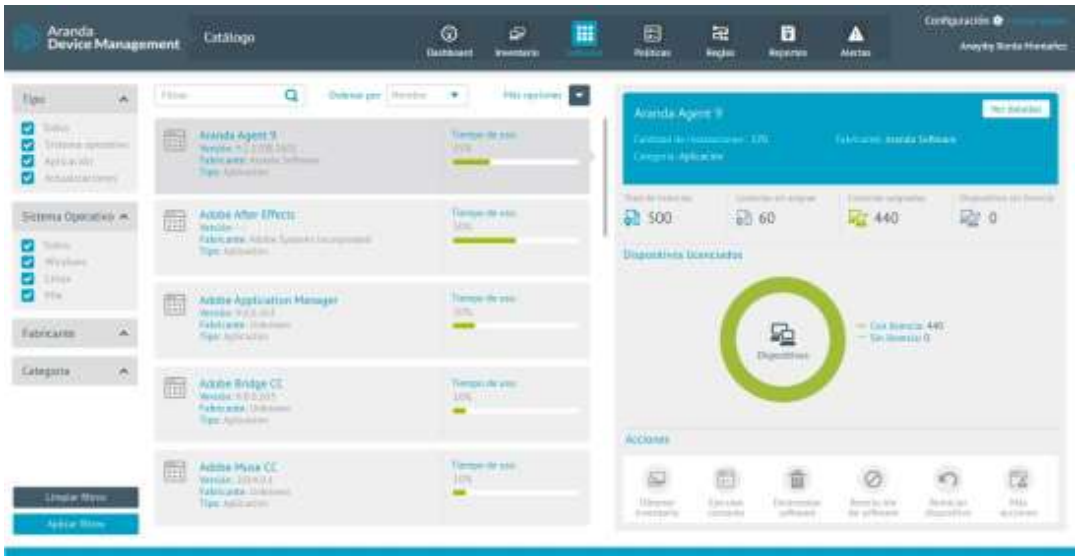


Figura 9. Interfaz de *Aranda Software Metrix (ASM).*
Obtenido de arandasoft.com.

Aranda Power Management o Gestión de energía de Aranda (APWM)

Es una solución para gestionar las políticas de energía en los equipos de la compañía, facilitando la optimización del consumo de energía y permitiendo disminuir los costos de operación y el impacto ambiental. En su interfaz gráfica, permite evidenciar los consumos de energía y dinero en tiempo real. De igual forma facilita el agendamiento de acciones para controlar el consumo de energía por medio de políticas centralizadas (Aranda Software, 2017).

En la figura 10 se puede observar la interfaz de *Aranda Power Management* que se encarga de administrar la gestión centralizada de las políticas de ahorro de energía de los equipos de cómputo.

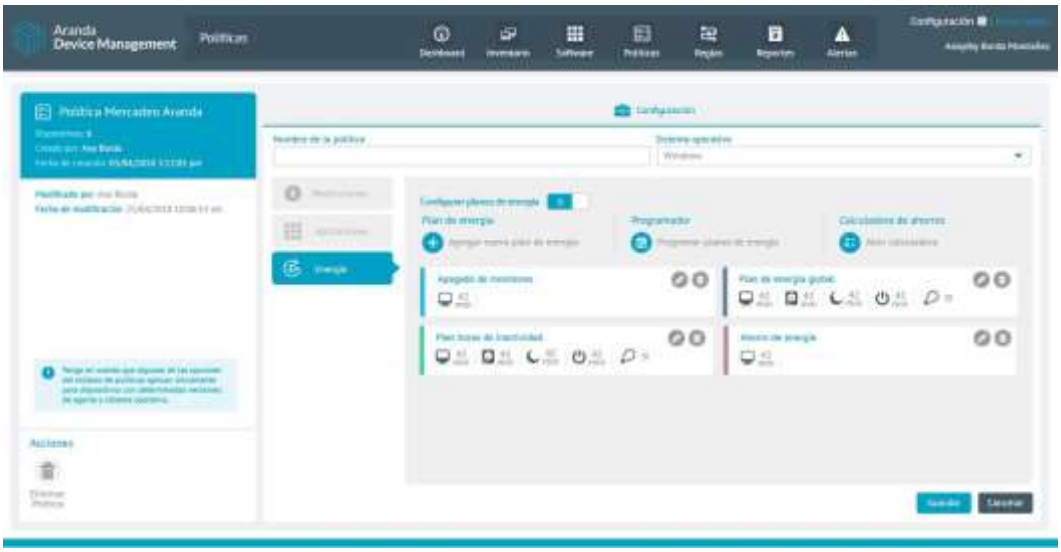


Figura 10. Interfaz de *Aranda Power Management (APWM).*
Obtenido de arandasoft.com.

Aranda Patch Management o Gestión de parches de Aranda (APM)

Todos los aplicativos necesitan ser actualizados constantemente y poseer los parches más recientes para evitar ataques externos. *Aranda Patch Management* brinda este servicio de seguridad, el cual realiza una programación automática para descargar las actualizaciones de software y mantener protegidos los equipos, eliminando riesgos y vulnerabilidades de seguridad en el sistema de las estaciones de trabajo (Aranda Software, 2017).

La figura 11, muestra la interfaz de *Aranda Patch Management*, cuya tarea principal es mantener actualizados todos los equipos de la compañía.

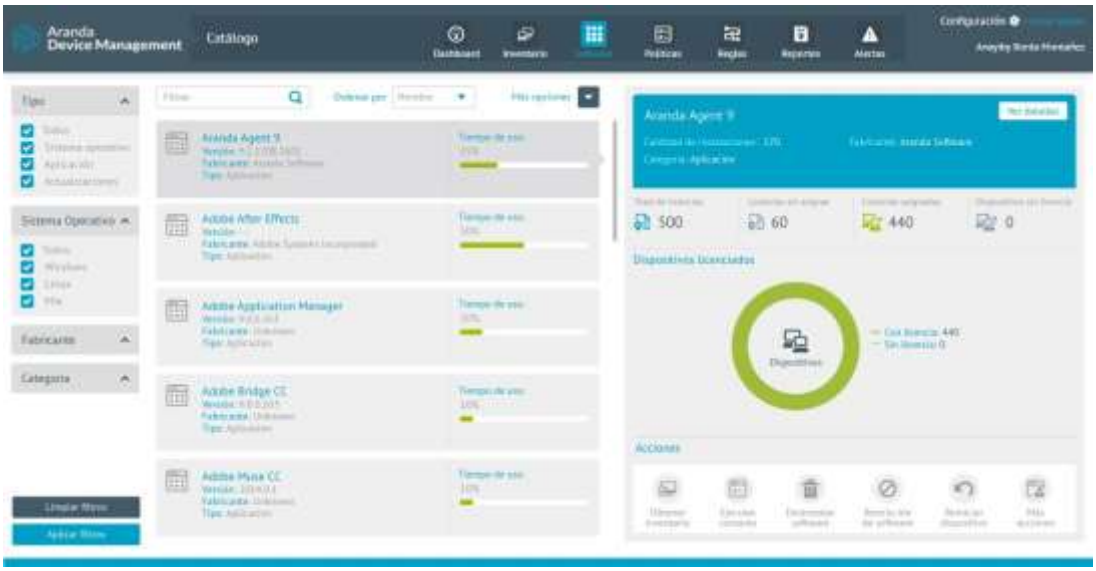


Figura 11. Interfaz de *Aranda Patch Management* (APM).
Obtenido de arandasoft.com.

Componentes y funcionalidades

- *Agente*: Es el encargado de recopilar y enviar toda la información de la estación de trabajo a la consola web. Además, es el encargado de ejecutar las acciones en los dispositivos.
- *Consola*: Es una interfaz en la cual se administra la información recopilada por el agente. Permite la administración remota y conocer el inventario de cada estación en detalle.
- *Base de datos:* Es el repositorio de almacenamiento de la información del inventario de las estaciones de trabajo y del sistema.
- *Conserver*: Es el módulo servidor que permite la comunicación entre los agentes y el servidor principal, según la topología usada se deberían instalar por cada segmento de red. Además, recolecta la información de los inventarios de software y hardware de cada estación de trabajo.
- *Repserver:* Es el nodo principal que comunica la base de datos y la consola web.
- *Cruncher:* Son los servicios encargados de procesar los inventarios de información de cada uno de los dispositivos.
    - *ArandaCruncherInventory:* Es el servicio encargado del inventario de software y hardware.
    - *ArandaCruncherEnergy:* Servicio para procesar los inventarios de energía.
    - *ArandaCruncherFile:* Encargado del inventario total e incremental de archivos.
    - *ArandaCruncherPatch:* Servicio para gestionar los inventarios de actualizaciones.

2.6.3. NETSCAN

SoftPerfect Network Scanner o “Software de escáner de red perfecto”, es una potente herramienta encargada de la administración y el mantenimiento de redes. Realiza escaneos IPV4 e IPV6 de manera eficiente y permite agilizar el soporte de red (SoftPerfect, 2020). Entre sus funciones más destacadas se encuentran:

1. Hacer barridos de ping y permitir visualizar los dispositivos conectados a la red en tiempo real.
2. Identificar direcciones IP y MAC.
3. Revelar las carpetas compartidas y ocultas.
4. Recuperar cuentas de usuario configuradas, tiempo de actividad, registro remoto y sistemas de archivos.
5. Permitir la conexión remota mediante comandos de SSH y PowerShell.
6. Admitir el apagado remoto y él envió de mensajes de red.
7. Soportar la exportación de resultados a formatos HTML, CVS, TXT Y JSON.
8. Integrado con herramientas como NMAP permite efectuar pruebas de vulnerabilidad.

Una de las políticas de seguridad de la información, es la prohibición de carpetas compartidas sin autorización y el almacenamiento de información sensible en las mismas. Debido a que cualquier persona que logre escanear la red podría tener acceso a los documentos alojados en dichas carpetas. Para ello se utiliza un escaneo de redes dividido en dos segmentos, donde se logran identificar los equipos y dispositivos conectados y si existen carpetas compartidas ilícitamente.

El resultado de los equipos escaneados en la red es comparado con una lista de IP de los servidores que son los únicos autorizados para compartir carpetas y se descartan del proceso.

Las IP que no coinciden con la lista anterior y contienen carpetas compartidas son registradas en una tabla que contiene la siguiente información:

- Dirección IP
- Nombre de Host
- Dirección Mac
- Nombre de la carpeta compartida
- Dirección de la carpeta compartida
- Observaciones

Adicionalmente al registro anterior, se anexan capturas de pantalla que dan evidencia del acceso a las carpetas compartidas y con toda la información se tramita una solicitud tipo requerimiento al área de tecnología, que se encarga de modificar los permisos de las carpetas para descompartirlas.

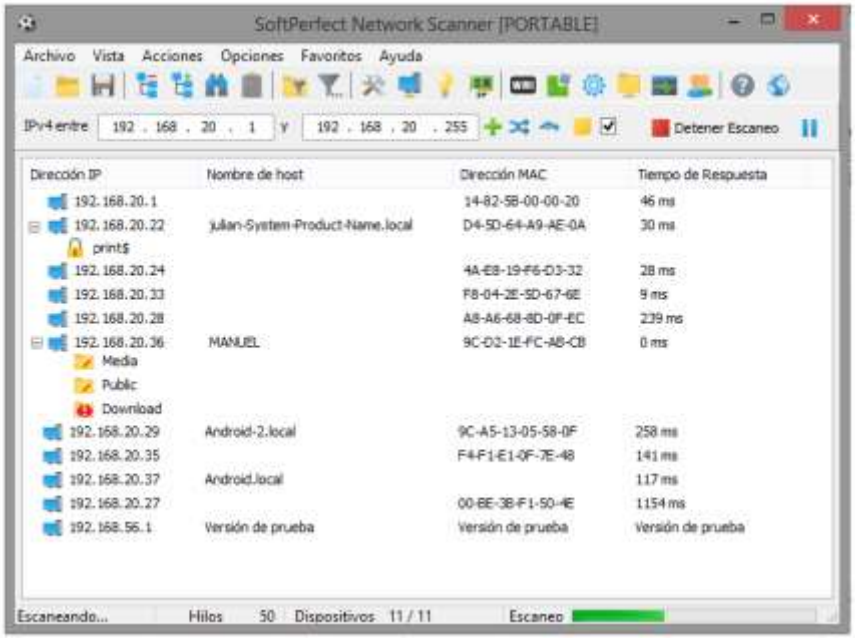


Figura 12. Ventana Principal de la herramienta NETSCAN.

En la figura 12, se observa un ejemplo de un escaneo de red, donde se utiliza el segmento de red (192.168.20.1 - 192.168.20.255). El escaneo arroja once dispositivos conectados a la red, donde dos de ellos tienen habilitadas carpetas compartidas.

El primero de dirección IP 192.168.20.22 cuenta con la carpeta “Print$’, la cual corresponde a una impresora común. El segundo de dirección IP 192.168.20.36 cuenta con diferentes carpetas compartidas, entre ellas una con un símbolo de advertencia, la carpeta “*Download*”, por lo que se debe restringir el acceso a este tipo de carpetas que colocan en riesgo la información sensible que pueda contener.

2.6.4. NEXAPLUS

En NEXA BPO, la innovación tecnología es fundamental, por ello se desarrolló VYSPlus ahora NEXAPLUS, una plataforma multifuncional que automatiza la administración de las bases de datos de clientes y la evolución de sus procesos. Además, estandariza los procesos, control y gestión de las diferentes operaciones de

servicio, venta, cobranza y BPO (*business process outsourcing o externalización de procesos de negocio)*. Esta solución tecnológica cuenta con herramientas fundamentales para cada área de servicio.

Para seguridad de la información, la plataforma NEXAPLUS es esencial al momento de gestionar la creación, seguimiento o cancelación de solicitudes, requerimientos o incidentes. Dependiendo de la naturaleza de la petición, se brinda una solución si pertenece al área de seguridad de la información o en su defecto se escala el proceso al área o dependencia correspondiente.

Figura 13. Interfaz para solicitudes de la plataforma NEXAPLUS.

En la figura 13, se muestra la interfaz de NEXAPLUS para realizar el proceso de creación o consulta de solicitudes (requerimientos o incidentes). Para crear una solicitud nueva se deben proporcionar una serie de datos que incluyen:

- Nombre del solicitante
- Cargo actual
- Código asignado
- Área y proceso perteneciente
- Correo empresarial
- Extensión telefónica
- Ubicación (Sede)
- Tipo de requerimiento solicitado
- Descripción de la solicitud
- Anexos (Si se requiere)

Finalmente, al terminar de diligenciar los datos anteriores, se genera un ID con el número del caso. Ver figura 14, con el cual se puede consultar el estado de la solicitud, donde se pueden presentan cuatro estados:

1. *En Proceso:* La solicitud se encuentra en curso o se reasigno al área correspondiente.
2. *Resuelto:* Se brindo una solución al requerimiento.
3. *Finalizado*: No se dio solución al caso y expiro por su fecha límite.
4. *Cancelado*: La solicitud es anulada por su creador.

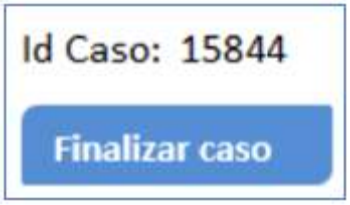


Figura 14. Ejemplo de un ID generado al solicitar un requerimiento.

Adicionalmente se pueden presentar tres novedades que son:

1. Reabrir un incidente, en cuyo caso se debe hacer máximo 1 día después de que se presente el cierre.
2. Para reabrir un requerimiento, se debe hacer máximo 3 días después de su cierre.
3. Cancelar una solicitud, lo debe hacer el solicitante o creador directamente desde el aplicativo.

