UNIVERSIDAD SANTO TOMAS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA
T U N J A

Apoyo en la implementación de protocolos preventivos y correctivos de seguridad de la información, aplicados en la Empresa de Energía de Boyacá S.A. E.S.P.

PROPONENTE(S)
Laura Michel Bolívar Rincón
1002365862
2252539

DIRECTOR
Ing.Andrea Cruz Yomayusa

Tunja

Contenido

Referencias de Tablas

Referencias de tabla de figuras

1. FICHA TÉCNICA DE LA PASANTÍA

Tabla 1

Ficha técnica de la pasantía

Título	Apoyo en la implementación de protocolos preventivos y correctivos de seguridad de la información, aplicados en la Empresa de Energía de Boyacá S.A. E.S.P.
Nombre Estudiante	Laura Michel Bolívar Rincón
Documento estudiante	1002365860
Correo electrónico	Laura.bolivarr@usantoto.edu.co
Director	Ing.Andrea Cruz Yomayusa
Entidad o sector de la empresa	Empresa de Energía de Boyacá S.A. E.S.P
Lugar de ejecución de la pasantía	Tunja, Boyacá
Duración	4 meses
Los abajo firmantes confirman que todos los datos incluidos en la presente propuesta son correctos y verídicos, que no incumplen ninguna ley o norma vigente. (Incluir nombres y firmas de estudiantes, director y tutor).	

Laura Michel Bolívar Rincón

Firma del director
Ing.Andrea Cruz Yomayusa

2. PLANTEAMIENTO DEL PROBLEMA

En la actualidad, la información se ha vuelto un activo clave en las organizaciones, tanto públicas como privadas, puesto que todas ellas manejan datos para poder realizar sus actividades y necesitan garantizar su protección e integridad de acuerdo con las leyes vigentes. Por esta razón, la Empresa de Energía de Boyacá S.A. E.S.P ha venido implementando sistemas de seguridad de la información con soluciones tecnológicas y metodológicas, para permitir analizar las amenazas existentes internas y externas. Sin embargo, estos procesos se encuentran en una constante maduración a la política de seguridad de la información debido a que cada día aparecen nuevos riesgos y vulnerabilidades que ponen en peligro los datos de la empresa.

Dichas vulnerabilidades se pueden presentar por parte del personal, debido a que no se capacita debidamente frente a las amenazas existentes o realiza un mal manejo de las herramientas suministradas, de tal forma que la empresa queda expuesta a recibir ataques tales como suplantación de identidad (phishing) o conceder el ingreso de un malware a los sistemas de información por medio de algún correo, archivo, fotografía, entre otros.

Así mismo, la falta de actualizaciones en los sistemas operativos de los equipos de cómputo manejados pone en peligro la información sensible y confidencial de la empresa, permitiendo que intrusos puedan hacer uso de ella con distintos fines.

Es de resaltar que el departamento de Seguridad de la Información ha estado en un proceso de consolidación en la empresa desde el año 2017 abarcando todo el departamento de Boyacá teniendo sedes en Tunja y Duitama , en dicho proceso se ha implementado el Marco de Ciberseguridad del Instituto de Estándares y Tecnología (NIST) para la mitigación de riesgos, el cual trata de una metodología simultanea y continua para reducir el riesgo vinculado a las amenazas cibernéticas que puedan comprometer la seguridad de la información (Pirani, 2023).

De acuerdo con lo anterior, el propósito de la pasantía busca conocer aquellos aspectos que ayuden a identificar, proteger, detectar y responder a los riesgos asociados al manejo de la información, por medio de protocolos preventivos y correctivos siguiendo el marco el Marco de Ciberseguridad del Instituto de Estándares y Tecnología (NIST).

3. OBJETIVOS

3.1 Objetivo General

Apoyar la implementación de protocolos preventivos y correctivos de seguridad para la mitigación de riesgos asociados al manejo de la información, aplicados en la Empresa de Energía de Boyacá S.A E.S.P.

3.2 Objetivos Específicos

1. Evaluar vulnerabilidades informáticas de la Empresa de Energía de Boyacá S.A. E.S.P. mediante las herramientas informáticas Tenable SC, AMP CISCO, MISP.

2. Proponer planes de remediación para disminuir las vulnerabilidades en la infraestructura de tecnologías de la información de la Empresa de Energía de Boyacá S.A. E.S.P.

3. Capacitar en temas de seguridad de la información al nuevo personal de la Empresa de Energía de Boyacá S.A. E.S.P. y a empleados que hayan estado expuestos a vulnerabilidades informáticas.

4. DESCRIPCIÓN DE LAS ACTIVIDADES REALIZADAS

Es importante aclarar que las actividades no se realizaron de forma secuencial o escalonada. Por el contrario, se mantuvieron constantes por periodos prolongados durante la pasantía.

4.1. *Evaluación de vulnerabilidades informáticas*

4.1.1. *Inducción del uso de metodologías y uso de herramientas*

La Empresa de Energía de Boyacá está categorizada como infraestructura crítica, la cual se entiende como todos aquellos sistemas físicos, tecnológicos o humanos esenciales para el funcionamiento continuo de la sociedad y la economía. La interrupción o colapso de una infraestructura crítica puede tener efectos graves y amplios en otros sectores, así como en la sociedad en general debido a su importancia. Las infraestructuras críticas son objetivos potenciales de ataques cibernéticos, terrorismo y otras formas de amenazas, por lo tanto, la protección de estas infraestructuras es fundamental para garantizar la resiliencia y la continuidad de los servicios esenciales para la sociedad.

Es por ello que el Departamento de Seguridad de la Información ha venido implementando el Marco de Ciberseguridad del Instituto de Estándares y Tecnología (NIST) para la gestión de riesgos en la infraestructura tecnológica de la empresa. Para ello, aplica las cinco categorías básicas del marco NIST, que son: identificar, proteger, detectar, responder y recuperar, mediante la integración de protocolos preventivos y correctivos.

Para el Inicio de la pasantía, el Departamento de Seguridad de la información brindó dos capacitaciones dirigidas por el jefe del Departamento, con el objetivo proporcionar los conocimientos, habilidades y competencias necesarias para desarrollar las demás actividades de la pasantía. Cada capacitación tuvo duración de una semana. Para el desarrollo de las capacitaciones se proporcionaron diferentes recursos, como manuales, documentos, artículos y tutorías. Durante la primera capacitación, se presentaron ejemplos concretos del marco NIST, junto con sus protocolos preventivos y correctivos, utilizando los manuales de seguridad establecidos por la empresa. Además, se realizó el reconocimiento de la infraestructura tecnológica de Tunja y Duitama mediante documentos y guías proporcionados por el departamento de seguridad de la información.
En la segunda capacitación, el jefe del Departamento de Seguridad de la Información proporcionó manuales y tutorías para explicar el uso de herramientas informáticas como Tenable SC, AMP de Cisco y MISP, las

cuales se utilizaron para monitorear vulnerabilidades en la infraestructura tecnológica. Así mismo, el jefe del departamento brindó los conocimientos necesarios por medio de guías y videos instructivos para administrar la plataforma de Knowbe4 con el fin de llevar a cabo cursos de ciberseguridad a los trabajadores de la empresa.

Cabe destacar que las siguientes actividades no se llevaron a cabo de forma secuencial o escalonada, por el contrario, se mantuvieron constantes por periodos prolongados durante la pasantía. De esta manera, el contenido cubierto en las capacitaciones fue:

- Introducción al marco NIST y su aplicabilidad en la infraestructura tecnológica de la empresa.
- Revisión de las cinco categorías del marco NIST: identificar, proteger, detectar, responder y recuperar.
- Protocolos correctivos y preventivos implementados en cada una de las cinco categorías del marco NIST.
- Ejemplos de aplicación del marco NIST en la empresa.
- Manejo de la herramienta Tenable SC para el análisis y monitoreo de vulnerabilidades mensualmente.
- Manejo de la herramienta AMP de CISCO para la detección diaria de amenazas en tiempo real en los Endpoints.
- Manejo de la herramienta Knowbe4 para la administración de cursos de ciberseguridad impartidos a los empleados de la empresa.
- Consideraciones para la implementación del marco NIST en la infraestructura tecnológica de la empresa.

Por otra parte, en el manejo de las herramientas tecnologías se utilizan los siguientes recursos:

1. En la tabla 2 se presentan los medios, herramientas e instrumentos que el jefe del departamento proporcionó para llevar a cabo las capacitaciones mencionadas anteriormente.

Tabla 2

Recursos otorgados por el Departamento de Seguridad de la Información

Recursos	Elementos
Medios	• Documentos y artículos de la empresa • Manuales • Sitios Web • Tutoriales
Instrumentos y/o herramientas	• Sitio de trabajo • Conexión a internet • Computador • Programas del computador ✓ Navegador Web ✓ Herramienta Tenable SC ✓ Herramienta AMP de CISCO ✓ Knowbe4
Salidas	Conocimiento y fortalecimiento de herramientas informáticas para la detección de vulnerabilidades en la infraestructura tecnológica de la empresa.

Fuente: Autor

2. En la tabla 3 se especifican los protocolos preventivos y correctivos necesarios para cubrir todos los riesgos potenciales, clasificados según las cinco categorías del marco NIST: identificar, proteger, detectar, responder y recuperar.

Tabla 3

Protocolos preventivos y correctivos del marco NIST

Categoría	Descripción	Protocolos
Identificar	Se enfoca en identificar y comprender los activos, sistemas, procesos y personas que necesitan protección contra posibles amenazas de ciberseguridad. Implica comprender riesgos y las vulnerabilidades existentes en la empresa.	• Gestión de activos (ID.AM) • Entorno empresarial (ID.BE) • Gobernanza (ID.GV) • Evaluación de riesgos (ID.RA) • Estrategia de gestión de riesgos (ID.RM) • Gestión del riesgo de la cadena de suministro (ID.SC)

Categoría	Descripción	Protocolos
Proteger	Establece medidas y controles para proteger los sistemas, activos y datos críticos de la empresa. Esto incluye la implementación de políticas y procedimientos, la asignación de roles y responsabilidades de seguridad y la capacitación del personal.	• Gestión de identidad, autenticación y control de acceso (PR.AC) • Concienciación y capacitación (PR.AT) • Seguridad de los datos (PR.DS) • Procesos y procedimientos de protección de la información (PR.IP): • Mantenimiento (PR.MA): • Tecnología de protección (PR.PT)
Detectar	Identifica las posibles amenazas y ataques de ciberseguridad que puedan afectar a la empresa. Esto incluye la implementación de herramientas y tecnologías de detección de amenazas con el fin de reportar incidentes de seguridad.	• Anomalías y Eventos (DE.AE) • Monitoreo Continuo de la Seguridad (DE.CM) • Procesos de Detección (DE.DP)
Responder	Establecen procedimientos para responder rápidamente a los incidentes de seguridad que se produzcan. Esto implica la creación de planes de respuesta a incidentes, la asignación de roles y responsabilidades	• Planificación de la Respuesta (RS.RP) • Comunicaciones (RS.CO): • Análisis (RS.AN) • Mitigación (RS.MI): • Mejoras (RS.IM)
Recuperar	Se enfoca en la recuperación de una organización después de un incidente de seguridad. Esto incluye la implementación de planes de continuidad del negocio y la recuperación de desastres, la restauración de sistemas y datos del impacto del incidente de la organización	• Planificación de la recuperación (RC.RP) • Mejoras (RC.IM) • Comunicaciones (RC.CO)

Fuente: Autor

4.1.2. *Evaluación y análisis de vulnerabilidades*

4.1.2.1 Uso de herramienta Tenable SC

Tenable SC es una plataforma de gestión de vulnerabilidades y cumplimiento de seguridad desarrollada por la empresa Tenable. Esta herramienta se enfoca en la recopilación, gestión y análisis de datos relacionados con la seguridad de la red y los sistemas, incluyendo información sobre vulnerabilidades, configuraciones, eventos de seguridad y cumplimiento de políticas y regulaciones. Tenable SC utiliza diversas técnicas para detectar y evaluar vulnerabilidades en sistemas y dispositivos de red, incluyendo escaneo de puertos,

detección de servicios y vulnerabilidades conocidas, y el análisis de configuraciones. Además, permite la creación de políticas de seguridad personalizadas y el seguimiento del cumplimiento de los estándares de seguridad y regulaciones, como el PCI-DSS, HIPAA y SOX. (Tenable, 2023).

Teniendo en cuenta la categoría Detectar (DE) del marco NIST, se implementó el protocolo de Monitoreo Continuo de la Seguridad (DE.CM) mediante el uso de la herramienta Tenable SC. Durante la primera semana de enero, febrero y marzo, se llevó a cabo el seguimiento de las vulnerabilidades en los servidores de la empresa, ubicados en Tunja y Duitama, con el fin de detectar y evaluar posibles riesgos de seguridad. En enero de 2023, se generó mediante de la herramienta Tenable SC un informe del monitoreo de las vulnerabilidades encontradas en los servidores de la empresa, las cuales se clasificaron para su correspondiente análisis.

Para dicha clasificación, se empleó el sistema de categorización de Tenable, el cual consta de cuatro categorías con distintos niveles de gravedad. La tabla 4 se presenta la categorización por niveles de gravedad para las vulnerabilidades informáticas.

Tabla 4

Categorización de vulnerabilidades informáticas

Nombre	Descripción
Vulnerabilidades Criticas (9.0-10.0)	Estas vulnerabilidades representan la amenaza más grave y pueden comprometer la seguridad de un sistema de manera significativa. Permiten a los atacantes acceder a información confidencial, ejecutar código malicioso, tomar control del sistema, entre otros.
Vulnerabilidades de Alta gravedad (7.0-8.9)	Estas vulnerabilidades pueden permitir a los atacantes el acceso no autorizado, eludir mecanismos de seguridad, ejecutar código malicioso, entre otros.
Vulnerabilidades de gravedad media (4.0-6.9)	Estas vulnerabilidades pueden permitir a los atacantes realizar diversas acciones maliciosas, como la ejecución remota de código, la obtención de información confidencial, entre otros.
Vulnerabilidades de baja gravedad	Estas vulnerabilidades son menos graves que las anteriores, pero aun así pueden permitir a los atacantes

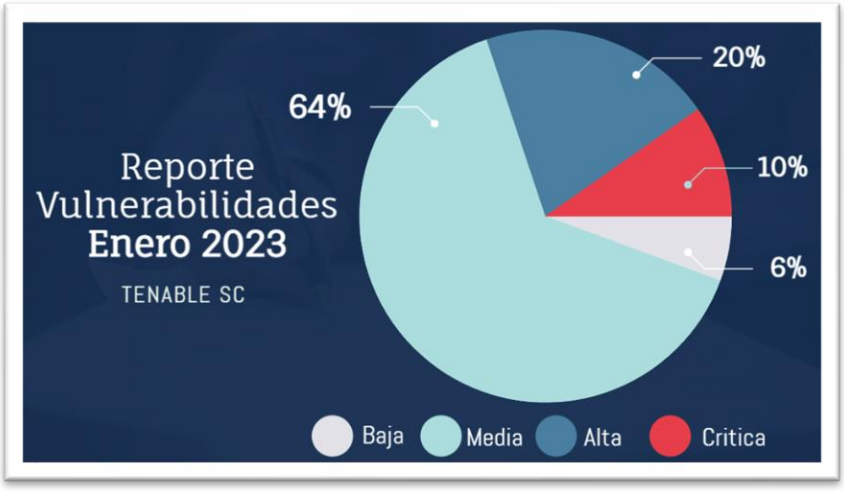
(0.1-3.9)	realizar ciertas acciones no autorizadas o comprometer la seguridad de un sistema de alguna manera.

Fuente: Tenable

Considerando el reporte suministrado por Tenable SC y la tabla de vulnerabilidades, se realiza el análisis de los riesgos informáticos encontrados en el mes de enero del 2023 representados en la figura 1:

Figura 1

Reporte de vulnerabilidades enero 2023



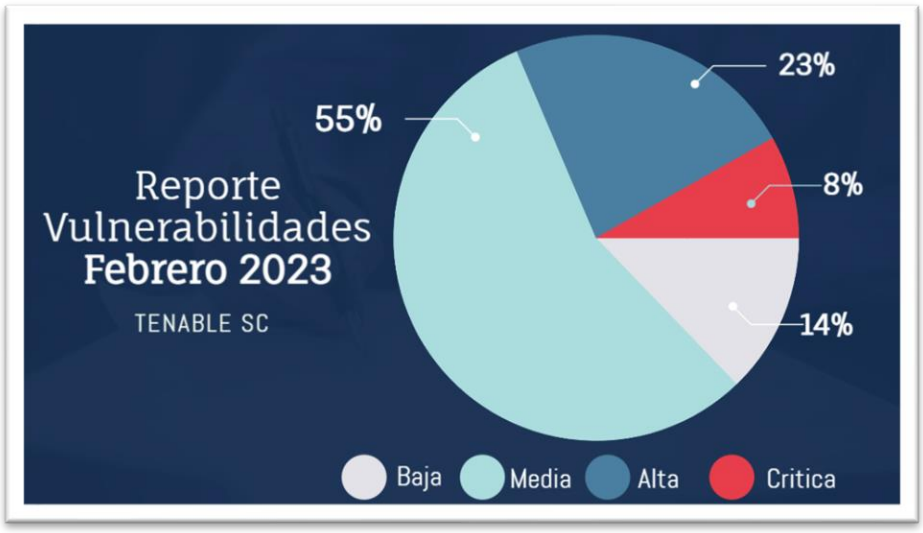
Fuente: Autor

De acuerdo con el informe generado por la herramienta Tenable SC correspondiente al mes de enero 2023, se realizó un análisis estadístico que permitió determinar que las vulnerabilidades de gravedad media son las más comunes, representando el 64% de los riesgos informáticos detectados, por lo tanto, se requiere una atención prioritaria para su mitigación y corrección. Asimismo, se destaca la importancia de la pronta atención a los riegos informáticos críticos y de alta gravedad, con el fin de evitar posibles consecuencias perjudiciales para la infraestructura tecnológica de la empresa

Debido a las disposiciones de confidencialidad de la información de la empresa, no es permitido proporcionar el número total y el nombre de las vulnerabilidades encontradas en cada mes. No obstante, es relevante resaltar que en el mes de febrero se registró un aumento en los riesgos informáticos debido a la presencia de fallos de seguridad que no fueron corregidos durante el mes anterior, así como a la aparición de nuevas vulnerabilidades detectadas en dicho mes como se puede observar en la figura 2.