3. Marco de referencia

Para la implementación del proyecto de actualización de riesgos asociados a la seguridad de la información es necesario adquirir el conocimiento básico del modelo de SGSI y del campo de seguridad de la información, los cuales describen conceptos generales y facilitan el proceso de comprensión e interpretación del lector hacia el enfoque del proyecto. Además de tener en cuenta los estándares normativos vigentes para la elaboración de etapas a través de metodologías establecidas por especialistas en el tema.

3.1. Marco conceptual

A continuación, se describen los conceptos que darán el enfoque al campo de seguridad de la información, considerando los fundamentos y estructura que componen el modelo SGSI, seguido de la normatividad legal vigente que proporciona los estándares utilizados en el desarrollo del documento respecto a la ISO.

Seguridad de la información:

Se entiende como el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. Dicho de otro modo, son todas aquellas políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización.

La seguridad de la información es una pieza fundamental para que la empresa pueda llevar a cabo sus operaciones sin asumir demasiados riesgos, puesto que los datos que se manejan son esenciales para el devenir del negocio. Además, también hay que tener en cuenta que la seguridad de la información debe hacer frente a los riesgos, analizarlos, prevenirlos y encontrar soluciones rápidas para eliminarlos si se diera el caso (Tecon, 2019).

Sistema de Gestión de Seguridad de la Información (SGSI):

Es el concepto central sobre el que se construye ISO 27000. De acuerdo con la norma la seguridad de la información consiste en la preservación de la confidencialidad, integridad y disponibilidad, bajo estos tres términos se realiza el análisis y evaluación de los activos de información (riesgoscero, 2020).

Este concepto se encuentra enfocado en cuatro fundamentos (riesgoscero, 2020):

1. Disponibilidad: Tener acceso a la información necesaria. En este punto es importante evitar que el sistema tenga problemas o que algún ente externo intente acceder de manera ilícita a los programadores de la compañía.
2. Confidencialidad: Información que solo está disponible para el personal autorizado, por ende, esta no debe ser distribuida por terceros.

3. Integridad: La información que está registrada debe ser la correcta y no contar con errores o algún tipo de modificaciones. Esto se hace con el fin de evitar amenazas externas o errores humanos.
4. Autenticación: Esta información la brinda directamente un usuario y se debe validar que los datos otorgados son los correctos.

Un SGSI es un instrumento de gran ayuda para cumplir con la legalidad y la protección de los datos, pues este permite que se definan los procedimientos y controles que se llevarán a cabo para mantener los datos blindados. Además, permite que se establezcan las políticas que se le darán a conocer a todos los miembros de la organización y saber a profundidad cuáles son los riesgos que pueden sufrir y de qué manera pueden mitigarlos (riesgoscero, 2020).

El SGSI debe incluir los siguientes parámetros:

Manual de seguridad: Este es el documento el cual contiene la guía de cómo se debe implementar y seguir el sistema de gestión de seguridad de la información. Allí se va a radicar toda la información como objetivos, alcance, responsables, políticas, directrices, entre otras actividades que se decidan llevar a cabo.

Procedimientos: Estos van relacionados a las actividades operativas, ya que estos serán los encargados de dar los parámetros que se deben seguir para que la gestión sea eficaz, la planificación, la operación y el control sean los adecuados en los procesos de seguridad de la información.

Instrucciones: Es la descripción de lo que se debe hacer paso a paso, cuáles son las tareas y actividades que se deben cumplir para que la gestión sea eficiente.

Registros: Es la evidencia de la información que ha sido documentada a lo largo de la gestión, para verificar que se estén cumpliendo con los objetivos propuestos. (riesgoscero, 2020)

ISO 27001

La norma ISO 27001 es una solución de mejora continua en base a la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros.

Por otro lado, también permite establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros.

Como ocurre con todas las normas ISO, la 27001 es un sistema basado en enfoque basado en el ciclo de mejora continua o de *Deming*. Dicho ciclo consiste, como ya sabemos, en Planificar-Hacer-Verificar-Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés *Plan-Do-Check-Act*). (ISOTools, 2020)

ISO 27005

La norma ISO 27005 es el estándar internacional que se ocupa de la gestión de los riesgos relativos a la seguridad de información. La norma suministra las directrices para la gestión de riesgos, apoyándose fundamentalmente en los requisitos sobre esta cuestión definidos en la ISO 27001.

Se trata de una norma aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización y sustituye a las normas ISO / IEC TR 13335-3:1998 e ISO / IEC TR 13335-4:2000 de Gestión de la Información y Comunicaciones Tecnología de Seguridad.

El aumento en el uso de tecnologías de la información puede posibilitar brechas o fisuras en aspectos de seguridad con respecto a su utilización, por ello se hace necesaria una gestión de la información desde una perspectiva tecnológica a tres niveles: aseguramiento y control sobre la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano) desde la perspectiva tecnológica. (ISOTools, 2015)

ISO 31000

La norma ISO 31000 es una herramienta que establece una serie de principios para la implementación de un Sistema de Gestión de Riesgos en las empresas, puede aplicarse a cualquier tipo de organización independiente de su tamaño, razón social, mercado, fuente de capital, espectro comercial o forma de financiación. No especifica ningún área o sector en concreto.

La norma parte del hecho de que todas las empresas, en mayor o menor medida, llevan a cabo prácticas para la gestión de los riesgos. La diferencia radica en la coordinación y alineamiento de dichas prácticas.

Aunque no es certificable, el estándar busca minimizar, gestionar y controlar cualquier tipo de riesgo, más allá de su naturaleza, causa, origen o grado de incidencia. Esto se logra a través de la integración del Sistema de Gestión de Riesgos a la estrategia de cada organización, así como a sus procesos, políticas y cultura. De hecho, no es una norma pensada para circunstancias concretas, sino que busca una aplicación continua y permanente en el tiempo. De esta manera, beneficia el grueso de las acciones, decisiones, operaciones, procesos, funciones, proyectos, servicios y activos que tengan lugar en las empresas. (ISOTools, 2020)

3.2. Marco legal

La normatividad en materia de seguridad de la información es amplia debido a que abarca leyes, políticas, decretos y resoluciones, entre otros, tendientes a su reglamentación en el estado Colombiano. Como soporte para la realización del proyecto de pasantía en Nexa BPO la Constitución Política de Colombia 1991 en su Artículo 15 (CONSTITUCIÓN POLITICA DE LA REPÚBLICA DE COLOMBIA [Const].Art.15, 1991). Reconoce como Derecho Fundamental el Habeas Data fortalecido por la Ley 1266 de 2008, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales (LEY ESTATUTARIA 1266, 2008).

En Nexa BPO la seguridad de la información también abarca el control interno de la empresa reglamentado con la Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes (LEY 87, 1993).

En materia disciplinaria la compañía se apoya en el Código Penal Colombiano reglamentado en el Decreto 599 de 2000 específicamente en el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones" (LEY 599 , 2000).

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes. El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del 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" (LEY 1273, 2009).

De igual manera, es necesaria la protección de información personal en la empresa Nexa BPO para ello se reglamenta la Ley 1581 de 2012 , por la cual se dictan disposiciones generales para la protección de datos personales. Aquellas actividades que se inscriben en el marco de la vida privada o familiar de las personas naturales (LEY ESTATUTARIA 1581, 2012).

En el desarrollo de la pasantía es necesaria la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, según la ISO 27001, que tiene por objeto proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en el mapa de procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las TIC, a través de políticas y programas, para mejorar la calidad de vida de cada colombiano y el incremento sostenible del desarrollo del país, en general, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

La ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

En la familia de las ISO también cabe señalar la norma ISO 31000 utilizada como una guía para la gestión de riesgos. Es una norma de aplicación internacional y voluntaria. Según estadísticas, Colombia es uno de los países que más se preocupa por la gestión de riesgos y que, entre otras herramientas, hace uso de la norma ISO 31000. El éxito de la gestión de riesgos va a depender de la eficacia de la herramienta que una organización utilice. ISO 31000 ayuda a la gestión de riesgos de forma efectiva mediante la aplicación del proceso de gestión de riesgos que propone en todos los niveles y contextos de la organización. La información que se recoge del proceso de gestión de riesgos debe ser la base de la toma de decisiones y rendición de cuentas en todos los niveles de la organización.

La norma ISO 31000 no establece un sistema de gestión para ello está la ISO 27001 especificada anteriormente; Sin embargo, dicha norma sirve para ayudar a la organización a integrar la gestión de riesgos en su sistema de gestión global; Nexa BPO adapta los componentes de esta norma a sus necesidades particulares. La ISO 31000 que busca ayudar a manejar la incertidumbre que se presenta en cada decisión de una organización hace frente al riesgo, en parte de la gobernanza y el liderazgo, y es fundamental para la gestión de una organización en todos los niveles.

4. Plan de trabajo

Para el desarrollo del plan de trabajo se plantearon cuatro etapas comenzando por la identificación y clasificación de activos de la compañía. Seguido de una breve introducción a los componentes y procesos de la gestión del riesgo en la seguridad de la información. Luego se hace énfasis en el análisis y valoración de riesgos identificados, para finalmente concluir con las opciones y controles que facilitan el correcto tratamiento de riesgos.

4.1. Activos

Los activos son todos aquellos bienes, recursos, derechos y valores con los que cuenta una empresa, es decir, todo aquello que suma a su favor (OBS, 2020). Para NEXA BPO los activos son una pieza fundamental, por ello se deben identificar ,valorar y clasificar para facilitar su gestión dentro de la compañía. Es importante saber que se posee ,para saber que se protege.

4.1.1. Identificación de activos

Las compañías poseen información que debe ser protegida ante posibles riesgos y amenazas para lograr mantener la continuidad del negocio. Por lo que se debe contar con un robusto sistema de gestión de seguridad de la información que tiene como objetivo la protección del activo más esencial de una organización denominado información.

Como primera medida se deben definir los activos de información con los que cuenta la compañía para lograr determinar su respectiva clasificación y valoración frente a los criterios de los pilares de la seguridad de la información (Integridad, confidencialidad y disponibilidad). Según la norma ISO/IEC 27001:2013 se define un activo como todo aquello que tiene algún valor para la entidad y que, por lo tanto, requiere de protección.

Para la compañía NEXA BPO uno de sus activos más valiosos es la información, la cual se divide en dos tipos:

- Información digital
- Información física

Se considera como información digital a toda aquella información que es almacenada o transmitida usando unos y ceros, es decir, empleando el sistema binario.

(documentos digitales, archivos, imágenes, bases de datos, bitácoras, correos electrónicos, etc.).

La información física es de tipo impresa y palpable (informes impresos, libros de contabilidad, solicitudes, contratos, cartas, recibos, archivadores, etc.). Otros activos de la compañía son:

- El software y hardware que se utiliza para realizar el procesamiento, transporte y almacenamiento de la información corporativa.
- Software (aplicaciones de Microsoft office como Word, Excel y Outlook, Adobe, Google, antivirus, herramientas de desarrollo, aplicativos, interfaces, etc.).
- Hardware (computadores, laptops, celulares, discos duros, memorias USB, modem, Router, impresoras, entre otros).
- Los servicios utilizados para realizar el control de la información, tanto en su transmisión como en su recepción.
- Las personas o recursos humanos, encargadas de manejar los datos, servicios o un conocimiento especifico primordial para la compañía.

Además, es necesario identificar como estos activos deben ser gestionados y administrados para lograr establecer los controles de protección, los responsables directos y el nivel de compromiso que tiene la compañía con la seguridad de la información de sus trabajadores, clientes y proveedores.

La correcta identificación de activos debe proporcionar la información suficiente para la evaluación de riesgos asociados a cada caso, para ello se hace uso de un inventario de activos que debe incluir al menos, la identificación del activo, descripción, localización y responsable o propietario.

Nota: La información cuantitativa de los activos se mantiene confidencial de acuerdo con las políticas de seguridad y privacidad de datos corporativos de NEXA BPO.

4.1.2. Propiedad de los activos

Todos los activos identificados anteriormente deben tener designado un propietario dentro de la compañía, puede ser una entidad, un cargo, proceso o un grupo de trabajo, el cual tiene como responsabilidad definir y garantizar los controles adecuados para clasificar apropiadamente los activos y la información asociada al mismo. Revisando periódicamente las restricciones y distribución de acceso de acuerdo con las políticas aplicables para velar por la protección del activo.

4.1.3. Clasificación de activos

Una vez realizada la correcta identificación de activos, se debe hacer la clasificación de la información siguiendo los lineamientos establecidos por la compañía, cuyas bases son las características principales de la información: confidencialidad, integridad y disponibilidad como fundamento para el tratamiento de datos. Además del requerimiento legal, criticidad, valor, modificación y divulgación.

Se definen tres niveles que permiten determinar la prioridad del activo:

1. Alto: Cuando el activo de información está clasificado en nivel alto en dos o tres pilares (confidencialidad, integridad y disponibilidad). Este tipo de información es sensible y de carácter restringido y confidencial, por lo que es conocida por un número limitado de personas y su divulgación está reservada y protegida para salvaguardar los intereses de la compañía.

2. Medio: Cuando el activo de información está clasificado en nivel medio o alto para uno de los tres pilares de la información. Esta información es conocida por un grupo específico de personas dentro de la organización y es usada con fines comerciales.

3. Bajo: La clasificación del activo de información es bajo en todos sus niveles. Es de carácter no sensible por lo que su divulgación no es perjudicial para la organización y es conocida tanto por personal interno como externo.

En la tabla 3, se muestra un ejemplo para la clasificación de activos según las condiciones anteriormente nombradas.

Tabla 3. Demostración de la clasificación de activos de información.

Activos	Confidencialidad			Integridad			Disponibilidad			Clasificación
	A	M	B	A	M	B	A	M	B	
Activo 1	X			X				X		Alto
Activo 2	X				X				X	Medio
Activo 3			X			X			X	Bajo

Este nivel de clasificación es definido por el propietario del activo, pero no implica que necesariamente sea quien lo gestione. Una vez identificados y clasificados todos los activos se debe realizar un análisis de dependencias, es decir, un árbol de dependencias de activos donde se pueda observar la relación entre los diferentes

activos dentro de la organización desde los de más alto nivel hasta los de más bajos nivel. Además, se debe realizar una valoración de los activos de acuerdo con su relevancia dentro de la organización y el impacto que pueda presentar si se ve comprometido.

El formato ***Estándar de identificación de activos (ANEXO_4)*** contiene un modelo de la información básica para el registro de los diferentes activos de una organización, conformado por las siguientes pautas:

- Id/Serial*:* Es un código único que permite la identificación del activo en un inventario.
- Proceso: Denominación del proceso al cual corresponde el activo.
- Nombre del Activo: Nombre con el que se identifica el activo en la organización.
- Descripción: Reseña breve y clara que permite reconocer el activo por cualquier miembro.
- Tipo: Determina a qué clase de activo pertenece, entre los siguientes:
    - Información: Datos de información de tipo física o digital.
    - Software: Sistemas, aplicaciones, interfaces y herramientas asociadas.
    - Hardware: Dispositivos electrónicos de comunicaciones, equipos de cómputo entre otros.
    - Servicio: Internet, directorios, repositorios, suscripciones, etc.
    - Recursos Humanos: Personas con conocimientos o experiencia fundamental para la continuidad del negocio.
    - Otro: Activos no categorizados, pero obligatoriamente valorados para comprender su criticidad.
- Ubicación: Especifica la ubicación física y electrónica del activo.
- Clasificación: Determina el nivel de protección del activo, basado en los pilares de la seguridad de la información (integridad, confidencialidad y disponibilidad).
    - Alta: El activo de información está clasificado en nivel alto en dos o tres pilares de la información.
    - Media: El activo de información está clasificado en nivel medio o alto para uno de los tres pilares de la información
    - Baja: El activo de información es bajo en todos sus tres niveles.
- Justificación: Describe brevemente el motivo de clasificación del activo.
- Criticidad: Precisa el valor general del activo, según su clasificación.
    - Alta: Información restringida o confidencial.
    - Media: Información sensible y de conocimiento limitado de personas.
    - Baja: Información no sensible y de libre publicación.

- Propietario: Persona, entidad, proceso o grupo encargado de garantizar la protección del activo.
- Custodio: Persona, entidad, proceso o grupo encargado de hacer efectivos los controles de restricción y clasificación, establecidos por el propietario para el acceso al activo.
- Usuario: Nombre de usuario asignado para acceder a los sistemas de la compañía.
- Fecha de ingreso: Establece el tiempo en el que se ingresó el activo al inventario.
- Fecha de salida: Establece el periodo de exclusión del activo en el inventario.

El registro de activos de información es un documento de clasificación “confidencial”, por lo que solo puede ser manipulado por el líder del proceso con aprobación del CISO (*Chief Information Security Officer* u oficial principal de seguridad de la información).

4.1.4. Etiquetado de activos de información

Después de la clasificación de activos, el propietario del activo debe desarrollar e implementar un conjunto de procedimientos para etiquetar la información de forma adecuada basados en el esquema de clasificación adoptado por la organización.

Algunas pautas que se deben tener en cuenta son:

- Se deben etiquetar los activos de información clasificados bajo los tres pilares de la información: (Integridad, Confidencialidad y Disponibilidad) en relación con el nivel de clasificación obtenido.

- Las etiquetas para los activos de información clasificados en integridad son:

Tabla 4. Clasificación por criterios de integridad.

Clasificación	Etiqueta
Alta	A
Media	M
Baja	B

- Las etiquetas para los activos de información clasificados en disponibilidad son:

Tabla 5. Clasificación por criterios de disponibilidad.

Clasificación	Etiqueta
Alta	**1**
Media	**2**
Baja	**3**

- Las etiquetas de los activos de información clasificados de acuerdo con la confidencialidad son:

Tabla 6. Clasificación por criterios de confidencialidad.

Clasificación	Etiqueta
Alta	IPR
Media	IPC
Baja	IPB

Donde:

- IPR: Información Publica Reservada.
- IPC: Información Publica Clasificada.
- IPB: Información Pública.

- Cuando un activo de información no cuenta con etiqueta, debe ser empleado en todos los niveles como: Integridad (A), confidencialidad (IPR) y disponibilidad (3) y debe ser incluido en el inventario como un activo NO CLASIFICADO.

En la figura 15 se logra apreciar un ejemplo para etiquetar activos de información física, como lo son los documentos en papel; Estos documentos contienen una etiqueta en la parte superior derecha de la carpeta contenedora y un sello o cinta de seguridad en la portada del archivo y cada página posterior.

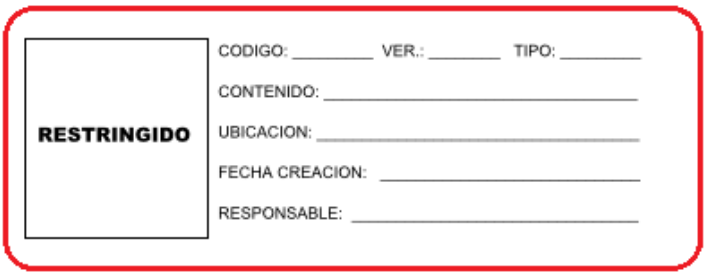


Figura 15. Estampilla de seguridad para archivos restringidos.

En la figura 16 se puede observar una de las formas de etiquetar los activos de información digital como los correos electrónicos provenientes de la compañía, donde se utiliza una firma digital y un formato de texto que contiene los parámetros de confidencialidad de la información recibida.

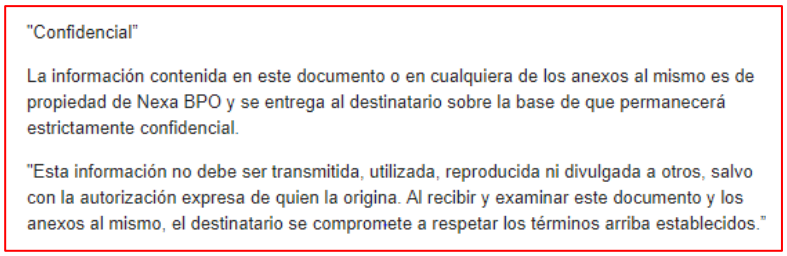


Figura 16. Etiqueta de confidencialidad de correos electrónicos.

4.2. Principios y directrices

La norma ISO 31000 sirve de referencia para otros estándares sobre Gestión de Riesgos. Además, complementa la información de diversas normativas en el plano local, regional, nacional o incluso continental. En este primer apartado, se explica no sólo el alcance de la misma, sino que se detallan las prácticas básicas que debe tener en cuenta cualquier organización dispuesta a implementar un Sistema de Gestión de Riesgos (ISOTools, 2020). Los 11 principios expuestos son:

- La gestión crea valor a la organización.
- Debe estar integrada a los procesos.
- Forma parte de la toma de decisiones en la empresa.
- Trata de forma explícita la incertidumbre.
- Debe ser sistemática, estructurada y adecuada.
- Es necesario que esté basada en la mejor información disponible.
- Debe adaptarse a la medida de cada caso.
- Implica la inclusión de factores humanos y culturales.
- Debe ser transparente, eficaz e inclusiva.
- Es necesario que sea iterativa y sensible al cambio.
- Tiene que ir orientada a la mejora continua de la organización.

4.3. Marco de referencia

El éxito de la gestión del riesgo dependerá de la eficacia del marco de referencia para la gestión, el cual brinda las bases y las disposiciones que se introducirán en todos los niveles de la organización. El marco ayuda a la gestión eficaz del riesgo a través de la aplicación del proceso para la gestión del riesgo en los diversos niveles y en contextos específicos de la organización. El marco garantiza que la información acerca del riesgo

derivada del proceso para la gestión del riesgo se reporte de manera adecuada y se utilice como base para la toma de decisiones y la rendición de cuentas en todos los niveles pertinentes de la organización.

Este marco de referencia no tiene como finalidad prescribir un sistema de gestión sino facilitar a la organización la integración de la gestión del riesgo en su sistema de gestión global. Por lo tanto, las organizaciones deberían adaptar los componentes del marco a sus necesidades específicas.

Si las prácticas y procesos de gestión existentes de la organización incluyen componentes de la gestión del riesgo, o si la organización ya ha adoptado un proceso formal para la gestión del riesgo para tipos particulares de riesgos o situaciones, entonces éstos se deberían revisar y valorar de forma crítica frente a esta norma, incluyendo los atributos del Anexo A, con el fin de determinar su eficacia y conveniencia. (ISO 31000: 2018 Gestión de riesgos: Principios y directrices, 2018)

4.4. Gestión del riesgo

La gestión de riesgos de seguridad de la información es el procedimiento encargado de identificar, analizar, evaluar, controlar, minimizar, mitigar o eliminar los diferentes riesgos a los que se ven expuestos los activos de información de las organizaciones, reduciendo así el impacto negativo sobre las mismas.

4.4.1. Componentes del riesgo de seguridad de la información

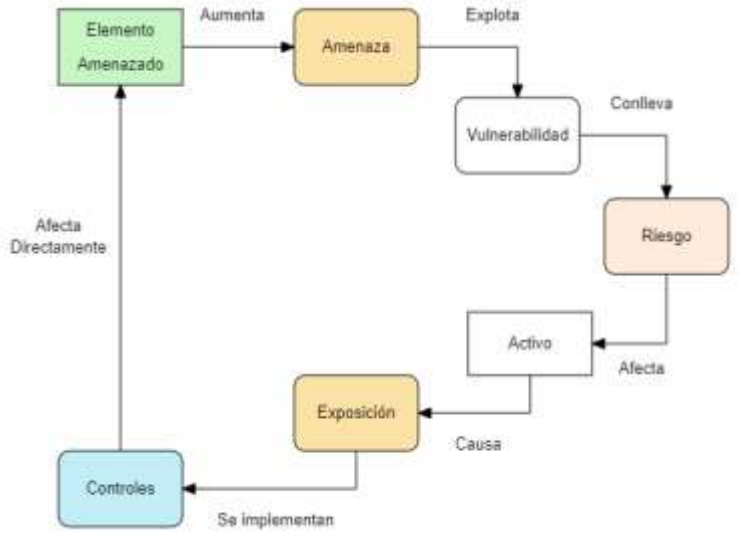


Figura 17. Cadena de detección y tratamiento de amenazas.

En la figura 17 se pueden observar algunos de los componentes más importantes del riesgo de seguridad de la información, como:

- Amenazas: Es cualquier daño potencial en los sistemas o información que se puede derivar en un incidente, ocasionando afectaciones materiales o inmateriales en los activos.
- Vulnerabilidad: Es toda aquella debilidad en el software, hardware o procedimiento que pueden ser aprovechadas por una amenaza.
- Riesgo: Es la probabilidad de que un componente de la amenaza tome ventajas de una vulnerabilidad y genere una exposición de un activo con impacto negativo en el negocio.
- Activos: Es todo aquel componente que posee un valor para la organización.
- Exposición: Son las consecuencias de la materialización de una amenaza sobre un activo.
- Controles: Es la contra medida para reducir o mitigar el riesgo potencial.

4.4.2. Proceso de gestión del riesgo en seguridad de la información

Basados en la norma técnica colombiana NTC-ISO/IEC 27005, la cual provee las directrices para una adecuada gestión del riesgo en la seguridad de la información en una organización en su totalidad o en una parte separada como un servicio o departamento en particular, se establecen algunos lineamientos y actividades para llevar acabo el correcto proceso de gestión del riesgo en la seguridad de la información brindando soporte a la relación con la norma NTC-ISO/IEC 27001:2013 en los SGSI implementados en la compañía.

La norma NTC ISO/IEC 27005 permitió la mejora de la gestión interna, brindando una mayor eficiencia en los procesos de la compañía como una herramienta de medición de resultados y favoreciendo la toma de decisiones. Además de facilitar la integración de sistemas de gestión de calidad. Finalmente presenta un mayor entendimiento del modelo PHVA (Planificar, Hacer, Verificar ,Actuar), cuya finalidad es establecer un proceso de gestión con enfoque en la mejora continua del negocio. Este esquema comprende:

- Planificar: Conseguir resultados acordes a las políticas y objetivos de la organización.
- Hacer: Implementación y operación de controles, procesos y procedimientos.
- Verificar: Evaluar y medir el desempeño de los procesos y objetivos de seguridad.
- Actuar: Establecer políticas de gestión de riesgos e implementar cambios para mejorar los procesos.

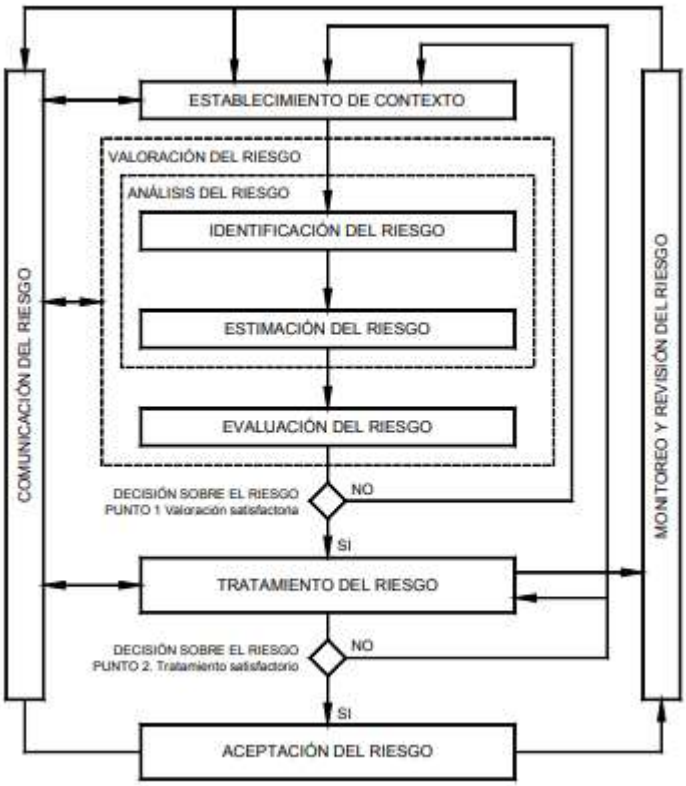


Figura 18. Proceso de gestión del riesgo en la seguridad de la información. Obtenido de NTC-ISO/IEC 27005.

Como se observa en la Figura 18, el proceso de gestión del riesgo en la seguridad de la información comienza con el establecimiento del contexto donde se reúne toda la información pertinente de la compañía y se especifican los criterios básicos, sus alcances, limitaciones y la organización para la gestión del riesgo en la seguridad de la información. Posteriormente se realiza la valoración del riesgo donde se suministra información específica para identificar, estimar y evaluar el riesgo, si la información suministrada es determinante se establecen las acciones pertinentes y sigue el tratamiento del riesgo, pero si la información no es la adecuada se realiza otra valoración del riesgo desde otro contexto (véase la Figura 18, Decisión Sobre El Riesgo, Punto 1 -Valoración satisfactoria). El correcto tratamiento del riesgo se encuentra ligado a los resultados de la valoración anterior, por lo que se puede tratar directamente o si es necesario, volver a valorar el riesgo desde otro contexto (véase la Figura 18, Decisión Sobre El Riesgo, Punto 2-Tratamiento satisfactorio). Finalmente, la actividad de aceptación del riesgo debe ser conocida por los directores de la entidad y el personal operativo correspondiente, para lograr implementar los controles o medidas necesarias para reducir el daño potencial (Norma ISO 27005, 2018).

4.5. Análisis y valoración de riesgos

El análisis de riesgos es el primer paso de la gestión de riesgos, debido a que tiene como objetivo principal determinar los componentes del sistema que necesitan protección, sus posibles vulnerabilidades y las amenazas a los que se encuentran expuestos. Además, permite identificar el impacto y la probabilidad realista de un fallo de seguridad, donde se vea comprometida la confidencialidad, integridad y disponibilidad de la información.

Basados en la metodología MAGERIT (Metodología de análisis y gestión de los sistemas de información) se establecen 5 pasos para realizar un correcto análisis de riesgos (MAGERIT v3.0, 2012).

1. Definir y valorar los activos más relevantes para la organización.
2. Establecer las amenazas a los que se ven expuestos los activos.
3. Determinar las estrategias y mecanismos dispuestos para afrontar el riesgo.
4. Evaluar la magnitud del impacto derivado de una amenaza que se materializa.
5. Estimar el riesgo, basados en el impacto y la expectativa de materialización de la amenaza.

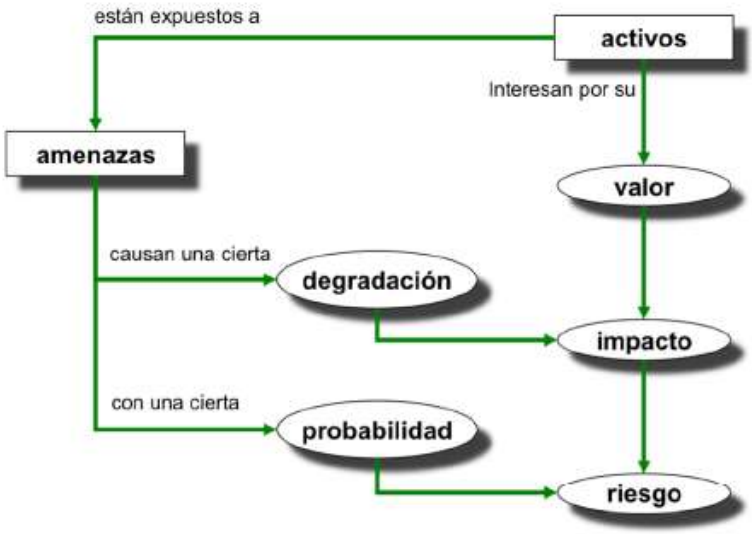


Figura 19. Elementos del análisis de riesgos potenciales.
Obtenido de MAGERIT-Versión 3.0.