Figura 2

Reporte de vulnerabilidades febrero 2023

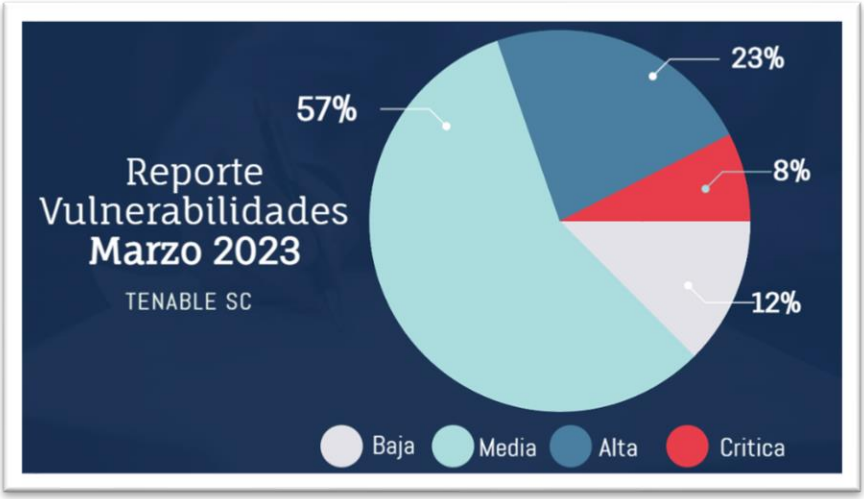


Fuente: Autor

Según el análisis del reporte generado por Tenable SC, las vulnerabilidades de gravedad media se mantienen como las más comunes, representando el 55% de los riesgos informáticos monitoreados. Aunque los porcentajes mostrados en la gráfica son menores en comparación con la del mes de enero, las cifras de febrero registradas indican que se hallaron el doble de vulnerabilidades que el mes anterior. Así mismo, según el análisis del reporte de Tenable SC en el mes de marzo, se observó un incremento de riesgos informáticos en comparación con los meses anteriores como se observa en la *figura 3.*

Figura 3

Reporte de vulnerabilidades marzo 2023



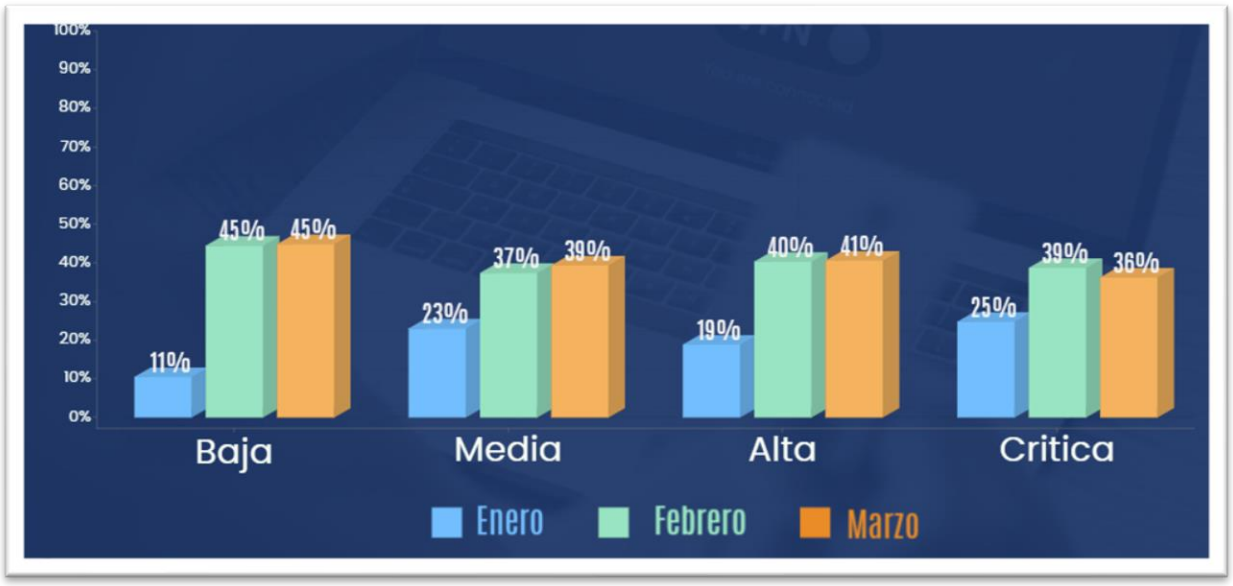
Fuente: Autor

De acuerdo con la figura 3, se puede observar que las vulnerabilidades de gravedad alta y crítica representan una proporción significativa del total de vulnerabilidades encontradas. Esta tendencia sugiere que los sistemas informáticos continuaron siendo vulnerables a ataques cibernéticos graves debido a que no se tomaron las medias de seguridad pertinentes para reducir estos riesgos.

A partir de las vulnerabilidades encontradas de los análisis realizados mediante los diversos informes de Tenable SC, se ha elaborado un plan de remediación que se detalla en la sección "Elaboración de planes de remediación en la infraestructura tecnológica". El objetivo principal de estos planes es abordar los riesgos informáticos monitoreados y reducir el riesgo de posibles ataques cibernéticos. Parala figura 4 , se consideró el 100% de las vulnerabilidades monitoreadas durante los tres meses, con el fin de comparar el incremento de los tipos de riesgos informáticos en cada mes. Este análisis permitió identificar las tendencias y cambios en el panorama de riesgos informáticos a lo largo del tiempo, lo cual es importante para evaluar la efectividad de las medidas de seguridad implementadas y para ajustar las estrategias de seguridad en consecuencia.

Figura 4

Comparación incremento de tipos de vulnerabilidades



Fuente: Autor

Como se puede observar en la figura 4, se evidencia un aumento significativo en la cantidad total de tipos de vulnerabilidades encontradas a lo largo de los meses. El incremento más notable se registró de enero a febrero en todas las categorías (baja, media, alta y crítica). Esto se debe a la falta de implementación de medidas de mitigación en todos los riesgos informáticos, identificados en cada mes, lo que generó una acumulación de fallos de seguridad.

4.1.2.2 Uso las herramientas AMP de CISCO y MISP

El antivirus Cisco AMP es una solución antivirus de última generación diseñada para proteger a las organizaciones contra amenazas avanzadas y malware. Utiliza técnicas avanzadas de detección como el análisis de comportamiento, la inteligencia artificial y el aprendizaje automático para detectar y bloquear amenazas en tiempo real, antes de que puedan causar daño a los sistemas y dispositivos de una organización. Cisco AMP ofrece una mayor visibilidad de la actividad de la red y de los dispositivos, lo que permite a los equipos de seguridad responder de manera más rápida y eficiente a las amenazas y tomar medidas preventivas. La solución también cuenta con capacidades de respuesta automática para acelerar la eliminación de las amenazas. (CISCO, 2023).

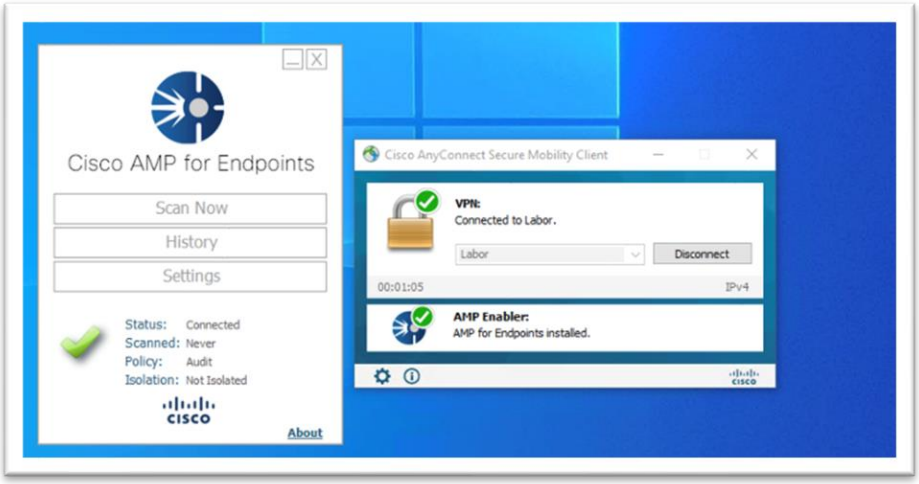
Para garantizar la seguridad de los dispositivos finales (endpoints) de la empresa, los cuales se utilizan para conectarse a la red y acceder a recursos y servicios, se ha implementado el protocolo de Gestión de Identidad, Autenticación y Control de Acceso (PR.AC) de la categoría Proteger (PR) del marco NIST. Este protocolo incluye medidas de seguridad sólidas como el cifrado de datos, el uso de contraseñas seguras y la autenticación multifactor, con el fin de mitigar los riesgos de vulnerabilidades y ataques informáticos en los endpoints.

Para aplicar el protocolo mencionado, se ha instalado el software antivirus AMP de Cisco en los equipos electrónicos de los empleados y en los servidores virtualizados. Esta herramienta se encarga de monitorear continuamente los archivos descargados a través de aplicaciones empresariales, correo electrónico y/o el navegador como imágenes, documentos y videos. Si se detecta algún archivo con fallos de seguridad, la herramienta lo aísla para su análisis, además, en caso de encontrar alguna vulnerabilidad informática en el archivo, el dispositivo se suspende para realizar las pruebas necesarias y remediar la brecha de seguridad.

En la figura 5 se puede observar que el antivirus AMP de Cisco previamente instalado y configurado, el cual permanece funcionando constantemente en los dispositivos finales.

Figura 5

Antivirus AMP de Cisco instalado en un endpoint

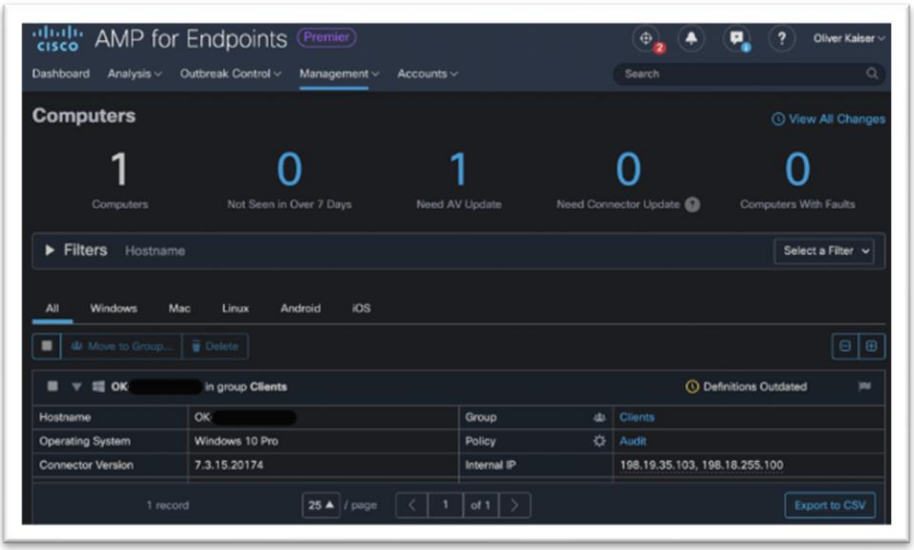


Fuente: Autor

Cuando se detecta que un empleado ha descargado un archivo que contiene una amenaza informática, se genera un informe y se le ofrece al empleado una capacitación educativa sobre los riesgos informáticos, la cual se detalla en la sección "ejecución de capacitaciones de seguridad de la información". Además, el antivirus AMP de Cisco permite identificar las actualizaciones que necesitan las aplicaciones instaladas en los endpoint, con el fin de prevenir brechas de seguridad informáticas. En la figura 6 se muestra el panel de control del antivirus AMP de Cisco en la sección de actualizaciones de los endpoints. Este panel se utilizaba diariamente para monitorear la cantidad de parches que debían ser implementados en cada dispositivo, con el fin de elaborar un informe semanal.

Figura 6

Panel de control del antivirus AMP de Cisco



Fuente: Autor

En la sección “Elaboración de planes de remediación en la infraestructura tecnológica” se especifica el plan de remediación para el informe semanal del antivirus AMP de Cisco, en el cual se registraba el nombre del endpoint junto con su respectiva IP y el tipo de actualización que requería cada aplicación. Esta información es esencial para planificar las acciones necesarias, a fin de mantener la seguridad y el buen funcionamiento de la infraestructura tecnológica.

A su vez, siguiendo el protocolo Evaluación de riesgos (ID.RA) de la categoría Identificar (ID) del marco NIST, se utiliza la herramienta MISP (Malware Information Sharing Platform), la cual es una herramienta de código abierto que permite el intercambio seguro de información sobre amenazas informáticas, incluyendo malware, indicadores de compromiso (IoC) y tácticas, técnicas y procedimientos (TTP) utilizados por los atacantes. MISP está diseñado para ser utilizado por organizaciones de seguridad, empresas, gobiernos y comunidades de investigación en todo el mundo. La herramienta permite a los usuarios compartir información de manera confidencial y controlada, lo que significa que los datos compartidos solo están disponibles para aquellos que tienen permisos específicos. Esto ayuda a garantizar que la información se comparta solo con las partes interesadas y limita el riesgo de que la información se divulgue de manera inapropiada. (MISP, 2023).

Diariamente se realizaba un seguimiento de los eventos registrados en la plataforma MISP por otras empresas, con el fin de documentar y mitigar las posibles amenazas cibernéticas que se pudieran presentar. En la tabla 5 se especifican los eventos registrados durante el desarrollo de la presente pasantía:

Tabla 5

Amenazas cibernéticas

Nombre del evento	Descripción
Ransomware Sector Salud Colombia	Los sistemas y datos de las instituciones de salud son secuestrados y encriptados. Los atacantes exigen un rescate para liberar los datos y restaurar el acceso a los sistemas. Esto puede tener graves consecuencias en la atención médica y la privacidad de los pacientes. En el caso de Colombia el ransomware denegó el acceso al uso de los servicios virtuales para reclamar medicamentos y asignar citas médicas. Uno de los puntos más graves se dio por causa de los ciberdelincuentes al publicar pruebas de información sobre los pacientes y algunos datos fiscales de la EPS en internet.
Crywiper	Es un malware identificado por los investigadores de Kaspersky. Aunque inicialmente se parece a un ransomware, en realidad es un limpiador. Modifica archivos, agrega la extensión. CRY y muestra una nota de rescate, pero en realidad no encripta los archivos, los sobrescribe de manera aleatoria. El objetivo de los ciberdelincuentes detrás del malware es causar daño destruyendo datos en lugar de buscar un rescate económico. CryWiper corrompe archivos y bases de datos, reinicia el sistema regularmente,

Nombre del evento	Descripción
	detiene procesos relacionados con servidores y deshabilita la conexión remota RDP.
Ransomware BlackCat	Se descarga a través de archivos Microsoft Office que contiene un ejecutable malicioso incrustado. La carga útil contiene un código que permite que el malware se extienda a través de la red comprometida, apuntando tanto a sistemas Windows como Linux. Se describe como un ataque "multetapa" con el objetivo de explotar las cuentas de usuario y de administrador de Active Directory para cifrar los archivos de los ordenadores objetivo. Además, aprovecha las credenciales de usuario previamente comprometidas para obtener el acceso inicial al sistema víctima.
Phishing - Cambio credenciales Office 365	El Laboratorio de Investigación de ESET descubrió una campaña de phishing que busca obtener las credenciales de acceso a los servicios de correo electrónico de Microsoft. El correo falso, que se hace pasar por Microsoft Outlook, afirma detectar actividad inusual en la cuenta y solicita al usuario hacer clic en un enlace para revisar la actividad reciente. El enlace conduce a una página falsa con un certificado que aparenta ser legítimo. En esta página, se solicitan las credenciales de acceso, lo que permite a los atacantes obtener los datos de la cuenta de la víctima. Aunque hay indicios que pueden revelar la falsedad del sitio, como errores en la dirección URL y en la interfaz, muchos usuarios incautos pueden caer en la trampa. Una vez que los atacantes obtienen la información sensible, la estafa finaliza.
Malware Pyration	Se propaga a través de correos electrónicos de phishing que contienen un archivo adjunto malicioso protegido por contraseña. Al descomprimirlo, se ejecutan archivos de acceso directo que descargan archivos adicionales en la carpeta temporal del usuario. Estos archivos incluyen un script de Python disfrazado como "CortanaAssistance.exe" para hacer que parezca un archivo del sistema. El malware PY#RATION ha evolucionado con versiones más avanzadas que pueden realizar escaneos en redes comprometidas y ocultar su código utilizando cifrado. También tiene la capacidad de transferir archivos, registrar pulsaciones de teclas, ejecutar comandos del sistema, extraer contraseñas y cookies de navegadores web, capturar datos del portapapeles y verificar la presencia de software antivirus. El malware PY#RATION es difícil de detectar y su flexibilidad radica en que está compilado en Python, lo que permite su ejecución en sistemas operativos Windows, OSX y Linux.

Nombre del evento	Descripción
IOCs explotación vulnerabilidad VMWARE	El CCN-CERT ha alertado sobre una campaña de explotación de vulnerabilidades dirigida a servidores VMware ESXi, un sistema operativo utilizado para alojar máquinas virtuales. Los ataques aprovechan una vulnerabilidad identificada como CVE-2021-21974, la cual fue notificada por VMware en un aviso de seguridad. Se estima que más de 3200 servidores han sido comprometidos, afectando a organizaciones en diferentes países, VMware ha publicado una actualización de seguridad para abordar esta vulnerabilidad.
Malware BitRAT/QuasarRAT	Hackers están robando a otros hackers a través de foros frecuentados por ellos, ofreciendo programas que contienen malware. Los hackers inexpertos caen en la trampa al descargar estos programas gratuitos y se infectan con malware que les roba información o realiza acciones maliciosas. Este tipo de ataques está en aumento y se ha observado en diferentes casos, como la oferta de secuestradores de portapapeles y programas de robo de criptomonedas. Los hackers más experimentados están aprovechando la confianza y la búsqueda de herramientas gratuitas para engañar a otros hackers y obtener beneficios.
Muestras Killnet	Ha sido descubierto en VirusTotal y se caracteriza por encriptar archivos y exigir un rescate para descifrarlos. Después de ejecutarlo, los archivos se renombran con la extensión ".killnet" y se crea una nota de rescate en ruso llamada "Ru.txt". El ransomware cambia el fondo de pantalla del escritorio y ofrece contactos para comunicarse con los atacantes. Aunque se cumplan las demandas de rescate, no se garantiza la recuperación de los datos y pagar apoya la actividad delictiva. Se recomienda eliminar el ransomware del sistema y contar con copias de seguridad como medida preventiva ante la pérdida permanente de datos.