La figura 19 muestra el análisis de riesgos potenciales en los que se pueden ver comprometidos los activos de la compañía. El mayor interés de un atacante es la obtención de información que contenga un alto valor para la compañía, lo que genera

que constantemente se encuentren expuestos a amenazas tanto internas como externas. Para impedir que estas amenazas se materialicen existen diferentes tipos de salvaguardas encargados de detectar e impedir que la amenaza se materialice completamente, reduciendo el impacto negativo y la probabilidad de riesgo.

Metodologías practicas

Magerit

Se trata de una metodología de análisis y gestión de riesgos que ha sido elaborada por el Consejo Superior de Administración. Está específicamente diseñada para las compañías que trabajen con información digital y servicios de tipo informático. Su función principal es evaluar cuánto valor pone en juego una compañía en un proceso y cómo protegerlo. También ayuda a la planificación de tratamientos oportunos y a preparar a las organizaciones de cara a procesos de auditoría, certificación o acreditación. (ISOTools, 2020)

Delphi

Es un método orientado a conocer la opinión de expertos. En un primer momento, un grupo de especialistas anónimos responde a un cuestionario que elabora una organización sobre un tema específico, en este caso la Gestión de Riesgos. Tras analizar los resultados, los responsables piden su opinión a cada uno de los integrantes del grupo. Finalmente, la empresa elabora un segundo cuestionario, aunque éste con preguntas más precisas y focalizadas. La idea es que al final se elabora un texto con las conclusiones. (ISOTools, 2020)

Cobit

El marco de la metodología COBIT fue creado con las características principales se centran en los negocios, el proceso de orientación se basará en los controles e impulsado por métricas. La adopción de COBIT ayuda a una empresa para implementar las mejores prácticas de gobierno de TI , ya que ofrece una guía de mejores prácticas y la dirección. Su estructura clasifica los procesos en cuatro dominios, y presenta actividades en una estructura manejable y lógica. (Metodoss , 2020)

4.5.1. Amenazas

El segundo paso del análisis de riesgos es establecer las amenazas a las que se ven expuestos los activos, es decir, toda fuente potencial que pueda causar daños en los sistemas de información o directamente a la compañía.
En la tabla 7 se muestran los diferentes tipos de amenazas que pueden ser de origen natural o humano, pero que de igual manera comprometen los activos de la compañía. Se debe aclarar que existe una relación entre el activo y la ocurrencia de la amenaza, por lo que no todas las amenazas afectan completamente a los activos, pero si pueden causar diferentes impactos dependiendo del número de activos que se vean involucrados.

Tabla 7. Amenazas que pueden afectar los activos de la compañía.

Tipo de Amenaza	Descripción	Ejemplos
Origen natural	Se dan por circunstancias naturales	Pandemias ,terremotos, inundaciones, y todos otros desastres naturales
Origen industrial	Son eventualidades industriales	Fallos del servicio eléctrico y del suministro hídrico, explosiones, entre otros
Defectos de fabrica	Productos de procedencia defectuosa	Imperfecciones de software o hardware
Accidental	Son problemas no intencionados	Error u omisión de información
Deliberado	Sucesos ocasionados intencionalmente	Ataques deliberados, daños materiales, destrucción, robo o secuestro de información

Identificación de amenazas

Una amenaza es toda aquella acción que se materializa a partir de una vulnerabilidad y que puede causar daños sobre los activos de la organización. Puede ser de origen natural o humano con actuación accidental o deliberada , se pueden ocasionar de manera interna o externa a la compañía.
Para la identificación de amenazas de los activos de información existe un área delegada y capacitada que cuenta con especialistas en seguridad de la información encargados del análisis y la estimación de probabilidad de ocurrencia de la materialización de una amenaza sobre los activos que custodian.

Valoración de las amenazas

En la valoración de amenazas actuales se debe considerar la experiencia interna adquirida anteriormente con incidentes y valoraciones de amenazas. Además, se debe hacer una constante actualización del catálogo de amenazas apoyándose en las bases de datos disponibles de compañías especializadas en la identificación de estas.

Se puede determinar qué tan perjudicial es una amenaza para un activo, valorándolo en base a dos percepciones:

1. Degradación: Que tan malo resulta impactado el valor del activo ante una amenaza.
2. Probabilidad: Cual es la probabilidad o improbabilidad de que se logre materializar la amenaza.

En estos puntos se debe tener en cuenta los factores de intencionalidad. Cuando la afectación es de tipo no intencional se puede estimar el valor que se pierde sobre el activo, pero cuando la amenaza es intencional, se requiere valorar detalladamente el impacto debido a que el daño puede ser incalculable. Por medio de la tabla 8 se logra comprender en escalas el resultado perjudicial de la degradación que tiene el valor de un activo al verse expuesto ante una amenaza y en la tabla 9 se puede establecer la probabilidad de ocurrencia de una amenaza con su respectiva valoración ,a pesar de ser más compleja su determinación por ser una incertidumbre para cualquier compañía.

Tabla 8. Niveles de degradación del valor de un activo.

Nivel de degradación	Abreviatura	Probabilidad	Condición
Muy Alto	M.A	Seguramente ocurrirá	Factible
Alto	A	Muy alta	Medio
Medio	M	Puede ocurrir	Complejo
Bajo	B	Poco probable	Muy complejo
Muy Bajo	M.B	Remotamente puede ocurrir	Extremadamente complejo

Tabla 9. Probabilidad de ocurrencia de la materialización de una amenaza.

Ocurrencia	Definición	Valor
Casi seguro	Con certeza se presentará	5
Probable	Posiblemente se presente	4
Posible	Posiblemente se presente de vez en cuando	3
Improbable	Puede ocurrir en cualquier momento	2
Muy Improbable	Jamás puede ocurrir	1

Impacto potencial

El impacto es todo aquel daño que recibe el activo como consecuencia de la materialización de una amenaza. Cuando se conoce el valor de los activos de la compañía y el posible valor de degradación de este, se puede determinar el impacto potencial que recibirán los sistemas internos de la compañía. Se pueden precisar dos tipos de impacto.

El impacto acumulado: Se calcula basándose en el valor propio del activo y en su valoración total cuando otros activos dependen de él. Además, se debe tener en cuenta cada amenaza a la que se ve expuesto el activo. Debido a que entre mayor es el valor del activo, mayor es su exposición a la degradación, lo que ocasionaría un impacto considerable en la organización (MAGERIT v3.0, 2012).
El Impacto repercutido: Es calculado con respecto al valor propio del activo, pero se ve expuesto cuando es amenazado el activo del que depende, por lo que su degradación es en función del impacto que recibe el activo principal (MAGERIT v3.0, 2012).

Una vez que se conoce el impacto que tienen las amenazas sobre los activos, se puede determinar el riesgo potencial según la probabilidad de ocurrencia. Como se observa en el mapa de calor de la figura 20 ,se tienen cuatro zonas que se deben tener en cuenta al momento de determinar el riesgo potencial.

- Zona 1 (Roja): Son los riesgos de más alto impacto y con ocurrencia muy probable.
- Zona 2 (Franja amarilla): Pueden ser riesgos improbables, pero de impacto medio o riesgos muy probables con impacto bajo.
- Zona 3 (verde): Son riesgos improbables y de bajo impacto.
- Zona 4 (Naranja): Son riesgos improbables pero que tienen un alto impacto.

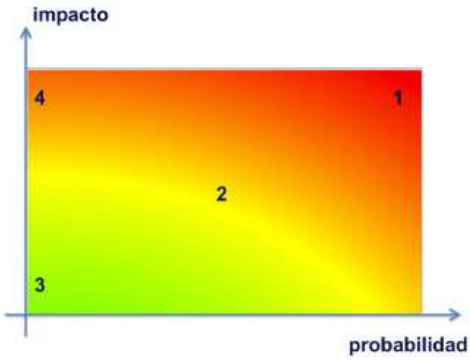


Figura 20. El riesgo en función del impacto y la probabilidad.
Obtenido de MAGERIT-Versión 3.0.

4.5.2. Vulnerabilidades

Una vulnerabilidad es toda aquella debilidad que puede ser explotada por una amenaza, ocasionando daños a los activos o la organización. Es importante aclarar que la sola presencia de una vulnerabilidad no puede ocasionar afectaciones por sí misma, debido a que necesita ser aprovechada por una amenaza para provocar daños. Este tipo de vulnerabilidades deben ser identificadas y monitoreadas para establecer posibles cambios que representen un riesgo en el futuro.

A continuación, se describe el proceso para la identificación de vulnerabilidades, las organizaciones que se encuentran involucradas en la gestión de estas y los aplicativos que permiten realizar consultas y diagnósticos de manera profesional. Finalmente se presenta un análisis de vulnerabilidades del año 2020 por parte del autor.

Identificación de vulnerabilidades

Una vulnerabilidad se puede identificar por medio del escaneo frecuente a los sistemas de información de la compañía. Aunque también se deben tener en cuenta los catálogos que registran las nuevas vulnerabilidades encontradas, con el fin de mantener actualizados los procedimientos y controles aplicados en el sistema de gestión de seguridad de la compañía.

NIST (*National Institute of Standards and Technology*)

El instituto nacional de estándares y tecnología (NIST) "*National institute of standards and technology",* en inglés. Es una agencia que promueve estándares, innovación y el desarrollo en diferentes áreas de la ciencia y tecnología, entre la que se destaca la tecnología de la información y las comunicaciones, donde se encuentran servicios y recursos, que contienen catálogos con listas de vulnerabilidades recientes y antiguas. Además, promueven programas de mejores prácticas en ciberseguridad que ayudan a las organizaciones a comprender mejor la administración y protección de sus redes y datos ante posibles riesgos (NIST, 2020).

NVD (*National Vulnerability Database*)

La base de datos nacional de vulnerabilidades o *"National Vulnerability Database",* siglas (NVD). Es uno de los repositorios más grandes del gobierno de EE.UU, debido a que cuenta con bases de datos para la gestión de vulnerabilidades, basándose en el protocolo de automatización de contenido de seguridad o "*Security Content Automation Protocol*" conocido por sus siglas en inglés como (SCAP), un método

utilizado para estándares específicos que permiten automatizar la gestión de vulnerabilidades, midiendo la seguridad y evaluando el correcto cumplimiento de políticas aplicadas en una organización (NVD, 2020).

Las bases de datos de NVD son obtenidas a partir de reportes de fallas y malas configuraciones de software que se encuentran vinculados a temas de seguridad, listas de verificación de seguridad y métricas de impacto, entre otras fuentes.

CVE (*Common Vulnerabilities and Exposures*)

NVD utiliza la identificación de vulnerabilidades y exposiciones comunes (CVE) "*Common Vulnerabilities and Exposures*", en inglés. Para listar las vulnerabilidades conocidas de seguridad, permitiendo referenciar cada vulnerabilidad reportada con un identificar único (CVE-ID) que se utiliza para la identificación en búsquedas específicas y que además facilita la obtención de información detallada como la descripción, versión ,solución , configuración o forma de explotación de la vulnerabilidad. Esta nomenclatura única permite proveer conocimiento público y posibilita la compartición de datos para solucionar las brechas tecnológicas (Red Hat, 2020).

El formato de identificación de vulnerabilidades contiene la siguiente forma CVE-YYYY-NNNN, donde la entrada se identifica como CVE, seguido del ID donde se incluye el año en que se descubrió la vulnerabilidad (YYYY) y el número con el que se registró en la base de datos (NNNN).

Registro de vulnerabilidades para el año 2020

Figura 21. Registro de vulnerabilidades identificadas hasta septiembre de 2020.

En la figura 21, se muestra la cantidad de vulnerabilidades registradas mensualmente en la base de datos de vulnerabilidades y exposiciones comunes (CVE) para el año 2020. Como se puede observar en la gráfica, el primer mes del año registro un elevado número de casos de vulnerabilidades detectadas con una cifra cercana a los 1.900 casos, para el mes de febrero se logró reducir esta cifra en un 21% aproximadamente, pero para el mes de marzo nuevamente se incrementaron los casos, lo que conllevaría a que el mes de abril fuera el de mayor influencia debido a la contingencia causada por la epidemia covid-19, lo que provocó un aumento significativo en los ataques, registrando un aproximado de 73.6 casos diarios, para un total de 2.209 en el mes. Por lo cual las organizaciones tuvieron que incrementar los controles de seguridad para mitigar los riesgos a los que se podían ver expuestas y la prueba fehaciente de la correcta implementación de dichos controles se ve reflejada en el mes de mayo donde se logró disminuir la cantidad de vulnerabilidades registradas en más del 50% con respecto al mes anterior. Por otra parte, el mes de junio fue nuevamente un mes donde se reactivaron los ataques y se detectaron 801 casos más que el mes inmediatamente anterior, para los meses siguientes julio, agosto y septiembre se notó una disminución considerable para un año 2020 donde los delitos informáticos o ciberdelitos aumentaron mundialmente.

4.5.3. Riesgos asociados a la seguridad de la información

Para realizar la actualización de riesgos asociados a la seguridad de la información, se consultó la base de datos nacional de vulnerabilidades (NVD) y en base a las cinco palabras más comunes y usadas en las organizaciones actualmente (Windows, Microsoft office, Navegador, Antivirus y VPN). Se llevo a cabo un filtro con el fin de reducir la cantidad de resultados obtenidos, se tuvieron en cuenta factores como el tiempo de publicación de la vulnerabilidad que no fuera mayor de 3 meses a la fecha de realización de este documento, es decir, los meses de agosto, septiembre y octubre del año 2020. Además, una vez se obtuvieron las listas de vulnerabilidades filtradas por palabra y fecha de publicación, solo se tuvieron en cuenta las que contaban con una valoración de severidad alta o crítica y se seleccionaron 2 por cada termino de búsqueda para un total de 10 vulnerabilidades. Posteriormente se realizará un análisis en base a la información obtenida en las bases de datos y finalmente se hará una valoración por parte del autor.

CVSS Versión 3.1

La herramienta para realizar la valoración de amenazas es "*Common Vulnerability Scoring System Calculator" o* calculadora del sistema de puntuación de vulnerabilidad común en su versión 3.1.

El *Common Vulnerability Scoring System* (CVSS) es un marco abierto para comunicar las características y la gravedad de las vulnerabilidades del software. CVSS consta de tres grupos de métricas: Base, Temporal y Ambiental. El grupo Base representa las cualidades intrínsecas de una vulnerabilidad que son constantes a lo largo del tiempo y en todos los entornos de usuario, el grupo Temporal refleja las características de una vulnerabilidad que cambia con el tiempo y el grupo Ambiental representa las características de una vulnerabilidad que son exclusivas de un usuario. Las métricas Base producen una puntuación que va de 0 a 10, que luego se puede modificar al puntuar las métricas Temporal y Ambiental. Una puntuación CVSS también se representa como una cadena de vectores, una representación textual comprimida de los valores utilizados para derivar la puntuación. (FIRST.Org, Inc, 2019)
Nota: *Para el análisis y la valoración de vulnerabilidades por parte del autor no se tuvo en cuenta el puntaje de la métrica ambiental debido a las restricciones de las políticas de seguridad de la información de la compañía.*

4.5.4. Identificación, análisis y valoración de riesgos

A continuación, se muestran uno a uno los riesgos asociados a la seguridad de la información para los términos (Windows, Microsoft Office, Antivirus, VPN y Navegadores). Además del análisis y valoración por parte del autor para las vulnerabilidades identificadas para cada riesgo.

4.5.4.1. Riesgos en Windows

Identificación de vulnerabilidades en Windows

Windows es uno de los sistemas operativos más utilizados a nivel mundial, debido a que es una herramienta fundamental para cualquier tipo de organización por su practicidad y eficiencia. Pero debido a su alto uso es susceptible a continuos ataques por lo que se requiere mantener actualizando el sistema para solventar estas fallas. Por esto es necesario realizar una identificación de posibles vulnerabilidades que puedan causar afectaciones en los activos de información o en los procesos de la compañía.

Tabla 10. Vulnerabilidades identificadas para el sistema operativo Windows.

ID	Descripción	Puntaje Base	Fecha de Publicación
CVE-2020-1508	Ejecución remota de código del codificador de audio de Windows media	8.8	11/09/2020
CVE-2020-25826	Integración de *pingID* para el escalamiento de privilegios locales en el inicio de sesión de Windows.	7.8	23/09/2020

En la tabla 10, se muestran dos vulnerabilidades elegidas para analizar y evaluar bajo los parámetros de búsqueda de la palabra (*Windows*), consultado en la base de datos nacional de vulnerabilidades (NVD). A continuación se hará la descripción de cada una de estas vulnerabilidades con su respectivo procedimiento de análisis y valoración por parte del autor.

Análisis y valoración CVE-2020-1508

Existe una vulnerabilidad de ejecución remota de código cuando el decodificador de audio de Windows Media maneja objetos de manera incorrecta, también conocida como 'Vulnerabilidad de ejecución remota de código del decodificador de audio de Windows Media'. (National Vulnerability Database (NVD), s.f.)

Esta vulnerabilidad puede ser aprovechada por un atacante para tomar el control del sistema afectado. Existen dos formas de explotar la vulnerabilidad, la primera consiste en convencer a la víctima para que visite una página web maliciosa y la segunda es persuadir a el usuario para que abra un documento especialmente diseñado.

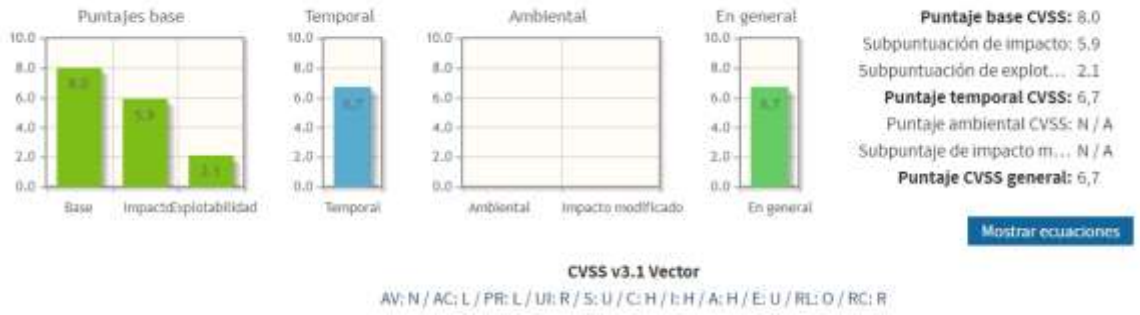


Figura 22. Impacto potencial de la vulnerabilidad CVE-2020-1508.
Obtenido de nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

En la figura 22 se observan los puntajes obtenidos en cada uno de los grupos de métricas para la vulnerabilidad CVE-2020-1508 basándose en el sistema de puntuación del aplicativo CVSS v3.1.

Según los criterios propios del evaluador para obtener el puntaje base se tienen en cuenta los siguientes parámetros: La vulnerabilidad solo puede ser explotada con acceso a la red, su complejidad es baja debido a que no requiere de conocimientos avanzados para ser empleada, se requiere de privilegios mínimos, pero a su vez necesita de la interacción del usuario para ser ejecutada lo que causaría un impacto alto en la confidencialidad, integridad y disponibilidad en los activos del usuario, pues el atacante tomaría el control del sistema. Por ello se consigue un puntaje base de 8.0 lo que clasifica la vulnerabilidad con una severidad alta y que a su vez coincide con la clasificación oficial asignada por los analistas de NVD con un puntaje base de 8.8 categorizada alta para esta vulnerabilidad.

El puntaje temporal demuestra que se ha consultado la base de datos de *exploits* sin encontrar resultados de explotación para esta vulnerabilidad y que cuenta con un arreglo oficial por parte del proveedor con parches o actualizaciones de seguridad disponible.

Análisis y valoración CVE-2020-25826

La integración de pingID para el inicio de sesión de Windows anterior a la versión 2.4.2 permite a los usuarios locales obtener privilegios modificando CefSharp.BrowserSubprocess.exe. (National Vulnerability Database (NVD), s.f.)

Esta vulnerabilidad permite el escalamiento de privilegios locales al aprovechar la ejecución del servicio pingID que agrega (2FA) doble factor de autenticación en el inicio de sesión de Windows y a su vez se ejecuta con privilegios administrativos del sistema. Una forma de explotar esta vulnerabilidad es por ejemplo sobrescribir el archivo *CefSharp.BrowserSubprocess.exe* ubicado en el directorio de instalación de pingID por el archivo *cmd.exe*, lo que ejecutaría el símbolo del sistema de Microsoft Windows para realizar modificaciones del sistema o ejecutar código malicioso.

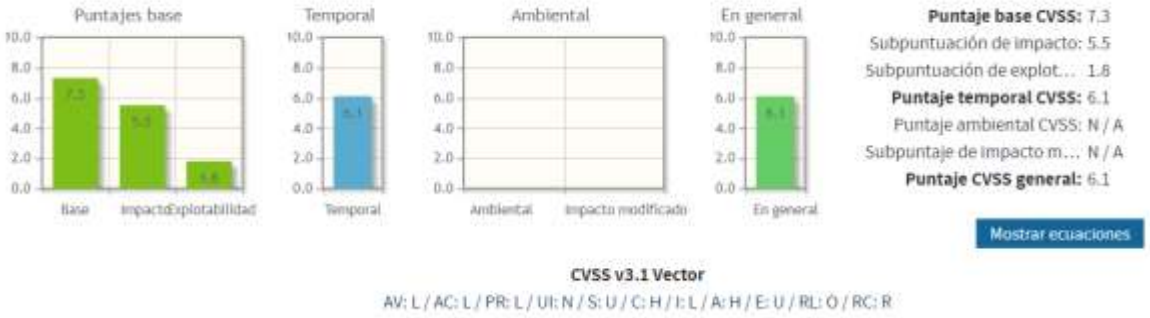


Figura 23. Impacto potencial de la vulnerabilidad CVE-2020-25826.
Obtenido de nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

En la figura 23 se muestra la valoración obtenida para los grupos de métricas temporal y de base para la vulnerabilidad CVE-2020-25826, según el sistema de calificación del CVSS v3.1.

Basándose en el criterio del evaluador, la vulnerabilidad obtiene un puntaje base de 7.3 con el sistema de puntuación de vulnerabilidades (CVSS) , donde se tuvieron en cuenta aspectos como la baja complejidad del ataque y la sola efectividad de explotación en redes locales, lo que facilita la identificación del activo vulnerado. Los factores que realmente tienen un impacto alto son la confidencialidad, integridad y disponibilidad, debido a que el atacante tendría acceso total al sistema del equipo. Esta vulnerabilidad tiene unas métricas de impacto y explotabilidad de 5.5 y 1.8 respectivamente, lo que indica que su impacto puede ser asumido con los controles de seguridad adecuados.

El puntaje obtenido en la métrica temporal es de 6.1 lo que se puede catalogar como severidad media, debido a que actualmente no se encuentran *exploits* disponibles en las bases de datos y su vez cuenta con una actualización disponible para solventar el fallo.

4.5.4.2. Riesgos en Microsoft Office

Identificación de vulnerabilidades en Microsoft Office

El uso de las herramientas de Microsoft Office es muy usual en las empresas corporativas actualmente, lo que representa un alto riesgo a la seguridad de la información de las compañía debido a los diversos métodos que han optado los atacantes para extraer datos por medio de archivos fraudulentos o por la interceptación de documentos; Por ello se deben identificar posibles vulnerabilidades a las que se ven expuestos los usuarios que tienen a su cargo activos de información valiosos para las organizaciones.

Tabla 11. Vulnerabilidades identificadas en Microsoft office.

ID	Descripción	Puntaje Base	Fecha de Publicación
CVE-2020-1338	Ejecución remota de código de Microsoft Word	8.8	11/09/2020
CVE-2020-1581	Elevación de privilegios de hacer clic y ejecutar de Microsoft Office	7.8	17/08/2020

En la tabla 11, se muestran las dos vulnerabilidades identificadas bajo los parámetros de búsqueda de la palabra *Microsoft Office* en la base de datos nacional de vulnerabilidades (NVD),con su respectiva descripción para posteriormente realizar su análisis y valoración por parte del autor.

Análisis y valoración CVE-2020-1338

Existe una vulnerabilidad de ejecución remota de código en el software de Microsoft Word cuando no puede manejar correctamente los objetos en la memoria, también conocida como 'Vulnerabilidad de ejecución remota de código de Microsoft Word'. (National Vulnerability Database (NVD), s.f.)

Esta vulnerabilidad puede ser aprovechada por un atacante por medio de correo electrónico o de un sitio web, la victima debe abrir un archivo especialmente diseñado en la versión afectada de Microsoft Word para que el atacante tenga éxito. Por lo que se requiere del uso de ingeniería social para persuadir a la víctima a que abra el archivo. El fin de esta vulnerabilidad es conseguir la ejecución de código arbitrario en el sistema de destino y la realización de acciones con los permisos y credenciales del usuario que inicio sesión.

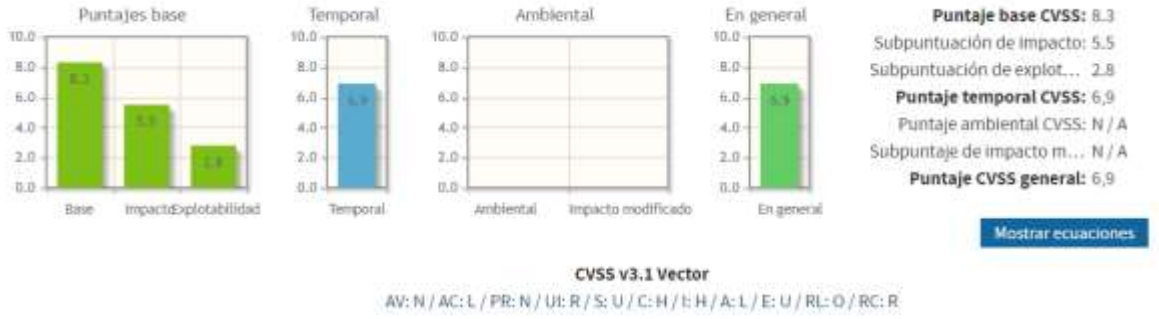


Figura 24. Impacto potencial de la vulnerabilidad CVE-2020-1338. Obtenido de nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

En la figura 24 se muestran los resultados obtenidos a través del sistema de puntuación de vulnerabilidades bajo los criterios del evaluador quien considero para las métricas de puntuación base que la vulnerabilidad solo puede ser aprovechada por medio de la red y no se requiere de una alta complejidad en el ataque, debdo a que no se necesitan de privilegios previos para su ejecución, pero el éxito para explotar la vulnerabilidad si depende de la interacción del usuario para que acceda a abrir el archivo afectado, lo que derivaría en un alto impacto a la confidencialidad y la integridad de los archivos de información del afectado y a su vez un impacto bajo en la disponibilidad, pues una de las opciones de Microsoft Word permite el inicio en varios equipos al tiempo, por lo que el afectado solo se percataría de la amenaza al notar archivos nuevos o modificaciones sospechosas. El puntaje base delegado por los analistas de NVD para esta vulnerabilidad es de 8.8 y se asemeja con el obtenido por el evaluador de 8.3, por lo que se categorizan de impacto alto. Además, la evaluación arroja una subpuntuación de impacto de 5.5 , lo que sugiere que esta amenaza explotada satisfactoriamente afectaría en más del cincuenta por ciento la confidencialidad, integridad y disponibilidad del activo involucrado. La subpuntuación de explotabilidad es 2.8 lo que quiere decir es que no representa un riesgo, debido a que el acceso a esta vulnerabilidad resulta un poco complicado.

El puntaje obtenido en la métrica temporal es de 6.9, muy sobreestimado para una vulnerabilidad que no cuenta con recursos existentes en la base de datos de *exploits* y su proveedor oficializo un parche de seguridad para solventar el fallo.

Análisis y valoración CVE-2020-1581

Existe una vulnerabilidad de elevación de privilegios en la forma en que los componentes Click-to-Run (C2R) de Microsoft Office manejan los objetos en la memoria, también conocida como 'Vulnerabilidad de elevación de privilegios de Microsoft Office Click-to-Run'. (National Vulnerability Database (NVD), s.f.)

Esta vulnerabilidad puede ser aprovechada por un atacante con conocimientos en la ejecución de código en el sistema de destino, debido a que se necesita que el usuario local ejecute una aplicación especialmente diseñada, lo que derivaría en daños en la memoria o en la elevación de privilegios. Esta vulnerabilidad explotada con éxito puede resultar en un compromiso total del sistema vulnerado.

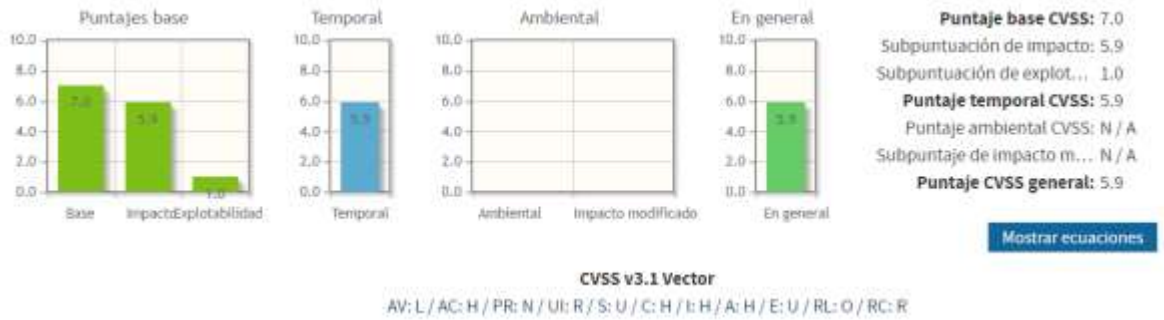


Figura 25. Impacto potencial de la vulnerabilidad CVE-2020-1581.
Obtenido de nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

En la figura 25 se observan los valores obtenidos bajo los criterios del evaluador con ayuda del sistema de puntuación de vulnerabilidades (CVSS) para la vulnerabilidad CVE-2020-1581. Los parámetros que se tuvieron en cuenta para esta valoración fueron las condiciones de explotabilidad como, por ejemplo, que necesariamente debe hacerse en un entorno local, pero a su vez requiere de un alto nivel de conocimiento del atacante, pues el usuario debe ejecutar una aplicación especialmente diseñada que se asemeje a la original provocando consecuencias severas debido a que se obtendría un impacto alto en la confidencialidad, integridad y disponibilidad del sistema vulnerado.