Fuente: Autor

En la tabla del registro de los eventos también se incluían las IPs, correos electrónicos y/o URLs que debían ser bloqueados en el firewall o en Office 365, para evitar los ciberataques que pudieran impactar en la empresa. El plan de remediación para la mitigación de los eventos se detalla en la sección "Elaboración de planes de remediación en la infraestructura tecnológica"

4.1.3. *Auditoría a empresas proveedoras de servicios críticos*

La realización de auditorías a los proveedores que prestan servicios críticos a la infraestructura de TI es crucial para garantizar la seguridad y eficacia de los sistemas y datos de la organización. A través de las auditorías se pueden identificar posibles riesgos de seguridad y privacidad, evaluar el desempeño del proveedor en cuanto a calidad de servicio, cumplimiento de requisitos y normativas, además de fortalecer la relación entre ambas partes. Estas actividades contribuyen a asegurar que los proveedores estén alineados con las necesidades y expectativas del negocio.

Para ello, el Departamento de Seguridad de la Información hace uso del protocolo de Gestión del riesgo de la cadena de suministro (ID.SC) de la categoría Identificar (ID) del marco NIST, el cual se enfoca en tres áreas claves: identificación, evaluación y mitigación de los riesgos asociados a los proveedores. En primer lugar, la identificación de proveedores implica recopilar información relevante sobre ellos, incluyendo sus políticas de seguridad, gestión de riesgos, historial de seguridad y otros factores. En este caso, se identificaron cuatro proveedores de servicios críticos en la infraestructura tecnológica, de los cuales solo se realizaron auditorías a tres. La empresa faltante no pudo ser auditada por cuestiones de tiempo, no obstante, por motivos de confidencialidad, no se puede revelar el nombre ni la función de dichas empresas, pero cabe destacar que todas las auditorías siguieron el mismo proceso.

Una vez identificadas las empresas y su relación con la organización, se procedió a realizar la auditoria. Para ello, el jefe del departamento envió por correo electrónico a los proveedores un formulario de evaluación. El objetivo era determinar si los proveedores estaban cumpliendo con las cláusulas del contrato, las cuales estipulan los siguientes aspectos: seguridad de la información de la empresa, soporte a las herramientas y el cumplimiento normativo y de calidad. El formulario constaba de cinco columnas con la siguiente información:

- Columna uno: Secciones de preguntas
- Columna dos: ¿Aplica para el objeto del vínculo?
- Columna tres: Cumple
- Columna cuatro: Observaciones/ Controles compensatorios
- Columna cinco: Revisión Seguridad de la Información

En la primera columna se dividieron 17 secciones que abarcaban diferentes temas de preguntas, los mismos están detallados en la tabla 6, a continuación.

Tabla 6

Descripción de las preguntas realizadas al proveedor

Nombre sección	Descripción	Total preguntas
Gestión de Riesgos	Estas preguntas se centran en la seguridad de la información en un entorno contratado. Se abordan temas como el análisis detallado de riesgos, pruebas de penetración, plan de respuesta ante incidentes, inspecciones periódicas y suscripciones a entidades de alerta. El objetivo es garantizar la protección de la información, evaluar el cumplimiento de políticas y controles, y tomar medidas preventivas frente a posibles amenazas.	5
Política de Seguridad de la Información	Las preguntas se centran en la seguridad de la información en la compañía. Se evalúa si existen políticas formales, un responsable designado y procedimientos de control de acceso documentados. También se indaga si se revisan regularmente las políticas y procedimientos, si se implementan a nivel operativo y tecnológico, y si se realizan auditorías periódicas a los controles de seguridad de la información.	6
Seguridad del Recurso Humano	Las preguntas se centran en distintos aspectos relacionados con la seguridad de la información y la gestión del personal dentro de una entidad o empresa. Se abordan temas como la verificación de antecedentes de los empleados, la firma de acuerdos de confidencialidad, la capacitación en seguridad de la información, las normas disciplinarias en caso de violaciones a la seguridad y los procedimientos de retiro del personal, incluyendo la desactivación inmediata de permisos de acceso. Estas preguntas reflejan la importancia de implementar medidas y políticas que salvaguarden la confidencialidad de la información y protejan los activos de la organización.	5
Controles Anti-fuga	Estas preguntas abordan aspectos como el acceso a correos electrónicos externos, el uso de dispositivos de almacenamiento externo, la instalación de software por parte de los usuarios finales, el control y registro de la consulta de fuentes físicas de información, el uso de clientes de correo autorizados, el acceso a carpetas compartidas con información confidencial, el cifrado de archivos transmitidos por medios no seguros, la seguridad en el intercambio de información, los controles para prevenir la fuga de información de dispositivos externos y el control de acceso no autorizado en el envío físico de información entre sedes. Estas preguntas buscan garantizar que se implementen medidas de seguridad adecuadas para proteger la información sensible y confidencial de la organización y prevenir la filtración o acceso no autorizado a los datos.	11

Nombre sección	Descripción	Total preguntas
Gestión de datos y Backups	Las preguntas planteadas se centran en la gestión de copias de respaldo y la garantía de la continuidad operativa. Se indaga si existen procedimientos bien documentados y aplicados que incluyan pruebas de restauración periódicas, al menos cada 6 meses. Esto implica asegurarse de que los procesos de respaldo estén correctamente establecidos y evaluar regularmente su efectividad. Además, se busca conocer si se ha definido qué información de respaldo debe ser custodiada externamente para protegerla de posibles incidentes que afecten al sitio principal de almacenamiento. Esta medida adicional de seguridad busca asegurar la disponibilidad y recuperación de los datos en situaciones adversas.	2
Control a Aplicaciones	Las preguntas abordan diversas áreas de seguridad y gestión de sistemas de información. Se indaga sobre la protección de contraseñas, ya sea evitando su visualización en pantalla o utilizando métodos de encriptación sólidos. También se pregunta si hay desarrollo interno y si se aplica una metodología segura en el proceso. Además, se busca conocer si se contrata desarrollo externo y cuáles son los criterios de seguridad que se exigen a los proveedores de software. Se pregunta acerca de la existencia de ambientes separados de desarrollo, pruebas y producción, así como de procedimientos para el transporte seguro de código entre ellos. Se aborda el control de acceso en aplicaciones con información confidencial y la restricción de acceso a claves o certificados digitales. Se pregunta sobre la protección de los datos de producción y si se utilizan en pruebas. Por último, se investiga si se cuenta con pistas de auditoría para garantizar la trazabilidad de los accesos y modificaciones en los sistemas de información.	9
Gestión de usuarios y contraseñas	Las preguntas abordan diferentes aspectos relacionados con la gestión de accesos y prácticas de seguridad. Se consulta sobre la existencia de un procedimiento formal para solicitar los accesos necesarios de nuevos funcionarios, así como sobre el uso de usuarios nombrados en lugar de genéricos. Se evalúa la implementación de buenas prácticas en contraseñas, como cambios periódicos, bloqueos después de intentos fallidos y requisitos de complejidad. Se busca determinar si se tienen roles y perfiles definidos para los accesos, así como si se eliminan o bloquean las cuentas inactivas. Se investiga la realización de revisiones periódicas de accesos, la centralización de contraseñas y el bloqueo de usuarios en ausencias prolongadas. En resumen, se abordan prácticas fundamentales para garantizar una gestión segura y eficiente de los accesos y contraseñas en los sistemas.	7
Gestión Tecnológica	Las preguntas abordan diferentes aspectos relacionados con el control, la operación y la gestión de la infraestructura tecnológica. Se consultan la existencia de procedimientos implementados para el control de cambios tecnológicos, la operación tecnológica documentada, la gestión de	5

Nombre sección	Descripción	Total preguntas
	capacidad de la infraestructura, y el control de software autorizado. También se investiga si hay un proceso formal para detectar y responder ante fallos en sistemas críticos. Estas preguntas buscan asegurar que se sigan prácticas adecuadas para gestionar los cambios, operar los sistemas, garantizar el rendimiento, controlar el software y responder ante problemas tecnológicos críticos de manera efectiva y oportuna.	
Continuidad del negocio	Las preguntas se centran en la existencia y aplicación de planes de contingencia, continuidad del negocio y un plan de crisis. Se busca determinar si se tienen documentados y implementados planes de contingencia y continuidad del negocio en relación a los servicios contratados, con el objetivo de mitigar los impactos de posibles contingencias y asegurar la continuidad de las operaciones. Además, se indaga sobre la existencia de un Plan de crisis que establezca el tiempo estimado de recuperación frente a un incidente, con el fin de contar con una respuesta efectiva y rápida en situaciones críticas. Estas preguntas buscan evaluar la preparación de la compañía ante eventos adversos y su capacidad para mantener la operatividad y minimizar los impactos en caso de interrupciones o emergencias.	2
Atención a Incidentes	Las preguntas se centran en la gestión de incidentes, el registro y monitoreo de actividades, y la comunicación de incidentes a la compañía contratante. Se indaga sobre la existencia de un procedimiento documentado para atender incidentes de alteración o manipulación, la activación de logs de auditoría en sistemas operativos y bases de datos relacionados con la operación contratada, y la comunicación formal de los incidentes a la compañía contratante. Además, se evalúa la presencia de controles para monitorear la infraestructura en tiempo real y la realización de auditorías diarias de los logs en busca de incidentes. Estas preguntas buscan garantizar una respuesta adecuada ante incidentes de seguridad, el registro y seguimiento de actividades, y una comunicación transparente con la compañía contratante.	6
Seguridad en computadores	Las preguntas se centran en aspectos relacionados con la seguridad de los sistemas, la protección contra virus y malware, el acceso de usuarios, el aseguramiento de las máquinas, y la protección de la información confidencial. Se busca determinar si se implementan las últimas actualizaciones y software antivirus en los sistemas operativos, si se lleva a cabo el aseguramiento de las máquinas, si se tienen procedimientos para la actualización diaria y análisis periódico de virus, si se asignan cuentas personales a los usuarios, si se aplican controles compensatorios en sistemas sin antivirus compatible, si se restringe la instalación y modificación de software por parte de los usuarios, si se realiza el borrado seguro de equipos con información confidencial, si se utiliza administración segura de servidores y equipos de red, y si se implementan políticas y controles para asegurar los dispositivos móviles.	10

Nombre sección	Descripción	Total preguntas
	Estas preguntas buscan garantizar la seguridad de los sistemas, la protección de la información y la implementación de buenas prácticas de seguridad.	
Seguridad en Redes	Las preguntas se centran en aspectos relacionados con la seguridad de la red y los dispositivos utilizados. Se busca determinar si se implementa una configuración de firewall que niega todo el tráfico por defecto y solo habilita los servicios específicos necesarios y documentados. Además, se verifica si se controla el acceso a internet para permitir únicamente la navegación a sitios web necesarios para la operación contratada. Se indaga si la entrega y recepción de información digital se realiza a través de canales seguros como VPN, correo electrónico con archivos cifrados y DVD/CD cifrados con algoritmos de protección y autenticación. También se pregunta sobre la existencia de sistemas de protección adicionales al firewall, como sistemas de detección de intrusos u otros dispositivos de seguridad de red. Se evalúa si se utiliza autenticación WPA, WPA2 o superior en redes inalámbricas y si se implementan medidas de seguridad adecuadas en los equipos que procesan información sensible. Se investiga si se utilizan zonas militarizadas con dispositivos de seguridad específicos para proteger las máquinas que almacenan o procesan información sensible. Además, se consulta si los puertos de los dispositivos de red en desuso están deshabilitados, si se tienen redes segmentadas para servidores y usuarios, si se restringe el acceso a internet desde los servidores a través de controles y si se implementa control de contenido y filtro de correo para combatir spam. Por último, se indaga sobre la presencia de IPS activo para filtrar ataques web o externos y si se tiene control de acceso y separación de las redes WiFi de la red de operación. Estas preguntas buscan garantizar una adecuada protección y seguridad de la red y los dispositivos utilizados en la operación.	13
Aspectos Legales	Estas preguntas se enfocan en aspectos legales y de propiedad relacionados con el software y la protección de la información. Se indaga si todo el software utilizado es de propiedad del proveedor o si está debidamente licenciado en su favor. Se establece la importancia de que el proveedor respete la propiedad intelectual de terceros y esté legalmente autorizado para licenciar o implementar el software requerido. En caso de que el servicio se preste en las instalaciones del proveedor, se consulta si se ha contratado una póliza de seguro con una compañía legalmente constituida en el país para cubrir daños materiales y costos de reposición de la información en caso de eventos como incendio, terremoto, actos malintencionados de terceros, entre otros. Además, se exige que el proveedor remita a la compañía contratante una confirmación de cobertura emitida por la aseguradora.	3

Nombre sección	Descripción	Total preguntas
	Asimismo, se menciona la importancia de incluir cláusulas de confidencialidad en el contrato con el proveedor y el reconocimiento de que la información es propiedad exclusiva de la compañía contratante. Estas preguntas buscan asegurar el cumplimiento legal y la protección de la propiedad intelectual y la información confidencial durante la prestación del servicio.	
Subcontratistas	Estas preguntas se centran en la gestión de subcontratistas por parte del tercero y cómo se asegura la confidencialidad y seguridad de la información de la compañía contratante. Se consulta si se informa a la compañía contratante sobre el uso de subcontratistas que requieran acceder a su información, si existen acuerdos de confidencialidad con los subcontratistas, si se revisan sus controles de seguridad y si cumplen con los requisitos de seguridad establecidos por la compañía contratante. El objetivo es garantizar la protección de la información en todo momento, incluso cuando se involucran subcontratistas en el servicio.	4
Seguridad Física	Estas preguntas se centran en la gestión de subcontratistas por parte del tercero y cómo se asegura la confidencialidad y seguridad de la información de la compañía contratante. Se consulta si se informa a la compañía contratante sobre el uso de subcontratistas que requieran acceder a su información, si existen acuerdos de confidencialidad con los subcontratistas, si se revisan sus controles de seguridad y si cumplen con los requisitos de seguridad establecidos por la compañía contratante. El objetivo es garantizar la protección de la información en todo momento, incluso cuando se involucran subcontratistas en el servicio.	8
Clasificación, etiquetado y manejo de la información	Estas preguntas se refieren a la gestión de activos de información en la compañía contratante. Se consulta si se cuenta con un inventario de activos de información que incluya su clasificación según su sensibilidad, si los activos de información están etiquetados de acuerdo a dicha clasificación, y si se tiene implementado un procedimiento para el manejo de los activos de información basado en su clasificación. El objetivo es asegurar una adecuada identificación, seguimiento y control de los activos de información, garantizando su protección y gestión adecuada de acuerdo a su nivel de sensibilidad.	3
Datos personales	La pregunta plantea si el tercero tiene implementados controles de seguridad que aseguren el cumplimiento de la Ley 1581 de Protección de Datos Personales. Esta ley establece disposiciones para la protección de la privacidad y los derechos de las personas en relación con el tratamiento de sus datos personales. Los controles de seguridad son mecanismos y medidas adoptados para garantizar la confidencialidad, integridad y disponibilidad de la información, incluyendo los datos personales. Estos controles pueden incluir políticas, procedimientos, tecnologías y prácticas específicas para proteger los datos personales y cumplir con los requerimientos de la ley. Su	1

Nombre sección	Descripción	Total preguntas
	implementación es fundamental para salvaguardar la privacidad de los individuos y cumplir con las obligaciones legales en materia de protección de datos personales.	

Fuente: Autor

La segunda columna, denominada “¿Aplica para el objeto del vínculo?”, está relacionada con las preguntas del formulario de evaluación. Si la sección evaluada estaba contemplada en el contrato del proveedor, esta casilla se marcaba como 'Sí'. En caso contrario, si la sección no estaba incluida en el contrato, se marcaba como 'No’. Es importante señalar que tanto esta columna como la columna número cuatro, “Observaciones/Controles compensatorios”, fueron llenadas por el proveedor. En la columna de observaciones, los proveedores podían justificar o hacer observaciones sobre la implementación de la sección evaluada.

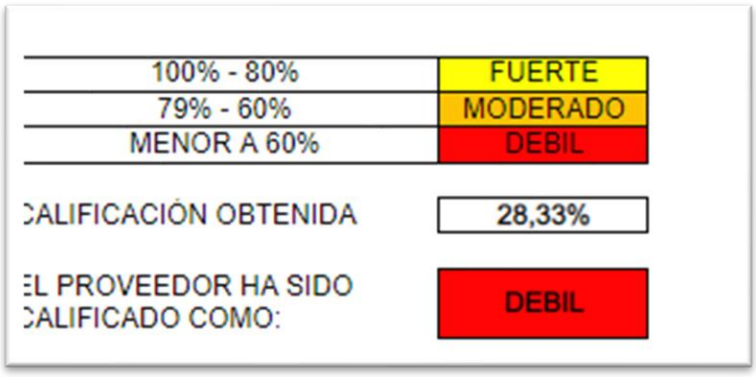
La respuesta al formulario de evaluación dependía del proveedor, por lo que podía tardar desde una semana hasta un mes en ser respondida. Una vez se respondía y se enviaba el formulario al Departamento de Seguridad se agendaba la auditoria, la cual se realizaba a través de una reunión remota con el proveedor con el propósito de completar las columnas faltantes y resolver cualquier duda que se hubiera generado con la lectura previa del documento. La duración promedio de la sesión era aproximadamente entre una y dos horas.

Durante la reunión, se nombraban cada una de las preguntas con el fin de que el proveedor pudiera justificar su respuesta frente a la implementación de estas. Si se encontraba una sección que estuviera incluida en el vínculo del contrato, pero que no estuviera siendo cumplida, se marcaba la tercera columna (cumple) con la palabra “No". En caso contrario, si se estaba cumpliendo con el vínculo del contrato, se marcaba como "Sí”. Por último, en la columna “Revisión de Seguridad de la información” se realizó un registro de las falencias que presentaban los proveedores. Estas dos últimas columnas fueron llenadas por el Departamento de Seguridad de la información en el trayecto de la reunión.

Una vez completado el formulario, se elaboró una tabla de clasificación que consideraba tanto el número total de preguntas relacionadas con el contrato del proveedor, como la cantidad total que se lograban cumplir. Con esta información, se calculó el porcentaje de cumplimiento del proveedor con respecto a la empresa. En la figura 7 se muestra un ejemplo de la rúbrica establecida para la calificación y un resultado hipotético de lo que se podría obtener.

Figura 7

Rubrica de evaluación para la calificación del proveedor



Fuente: Autor

Finalmente, teniendo en cuenta el formulario y la reunión remota con los proveedores, se realizó una matriz de riesgos detallada en la sección "Elaboración de matriz de riesgos asociados a los riegos informáticos encontrados en los proveedores", con el fin de identificar y mitigar las fallas de seguridad encontradas.

4.1.4. *Prueba controlada de ataque cibernético (phishing)*

En el año 2022, Colombia estuvo marcada por ciberataques contra empresas de infraestructuras críticas como fueron EPM (Empresas Públicas de Medellín), EPS de Sanitas, Electricaribe, Gas Caribe, Famisanar (infobae, 2023). En su mayoría fueron infectadas por el malware de tipo ransomware con el fin de secuestrar sus datos, bloqueando el uso de los ordenadores y encriptando la información, para posteriormente realizar una extorsión y pedir su rescate en pago por criptomonedas.

Este malware fue infectado por medio del ataque informático llamado phishing, el cual consiste en la suplantación de identidad para engañar a las personas y obtener información confidencial, como contraseñas, datos bancarios, números de tarjetas y otros datos sensibles. Los ciberdelincuentes también pueden usar phishing para instalar virus informáticos en los dispositivos de los usuarios en caso de que el usuario pulse sobre los enlaces y/o descarga algún documento de un correo sospechoso que ha abierto. El software malicioso puede ser usado para robar información personal, dañar el dispositivo, encriptar la información o permitir que los ciberdelincuentes controlen el dispositivo de forma remota.

Los empleados de las empresas son un objetivo frecuente de los ataques de phishing porque suelen tener acceso a información confidencial y pueden ser utilizados como puerta de entrada a la red corporativa. Es por esto que el Departamento de Seguridad de la Información realiza tres pruebas controladas de ataques cibernéticos al personal de la empresa cada año, basado en el protocolo Concienciación y capacitación (PR.AT) de la categoría Proteger (PR), con el fin de identificar los puntos débiles del sistema y las áreas que requieren mejoras en la seguridad, y así tomar medidas para prevenir ataques reales.

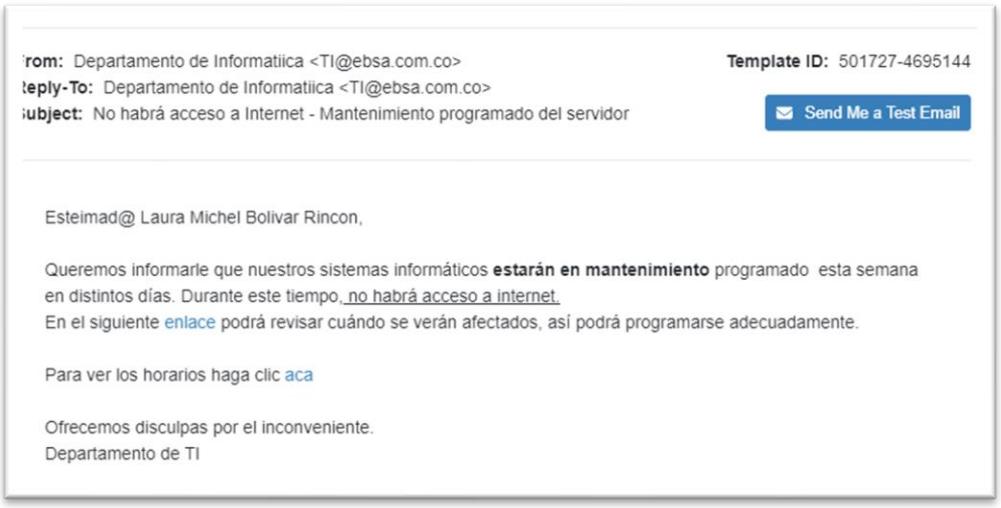
Además, las pruebas de ataques de phishing también son utilizadas para concientizar y entrenar a los empleados de la empresa sobre los riesgos de ataques informáticos, el cómo identificarlos y evitarlos. De esta manera se puede reducir el riesgo de que los empleados sean víctimas de phishing y se comprometa la seguridad de la empresa; en ese sentido, se realizó una propuesta de ataque simulado al Departamento de Seguridad de la Información la cual tenía como objetivo evaluar la efectividad de los cursos de ciberseguridad impartidos a los empleados, tal como se describe en la sección “Entrenamientos de concientización sobre seguridad de la información”. El contenido de los cursos se centró en la identificación de correos electrónicos fraudulentos.

La propuesta consistió en enviar un correo electrónico fraudulento, en el que se hacía pasar por el Departamento de Tecnología de la Información (TI). El correo notificaba a los empleados de la Empresa de Energía de Boyacá, sobre un supuesto mantenimiento programado en uno de los servidores de la empresa, lo que resultaría en la falta de acceso a Internet. Para acceder al horario de realización del mantenimiento, se insertaron dos URLs que redirigían a los empleados a una página web falsa que solicitaba sus credenciales empresariales como correo el electrónico y la contraseña.

En la figura 8 se puede observar la propuesta de suplantación de identidad (phishing) realizada al Departamento de Seguridad de la Información de la Empresa de Energía de Boyacá

Figura 8

Simulación de correo phishing

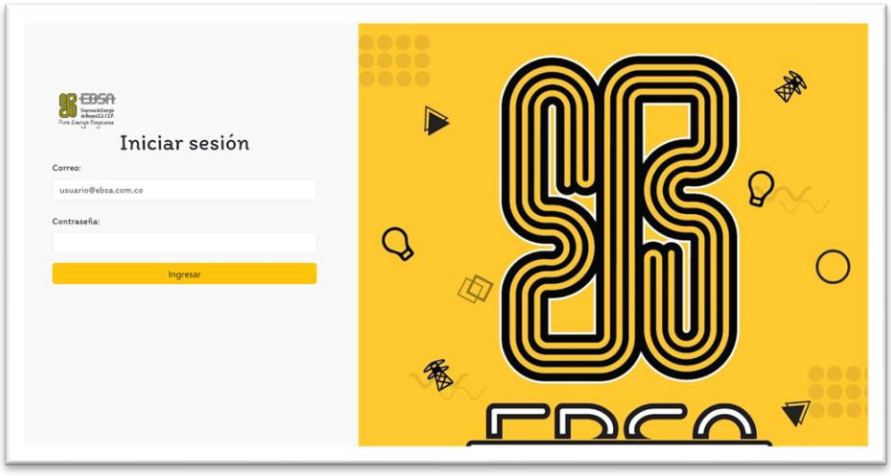


Fuente: Autor

Para el desarrollo de la página web falsa, se utilizó el lenguaje de programación PHP, y la base de datos MySQL.

Figura 9

Página web



Fuente: Autor

Nota. La figura 9 muestra la interfaz de la página web creada. Se presenta con el propósito de ilustrar el diseño y los elementos visuales implementados en la página. Se han tomado precauciones para evitar la inclusión de información personal o sensible en la imagen.

Cabe resaltar que, para el desarrollo del ejercicio, se tomaron medidas de seguridad como la encriptación de las contraseñas insertadas por los empleados. El propósito de esta prueba era verificar cuáles empleados caían en el correo malicioso y otorgaban sus datos. Sin embargo, no se recopiló la información de dichas credenciales ya que esto podría representar un riesgo de filtración de datos. En la figura 10 se muestra un ejemplo de las credenciales que fueron insertadas en la página web falsa y almacenadas en la base de datos. Como se puede observar, la contraseña fue almacenada en forma encriptada. Es importante destacar que el desarrollo de la página web falsa no incluía un Login. Al insertar las credenciales, los empleados eran redirigidos a la página oficial de la EBSA.

Figura 10

Credenciales insertadas en la página web falsa

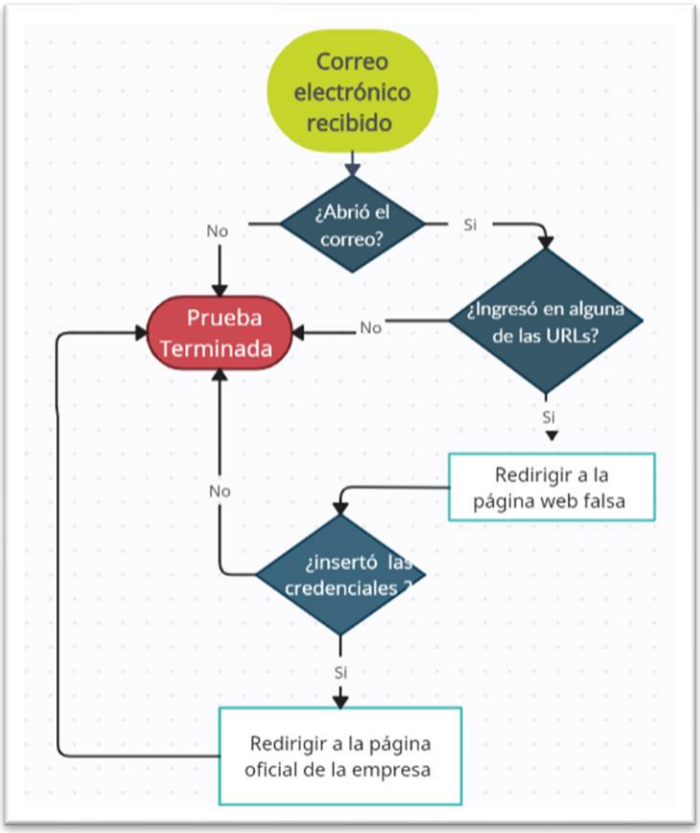
id	correo	contrase
3	usuariox@ebsa.com.co	e10adc3949ba59abbe56e057f20f883e
4	usuario2@ebsa.com	fcea920f7412b5da7be0cf42b8c93759

Fuente: Autor

La figura 11 representa el diagrama de secuencia de la propuesta para la prueba de phishing.

Figura 11

Diagrama de secuencia de la propuesta para la prueba de phishing



Fuente: Autor

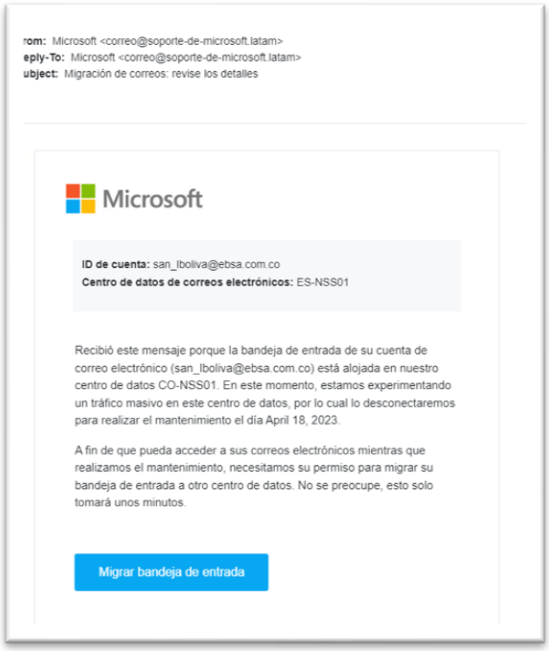
Sin embargo, la propuesta no fue aprobada por el jefe del Departamento de Seguridad de la Información debido a las políticas de la empresa. Por esta razón, el jefe del departamento recomendó investigar los casos de phishing con mayor éxito en Colombia e intentarlo replicar en la empresa, utilizando la herramienta Knowbe4 para tener un entorno más controlado. En la investigación se encontró que los correos fraudulentos que tienen los nombres de empresas conocidas como Microsoft, bancos, fiscalía general de la Nación, Mercado Libre, DIAN y SIMIT son los más utilizados por los ciberdelincuentes. Esto se debe a que los usuarios creen que su contenido es legítimo y descargan los archivos adjuntos al correo o se dirigen a las URLs contenidas en el mensaje.

Para la realización de la prueba se tuvo en cuenta al 100% de los empleados activos de los diferentes departamentos de la empresa, como Recursos Humanos, Personal de Operación, Personal de Tecnologías

de la Información, Personal Financiero, Personal EBSA y Directivos. El correo fraudulento se creó utilizando como referencia un correo de una empresa conocida (Figura 12) con el objetivo de engañar al usuario para que pulse en el botón que aparece en el mensaje. Al pulsar el botón, el usuario es redirigido a una nueva página (Figura 13) que indica que el correo es una simulación.

Figura 12

Correo de phishing enviado a los trabajadores

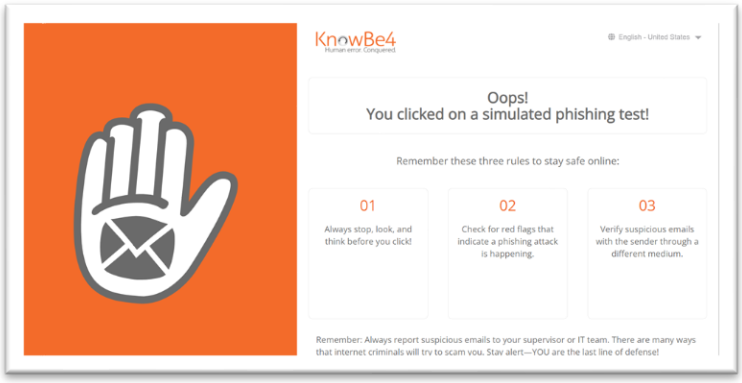


Fuente: Empresa de Energía de Boyacá

La prueba controlada de phishing comenzó el 14 de marzo de 2023 y se llevó a cabo durante tres días. Durante este tiempo, se utilizó la plataforma KnowBe4 para realizar un seguimiento diario de los usuarios que abrieron el correo electrónico: los que pulsaron en los enlaces incluidos en el correo, los que eliminaron el mensaje y los que reportaron el mensaje al Departamento de Seguridad de la Información.

Figura 13

Página de redireccionamiento

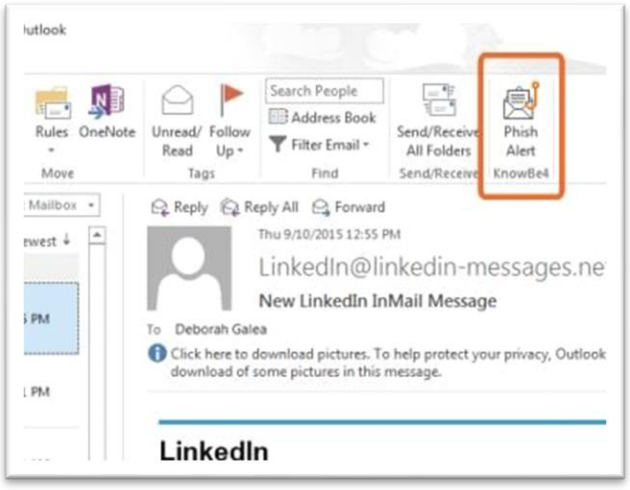


Fuente: Empresa de Energía de Boyacá

Los empleados tenían dos opciones para reportar el mensaje, la primera era utilizando la herramienta de Microsoft 365, que cuenta con la opción de reportar phishing como se muestra en la figura 14. La segunda opción era reenviar el mensaje al correo de ciberseguridad de la empresa. Estos métodos se detallan en la sección “Elaboración de planes de remediación en la infraestructura tecnológica”.

Figura 14

Reporte de correo phishing



Fuente: Empresa de Energía de Boyacá

No se pueden dar a conocer los resultados de la prueba controlada de phishing debido a que éstos podrían comprometer la seguridad de la empresa y exponer información confidencial. También podría afectar negativamente la reputación de la empresa y la confianza de sus clientes, por lo cual es importante recordar que estas pruebas son simulaciones y que no se busca sancionar o castigar a los empleados, sino mejorar la seguridad de la empresa en general. Por lo tanto, aquellos trabajadores que no lograron identificar el correo malicioso recibieron una capacitación detallada sobre los riesgos informáticos como se detalla en la sección "Capacitaciones de seguridad de la información". El objetivo de esta capacitación es ayudar a los empleados a comprender mejor las amenazas de seguridad y mejorar sus habilidades para detectar y evitar ataques de phishing en el futuro.

4.2. Planes de remedición para las vulnerabilidades informáticas

Para la implementación del segundo objetivo, se tuvieron en cuenta las vulnerabilidades encontradas en el desarrollo del objetivo anterior (ver secciones **¡Error! No se encuentra el origen de la referencia.**, **¡Error! No se encuentra el origen de la referencia.**, **¡Error! No se encuentra el origen de la referencia.**).

4.2.1. *Elaboración de planes de remediación para la mitigación de riegos informáticos*

Las vulnerabilidades encontradas en los sistemas informáticos de una empresa pueden ser aprovechadas por los atacantes cibernéticos para comprometer la seguridad empresarial y generar graves consecuencias en su operación y reputación. Es por ello que resulta esencial desarrollar planes de remediación que permitan identificar, evaluar y corregir de manera oportuna las vulnerabilidades detectadas, fortaleciendo así la protección y la continuidad del negocio.

Si un fallo de seguridad no se remedia, puede dejar a los sistemas de la empresa expuestos a posibles ataques cibernéticos. Dependiendo de la naturaleza de la vulnerabilidad, un atacante podría aprovecharla para obtener acceso no autorizado a los sistemas de la empresa, robar información confidencial, interrumpir el funcionamiento normal de los sistemas o incluso causar pérdidas financieras.

Por lo tanto, la remediación de las vulnerabilidades es esencial para proteger los sistemas informáticos de la empresa y garantizar su continuidad. Al implementar planes de remediación específicos para los fallos

de seguridad encontrados, se pueden identificar las soluciones más eficaces para cada caso y reducir significativamente el riesgo de que los atacantes cibernéticos puedan explotar estas debilidades. De esta manera, se pueden minimizar los posibles daños a la empresa, y a la vez cumplir con las regulaciones y requisitos legales relacionados con la seguridad de la información en la actualidad.

Además, los planes de remediación permiten establecer prioridades en cuanto a las vulnerabilidades más críticas, lo que facilita la toma de decisiones y la asignación de recursos para abordarlas.

Para elaborar los planes de remediación, el Departamento de Seguridad de la Información utiliza la guía de gestión de incidentes de seguridad informática del marco de referencia NIST (NIST, 2023)como herramienta clave. Esta guía proporciona un enfoque sistemático para identificar y gestionar los incidentes de seguridad informática, lo que facilita la tarea de remediar las vulnerabilidades detectadas en los sistemas informáticos de la empresa.

Es importante destacar que no es posible revelar públicamente las categorías de las brechas de seguridad encontradas en la infraestructura de la empresa, ya que esto podría incrementar el riesgo de que los atacantes aprovechen dichas vulnerabilidades para acceder a sistemas y datos confidenciales.
Para desarrollar los planes de remediación de las vulnerabilidades informáticas detectadas por las herramientas Tenable SC, AMP de Cisco y MISP, se siguió la siguiente metodología:

1. **Identificación de los activos comprometidos:** para tener una visión completa del entorno a analizar, se identificaron los activos comprometidos con las brechas de seguridad, incluyendo servidores, computadoras, aplicaciones, bases de datos, entre otros. En el caso de los endpoints, también se tuvo en cuenta la identificación de las direcciones IP asociadas a estos dispositivos.