Se consigue un puntaje base de (7.0) por parte del evaluador y al compararlo con el puntaje base de (7.8) dictado por los analistas de NVD, se considera que ambas puntuaciones entran en el rango de severidad alta establecido en el sistema CVSS.
La subpuntuación de impacto (5.9), es una estimación del alto impacto que tendría esta vulnerabilidad sobre la confidencialidad, integridad y disponibilidad del activo si llegase a ser explotada con éxito. También ,la subpuntuación de explotabilidad (1.0) sugiere que se trata de un ataque complejo que difícilmente podría ser ejecutado.
El puntaje obtenido en la métrica temporal es de (5.9) y tiene en cuenta factores técnicos de la vulnerabilidad como la inexistencia de *exploits* disponibles para su explotabilidad y que el nivel de remediación cuenta con un arreglo oficial por parte de la compañía proveedora.

4.5.4.3. Riesgos en antivirus

Identificación de vulnerabilidades en Antivirus

Los antivirus son una pieza fundamental para todo sistema de seguridad de una organización, pero muchas veces estos se ven expuestos a fallos que comprometen la seguridad de sus clientes. El constante monitoreo de vulnerabilidades en este tipo de herramientas permite crear controles adicionales ante posibles brechas de seguridad, por ello se deben identificar vulnerabilidades que puedan presentar los antivirus como cualquier otro tipo de software.

Tabla 12. Vulnerabilidades identificadas para antivirus.

ID	Descripción	Puntaje Base	Fecha de Publicación
CVE-2020-25776	Escalación de privilegios en Trend Micro Antivirus para Mac 2020 (Consumidor)	7.8	02/10/2020
CVE-2020-5839	Divulgación de información en *Symantec Endpoint Detection*	7.5	07/08/2020

En la tabla 12, se muestran dos vulnerabilidades elegidas para analizar y evaluar bajo los parámetros de búsqueda de la palabra (*Antivirus*), consultado en la base de datos nacional de vulnerabilidades (NVD). A continuación, se describen las vulnerabilidades identificadas con su respectivo análisis y valoración por parte del autor.

Análisis y valoración CVE-2020-25776

Trend Micro Antivirus para Mac 2020 (consumidor) es vulnerable a un ataque de escalada de privilegios de enlace simbólico en el que un atacante podría explotar un archivo crítico en el sistema para escalar sus privilegios. Un atacante debe primero obtener la capacidad de ejecutar código con pocos privilegios en el sistema de destino para aprovechar esta vulnerabilidad. (National Vulnerability Database (NVD), s.f.)

Para explotar esta vulnerabilidad un atacante debe primero poder ejecutar código con pocos privilegios en el sistema de destino para posteriormente aprovechar la vulnerabilidad en el módulo iTISPlugin del antivirus Trend Micro para usuarios Mac. Esta falla permite a un atacante local la escalada de privilegios de enlace simbólico, en la cual se puede explotar un archivo crítico del sistema para obtener mayores privilegios y permitir la ejecución de código en modo *root* cuando la vulnerabilidad es explotada con éxito.

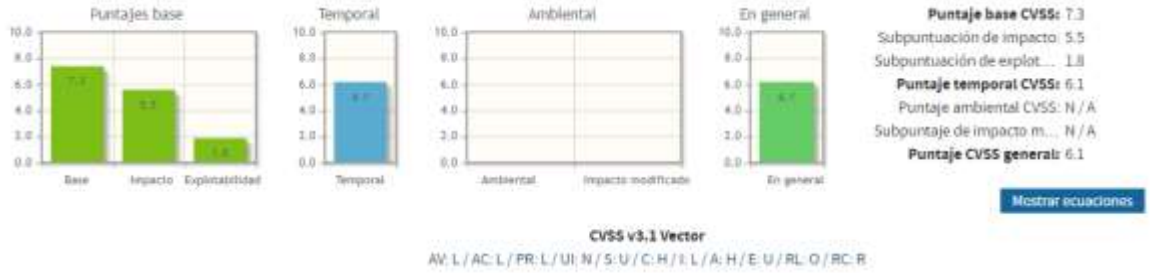


Figura 26. Impacto potencial de la vulnerabilidad CVE-2020-25776.
Obtenido de nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

En la figura 26 se observan los puntajes obtenidos en cada uno de los grupos de métricas para la vulnerabilidad CVE-2020-25776 basándose en el sistema de puntuación del aplicativo CVSS v3.1.

Según los criterios del evaluador, se obtiene un puntaje base de (7.3), lo que a su vez concuerda con la puntuación publicada por los analistas de NVD de (7.8), por lo que ambas valoraciones se consideran dentro del rango de criticad alta. En este sentido se tuvieron en cuenta factores como la baja complejidad del ataque, la forma de explotabilidad que solo puede llevarse a cabo de forma local y no necesita de la interacción del usuario, el aprovechamiento de los mínimos privilegios requeridos y el alto impacto para la confidencialidad y disponibilidad del activo afectado. Por otra parte, se obtiene una subpuntuación de impacto de 5.5, lo que representa el efecto sobre la integridad, disponibilidad y confidencialidad si se llegara a materializar la vulnerabilidad. De igual forma se consigue una subpuntuación de 1.8 en la explotabilidad, lo que se puede traducir como poco común su ocurrencia.

Se consulto la base de datos de *exploits* en busca de documentación disponible para esta vulnerabilidad, pero se comprobó la inexistencia de resultados. Además, se encontró un arreglo oficial por parte del proveedor Trend Micro antivirus para Mac, por lo que el puntaje en la métrica temporal de (6.1) es un poco alto para las condiciones anteriormente nombradas.

Análisis y valoración CVE-2020-5839

Symantec Endpoint Detection And Response, anterior a 4.4, puede ser susceptible a un problema de divulgación de información, que es un tipo de vulnerabilidad que podría permitir el acceso no autorizado a los datos. (National Vulnerability Database (NVD), s.f.)

Es una vulnerabilidad reportada para versiones hasta la 4.3 de *Symantec endpoint detection and response*, un *software* capaz de detectar amenazas de red y brindar respuestas de protección contra ellas. El método de explotación no se especifica, pero causa una vulnerabilidad de divulgación de información, lo que causa una repercusión sobre la confidencialidad del activo afectado.

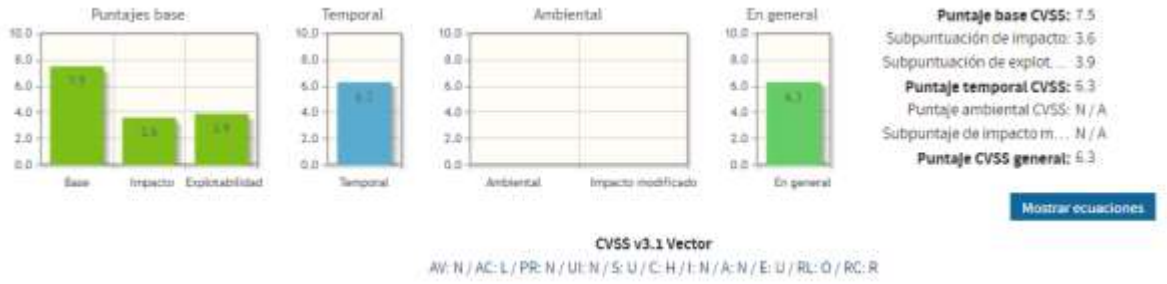


Figura 27. Impacto potencial de la vulnerabilidad CVE-2020-5839.
Obtenido de nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

En la figura 27 se observan los puntajes obtenidos para la vulnerabilidad CVE-2020-5839, bajo los criterios del evaluador y con el uso de la herramienta de puntuación de vulnerabilidades (CVSS). Por supuesto se tuvieron en cuenta algunos factores influyentes para la valoración de la vulnerabilidad, como la baja complejidad del ataque a través de la red, la carencia de privilegios e interacción del usuario para llevar acabo la explotación de la vulnerabilidad. Pero también se tuvo en cuenta que este tipo de ataque contiene un impacto alto en la confidencialidad del activo involucrado y en base a la poca información encontrada, se deduce que no causa ningún impacto en la integridad y disponibilidad del sistema afectado.

El puntaje de base personal obtenido con el CVSS es de (7.5), lo que coincide con el puntaje oficialmente publicado por los analistas de NVD (7.5) para esta vulnerabilidad que se categoriza con una severidad alta. Por otra parte, la subpuntuación de impacto de 3.6 es acorde debido a la naturaleza de la vulnerabilidad, pues solo causa un impacto alto a la confidencialidad. La subpuntuación de explotabilidad es de 3.9 lo que permite considerar que afecta de manera parcial el activo involucrado. Por último, el puntaje temporal de (6.3) demuestra que se consultó la base de datos de *exploits* sin encontrar resultados de explotación para esta vulnerabilidad y que cuenta con un arreglo oficial por parte del proveedor con una actualización disponible.

4.5.4.4. Riesgos en servicios de VPN

Identificación de vulnerabilidades en servicios de VPN

Las VPN o redes privadas virtual, son una de las tecnologías más utilizadas para realizar teletrabajo en las organizaciones debido a que garantizan el cifrado del tráfico en red y dificultan el robo de información confidencial por pate de terceros. Aunque estos sistemas son seguros muchas veces se presentan dificultades por parte de los prestadores del servicio, lo que puede comprometer la seguridad de los usuarios que utilizan el servicio. Por ello se requiere identificar posibles vulnerabilidades que presenten las compañías prestadoras del servicio y que pongan en riesgo la seguridad de los activos de información.

Tabla 13. Vulnerabilidades identificadas para VPN.

ID	Descripción	Puntaje Base	Fecha de Publicación
CVE-2020-12107	Inyección de comandos a través del portal web del módulo Wifi de VPNCrypt M10 2.6.5	9.8	12/08/2020
CVE-2020-17365	Escalada de privilegios en el software cliente Hotspot Shield VPN	7.8	24/09/2020

En la tabla 13, se muestran dos vulnerabilidades elegidas para analizar y evaluar bajo los parámetros de búsqueda de la palabra (*VPN*), consultado en la base de datos nacional de vulnerabilidades (NVD). con su respectiva descripción, análisis y valoración por parte del autor.

Análisis y valoración CVE-2020-12107

El portal web del módulo Wifi de VPNCrypt M10 2.6.5 permite la inyección de comandos a través de un campo de texto, lo que permite un control total sobre el sistema operativo de este módulo. (National Vulnerability Database (NVD), s.f.)

Esta vulnerabilidad se deriva de una función desconocida del módulo wifi de VPNCrypt que permite el acceso sin restricciones a funciones críticas del portal web del producto y admite la inyección de comandos. El alcance de esta vulnerabilidad se basa en la negación de servicio a través del módulo wifi afectado, lo que perjudica la entrega del tráfico cifrado. Además, puede verse comprometido el sistema operativo del dispositivo donde se logre explotar.

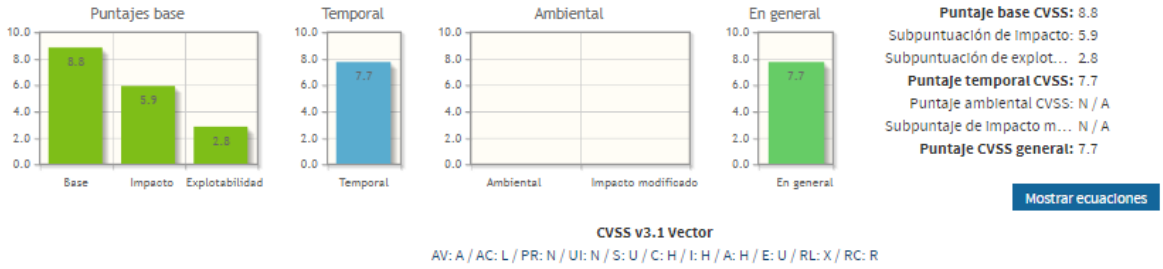


Figura 28. Impacto potencial de la vulnerabilidad CVE-2020-12107.
Obtenido de nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

En la figura 28 se muestran los puntajes obtenidos para la vulnerabilidad CVE-2020-12107 con el sistema de puntuación de vulnerabilidades CVSS. Esto basándose en los criterios y experiencia del evaluador. inicialmente se obtiene un puntaje base de 8.8 categorizando la vulnerabilidad como alta, pero el valor publicado oficialmente por los analistas de NVD es de 9.8, es decir una severidad critica. Lo que indica una desproporción considerable en alguna de las métricas de evaluación. Sin embargo, los parámetros seleccionados por el evaluador fueron en base a la información disponible en los sitios web. Por ejemplo, se encontró que solo es posible explotar esta vulnerabilidad por la red, debido a que es un servicio VPN. Adicionalmente se consideró la baja complejidad del ataque, que no requiere de interacción del usuario ni de privilegios avanzados para ser explotada. Además, se tuvo en cuenta la repercusión del alto impacto en la confidencialidad, integridad y disponibilidad del activo comprometido. Por otra parte, la subpuntuación del impacto de 5.9 es considerable, debido a que refleja los efectos perjudiciales si la amenaza se llegara a materializar.

El puntaje obtenido en la métrica temporal de (7.7) permite evidenciar que el nivel de remediación aún no se ha definido para solventar esta vulnerabilidad, a pesar de que no se conocen detalles técnicos ni hay ningún exploit disponible en las bases de datos.

Análisis y valoración CVE-2020-17365

Los permisos de directorio incorrectos en el software cliente Hotspot Shield VPN para Windows 10.3.0 y versiones anteriores pueden permitir que un usuario autorizado habilite potencialmente la escalada de privilegios a través del acceso local. La vulnerabilidad permite que un usuario local corrompa los archivos del sistema: un usuario local puede crear un enlace simbólico especialmente diseñado a un archivo crítico en el sistema y sobrescribirlo con los privilegios de la aplicación. (National Vulnerability Database (NVD), s.f.)

Esta vulnerabilidad permite que un atacante pueda escalar privilegios para crear o escribir archivos arbitrariamente utilizando los permisos del sistema. Esto, debido a

una afectación de una función desconocida del componente *Directory permission del popular Hotspot Shield VPN client* que, al ser modificación, se deriva en una posible rotura del sistema y sus componentes.

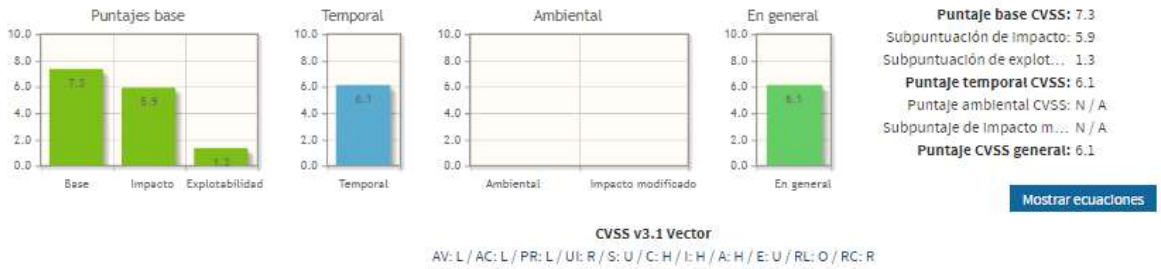


Figura 29. Impacto potencial de la vulnerabilidad CVE-2020-17365.
Obtenido de nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

En la figura 29 se muestra la valoración obtenida para los grupos de métricas de base y temporal para la vulnerabilidad CVE-2020-17365, según los criterios del evaluador y reflejado con ayuda del sistema de puntuación de vulnerabilidades CVSS v3.1.