2. **Estudio de las vulnerabilidades informáticas:** a partir de las brechas de seguridad detectadas por las herramientas Tenable SC y AMP de Cisco, se obtuvo una lista de CVE (Vulnerabilidades y Exposiciones Comunes). Cada CVE es un identificador alfanumérico único que se asigna a una vulnerabilidad específica en un producto de software. Su finalidad es proporcionar un estándar de identificación de vulnerabilidades para facilitar la gestión y divulgación de información sobre seguridad, tanto para los desarrolladores de software como para los usuarios finales. El CVE es mantenido por el MITRE Corporation y se utiliza en todo el mundo como una forma estandarizada

de referirse a las vulnerabilidades de seguridad detectadas en distintos sistemas y productos de software.

Teniendo en cuenta el CVE de cada brecha de seguridad detectada, se comenzó a recopilar información sobre los detalles técnicos de las vulnerabilidades, incluyendo el tipo, el nivel de gravedad y las posibles consecuencias para la seguridad del sistema afectado.
Para ello, se indagó en cada una de las siguientes plataformas:

- **NIST National Vulnerability Database (NVD):** es una base de datos que contiene información sobre vulnerabilidades de seguridad conocidas, incluyendo CVE. Proporciona una descripción detallada de cada vulnerabilidad, incluyendo información sobre el impacto potencial en el sistema afectado. (NIST, 2023)
- **Mitre CVE:** es una organización sin fines de lucro que mantiene la base de datos de CVE. Proporciona información detallada sobre cada CVE, incluyendo una descripción de la vulnerabilidad, el nivel de gravedad y las soluciones disponibles. (CVE, 2023)
- **SecurityFocus**: es una plataforma que ofrece información sobre vulnerabilidades de seguridad y amenazas de ciberseguridad. Incluye una sección dedicada a CVE, donde se puede acceder a información detallada sobre cada vulnerabilidad. (Securityfocus, 2023)
- **MSRC (Microsoft Security Response Center):** es el equipo de seguridad de Microsoft encargado de identificar, investigar y responder a las vulnerabilidades de seguridad en los productos y servicios. (Microsoft, 2023)
- **Tenable CVEs:** lista de vulnerabilidades y exposiciones comunes de los endpoints afectados (Tenable, 2023)

3. **Organización por gravedad de las vulnerabilidades encontradas:** una vez realizado el estudio de las vulnerabilidades, se priorizó su nivel de gravedad, enfocándose principalmente en aquellas clasificadas como críticas o de alto riesgo. A cada una de ellas se les asignó un tiempo de remediación determinado, dependiendo de su nivel de gravedad. De esta manera, se logró una atención eficiente y oportuna para mitigar los riesgos asociados a las vulnerabilidades identificadas en la infraestructura de la empresa.

- Gravedad crítica y alta: 1-2 semanas

- Gravedad media: 3 - 5 semanas
- Gravedad baja: 5 semanas o más

4. **Propuesta de soluciones a los riegos informáticos:** después de priorizar las vulnerabilidades, se planteó un conjunto de soluciones, para mitigar o eliminar las brechas de seguridad encontradas. Estas soluciones fueron:

    - **Instalación de parches de seguridad:** si la vulnerabilidad detectada se debe a una falta de actualización del software o sistema operativo, se propone la instalación de parches de seguridad. Estos parches están diseñados para cerrar brechas de seguridad que se ha identificado y reducir la posibilidad de que un atacante pueda explotar la vulnerabilidad.

    - **Actualización de software:** en algunos casos, la vulnerabilidad puede deberse a una versión obsoleta del software. Se recomienda actualizar el software a la última versión disponible.

    - **Implementación de políticas de seguridad:** las políticas de seguridad son un conjunto de reglas y prácticas que se utilizan para proteger la seguridad de los sistemas informáticos. Se pueden establecer políticas de seguridad para regular el uso de contraseñas, administración de parches, entre otros aspectos que pueden afectar la seguridad de los sistemas informáticos.

    - **Configuración de medidas de protección adicionales:** en algunos casos, podía ser necesario implementar medidas adicionales de protección para mitigar las vulnerabilidades encontradas. Esto puede incluir la configuración de firewall, la implementación de soluciones de detección y prevención de intrusiones, la utilización de soluciones de encriptación, cambio de contraseñas, entre otros.

5. **Asignación de personal responsable:** para solucionar las vulnerabilidades informáticas detectadas, se asignaba a un departamento como responsable de supervisar el buen comportamiento en términos de seguridad, de los activos involucrados. El Departamento de Infraestructura se

encargaba de la implementación de parches de seguridad, debido a que son los responsables de garantizar el correcto funcionamiento de los servidores y su disponibilidad. Por otro lado, el Departamento de Redes es el encargado de la configuración de los firewalls y la protección de la red empresarial contra posibles intrusiones externas. Finalmente, el Departamento de Seguridad Informática es responsable de garantizar que las computadoras de la empresa estén actualizadas con los últimos parches de seguridad y de aplicar políticas de seguridad sólidas. Estos departamentos trabajan en conjunto para mitigar las brechas de seguridad y proteger la empresa contra posibles amenazas informáticas.

En situaciones donde se presentaban múltiples vulnerabilidades críticas o altas en los servidores, el Departamento de Seguridad de la Información brindaba apoyo en la implementación y pruebas de los parches de seguridad correspondientes. Esto se debía a que estas vulnerabilidades podían tener un impacto significativo en la seguridad de la empresa, por lo que era necesario garantizar que las soluciones implementadas fueran efectivas y no comprometieran la estabilidad del sistema. De esta manera, el Departamento de Seguridad de la Información colaboraba con el Departamento de Infraestructura en la mitigación de las brechas de seguridad más críticas para la empresa.

El procedimiento para la implementación de parches de seguridad en los servidores constaba de varias etapas, como fueron:

- **Identificar los servidores afectados por la vulnerabilidad**. En este proceso se revisaba cada servidor para detectar si presentaba alguna brecha de seguridad. Es importante mencionar que era común que varios servidores presentaran la misma vulnerabilidad.
- **Captura del estado previo a la implementación del parche de seguridad**. Como medida preventiva se tomaba una imagen instantánea del estado actual del servidor, conocido como "snapshot". En caso de que el parche no funcionara correctamente o causara problemas, se podía revertir el servidor al estado anterior utilizando el snapshot previamente tomado. Esto permitía minimizar los riesgos y evitar interrupciones en los servicios de la empresa.
- **Instalación del parche de seguridad**. La duración de este proceso podía variar desde una hora hasta un día completo. En ocasiones, la implementación del parche podía bloquearse o no realizarse de manera oportuna. En estos casos, se intentaba nuevamente la instalación del parche.

- **Finalización**. Una vez culminada la instalación del parche, se procedía a verificar el correcto funcionamiento del servidor. Si se presentaban fallas o errores, se registraban y se informaban al jefe del Departamento de Seguridad de la Información para tomar las medidas necesarias.

Cabe resaltar que, como pasante universitario, tenía como objetivo, proponer planes de remediación para la mitigación de vulnerabilidades informáticas. Por tanto, no estaba autorizada a realizar la ejecución de parches de seguridad o cualquier otro plan de remediación. Estas tareas eran desarrolladas por el personal del departamento asignado para cada activo afectado. Sin embargo, en algunos planes de remediación, se presentó la oportunidad de participar como refuerzo.

En tabla 7 se observa el formato que se completaba por cada vulnerabilidad encontrada. Estos reportes se subían a la plataforma JIRA y eran denominados incidencias, lo que permitía hacer un seguimiento del proceso de cada brecha de seguridad.

Tabla 7

Formato de incidencias

Nombre de la incidencia/ Vulnerabilidad	
Nombre de los servidores o IP de los dispositivos afectados	Personal Encargado
Descripción	Tiempo de Solución
Solución	Proceso de la incidencia: ▪ Inactiva ▪ En proceso ▪ Finalizada
Pruebas del proceso:	

Nota: La tabla 7, presentada anteriormente, muestra el formato de las incidencias asignadas a cada vulnerabilidad que se estaba monitoreando. Es importante destacar que, por razones de seguridad, no se pueden revelar las incidencias específicas generadas durante el transcurso de la pasantía. Sin embargo, estas incidencias desempeñaron un papel crucial en la identificación y abordaje de las vulnerabilidades detectadas.

Tal como se menciona en el capítulo “Evaluación y análisis de vulnerabilidades a través de la herramienta Tenable SC, AMP de Cisco y MISP”, se pudo constatar que no fue posible implementar todos los planes de remediación para las vulnerabilidades detectadas en cada mes debido a la falta de personal calificado para realizar estas actividades de manera oportuna. Como consecuencia, estas incidencias quedaron acumuladas y en espera para su solución.

4.2.2. *Socialización de los planes de remediación.*

La socialización de los planes de remediación de las vulnerabilidades informáticas es esencial para asegurar que todos los miembros del equipo de seguridad de la información estén alineados, promover la transparencia en el enfoque de seguridad de la empresa, evitar futuras vulnerabilidades, y fomentar una cultura de seguridad en toda la organización. Al discutir los planes de remediación y los avances en la protección de la infraestructura, se pueden identificar áreas de mejora y tomar medidas preventivas para evitar futuras vulnerabilidades.
Es por ello que, el departamento de Seguridad de la Información realiza reuniones periódicas virtuales o presenciales, con una duración aproximada de una a dos horas, para socializar y hacer seguimiento de los planes contra las vulnerabilidades detectadas en la infraestructura, teniendo en cuenta el protocolo de Comunicaciones (RS.CO) de la categoría Responder (RS) del marco NIST.

Durante estas reuniones, se compartió el progreso de las incidencias creadas para llevar a cabo la remediación de las vulnerabilidades identificadas en la infraestructura de la organización, lo que permitió a los miembros del equipo de seguridad de la información discutir los desafíos encontrados en el proceso de remediación y proponer soluciones alternativas.

Uno de los temas que se abordaron con mayor frecuencia durante estas reuniones fue la dificultad que se encontró al implementar algunos parches de seguridad en los servidores. En particular, se discutió cómo algunos aplicativos instalados en los servidores dejaban de funcionar después de instalar ciertos parches críticos. Se exploraron diversas estrategias para minimizar el impacto de estas actualizaciones en la funcionalidad de los sistemas.

Además de las reuniones del departamento de Seguridad de la Información, la Dirección de Informática también llevaba a cabo un encuentro híbrido (virtual y presencial) mensual denominado 'Encuentros para

crecer' con una duración aproximada de dos a tres horas. En los encuentros se abordaban las problemáticas de cada departamento y se buscaban soluciones para mitigar los riesgos potenciales. En estas reuniones, se fomentaba la colaboración y el intercambio de ideas entre los diferentes equipos de trabajo, lo que permitía una visión más amplia de los desafíos y las oportunidades de mejora en materia de seguridad de la información. Algunos de los temas tratados en estos encuentros incluían la actualización de software, progreso de los nuevos proyectos, la revisión de permisos de acceso y la identificación de posibles amenazas internas y externas. De esta manera, se fortalecía la cultura de seguridad en la organización y se promovía la responsabilidad compartida en la protección de los activos informáticos.

4.2.3. *Elaboración de matriz de riesgos*

Esta matriz es un instrumento asociado a los riesgos cibernéticos de los proveedores de la empresa, por lo tanto, es una herramienta valiosa para la gestión en esta área en el contexto empresarial actual. En consecuencia, ayuda a la empresa a identificar, evaluar y abordar los riesgos cibernéticos asociados con los proveedores de forma temprana, lo que permite a la empresa tomar medidas preventivas y corregir los riesgos antes de que se conviertan en problemas de difícil manejo. Además, contribuye a que la empresa pueda tomar decisiones asertivas sobre la selección de proveedores y las medidas de seguridad que se deben implementar para proteger su información confidencial.

Para elaborar la matriz de riesgos asociados a los resultados de la auditoría de proveedores de servicios, se consideraron varios campos clave. Cada uno de ellos se evaluó cuidadosamente y se documentó en la matriz de riesgos, lo que permitió identificar y clasificar los riesgos asociados a cada uno de ellos. La elaboración de la matriz se basó en los hallazgos de la auditoría realizada y en el formato de evaluación diligenciado por el proveedor. El análisis de la información y la construcción de la matriz tomó aproximadamente una semana para completarla.

La información contenida en dicha la matriz se especifica a continuación:

I. **Riesgo**: con este campo se buscó determinar cuáles eventos potenciales podrían causar pérdidas y comprender cómo, dónde y por qué podría ocurrir dicha pérdida.

II. **Activos de información o ciberactivos asociados**: se buscó identificar los activos de información y ciberactivos que suministraban los proveedores. En este apartado se encuentran: servidores, equipos del proveedor y endpoints.

III. **Agente de amenaza:** se identificaron las amenazas que tuvieran la intención o capacidad de explotar vulnerabilidades o debilidades en los sistemas de seguridad de la empresa, cómo, por ejemplo: crimen organizado, insider privilegiado, insider no privilegiado, malware, eventos naturales o proveedores.

IV. **Vulnerabilidades:** se identificaron y describieron las posibles vulnerabilidades en la seguridad de cada proveedor, tomando como referencia el cuestionario y la auditoría previamente realizados.

V. **Frecuencia de evento de amenaza:** se analizaron los diferentes agentes de amenazas a los que estuvieran expuestos los activos de la información y ciberactivos. El propósito de incluir esta información fue estimar la frecuencia probable con la que un agente de amenaza actuaría contra el activo de información, en un periodo de tiempo determinado. Para realizar esta estimación, el Departamento de seguridad de la información determino la siguiente escala:

Tabla 8

Frecuencia del evento de amenaza

Frecuencia del evento de amenaza (TEF)				
Calificación	**Descriptor**	**Descripción**	**Probabilidad de ocurrencia**	**Frecuencia**
5	**Altamente probable**	Se espera que el evento ocurra en forma reiterada	Más del 90 %	Ha ocurrido varias veces al año
4	**Probable**	Se espera que el evento ocurra con cierta regularidad	65 % - 90 %	Ha ocurrido una vez al año
3	**Ocasional**	El evento puede ocurrir de manera esporádica	35 % - 65 %	Ha ocurrido una vez en los últimos dos años
2	**Improbable**	El evento no es habitual	10 % - 35 %	Puede haber ocurrido en los últimos dos años
1	**Remota**	El evento solo puede ocurrir en circunstancias excepcionales	Menos del 10 %	No ha ocurrido en los últimos dos años

Fuente: Departamento de Seguridad de la Información

VI. **Capacidad de amenaza:** se relacionaba con la habilidad del agente de amenaza, en términos de conocimiento y experiencia, así como con los recursos disponibles, como el tiempo y los materiales que podrían ser utilizados contra los activos de información del tercero. Con el fin de estimar la capacidad de amenaza que podrían tener los ciberdelincuentes, el Departamento de Seguridad de la Información utilizaba la siguiente escala.

Tabla 9

Capacidad de amenaza

Capacidad de amenaza (Tcap)	
Categoría	**Descripción**
Muy alto (MA)	2% superior en comparación con la población general de amenazas
Alto (A)	16% superior en comparación con la población general de amenazas
Moderado (M)	Habilidad y recursos promedio (entre el 16% inferior y el 16% superior)
Bajo (B)	
Muy Bajo (MB)	2% inferior en comparación con la población general de amenazas

Fuente: Departamento de Seguridad de la Información

VII. **Controles:** se identificaron los controles reglamentarios existentes en la empresa, para prevenir la brecha de seguridad que se está presentando.

VIII. **Efectividad de controles:** para medir el nivel de implementación y eficacia de los controles, se empleó la siguiente escala:

Tabla 10

Efectividad de controles

Efectividad de los controles (CS)		
Calificación	**Descriptor**	**Definición**
1	**Fuerte**	• Los controles superan requerimientos normativos mínimos y se aplican las mejores prácticas • Se han adoptado todos o la gran mayoría de los controles económicamente viables y se aplican sistemáticamente • Atención significativa al riesgo • El control es altamente efectivo • Confiabilidad: ≥ 80 %

Efectividad de los controles (CS)		
Calificación	**Descriptor**	**Definición**
2	**Moderado**	• Los controles cumplen requerimientos normativos mínimos • Los controles se aplican, pero no están suficientemente formalizados o documentados • Atención moderada al riesgo • Los controles son medianamente efectivos • Confiabilidad: 50 % - 80 %
3	**Débil**	• Los controles no cumplen o cumplen parcialmente requerimientos normativos mínimos • Los controles aplicados son insuficientes para prevenir o mitigar el riesgo (o no se conocen). • Atención baja al riesgo • Muy poca o nula efectividad del control • Confiabilidad: < 50 %
4	**Incontrolable**	• Fuera del control de la organización en cuanto a su probabilidad de ocurrencia y a la posibilidad de gestionar sus consecuencias.

Fuente: Departamento de Seguridad de la Información

IX. Nivel de vulnerabilidad: teniendo en cuenta la vulnerabilidad descrita, se pudo determinar el grado de susceptibilidad frente a los daños, que tenía el sistema. Para evaluar este nivel de vulnerabilidad, el Departamento de Seguridad de la Información estableció la siguiente escala, que considera la capacidad de amenaza en relación con la efectividad de los controles.

Tabla 11

Capacidad de controles frente a efectividad

Nivel de la vulnerabilidad			**Efectividad de los controles**			
			1	2	3	4
			Incontrolable	**Débil**	**Moderado**	**Fuerte**
Capacidad de amenaza	5	**Muy alta**	Muy Alta	Muy Alta	Muy Alta	Moderada
	4	**Alta**	Muy Alta	Muy Alta	Alta	Baja
	3	**Moderada**	Muy Alta	Alta	Moderada	Muy Baja
	2	**Baja**	Alta	Moderada	Baja	Muy Baja
	1	**Muy baja**	Moderada	Baja	Muy Baja	Muy Baja

Fuente: Departamento de Seguridad de la Información

X. Frecuencia de eventos de pérdida: el análisis del riesgo consistió en determinar la magnitud del riesgo y ubicarlo cualitativamente, en relación con los niveles de aceptabilidad definidos por la

organización. Para ello, el Departamento de Seguridad de la Información estableció la siguiente escala, teniendo en cuenta la frecuencia de eventos de pérdida en comparación con la frecuencia de eventos de amenaza.

Tabla 12

Frecuencia de eventos de perdida frente a evento de amenaza

Frecuencia de eventos de pérdida (Probabilidad)			**Nivel de la vulnerabilidad**				
			1	2	3	4	5
			Muy bajo	**Bajo**	**Moderado**	**Alto**	**Muy alto**
Frecuencia de evento de amenaza	5	**Altamente probable**	Ocasional	Probable	Altamente probable	Altamente probable	Altamente probable
	4	**Probable**	Improbable	Ocasional	Probable	Probable	Probable
	3	**Ocasional**	Remota	Improbable	Ocasional	Ocasional	Ocasional
	2	**Improbable**	Remota	Remota	Improbable	Improbable	Improbable
	1	**Remota**	Remota	Remota	Remota	Remota	Remota

Fuente: Departamento de Seguridad de la Información

XI. Tipo de impacto con mayor nivel de afectación: se determinó el riesgo que podía afectar a los objetivos de la empresa, en alguna de las siguientes dimensiones, de acuerdo con lo definido en el "Manual de Gestión de riesgos" de la empresa.

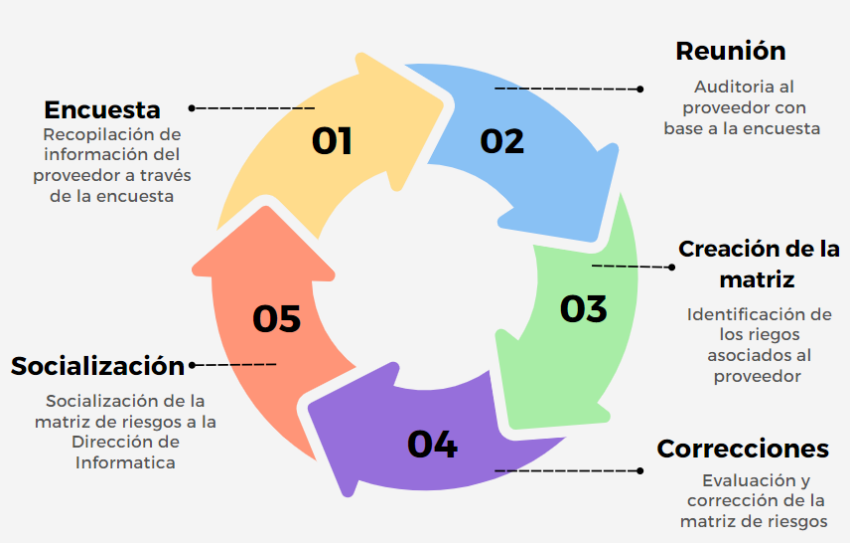
- **Financiero**: el impacto es monetario y se materializa para la compañía como menores ingresos, mayores costos o gastos o pérdida del valor de los activos, entre otros.
- **Reputacional**: impacto que afecta la imagen de la organización frente a los grupos de interés (accionistas, colaboradores, proveedores, medios de comunicación, comunidad, gobierno y autoridades).
- **Personas**: impacto que afecta al personal de la organización, retrasando los procesos.
- **Operacional/Interrupción del negocio**: impacto que afecta las operaciones del negocio, causando esfuerzos de diferente magnitud, para intentar normalizar la operación de las actividades.
- **Seguridad y Salud:** impacto que ocasiona lesiones, incapacidades o pérdida de vidas humanas de colaboradores o terceros.
- **Cumplimiento:** impacto relacionado con las faltas cometidas, en temas de regulación o incumplimiento de obligaciones por parte de la organización.

4.2.3.1 Socialización de la matriz de riesgos

Durante la auditoría se llevaron a cabo los procesos de encuesta, reunión, creación de la matriz, correcciones y socialización (Figura) con el objetivo de presentar a la Dirección de informática el análisis de los resultados obtenidos durante la auditoría.

Figura 15

Proceso de auditoria



Fuente: Autor

1. **Encuesta**: la primera etapa de la auditoría fue la recopilación de información del proveedor a través de una encuesta. Este instrumento se utilizó para obtener información general sobre la empresa, sus operaciones, prácticas de gestión y control interno, así como sus procesos y procedimientos (ver sección **¡Error! No se encuentra el origen de la referencia.**).
2. **Reunión con el proveedor:** tras recibir los resultados de la encuesta, se programó una reunión remota con el proveedor para obtener información adicional o aclarar cualquier duda (ver sección **¡Error! No se encuentra el origen de la referencia.**).
3. **Creación de la matriz:** se analizó la información recopilada para crear una matriz de riesgos que identificaran las posibles amenazas asociadas al proveedor (ver sección 4.2.3).

4. **Correcciones:** una vez creada la matriz de riesgos, el jefe del Departamento de Seguridad de la Información evaluó su precisión y adecuación. Si era necesario, se realizaron ajustes y correcciones para asegurar que reflejara de manera precisa los riesgos asociados al proveedor.
5. **Socialización:** por último, se socializó la matriz de riesgos con la Dirección de Informática para tomar medidas preventivas. Luego, el jefe del departamento contactó al proveedor para informar sobre las falencias encontradas y se pudieran realizar las correcciones necesarias.

4.3. Capacitaciones de seguridad de la información

El desarrollo del objetivo número tres se basó en la implementación del protocolo de Concientización y capacitación (PR.AT) de la categoría Proteger (PR) del marco NIST. Este protocolo se enfoca en fortalecer la conciencia y el conocimiento de los empleados en relación con la seguridad de la información. Mediante actividades de concientización y programas de capacitación, se busca educar a los empleados sobre las mejores prácticas de seguridad, los riesgos potenciales y cómo prevenir y responder ante incidentes de seguridad

4.3.1. *Diseño y desarrollo de infografías de seguridad*

Con el fin de incrementar conciencia sobre la importancia de proteger la información, se diseñan infografías que establecen políticas y procedimientos de seguridad precisos, mejorar la eficiencia en la gestión de la seguridad, cumplir con los requisitos regulatorios y legales, además de prevenir incidentes de seguridad y fugas de información. De esta manera, se buscaba garantizar que el personal de la empresa comprendiera su papel en la protección de la información crítica, siguiendo las políticas y procedimientos adecuados.

Para el diseño de las infografías, primero se realizó un estudio sobre los riesgos informáticos a los cuales los trabajadores de la empresa pudieran estar expuestos. Entre ellos, se encontró una variedad de amenazas, como ataques de phishing, malware, vulnerabilidades de software, robo de información, entre otros.

Con base a esta información, se crearon seis infografías, que se enviaron paulatinamente por correo electrónico a todos los trabajadores, con el asunto "Tips Informáticos". El jefe de Seguridad de la Información supervisaba el diseño de las infografías antes de ser desplegados.

Los temas de las infografías creadas fueron:

- Phishing: este tipo de infografía se enfocaba en brindar información y recomendaciones para identificar correos electrónicos fraudulentos, que buscaban engañar al usuario para robar sus datos personales o descargar malware. En el documento se incluían consejos para la verificación de la autenticidad del remitente de los correos recibidos, revisión de la dirección URL de los enlaces adjuntos y la validación del contenido del mensaje.
- Manejo de contraseñas: esta infografía incluía recomendaciones para la creación de contraseñas seguras y únicas. También se destacaban los riesgos de compartir las contraseñas o de no cambiarlas periódicamente.
- WIFI pública: esta infografía se enfocaba en los riesgos asociados a conectarse a una red WIFI pública. Incluía información sobre los peligros de utilizar una red no segura y los riesgos asociados a los datos personales e información privada que pudieran ser interceptados por terceros.
- Beneficios de almacenamiento en OneDrive: esta infografía se centraba en los beneficios de utilizar un servicio de almacenamiento en la nube como OneDrive, para la gestión documental de la empresa.
- FakeNews: incluía recomendaciones para identificar noticias falsas y evitar su propagación en las redes sociales. Incluían consejos para verificar la fuente de la noticia, buscar corroboración en otras fuentes confiables y evitar compartir noticias falsas, sin antes verificar su veracidad.

En el anexo 1 del documento se encuentran las infografías realizadas.

4.3.2. *Diseño y preparación de material complementario para las capacitaciones*

Para las capacitaciones se elaboraron cuatro presentaciones, donde se abordaron temas como: inducción seguridad de la información, phishing, manejo de contraseñas, pérdida de dispositivos electrónicos.

Además, se diseñó un taller llamado “reconocimiento de correos electrónicos fraudulentos con intentos de phishing”. Durante este taller, se proporcionó al personal de la empresa, nueve correos electrónicos recopilados de diferentes fuentes, con el fin de identificar las características o señales de alerta, que les permitieran determinar si un correo era legítimo o era fraudulento. El objetivo del taller fue enseñar a los participantes cómo identificar y reportar los correos electrónicos fraudulentos, que intentan obtener información confidencial a través de técnicas de ingeniería social.

Las imágenes de las diapositivas y taller elaborado se encuentran en el anexo 2 del documento.

4.3.3. *Ejecución de capacitaciones*

El propósito de las capacitaciones de seguridad de la información dadas al personal de la empresa era proteger los activos de información críticos y asegurar la continuidad del negocio. Al ser una empresa que maneja información sensible y operaciones críticas, es esencial que los empleados estén capacitados para comprender los riesgos asociados con la seguridad de la información, como el robo de datos confidenciales, la interrupción del suministro de energía y los riesgos para la seguridad pública. Además, el objetivo de las capacitaciones era enseñar a los empleados a prevenir y responder a los ataques cibernéticos, identificar señales de alerta de fraude, y proteger los datos personales de los clientes.

En cada capacitación se abordaron diferentes temas, como:

- **Inducción** a la seguridad de la información: esta capacitación se orientó al personal de nuevo ingreso, con el propósito de brindar conocimiento del proceso de confidencialidad y las políticas de seguridad de la información de la empresa.
- **Phishing**: esta capacitación estaba dirigida al personal que no había superado las pruebas de phishing, y a aquellos empleados que hubieran descargado archivos o abiertos enlaces maliciosos.
- **Manejo de contraseñas seguras**: esta capacitación fue creada debido a que algunos empleados comprometieron sus credenciales empresariales, lo que puso en riesgo la seguridad institucional.
- **Pérdida de dispositivos electrónicos:** a raíz de la ocurrencia de este incidente, se diseñó una capacitación para concientizar a los empleados sobre la fuga de información y la importancia de proteger los dispositivos que utilizan para el trabajo. En esta capacitación se brindaron recomendaciones sobre medidas de seguridad y procedimientos para reportar la pérdida de dispositivos de manera oportuna.

En la siguiente tabla se detallan algunos aspectos importantes relacionados con las capacitaciones

Tabla 13

Capacitaciones al personal de la empresa

Nombre Capacitación	Número de asistentes	Modalidad	Fecha	Duración [Horas]
Inducción seguridad de la información	8	Presencial	12/12/2022	1
Phishing	10	Presencial	01/02/2023	2
Phishing	4	Remoto	08/02/2023	2
Manejo de contraseñas	3	Presencial	21/02/2023	1
Inducción seguridad de la información	11	Presencial	08/03/2023	1
Pérdida de dispositivos electrónicos	5	Remoto	14/03/2023	1 hora

Fuente: Autor

La mayoría de las capacitaciones se realizaron de manera presencial, en las instalaciones de la Empresa de Energía de Boyacá sede Tunja. Sin embargo, algunas de ellas se llevaron a cabo de forma remota, por medio de la plataforma Teams, especialmente para aquellos trabajadores que se encontraban en otros municipios de Boyacá y no podían asistir de forma presencial.

Figura 16

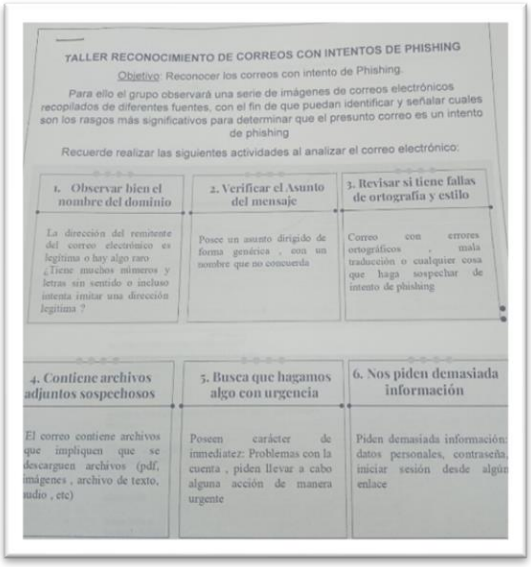
Capacitación modalidad presencial

Fuente: Autor

Para la capacitación de phishing presencial, se utilizó el taller de reconocimiento de correos electrónicos fraudulentos como se muestra en la Figura 16. Durante el taller se organizaron grupos de tres personas, para poder discutir y analizar los correos electrónicos presentados. Al final de la actividad, se brindó una realimentación detallada sobre las respuestas dadas por los empleados, con el propósito de comparar y mejorar su capacidad de identificación de correos fraudulentos. Por otra parte, durante el desarrollo de la capacitación de phishing en modalidad remota, se envió a los participantes el instructivo del taller mencionado. Una vez completado, se brindó realimentación individual a cada uno de ellos.

Figura 17

Taller de phishing



TALLER RECONOCIMIENTO DE CORREOS CON INTENTOS DE PHISHING

Objetivo: Reconocer los correos con intento de Phishing.

Para ello el grupo observará una serie de imágenes de correos electrónicos recopilados de diferentes fuentes, con el fin de que puedan identificar y señalar cuales son los rasgos más significativos para determinar que el presunto correo es un intento de phishing

Recuerde realizar las siguientes actividades al analizar el correo electrónico:

1. Observar bien el nombre del dominio	2. Verificar el Asunto del mensaje	3. Revisar si tiene fallas de ortografía y estilo
La dirección del remitente del correo electrónico es legítima o hay algo raro ¿Tiene muchos números y letras sin sentido o incluso intenta imitar una dirección legítima ?	Posee un asunto dirigido de forma genérica , con un nombre que no concuerda	Correo con errores ortográficos , mala traducción o cualquier cosa que haga sospechar de intento de phishing
4. Contiene archivos adjuntos sospechosos	**5. Busca que hagamos algo con urgencia**	**6. Nos piden demasiada información**
El correo contiene archivos que impliquen que se descarguen archivos (pdf, imágenes , archivo de texto, udio , etc)	Poseen carácter de inmediatez: Problemas con la cuenta , piden llevar a cabo alguna acción de manera urgente	Piden demasiada información: datos personales, contraseña, iniciar sesión desde algún enlace

Fuente: Autor

Al finalizar cada capacitación, se ofrecía un espacio de preguntas por parte de los trabajadores. Este espacio resultó muy útil para que los empleados pudieran expresar sus dudas con respecto a los temas de seguridad de la información abordados, así como también para proponer mejoras en la planificación de las capacitaciones.

Cabe aclarar que estas capacitaciones eran de gran importancia y alcance, debido a que estaban abiertas a todo el personal de la empresa. Además, es importante mencionar que estas capacitaciones no solo ofrecían información relevante y actualizada sobre seguridad de la información, sino que también fomentaban una cultura de prevención y conciencia entre los empleados. De esta manera, se les brindaban las herramientas necesarias para identificar posibles riesgos y prevenir cualquier tipo de fuga de información que pudiera afectar a la empresa.

4.3.4. *Administración de la plataforma Knowbe4*

KnowBe4 es una plataforma que se enfoca en proporcionar capacitación y concientización en seguridad de la información y ciberseguridad a empresas y organizaciones en todo el mundo. A través de cursos en línea y videojuegos interactivos, KnowBe4 ayuda a los empleados a identificar y prevenir amenazas de seguridad informática, como los ataques de ingeniería social y el phishing. (Knowbe4, 2023)

Es importante destacar que las capacitaciones ofrecidas por KnowBe4 no solo ayudan a las empresas a proteger sus sistemas y datos, sino que también pueden mejorar la cultura de seguridad dentro de la organización. La plataforma también ofrece simulaciones de ataques de phishing, para ayudar a las empresas a evaluar la efectividad de su capacitación en seguridad y tomar medidas correctivas donde sea necesario. Además, proporciona informes y análisis detallados, para ayudar a las empresas a medir su progreso y mejorar su postura de seguridad en el futuro.

Teniendo esto en cuenta, el Departamento de Seguridad de la Información utiliza la plataforma KnowBe4 para impartir cursos de ciberseguridad a los empleados, cada tres meses, lo que resulta en un total de cuatro cursos al año. El contenido de estos cursos se personaliza según el tipo de empleados, organizados en seis grupos: personal financiero, personal de TI, personal operacional, personal de recursos humanos, personal directivo y personal conjunto de la EBSA. Cada curso fue cuidadosamente evaluado y seleccionado de acuerdo a los requerimientos del grupo correspondiente. Esto garantizó que los empleados recibieran una formación adaptada a sus necesidades y que estuviera alineada con los objetivos del Departamento de Seguridad de la Información.

El contenido de cada curso tenía una duración aproximada de 30 minutos, y a los empleados se les otorgó un plazo de un mes para completarlo. Es importante destacar que estos cursos eran interactivos y estaban diseñados para mantener el interés y la participación de los empleados, durante todo el proceso de aprendizaje. Además, la plataforma KnowBe4 cuenta con un sistema de seguimiento, que permitía al Departamento de Seguridad de la Información monitorear el progreso de los empleados y asegurarse de que se completaran los cursos en el plazo asignado.

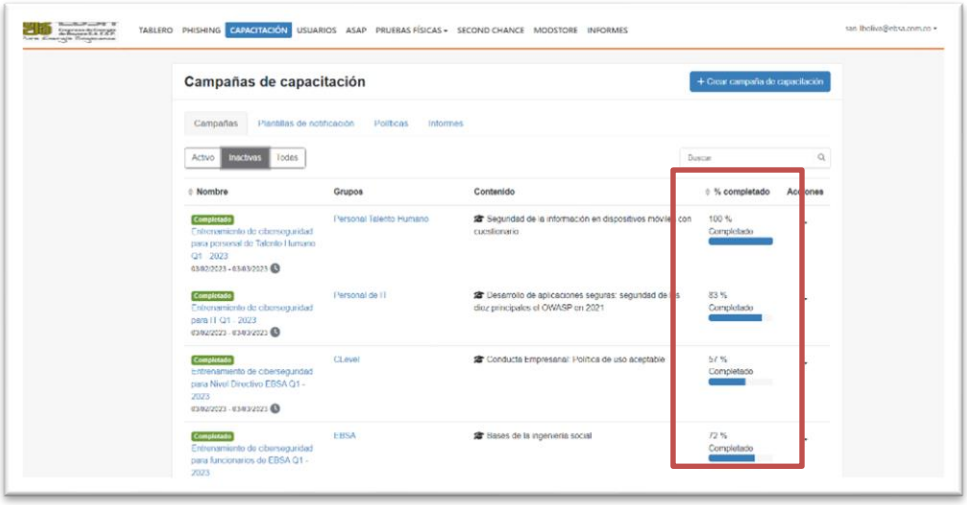
Con el fin de detectar oportunamente aquellos empleados con riesgo de no completar el curso, se realizó un proceso de seguimiento. Este proceso incluía una comunicación directa con el trabajador, para identificar y resolver cualquier problema o dificultad que éste pudiera tener, para cumplir con el plazo establecido. El objetivo de esta medida no solo era garantizar que los empleados recibieran una formación en ciberseguridad adecuada, sino también fomentar una cultura de seguridad y responsabilidad en toda la organización.