Como primera medida se hace la comparación del puntaje publicado por los analistas de NVD que corresponde al valor de (7.8) y el obtenido por el evaluador de (7.3), lo que indica que ambas calificaciones cumplen con la valoración de severidad Alta. Por consiguiente, los parámetros que se tuvieron en cuenta para obtener este resultado se basan en la complejidad del ataque, debido a que necesita de un bajo nivel de privilegios para ser ejecutado, su vector de ataque se encuentra disponible de manera local y no requiere de autenticación para ser explotada. Por otro lado, el subpuntaje de impacto (5.9) permite reflejar el alto grado de afectación que se tendrían en la confidencialidad, integridad y disponibilidad del activo afectado si la amenaza llegara a materializarse por completo. Por último, el puntaje de 6.1 en la métrica temporal permite corroborar que no se encontraron *exploits* disponibles para ejecutar esta vulnerabilidad y que el nivel de remediación cuenta con una actualización oficial para solventar la falla en el sistema.

4.5.4.5. Riesgos en navegadores

Identificación de vulnerabilidades en navegadores

Los navegadores son una pieza fundamentan para todo empleado de una compañía, debido a que representa la herramienta de búsqueda más esencial para una persona en la actualidad. Así como es indispensable para realizar búsquedas en red también es peligroso para un usuario que visita sitios poco seguros y que pueden comprometer la información que almacena en el dispositivo. Para evitar estas exposiciones se deben identificar posibles vulnerabilidades a las que pueden acceder usuarios con poca experiencia o que representen un riesgo para la información personal o corporativa de la compañía.

Tabla 14. Vulnerabilidades identificadas para navegadores.

ID	Descripción	Puntaje Base	Fecha de Publicación
CVE-2020-15663	Gestión de privilegios incorrecta en Mozilla	8.8	01/10/2020
CVE-2020-15963	Aplicación de políticas insuficiente en las extensiones de Google Chrome	9.6	21/09/2020

En la tabla 14, se muestran dos vulnerabilidades elegidas para analizar y evaluar bajo los parámetros de búsqueda de la palabra (Navegador), consultado en la base de datos nacional de vulnerabilidades (NVD).Adicionalmente se hace énfasis en la descripción de la vulnerabilidad con un análisis y valoración por parte del autor.

Análisis y valoración CVE-2020-15663

Si Firefox está instalado en un directorio en el que el usuario puede escribir, el Servicio de mantenimiento de Mozilla ejecutará Updater.exe desde la ubicación de instalación con privilegios del sistema. Aunque el servicio de mantenimiento de Mozilla garantiza que el archivo actualizador.exe esté firmado por Mozilla, la versión podría haberse revertido a una versión anterior, lo que habría permitido la explotación de un error anterior y la ejecución de código arbitrario con privilegios del sistema. * Nota: este problema solo afectó a los sistemas operativos Windows. Otros sistemas operativos no se ven afectados. *. Esta vulnerabilidad afecta a *Firefox* <80, *Thunderbird* <78.2, *Thunderbird* <68.12, *Firefox* ESR <68.12 y *Firefox* ESR <78.2. (National Vulnerability Database (NVD), s.f.)

Esta vulnerabilidad puede ser aprovechada por un atacante por medio de la ingeniería social para persuadir a la víctima de que visite un sitio web especialmente diseñado para descargar y ejecutar una actualización de mantenimiento de Mozilla Firefox (updater.exe) con privilegio administrativos, lo que derivaría en una elevación de privilegios en el sistema y ocasionando una degradación del servicio de mantenimiento de Mozilla.

Figura 30. Impacto potencial de la vulnerabilidad CVE-2020-15663.
Obtenido de nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

En la figura 30 se muestran los resultados obtenidos a través del sistema de puntuación de vulnerabilidades CVSS según los criterios del evaluador quien considero para la puntuación base que las métricas de explotabilidad requieren de la interacción del usuario en la red y en la ejecución del archivo malicioso. Además, que el ataque no requiere de mayor complejidad para ser ejecutado. Teniendo en cuenta todas estas medidas se obtuvo una puntuación de 8.0 por parte del evaluador y se comparó por la publicada oficialmente por los analistas de NVD, donde su puntuación fue 8.8 lo que afirma que ambas cumplen con el rango para ser calificadas con una severidad alta. En cuanto a las métricas de impacto se obtiene un puntaje de 5.9 , lo que indica que se compromete totalmente la integridad, confidencialidad y disponibilidad del sistema. Por otra parte, se consultó la base de datos de *exploit* en busca de información de la forma de explotación de esta vulnerabilidad, pero no se encontraron resultados. Por último, se considera que se cuenta con un nivel de remediación disponible por parte del proveedor que lanzo una actualización disponible para solventar el fallo, por lo que se obtiene una puntuación en la métrica temporal de 6.7.

Análisis y valoración CVE-2020-15963

La aplicación de políticas insuficiente en las extensiones de Google Chrome antes de 85.0.4183.121 permitió a un atacante que convenció a un usuario de instalar una extensión maliciosa para realizar potencialmente un escape de la zona de pruebas a través de una extensión de Chrome diseñada. (National Vulnerability Database (NVD), s.f.)

Esta vulnerabilidad es aprovechada por un atacante que persuade a un usuario de instalar una extensión especialmente diseña lo que se derivó en una evasión del *sandbox* de Chrome, un entorno seguro para aislar la interacción entre los programas ejecutados en el sistema operativo y otros programas sin el permiso del usuario. Por lo que se generó una violación de políticas de seguridad.

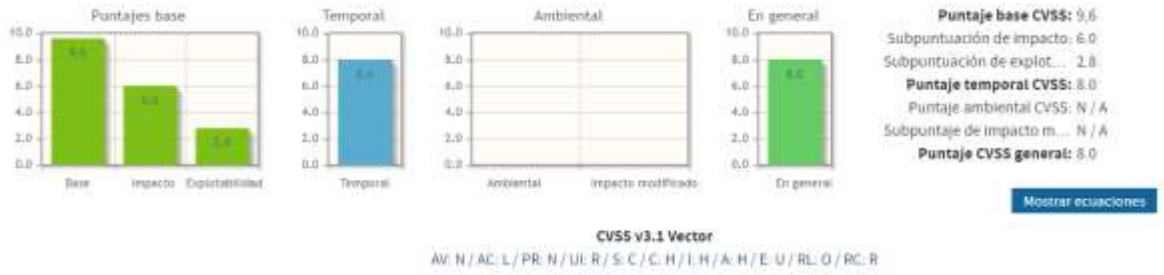


Figura 31. Impacto potencial de la vulnerabilidad CVE-2020-15963.
Obtenido de nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

En la figura 31 se muestran la valoración de la vulnerabilidad CVE-2020-15963 según los criterios del evaluador utilizando el sistema de puntación de vulnerabilidades CVSS v3.1. Como primera medida se establece que la puntuación obtenida por el evaluador

y los analistas de NVD coinciden totalmente con un puntaje base de 9.6 categorizando la vulnerabilidad como crítica. por consiguiente se establece que las métricas de explotabilidad necesitan ser por medio de la red, no se requieren privilegios previos y el ataque se considera de complejidad baja, pero a su vez se necesita de la interacción del usuario para llevar a cabo el ataque, en este caso accediendo a una extensión especialmente diseñada por el atacante y con un alcance cambiante, es decir que la vulnerabilidad explotada puede afectar otros recursos más allá de los privilegios autorizados, esto, debido a que logro salir del entorno de seguridad controlado de Chrome. Además, se obtiene un puntaje de impacto de 6.0 lo que sugiere que la materialización de esta amenaza afectaría totalmente la integridad, confidencialidad y disponibilidad del activo vulnerado. Finalmente se establece un puntaje temporal de 8.0 debido a su nivel de criticidad, a pesar de que no hay ningún *exploit* disponible en las bases de datos y actualmente se cuenta con un parche oficial para la corrección de este fallo.

Métricas de riesgos identificados

Los grupos de métricas: base, temporal y ambiental obtenidas por el evaluador con la herramienta CVSS "*Common Vulnerability Scoring System" versión 3.1***,** Se pueden consultar en la ***Tabla de métricas (ANEXO_5)*** , identificando cada vulnerabilidad con su CVE-ID correspondiente.

4.5.5. Matriz de valoración de riesgos en la seguridad de la información

Un riesgo es la combinación de la probabilidad de ocurrencia de un evento y las consecuencias negativas que provocaría. El riesgo se compone de dos factores que son:

RIESGO = (AMENAZA) x (VULNERABILIDAD)

En la tabla 15 se muestra una matriz de valoración de riesgos, donde se utiliza una escala de 0 a 8 que se puede valorar y evaluar el riesgo frente a los criterios de aceptación de este. Se tienen en cuenta factores como la probabilidad de ocurrencia y las consecuencias de degradación del activo afectado (Norma ISO 27005, 2018).

se realiza la clasificación del riesgo de la siguiente manera:

- Riesgo Bajo: 0 - 2
- Riesgo Medio: 3 – 5
- Riesgo Alto: 6 – 8

Tabla 15. Matriz de valoración del riesgo.
Obtenido de NTC-ISO/IEC 27005, adecuación del Autor.

Matiz de valoración de riesgos		*Probabilidad*				
		Muy baja (Muy Improbable)	Baja (Improbable)	Media (Posible)	Alta (probable)	Muy alta (Casi seguro)
Consecuencia	Muy baja	0	1	2	3	4
	Baja	1	2	3	4	5
	Media	2	3	4	5	6
	Alta	3	4	5	6	7
	Muy Alta	4	5	6	7	8

Una vez que se han identificado las vulnerabilidades, se considera un escenario donde diferentes amenazas se logran materializar. El riesgo resultante se clasifica de acuerdo con el puntaje base obtenido en el análisis y valoración de la vulnerabilidad y con respecto a otros factores que influyen en el desarrollo de este riesgo, como, por ejemplo, el uso de software vulnerable, el grado de complejidad del ataque y los requerimientos de ejecución de acciones maliciosas o deliberadas; Considerando un escenario real.

Los resultados se pueden apreciar en la tabla 16, donde se logra apreciar que, debido a la naturaleza de la amenaza, es decir, la valoración del nivel de severidad alto o crítico de la vulnerabilidad y asumiendo que representan una amenaza: la valoración del riesgo se considera medio o alto, pero no bajo.

Tabla 16. Matriz de valoración del riesgo para las vulnerabilidades identificadas.

Matiz de valoración de riesgos		*Probabilidad*				
		Muy baja (Muy Improbable)	Baja (Improbable)	Media (Posible)	Alta (probable)	Muy alta (Casi seguro)
Consecuencia	Muy baja					
	Baja				**CVE-2020-1581**	
	Media		**CVE-2020-1581**	**CVE-2020-25776**		
	Alta			**CVE-2020-1508**	**CVE-2020-15963**	**CVE-2020-12107**
	Muy Alta	**CVE-2020-25826**	**CVE-2020-17365**	**CVE-2020-5839**	**CVE-2020-1338**	

4.6. Tratamiento de riesgos

Una vez que se han logrado identificar los riesgos asociados a la seguridad de la información, se deben establecer las medidas y controles adecuados para hacer frente a los mismos. Para ello existen cinco acciones que son proporcionadas por la norma ISO 31000 para el tratamiento de riesgos y que pueden ser aplicados de acuerdo con las condiciones del riesgo.

4.6.1. Opciones de tratamiento del riesgo

Mitigación

Esta estrategia se basa en la reducción de la probabilidad de materialización de una amenaza o en la reducción del impacto causado por la amenaza, o ambos sobre la compañía. Es utilizada cuando el riesgo es inevitable o no depende directamente de la compañía (Norma ISO 31000, 2018).

Transferencia

Consiste en trasladar el riesgo a otra dependencia de la compañía o a entidades externas donde puedan gestionar de manera más eficaz el problema. Esta opción es muy común entre compañías filiales (Norma ISO 31000, 2018)

Aceptación

El uso de esta medida se opta cuando el nivel de riesgo puede ser asumido por la compañía, sin la implementación de acciones adicionales, pero teniendo en cuenta que la evaluación del riesgo satisface los criterios para su aceptación (Norma ISO 31000, 2018).

Explotación

Algunas veces se presentan riesgos que no son totalmente negativos, por lo que en vez de mitigarlos o eliminarlos son aprovechados bajo ciertas circunstancias y estrategias para mejorar la compañía, sacando el máximo provecho a las circunstancias (Norma ISO 31000, 2018).

Supresión

Es la acción menos habitual, debido a que consiste en la eliminación total de los riesgos asociados a los procesos de la compañía. Pero para lograrlo se requiere de la implementación exitosa en la previsión y planificación de riesgos (Norma ISO 31000, 2018).

En la compañía NEXA BPO el área de seguridad de la información tiene como medidas para el tratamiento de riesgos la implementación de acciones como la mitigación, transferencia y aceptación del riesgo. Las opciones de explotación y supresión del riesgo son de consideración, pero usadas en menor medida.

4.6.2. Selección de las opciones para el tratamiento del riesgo

Cuando se hace la elección de alguna de las cinco opciones para tratar el riesgo, se debe hacer en base al costo y esfuerzo que demande la implementación de esté, frente a los beneficios que se conseguirán. Una adecuada selección para el tratamiento del riesgo debe identificar el orden de prioridad en el que se deben implementar las opciones de tratamiento, los valores y percepciones de las partes involucradas interna o externamente a la compañía (si las hay) y realizar un nuevo análisis para establecer su efectividad.

Se puede hacer uso de una matriz como la presentada en la tabla 17 para establecer las opciones de tratamiento aplicables a cada riesgo, según la zona en la que se encuentren localizados. Esto, teniendo en cuenta la probabilidad y el nivel de impacto causado por el riesgo.

Zona A (Riesgo Bajo) : Aceptar, Explorar o Suprimir (Si se puede) el riesgo

Zona B (Riesgo Medio): Aceptar o Mitigar el riesgo

Zona C (Riesgo Alto): Mitigar, Aceptar o Transferir el riesgo

Tabla 17. Matriz para el tratamiento de riesgos.
Obtenido de NTC-ISO/IEC 27005, adecuación del Autor.

Matiz de tratamiento del riesgo		*Nivel de impacto (Severidad)*				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
Probabilidad de ocurrencia	Muy improbable	A	A	A	B	B
	Improbable	A	A	B	B	B
	Posible	A	B	B	B	C
	Probable	B	B	B	C	C
	Casi seguro	B	B	C	C	C

4.6.3. Controles existentes

Con el fin de brindar medidas y/o soluciones a cada riesgo identificado previamente. La norma ISO 27001 en su anexo A estableció una serie de 114 controles aplicables a cualquier circunstancia que se presente en las organizaciones. Es importante resaltar que la compañía puede escoger que controles aplicar y luego implementarlos. Generalmente el 90% de los controles son aplicables para todas las organizaciones, pero también existe la posibilidad de declarar controles no aplicables debido a la actividad comercial a la que se dedica la compañía. Estos controles se separan en dos grandes grupos que comprenden las políticas de seguridad de la información y los controles operacionales (Norma ISO 27001, 2013).

Por otro lado, la clasificación y valoración de controles establece dos tipos, que son:

- **Preventivos:** Son los controles que se ejercen para eliminar las causas del riesgo, previniendo que ocurran o se materialicen.
- **Correctivos**: Estos controles son los que permiten modificar las acciones que favorecen la evolución del riesgo para restablecer las actividades después de que se han detectado.

La elección del control adecuado se debe fundamentar en mantener el equilibrio entre el costo de la ejecución de la actividad de control, el valor del activo de información para los procesos de la compañía y el nivel de criticidad del riesgo identificado.

4.6.4. Declaración de aplicabilidad de controles

Los controles seleccionados por la compañía deben ser consignados en un documento formal que es requisito del estándar ISO/IEC 27001, donde se indica si son aplicables los controles establecidos o si, por el contrario, carecen de sentido. Este documento es conocido por las siglas *SOA,* declaración de aplicabilidad o *Statement of Applicability*, en inglés.