Algunas de las temáticas de los cursos que se ofrecieron a los empleados incluyeron: desarrollo de aplicaciones seguras, amenazas internas para usuarios finales, ingeniería social, phishing, manejo de contraseñas y navegación web segura. Además, la plataforma ofreció una gran variedad de recursos y herramientas de aprendizaje, como videos, simulaciones y juegos, para hacer que la formación fuera más interactiva y amena para los empleados.

En la figura 18 se puede observar la administración de los cursos impartidos. A través de ella se hacía un seguimiento del porcentaje de empleados de cada grupo que completaban los cursos asignados.

Figura 18

Panel de control de la herramienta Knowbe4



Fuente: Empresa de Energía de Boyacá

Sin embargo, a pesar de los esfuerzos del Departamento de Seguridad de la Información y la disponibilidad de los cursos, se observó que no hubo interés por parte de los empleados para completarlos en su totalidad. Esta falta de contribución llevó al departamento a considerar otras medidas de capacitación, para mejorar la concientización sobre los conceptos de ciberseguridad entre los empleados. Dentro de las alternativas propuestas se encuentra la divulgación de infografías, anteriormente mencionadas y, adicionalmente, se lanzó una campaña de concientización llamada “No de papaya”. Los recursos incluidos en la campaña, tales como videos relacionados con delitos informáticos y cómo evitarlos, se enviaban por correo electrónico a los trabajadores.

4.4. Herramientas utilizadas en el desarrollo del proyecto

Tabla 14

Herramientas utilizadas para el desarrollo del proyecto

Herramienta utilizada	Para qué la utilizó
Tenable SC	Se implemento para monitorear y evaluar la postura de seguridad de la red de la empresa. La información recopilada por la herramienta se utilizó para generar informes detallados sobre las vulnerabilidades y riesgos identificados en la red, lo que permitió al Departamento de Seguridad de la Información tomar medidas proactivas para abordarlos. Además, la herramienta también permitió la gestión de parches y la implementación de políticas de seguridad en toda la red.
Antivirus AMP de Cisco	Se utilizó para proteger los dispositivos y redes de posibles amenazas informáticas, como virus, malware y otros tipos de ataques. Además, la herramienta permitía la detección y el bloqueo de actividades sospechosas en tiempo real, lo que mejoraba la capacidad de la empresa para responder a incidentes de seguridad. Se utilizaba la herramienta para realizar análisis de vulnerabilidades y para aplicar políticas de seguridad en los dispositivos de la empresa. Además, el uso de la herramienta permitía la generación de informes detallados sobre el estado de seguridad de los dispositivos y la red, lo que facilitaba la toma de decisiones informadas para mejorar la seguridad en la empresa.
MISP	Se implemento para para la gestión y el intercambio de información sobre amenazas y vulnerabilidades de seguridad en la organización. Esta herramienta permitió la colaboración

Herramienta utilizada	Para qué la utilizó
	y el intercambio de información en tiempo real con otros equipos de seguridad, así como el análisis de eventos y la identificación de patrones de ataque. Además, MISP facilitó la identificación de vulnerabilidades y la implementación de medidas preventivas y correctivas para mitigar los riesgos de seguridad en la organización.
Knowbe4	Se utilizó para la administración de cursos de ciberseguridad a los empleados y la simulación de ataque controlado de phishing.

Fuente: Autor

5. CONCLUSIONES

- A lo largo de la pasantía, se lograron implementar protocolos preventivos y correctivos, asociados a la seguridad de la información de la Empresa de Energía de Boyacá. Esto fortaleció la protección de los datos, redujo la vulnerabilidad ante posibles amenazas cibernéticas y salvaguardó la confidencialidad e integridad de los datos, fortaleciendo así, la reputación de la empresa en el sector energético.

- A pesar de haber realizado con éxito las capacitaciones y cursos, se evidenció dificultad al no recibir el respaldo del personal de la empresa, quienes no estaban dispuestos a participar dinámicamente en estas actividades. Esta situación motivó la búsqueda de otras herramientas o metodologías, para captar la atención del público. Es importante explorar enfoques innovadores y creativos, que generen interés y compromiso por parte del personal en temas de seguridad informática.

- Durante la pasantía, se logró apreciar de manera significativa la importancia de estar capacitado y actualizado en temas de seguridad, para hacer frente a las constantes amenazas. Esta experiencia reforzó el compromiso de seguir adquiriendo conocimientos y habilidades en seguridad informática, con el objetivo de estar preparado para enfrentar los desafíos y salvaguardar la integridad de los activos.

- Durante mi experiencia como pasante en el departamento de seguridad de la información, desempeñé un papel crucial al crear conciencia sobre la importancia de la seguridad de la información. A través de charlas y la elaboración de infografías, logré concientizar al personal

sobre las mejores prácticas en términos de protección de la información y los riesgos potenciales a los cuales se pueden ver expuestos. Además, al monitorear las vulnerabilidades de la infraestructura de TI y desarrollar planes de contingencia, contribuí activamente a fortalecer la postura de seguridad de la organización. Mi participación como pasante fue de importancia para promover un entorno más seguro en el ámbito de seguridad de la información.

6. GLOSARIO

- **Vulnerabilidad**: es cualquier fallo de diseño o error en el software o en el hardware. Esto hace posible a un atacante o hacker comprometer la integridad y confidencialidad de los datos que procesa un sistema (Delta Protect, 2023).

- **Malware:** es un término que abarca cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable. Los delincuentes cibernéticos generalmente lo usan para extraer datos que pueden utilizar como chantaje hacia las víctimas para obtener ganancias financieras. Dichos datos pueden variar desde datos financieros, hasta registros de atención médica, correos electrónicos personales y contraseñas (McAfee, 2023).

- **Riesgos informáticos:** posibles eventos o situaciones que pueden amenazar la seguridad de los sistemas informáticos y la información que contienen (IN FORDISA, 2023).

- **Ataques cibernéticos**: acciones maliciosas llevadas a cabo por personas o programas informáticos con el objetivo de comprometer sistemas o robar información (IBM, 2023).

- **Endpoints**: dispositivos finales, como computadoras, teléfonos móviles o tablets, que se conectan a una red informática (ADMWARE, 2023).

- **Amenaza informática:** Una amenaza informática se refiere a cualquier evento, acción o circunstancia que tiene el potencial de dañar o comprometer la seguridad, integridad o disponibilidad de los sistemas informáticos y la información que contienen (DragonJar, 2023).

- **Plan de remediación**: plan que establece las medidas y acciones a tomar para corregir o mitigar los efectos de un incidente de seguridad (Ingecom, 2023).

- **Indicadores de compromiso:** son medidas o métricas utilizadas para evaluar el nivel de compromiso de una persona o grupo hacia un objetivo, tarea o proyecto específico. Estos indicadores proporcionan información cuantitativa o cualitativa sobre el grado de dedicación, motivación y responsabilidad que muestra un individuo o equipo en relación con sus responsabilidades (CRONUP, 2023).

- **Mitigar**: acción de reducir, aliviar o minimizar los efectos negativos, daños o riesgos asociados a una situación o problema específico. El objetivo de la mitigación es disminuir o contrarrestar los impactos adversos y promover la seguridad, el bienestar y la sostenibilidad (Cibernos, 2023).

- **Auditoria informática:** proceso sistemático y objetivo de evaluación y examen de la infraestructura, sistemas, políticas y procedimientos de seguridad informática de una organización. Su objetivo es identificar vulnerabilidades, riesgos y deficiencias en los controles de seguridad, así como garantizar el cumplimiento de políticas y regulaciones establecidas (EUROINNOVA, 2023).

- **Ciberataque**: intento malicioso de comprometer la seguridad de sistemas informáticos, redes o dispositivos conectados a Internet. Consiste en acciones emprendidas por individuos o grupos con el objetivo de acceder, dañar, alterar, robar o destruir información confidencial, interrumpir operaciones normales, obtener beneficios económicos ilícitos o causar perjuicio a organizaciones o personas (IBM , 2023).

- **Firewall**: es una medida de seguridad que controla el tráfico de red entre una red interna y externa. Se utiliza para proteger los sistemas informáticos de amenazas externas, como ciberataques y malware. (CISCO, 2023)

- **Fallas de seguridad**: debilidades, vulnerabilidades o errores en sistemas, redes, aplicaciones o procesos que comprometen la seguridad de la información y pueden permitir a personas no autorizadas acceder, modificar, robar o dañar datos sensibles o recursos protegidos (Peritos informaticos , 2023).

- **Riesgos**: en el contexto de la seguridad informática, los riesgos se refieren a las posibilidades de que ocurran eventos o incidentes no deseados que puedan afectar negativamente los sistemas y la información. Estos riesgos pueden ser originados tanto interna como externamente (Concepto, 2023).

- **Insider privilegiado:** individuo que tiene acceso autorizado a información confidencial o sistemas de una organización debido a su posición o responsabilidades. Este acceso puede ser explotado de manera malintencionada para llevar a cabo acciones fraudulentas o dañinas (RedHat, 2023).

- **Insider no privilegiado:** persona que tiene acceso limitado a los sistemas o información de una organización debido a su posición o responsabilidades laborales, pero que aún puede representar un riesgo de seguridad si utiliza su acceso para realizar actividades maliciosas o divulgar información confidencial (RedHat, 2023).

- **Crimen organizado**: grupos estructurados que se dedican a actividades ilegales de forma sistemática y coordinada. Estas organizaciones buscan obtener ganancias económicas mediante actividades como el tráfico de drogas, el contrabando, la extorsión y otros delitos graves (figón, 2023).

- **Phishing:** técnica de ciberdelincuencia en la cual los atacantes se hacen pasar por entidades confiables, como bancos o empresas, para obtener información personal o financiera de las víctimas. Esto se logra mediante el envío de correos electrónicos falsos o la creación de sitios web fraudulentos (AULA CM, 2023).

- **Fake News:** noticias falsas o desinformación deliberada que se presenta como información verídica y se difunde a través de diversos medios de comunicación, especialmente en plataformas digitales

y redes sociales, pueden tener impactos negativos en la sociedad, la política y la confianza pública (ARIMETRICS, 2023).

- **Wi-Fi pública:** red inalámbrica disponible de forma pública en lugares como cafeterías, aeropuertos o parques, que permite a los usuarios acceder a Internet de forma inalámbrica. Sin embargo, las redes Wi-Fi públicas pueden representar riesgos de seguridad, ya que los datos transmitidos pueden ser interceptados por personas no autorizadas (Xataka, 2023).

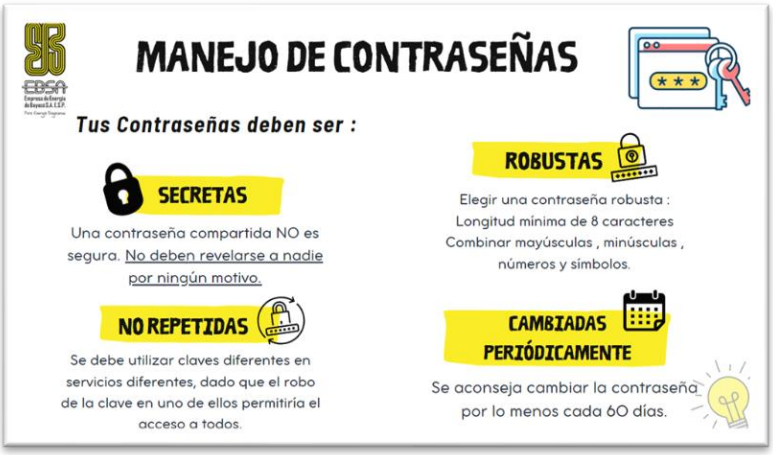
7. ANEXOS

Anexo 1 Infografías

Figura 19 *Consejos para identificar correo phishing*

Fuente: Autor

Figura 20 *Manejo de contraseñas seguras*



Fuente: Autor

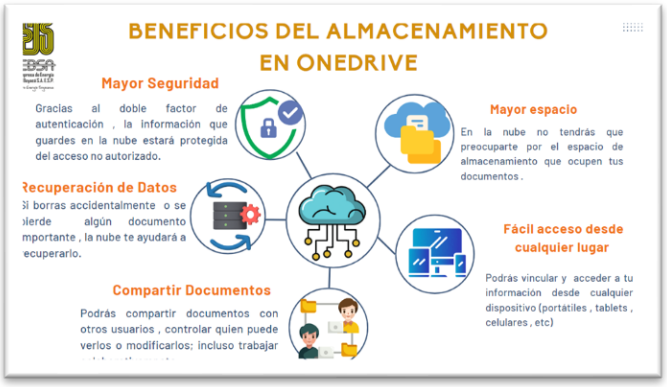
Figura 21 *Riesgos de conectarse a una red WIFI pública*

Fuente: Autor

Figura 22 *Correo phishing*

Fuente: Autor

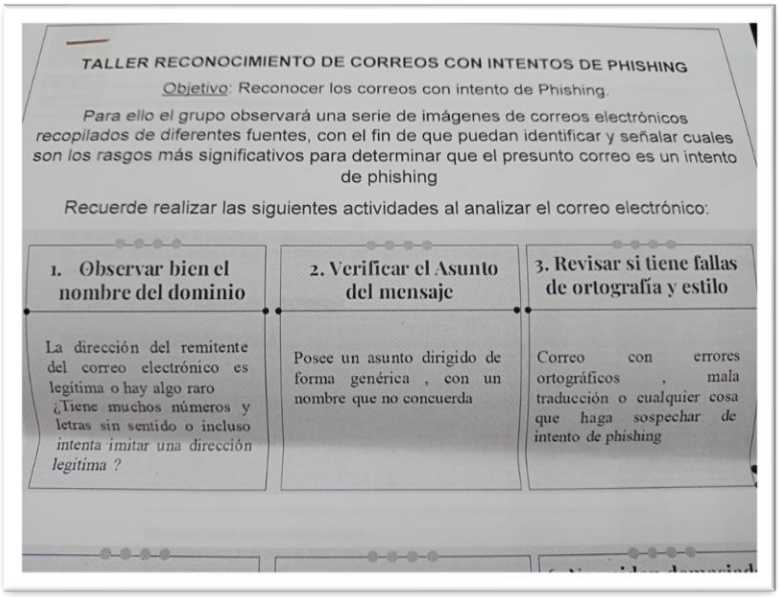
Figura 23 *Beneficios de onedrive*



Fuente: Autor

Anexo 2 Recurso de apoyo

Figura 24 *Taller reconocimiento de phishing*



TALLER RECONOCIMIENTO DE CORREOS CON INTENTOS DE PHISHING

Objetivo: Reconocer los correos con intento de Phishing.

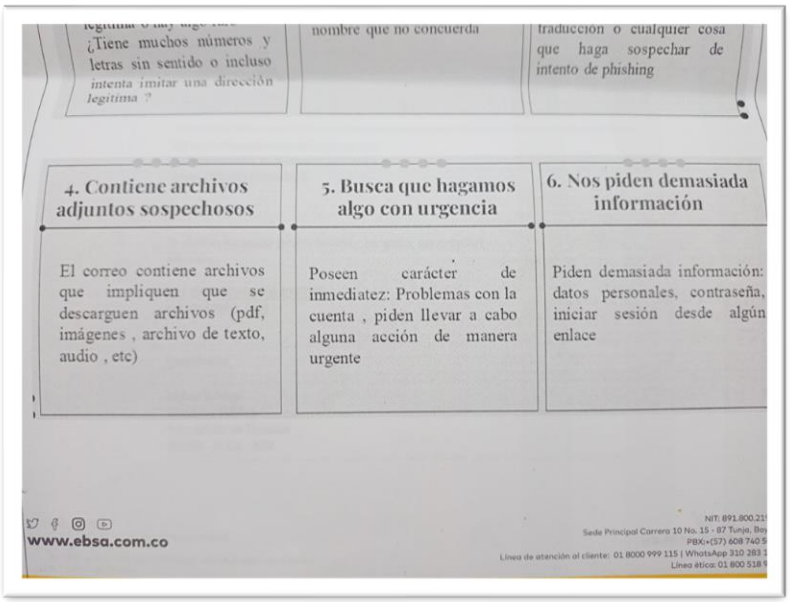
Para ello el grupo observará una serie de imágenes de correos electrónicos recopilados de diferentes fuentes, con el fin de que puedan identificar y señalar cuales son los rasgos más significativos para determinar que el presunto correo es un intento de phishing

Recuerde realizar las siguientes actividades al analizar el correo electrónico:

1. Observar bien el nombre del dominio	2. Verificar el Asunto del mensaje	3. Revisar si tiene fallas de ortografía y estilo
La dirección del remitente del correo electrónico es legitima o hay algo raro ¿Tiene muchos números y letras sin sentido o incluso intenta imitar una dirección legitima ?	Posee un asunto dirigido de forma genérica , con un nombre que no concuerda	Correo con errores ortográficos , mala traducción o cualquier cosa que haga sospechar de intento de phishing

Fuente: Autor

Figura 25 *Taller reconocimiento de phishing parte 2*

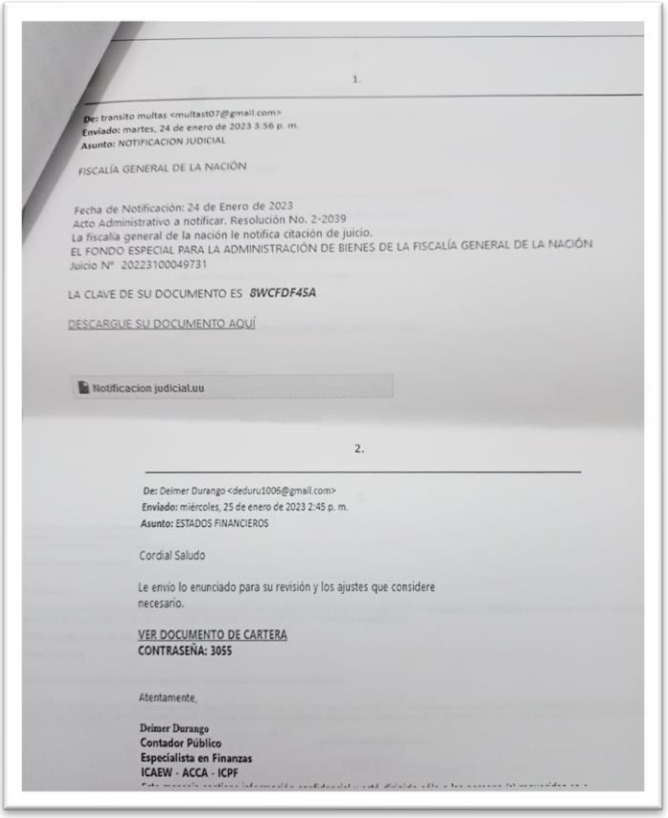


¿Tiene muchos números y letras sin sentido o incluso intenta imitar una dirección legitima ?	nombre que no concuerda	traducción o cualquier cosa que haga sospechar de intento de phishing
4. Contiene archivos adjuntos sospechosos	**5. Busca que hagamos algo con urgencia**	**6. Nos piden demasiada información**
El correo contiene archivos que impliquen que se descarguen archivos (pdf, imágenes , archivo de texto, audio , etc)	Poseen carácter de inmediatez: Problemas con la cuenta , piden llevar a cabo alguna acción de manera urgente	Piden demasiada información: datos personales, contraseña, iniciar sesión desde algún enlace

www.ebsa.com.co

Fuente: Autor

Figura 26 *Taller reconocimiento de phishing parte 3*



1.

De: transito multas <multast07@gmail.com>
Enviado: martes, 24 de enero de 2023 3:56 p. m.
Asunto: NOTIFICACION JUDICIAL

FISCALÍA GENERAL DE LA NACIÓN

Fecha de Notificación: 24 de Enero de 2023
Acto Administrativo a notificar. Resolución No. 2-2039
La fiscalia general de la nación le notifica citación de juicio.
EL FONDO ESPECIAL PARA LA ADMINISTRACIÓN DE BIENES DE LA FISCALÍA GENERAL DE LA NACIÓN
Juicio N° 20223100049731

LA CLAVE DE SU DOCUMENTO ES ***8WCFDF45A***

DESCARGUE SU DOCUMENTO AQUÍ

Notificacion judicial.uu

2.

De: Deimer Durango <deduru1006@gmail.com>
Enviado: miércoles, 25 de enero de 2023 2:45 p. m.
Asunto: ESTADOS FINANCIEROS

Cordial Saludo

Le envio lo enunciado para su revisión y los ajustes que considere necesario.

VER DOCUMENTO DE CARTERA
CONTRASEÑA: 3055

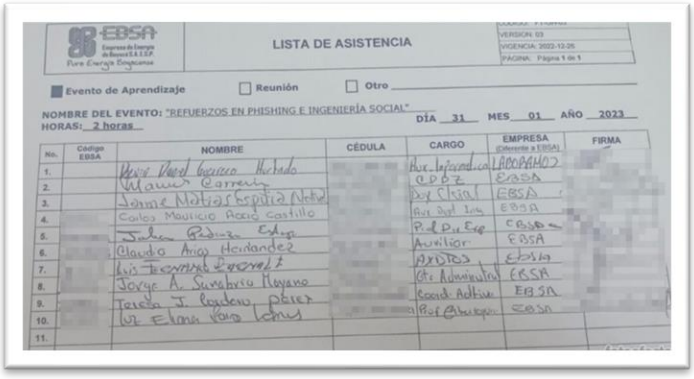
Atentamente,

Deimer Durango
Contador Público
Especialista en Finanzas
ICAEW - ACCA - ICPF

Fuente: Autor

Anexo 3 Listado de asistencia a la capacitación de phishing

Figura 27 *Lista de asistencia capacitación de phishing*



LISTA DE ASISTENCIA

Evento de Aprendizaje ☐ Reunión ☐ Otro

NOMBRE DEL EVENTO: "REFUERZOS EN PHISHING E INGENIERÍA SOCIAL"
HORAS: 2 horas
DÍA 31 MES 01 AÑO 2023

No.	Código EBSA	NOMBRE	CÉDULA	CARGO	EMPRESA (Diferente a EBSA)	FIRMA
1.		[illegible]		[illegible]	[illegible]	
2.		[illegible]		[illegible]	EBSA	
3.		[illegible]		[illegible]	EBSA	
4.		[illegible]		[illegible]	EBSA	
5.		[illegible]		[illegible]	EBSA	
6.		[illegible]		[illegible]	EBSA	
7.		[illegible]		[illegible]	EBSA	
8.		[illegible]		[illegible]	EBSA	
9.		[illegible]		[illegible]	EBSA	
10.		[illegible]		[illegible]	EBSA	
11.						

Fuente: Autor

Anexo 4 Contenido de presentaciones para las capacitaciones

A continuación, se puede observar los títulos de las presentaciones y su respectivo contenido, del material utilizado en las capacitaciones.

Figura 28 *Capacitación de phishing*

Fuente: Autor

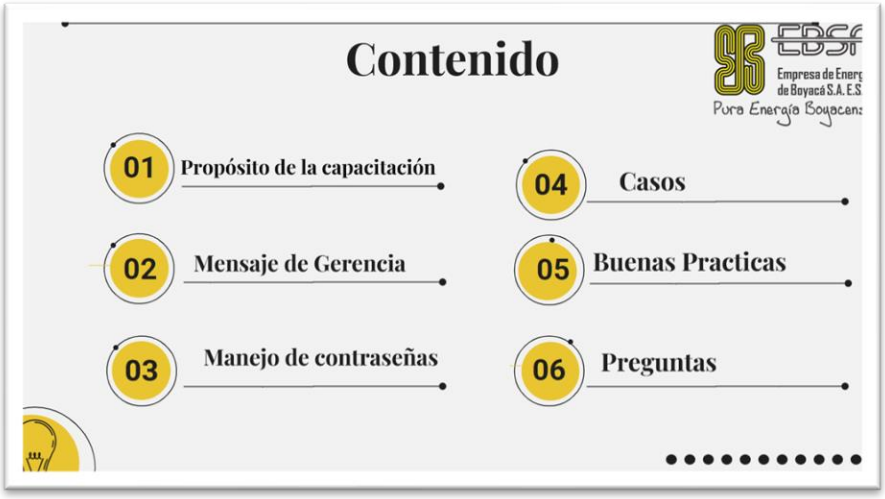
Figura 29 *Contenido capacitación de phishing*

Fuente: Autor

Figura 30 *Capacitación de manejo seguro de contraseñas*

Fuente: Autor

Figura 31 *Contenido capacitación manejo de contraseñas seguras*

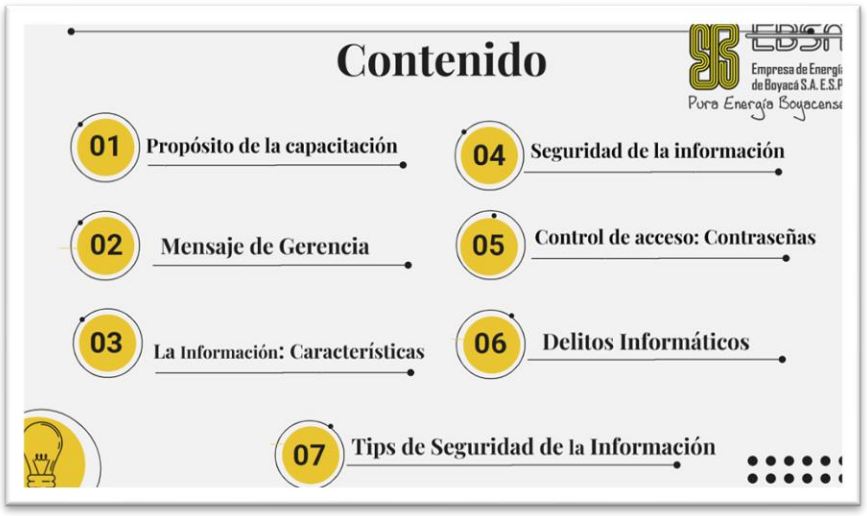


Fuente: Autor

Figura 32 *Capacitación inducción seguridad de la información*

Fuente: Autor

Figura 33 *Contenido capacitación inducción seguridad de la información*

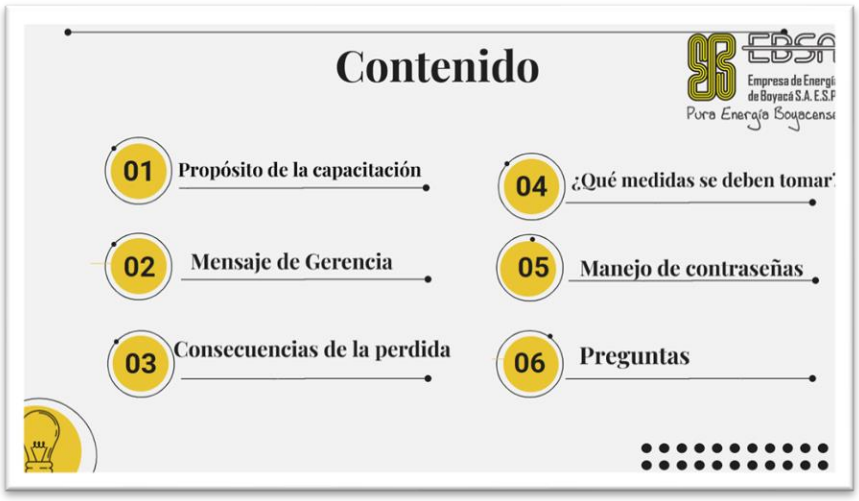


Fuente: Autor

Figura 34 *Capacitación perdida de dispositivos electrónicos*

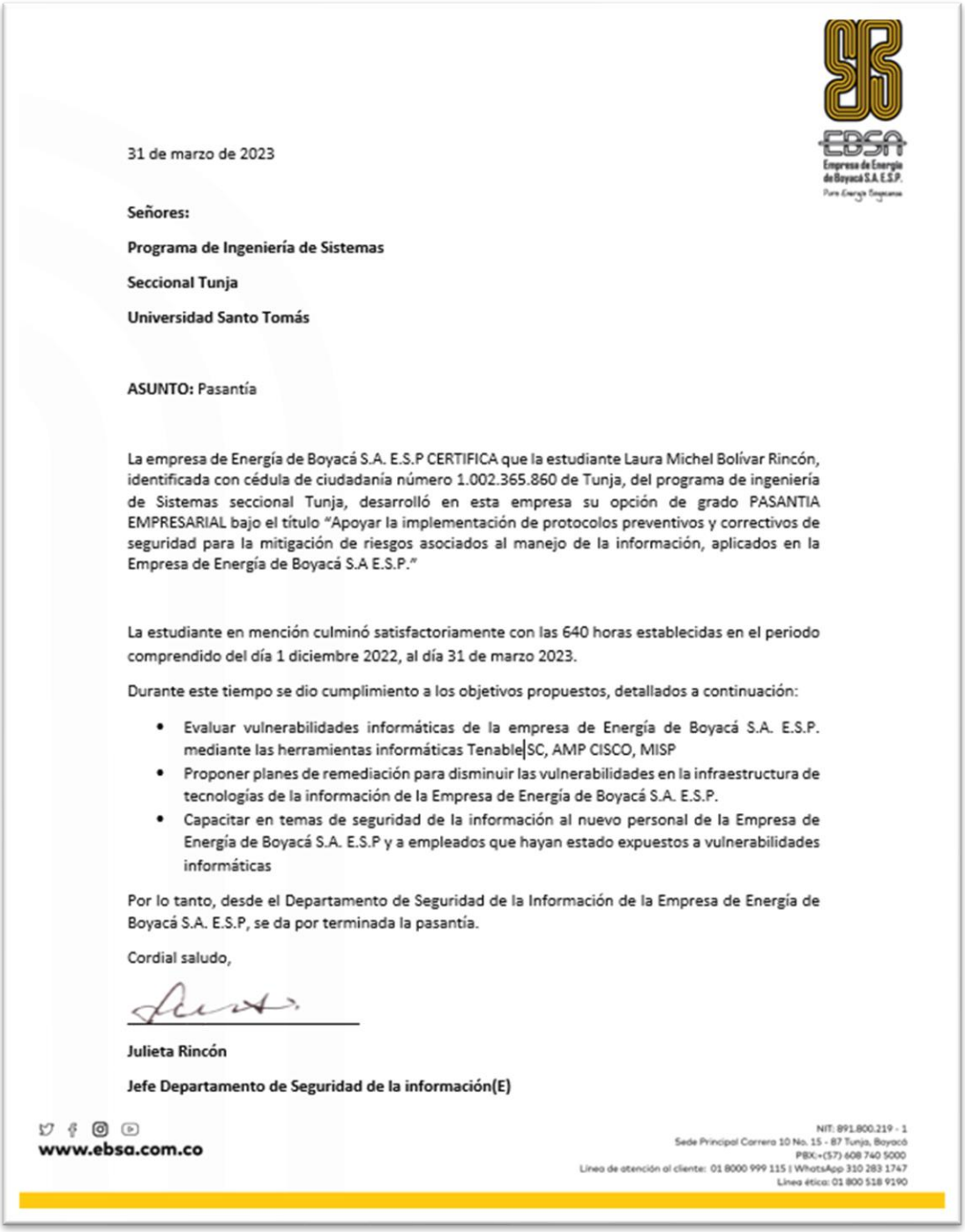
Fuente: Autor

Figura 35 *Contenido capacitación dispositivos electrónicos*



Fuente: Autor

Anexo 4 Carta de aprobación finalización de la pasantía



31 de marzo de 2023

Señores:

Programa de Ingeniería de Sistemas

Seccional Tunja

Universidad Santo Tomás

ASUNTO: Pasantía

La empresa de Energía de Boyacá S.A. E.S.P CERTIFICA que la estudiante Laura Michel Bolívar Rincón, identificada con cédula de ciudadanía número 1.002.365.860 de Tunja, del programa de ingeniería de Sistemas seccional Tunja, desarrolló en esta empresa su opción de grado PASANTIA EMPRESARIAL bajo el título "Apoyar la implementación de protocolos preventivos y correctivos de seguridad para la mitigación de riesgos asociados al manejo de la información, aplicados en la Empresa de Energía de Boyacá S.A E.S.P."

La estudiante en mención culminó satisfactoriamente con las 640 horas establecidas en el periodo comprendido del día 1 diciembre 2022, al día 31 de marzo 2023.

Durante este tiempo se dio cumplimiento a los objetivos propuestos, detallados a continuación:

- Evaluar vulnerabilidades informáticas de la empresa de Energía de Boyacá S.A. E.S.P. mediante las herramientas informáticas Tenable SC, AMP CISCO, MISP
- Proponer planes de remediación para disminuir las vulnerabilidades en la infraestructura de tecnologías de la información de la Empresa de Energía de Boyacá S.A. E.S.P.
- Capacitar en temas de seguridad de la información al nuevo personal de la Empresa de Energía de Boyacá S.A. E.S.P y a empleados que hayan estado expuestos a vulnerabilidades informáticas

Por lo tanto, desde el Departamento de Seguridad de la Información de la Empresa de Energía de Boyacá S.A. E.S.P, se da por terminada la pasantía.

Cordial saludo,

Julieta Rincón

Jefe Departamento de Seguridad de la información(E)

www.ebsa.com.co

NIT: 891.800.219 - 1
Sede Principal Carrera 10 No. 15 - 87 Tunja, Boyacá
PBX:+(57) 608 740 5000
Línea de atención al cliente: 01 8000 999 115 | WhatsApp 310 283 1747
Línea ética: 01 800 518 9190

Fuente: Departamento Seguridad de la Información

8. REFERENCIAS

ADMWARE. (8 de 05 de 2023). *ADMWARE*. https://admware.es/que-es-un-endpoint/

ARIMETRICS. (6 de 05 de 2023). *ARIMETRICS*. https://www.arimetrics.com/glosario-digital/fake-news

AULA CM. (6 de 05 de 2023). *AULA CM*. https://aulacm.com/que-es/phishing-significado-definicion-ejemplos/

Cibernos. (8 de 05 de 2023). *Cibernos*. https://www.grupocibernos.com/blog/que-son-los-controles-de-mitigacion-y-como-garantizarla

CISCO. (03 de 09 de 2023). *CISCO*. https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html

CISCO. (6 de 05 de 2023). *CISCO*. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Concepto. (6 de 05 de 2023). *Concepto*. https://conceptodefinicion.de/riesgo/

CRONUP. (16 de 05 de 2023). *CRONUP*. https://www.cronup.com/la-importancia-de-los-indicadores-de-compromiso-ioc-en-la-ciberseguridad/

CVE. (16 de 3 de 2023). *CVE*. https://cve.mitre.org

Delta Protect. (6 de 05 de 2023). *Delta Protect*. https://www.deltaprotect.com/blog/vulnerabilidad-informatica

DragonJar. (8 de 05 de 2023). *DragonJar*. https://www.dragonjar.org/vulnerabilidades-y-amenazas-informaticas.xhtml

EUROINNOVA. (6 de 05 de 2023). *EUROINNOVA*. https://www.euroinnova.edu.es/blog/que-es-una-auditoria-informatica

figón, L. c. (2023). Crimen organizado . *Luis carranza figón*, 2380.

IBM . (6 de 005 de 2023). https://www.ibm.com/es-es/topics/cyber-attack

IBM. (6 de 05 de 2023). *IBM*. https://www.ibm.com/mx-es/topics/cyber-attack

IN FORDISA. (6 de 05 de 2023). *IN FORDISA*. https://www.infordisa.com/es/prevencion-riesgos-informaticos/

infobae. (15 de 02 de 2023). *infobae*. infobae: https://www.infobae.com/america/tecno/2023/01/02/las-34-empresas-que-fueron-hackeadas-en-colombia-durante-2022/

Ingecom. (8 de 05 de 2023). *Ingecom*. https://www.ingecom.net/es/blog/75/remediacion-vs-mitigacion-de-vulnerabilidades-cual-es-la-diferencia/

Knowbe4. (25 de 03 de 2023). *Knowbe4*. Knowbe4: https://www.knowbe4.com

McAfee. (5 de 05 de 2023). *McAfee*. https://www.mcafee.com/es-co/antivirus/malware.html

Microsoft. (16 de 4 de 2023). *Microsoft Security Response Center*.

MISP. (09 de 04 de 2023). *MISP Threat Sharing*. https://www.misp-project.org

NIST. (16 de 3 de 2023). *NATIONAL VULNERABILITY DATABASE*. https://nvd.nist.gov

Peritos informaticos . (8 de 05 de 2023). *Peritos informaticos* . https://peritoinformatico.es/cuales-son-los-fallos-de-seguridad-informatica-mas-frecuentes/

Pirani. (25 de 03 de 2023). *Pirani*. Pirani: https://www.piranirisk.com/es/blog/marco-ciberseguridad-nist-que-es

RedHat. (6 de 05 de 2023). *RedHat*. https://www.redhat.com/es/topics/security/what-are-insider-threats

Securityfocus. (3 de 16 de 2023). *Securityfocus BugTraq (BID) Database*. https://www.securityfocus.com/bid

Tenable. (18 de 4 de 2023). *Tenable CVEs*. https://www.tenable.com/cve

Tenable. (08 de 04 de 2023). *Tenable.SC security center*. https://es-la.tenable.com/products/tenable-sc

Xataka. (6 de 05 de 2023). *Xataka*. https://www.xataka.com/seguridad/por-que-es-peligroso-conectarse-a-wifis-publicas-y-que-debes-hacer-para-protegerte