Según la norma técnica colombiana NTC-ISO/IEC 27001 para elaborar la declaración de aplicabilidad se deben incluir:

- Los controles implementados actualmente.
- La selección de controles nuevos y el argumento para su selección.
- La exclusión de controles y su respectiva justificación.

Todos los controles seleccionados o excluidos deben ser enumerados según se encuentren en el anexo A. Esta declaración de aplicabilidad permite resumir las decisiones tomadas para el tratamiento de riesgos y la justificación de exclusión de controles posibilita la validación de que ningún control fue omitido involuntariamente.

4.6.5. Plan de tratamiento de riesgos

El plan de tratamientos de riesgos permite planificar las acciones que se llevaran a cabo para implementar los controles correspondientes para cada uno de los riesgos que se han identificado. se puede resumir el plan de tratamiento de riesgos en una tabla que contenga:

- ID del riesgo: Es el identificador del riesgo.
- Nivel de riesgo: Es el grado de severidad (Bajo , Medio o Alto).
- Opción de tratamiento : Medida con la que se manejara el riesgo (Aceptar, Mitigar, Transferir, Suprimir, Explotar).
- Control : Indica la enumeración del control, según el anexo A de la norma ISO 27001.
- Descripción del control: Detalla el rotulo del control.
- Acciones: Son los procedimientos para implementar el control.
- Recurso responsable: Son los elementos que se requieren para implementar las acciones.

Tabla 18. Plan de tratamiento para los riesgos identificados.

ID RIESGO		DESCRIPCIÓN	NIVEL DE RIESGO	OPCIÓN DE TRATAMIENTO	CONTROL	DESCRIPCIÓN DEL CONTROL	ACCIONES	RECURSO RESPONSABLE
1	CVE 2020-1508	Ejecución remota de código del codificador de audio de Windows media	Medio	Mitigación	A.12.2.1	Controles contra códigos maliciosos	implementar controles para la detección, prevención y protección contra códigos maliciosos. Además de la concientización de los usuarios para el uso de herramientas seguras.	Área de ciberseguridad
2	CVE 2020-25826	Integración de *pingID* para el escalamiento de privilegios locales en el inicio de sesión de Windows	Medio	Mitigación	A.9.4.2	Procedimiento de ingreso seguro	Se debe hacer uso de políticas que garanticen el control de acceso a los sistemas y aplicaciones, mediante procesos de ingreso seguro que permitan al usuario utilizar diferentes métodos de inicio de sesión.	Área de tecnología
3	CVE 2020-1338	Ejecución remota de código de Microsoft Word	Alto	Mitigación	A.13.2.3	Mensajería electrónica	Los servicios de mensajería electrónica deben incluir sistemas de protección adicionales en los activos de información que se procesan por este medio.	Área de ciberseguridad
4	CVE 2020-1581	Elevación de privilegios de hacer clic y ejecutar de Microsoft Office	Medio	Mitigación	A.12.6.2	Restricciones sobre la instalación de software	Se debe incluir una política de seguridad que establezca las reglas de instalación de software por parte de los usuarios locales.	área de seguridad de la información
5	CVE 2020-25776	Escalación de privilegios en Trend Micro Antivirus para Mac 2020 (Consumidor)	Medio	Transferir	A.15.1.3	Cadena de suministro de tecnología de información y comunicación	En los acuerdos con proveedores de servicios de seguridad en software, se deben incluir requisitos para el tratamiento de riesgos de seguridad de la información que afecten sus productos.	Proveedor y área de seguridad de la información

6	CVE 2020-5839	Divulgación de información en *Symantec Endpoint Detection*	Alto	Transferir	A.16.1.3	Reporte de debilidades de seguridad de la información	Los proveedores de servicios deben informar de cualquier fallo de seguridad que represente un riesgo en los sistemas de información de la compañía contratista para que opten medidas adicionales mientras se solventa el daño.	Proveedor y área de seguridad de la información
7	CVE 2020-12107	Inyección de comandos a través del portal web del módulo Wifi de VPNCrypt M10 2.6.5	Alto	Mitigación	A.12.2.1	Controles contra códigos maliciosos	implementar controles para la detección, prevención y protección contra códigos maliciosos. Además de la concientización de los usuarios para el uso de herramientas seguras.	Área de ciberseguridad
8	CVE 2020-17365	Escalada de privilegios en el software cliente Hotspot Shield VPN	Medio	Mitigación	A.6.2.2	Teletrabajo	Implementar políticas de seguridad que permitan proteger y brindar soporte a los activos de información, cuando estos se encuentran en lugares remotos debido al teletrabajo. Además del monitoreo de las acciones que ejecuta el usuario.	Área de seguridad de la información, ciberseguridad y tecnología
9	CVE 2020-15663	Gestión de privilegios incorrecta en Mozilla	Medio	Mitigación	A.12.5.1	Instalación de software en sistemas operativos	Establecer políticas que permitan controlar la instalación de software de terceros en sistemas operativos.	Área de tecnología
10	CVE 2020-15963	Aplicación de políticas insuficiente en las extensiones de Google Chrome	Alto	Mitigación	A.9.1.2	Política sobre el uso de los servicios de red	Se deben establecer los permisos de acceso que tienen los usuarios en la red, así como el uso de servicios adicionales como lo son las extensiones en los navegadores web.	área de seguridad de la información

En la tabla 18, se puede observar el plan de tratamientos sugerido para implementar en los riesgos identificados anteriormente. Se hace un breve resumen del riesgo identificado con su respectiva descripción, el nivel de criticidad con el que fue evaluado, la opción de tratamiento más adecuada según su naturaleza, el control más idóneo para implementar con su respectiva descripción y acción basándose en los criterios del evaluador y el recurso responsable de ejecutar el procedimiento. Finalmente, este plan de tratamiento de riesgos es tomado en cuenta por los especialistas en el análisis de riesgos de seguridad de la información de la compañía, como parte de la actualización de riesgos asociados a la seguridad de la información.

5. Análisis de resultados

Con la propuesta de la *actualización de riesgos asociados a la seguridad de la información bajo la normas ISO 27001, ISO 27005 e ISO 31000,* el grupo de especialistas de seguridad de la información de la compañía NEXA BPO logra incorporar los datos recopilados a lo largo de la investigación de riesgos de seguridad de la información identificados en el último periodo del año 2020, donde se describen 10 posibles riesgos a los cuales se les realizó un análisis detallado y una valoración individual tomando en cuenta un escenario donde una amenaza se materializa a través de una vulnerabilidad y es explotada, convirtiéndose en un riesgo para los activos de la compañía. Además, se propone la opción de tratamiento de riesgos más adecuada con su respectivo control para ser implementada en un escenario real.

Las etapas de identificación, análisis, valoración y tratamiento de riesgos se fundamentan en el conocimiento y habilidades adquiridas a lo largo de la practica en el área de seguridad de la información, garantizando el cumplimiento de las actividades propuestas anteriormente, donde a través de capacitaciones, cursos y asesorías se logra comprender mejor el campo de seguridad de la información que contribuye al desarrollo personal y profesional del estudiante y facilita el elaboración del documento anterior.

6. Conclusiones

- Las revisiones técnicas de equipos de cómputo son esenciales para dar cumplimiento a las políticas de seguridad de la información establecidas en el SGSI, debido a que permiten garantizar el adecuado uso de los dispositivos del sector operativo y administrativo de la compañía.

- La validación de eventos e incidentes de seguridad es una de las actividades más importantes para el área de seguridad de la información porque permite establecer precedentes del incumplimiento de las políticas internas del SGSI.

- La elaboración de actas de borrado seguro permite garantizar la confidencialidad y privacidad de los activos de información, eliminando cualquiera rastro de información almacenada en un dispositivo o base de datos.

- La custodia de información es de vital importancia para el área de seguridad de la información, porque permite garantizar la integridad y disponibilidad de los activos transportados de principio a fin.

- Para administrar y gestionar una red corporativa se debe hacer uso de herramientas como el Directorio Activo de Windows que permite controlar la actividad de usuarios en red.

- El área de seguridad de la información cuenta con una variedad de herramientas que permiten monitorear, gestionar y administrar proactivamente los activos de información y las TIC.

7. Glosario

- ADWARE: Programa que automáticamente muestra u ofrece publicidad no deseada o engañosa.
- APIS: Interfaz de programación de aplicaciones.
- BOTNETS: Conjunto o red de robots informáticos o *bots*, que se ejecutan de manera autónoma y automática.
- BUFFER: Espacio de memoria en el que se almacenan datos de forma temporal mientras se están transfiriendo de un sitio a otro.
- CMD: El símbolo del sistema.
- Código SQL: Lenguaje de consulta estructurada.
- COOKIES: Son archivos que guardan información de los sitios visitados en la red.
- CSV: Formato de Excel.
- DHCP: Protocolo de configuración dinámica de host.
- DIRECCION MAC: es un identificador que corresponde de forma única a una tarjeta o dispositivo de red.
- DNS: Sistema de nombres de dominio.
- EXPLOITS: Fragmento de software, fragmento de datos o secuencia de comandos o acciones.
- FIREWALL: Un cortafuegos es la parte de un sistema o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
- GUSANOS: Malware que se replica para propagarse a otras computadoras.
- HOST: Hospedaje o anfitrión, es cualquier computadora o máquina conectada a una red.
- HTML: Lenguaje de marcado que se utiliza para el desarrollo de páginas de Internet.
- ICMP: Protocolo de control de mensajes de Internet.
- IP: Interfaz de programación.
- ISO: *International Organization for Standardization* u Organización Internacional de Normalización.
- JSON: Formato de texto sencillo para el intercambio de datos.
- KERBEROS: Protocolo de autenticación de redes de ordenador creado por el MIT que permite a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura.
- KEYLOGGERS: Registro de pulsaciones de teclas es un método mediante el que se registra cada tecla que el usuario pulsa en el teclado del ordenador.

- LDAP: Protocolo ligero de acceso a directorios.
- NMAP: Programa de código abierto que sirve para efectuar rastreo de puertos.
- OUTSOURCING: Subcontratación de servicios.
- PASSPOINT: Tarjeta de autenticación de usuarios.
- POWERSHELL: Herramienta avanzada de configuración y control de un sistema basado en Windows.
- RANSOMWARE: Tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.
- ROOT: El super usuario *o root* es el nombre convencional de la cuenta de usuario que posee todos los derechos en todos los modos.
- SEP: Symantec Endpoint Protection.
- SGSI : Sistema de Gestión de Seguridad de la Información.
- SOA: *Statement of Applicability* o declaración de aplicabilidad.
- SSH: Protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet con mecanismo de autenticación.
- TCP: Protocolo de control de transmisión.
- TIC: Tecnologías de la información y la comunicación.
- TROYANOS: Tipo de malware que a menudo se disfraza de software legítimo.
- TXT: Archivo de texto.
- UDP: Protocolo de datagramas de usuario.
- VPN*: Virtual Prívate Network* o red privada virtual.

8. Referencias

Broadcom. (2020). *Symantec Messaging Gateway*. Obtenido de Cómo mantener actualizadas las definiciones de virus: https://help.symantec.com/cs/SMG_10_7_0/SMG/v39944899_v132085995/C%C3%B3mo-mantener-actualizadas-las-definiciones-de-virus?locale=ES_ES

SoftPerfect. (2020). *Escáner de red SoftPerfect*. Obtenido de softperfect.co: https://www.softperfect.com/products/networkscanner/

Aranda Device Management. (2020, Septiembre). Obtenido de arandasoft.com: https://arandasoft.com/device-management/

Aranda Software. (2017). *Aranda Device Management V9 Manual de Instalacion y Uso .* Obtenido de arandasoft.com: https://arandasoft.com/downloads/manuales/aranda-device-management-v9-espanol.pdf

Aranda Software. (2020). *Aranda Device Management*. Obtenido de arandasoft.com: https://arandasoft.com/device-management/

Art.15 . (2020). *Constitución Política de la República de Colombia 1991.* Obtenido de secretariasenado.gov.co: http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

CONSTITUCIÓN POLITICA DE LA REPÚBLICA DE COLOMBIA [Const].Art.15. (1991, Julio 20). Obtenido de secretariasenado.gov.co: http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

FIRST.Org, Inc. (2019, Junio). *Common Vulnerability Scoring System version 3.1.* Obtenido de first.org/cvss/user-guide: https://www.first.org/cvss/v3-1/cvss-v31-user-guide_r1.pdf

ISO / IEC 27001: 2013 Tecnología de la información -Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos. (2013).

ISO / IEC 27005: 2018 Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información. (2018).

ISO 31000: 2018 Gestión de riesgos: Principios y directrices. (2018).

ISOTools. (2015, Octubre 05). *Cómo implantar eficazmente la norma ISO 27005*. Obtenido de isotools.org: https://www.isotools.org/2015/10/05/como-implantar-eficazmente-la-norma-iso-27005/

ISOTools. (2020, Agosto). *La norma ISO 27001 Aspectos clave de su diseño e implementación*. Obtenido de isotools.org: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

ISOTools. (2020, Julio). *Norma ISO 31000 El valor de la gestión de riesgos en las organizaciones*. Obtenido de isotools.org: https://www.isotools.org/pdfs-pro/ebook-iso-31000-gestion-riesgos-organizaciones.pdf

LEY 1273. (2009, Enero 05). Obtenido de secretariasenado.gov.co: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

LEY 599 . (2000, Julio 24). Obtenido de secretariasenado.gov.co: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

LEY 87. (1993, Noviembre 29). Obtenido de secretariasenado.gov.co: http://www.secretariasenado.gov.co/senado/basedoc/ley_0087_1993.html

LEY ESTATUTARIA 1266. (2008, Diciembre 31). Obtenido de secretariasenado.gov.co: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

LEY ESTATUTARIA 1581. (2012, Octubre 18). Obtenido de secretariasenado.gov.co: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

MAGERIT v3.0. (2012, Octubre). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método.* Madrid: Ministerio de Hacienda y Administraciones Públicas. Obtenido de administracionelectronica.gob.es: http://administracionelectronica.gob.es/

Metodoss . (2020). *Metodología Cobit*. Obtenido de metodoss.com: https://metodoss.com/metodologia-cobit/

National Vulnerability Database (NVD). (s.f.). *Search Vulnerability Database*. Obtenido de nvd.nist.gov: https://nvd.nist.gov/vuln/search

NIST. (2020). Obtenido de National Institute of Standards and Technology : https://www.nist.gov

Norma ISO 27001. (2013, Octubre). *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos*.

Norma ISO 27005. (2018, Julio). *Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información*.

Norma ISO 31000. (2018, Febrero). *Gestión de riesgos: directrices*.

NVD. (2020). Obtenido de NATIONAL VULNERABILITY DATABASE : https://nvd.nist.gov/

OBS. (2020). *¿Qué son los activos de una empresa y cómo se valoran?* Obtenido de obsbusiness.school: https://obsbusiness.school/es/blog-investigacion/finanzas/que-son-los-activos-de-una-empresa-y-como-se-valoran

Red Hat. (2020). *El concepto de CVE*. Obtenido de redhat.com: https://www.redhat.com/es/topics/security/what-is-cve

riesgoscero. (2020, Septiembre 25). *Manual para implementar la seguridad de la información,según la ISO 27001*. Obtenido de riesgoscero.com: https://www.riesgoscero.com/academia/especiales/manual-para-implementar-la-seguridad-de-la-informacion-segun-la-iso-27001

Symantec Corporation. (2007). *Guía de instalación para Symantec Endpoint Protection y Symantec Network Access Control.*

Tecon. (2019, Enero 28). *La Seguridad de la Información*. Obtenido de Tecon.es: https://www.tecon.es/la-seguridad-de-la-informacion/

Apéndice 1. Documentos adjuntos

- Anexos