DLP DATA LOSS PREVENTION COMO ESTRATEGIA DE SEGURIDAD EMPRESARIAL PARA LA DETECCIÓN DE PÉRDIDA DE DATOS EN LOS SISTEMAS DE COMUNICACIÓN Y PREVENIR LA FILTRACIÓN DE INFORMACIÓN

HECTOR FABIO PARRA TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2022

DLP DATA LOSS PREVENTION COMO ESTRATEGIA DE SEGURIDAD EMPRESARIAL PARA LA DETECCIÓN DE PÉRDIDA DE DATOS EN LOS SISTEMAS DE COMUNICACIÓN Y PREVENIR LA FILTRACIÓN DE INFORMACIÓN

HÉCTOR FABIO PARRA TORRES

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

YENNY STELLA NUÑEZ
Directora proyecto de grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Todo este empeño a ser cada vez mejor e ir logrando metas se debe a mi progenitora, a ella que siempre me ha apoyado y ha sido el respaldo incondicional en momentos difíciles, sus consejos y reflexiones han logrado hacer de mí una persona con unos valores muy bien cimentados y con una visión de lograr lo que se propone.

AGRADECIMIENTOS

Quiero dar un reconocimiento a la labor del cuerpo docente de la UNAD, que desde que ingrese a realizar mis estudios profesionales de pregrado como de postgrado siempre han sido una fuente de conocimiento dispuestos a transmitirlo para que nuestra formación sea de la mejor calidad. Su vocación de enseñanza se ve reflejada en profesionales que salen al campo laboral y profesional a transmitir todos estos valores a la sociedad para que esta sea cada vez mejor.

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

pág.

GLOSARIO

CLOUD:

Está asociado con la virtualización, que permite múltiples aplicaciones por cada nodo informático, cuando en el modelo tradicional sólo permitía una aplicación por cada nodo informático físico[1].

DATAMINING:

Es el conjunto de técnicas y tecnologías que permiten explorar grandes bases de datos, de manera automática o semiautomática, con el objetivo de encontrar patrones repetitivos, tendencias o reglas que expliquen el comportamiento de los datos en un determinado contexto[2].

DLP

Un DLP es una herramienta que tiene como finalidad prevenir las fugas de información cuyo origen está dentro de la propia organización, de una manera activa y sin perder productividad. Estas herramientas suelen incorporar inteligencia artificial que les permite aprender sobre el tipo de documentos confidenciales que se utilizan y qué acciones llevan a cabo los usuarios sobre los mismos, para volverse cada vez más efectivas en la prevención de fugas de información[3].

ENDPOINT:

Los Endpoint son cualquier punto que sea la parte final de una red. Las computadoras de las empresas, los portátiles o celulares podrían considerarse como Endpoint[4].

---

[1] ¿QUÉ ES CLOUD? [En línea]. Madrid, 2021. [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.acens.com/partners/

[2] Datamining (Minería de datos). [En línea]. Coruña, 2021. [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.sinnexus.com/business_intelligence/datamining.aspx

[3] DLP protege tus datos contra fugas de información. [En línea]. Madrid, 2019. [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/dlp-protege-tus-datos-fugas-informacion

[4] ¿Qué es un EndPoint? Fundamental para Proteger a tu Empresa. [En línea]. México DF, 2020. . [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.accessq.com.mx/que-es-un-endpoint

FORCEPOINT:

Empresa que presta los servicios de ciberseguridad con análisis conductual de entidades, cuantificación del riesgo, Aplicación en tiempo real[5].

NETWORK:

Conjunto de hardware y software de gestión necesario para la conexión de múltiples ordenadores con el fin de que puedan intercambiar información entre ellos y compartir recursos. La Red pueden ser de área local (LAN) o de área amplia (WAN)[6].

VULNERABILIDAD:

Es una debilidad que puede ser explotada por un ataque cibernético para obtener acceso no autorizado o realizar acciones no autorizadas en un sistema informático. Las vulnerabilidades pueden permitir a los atacantes ejecutar código, acceder a la memoria de un sistema, instalar malware y robar, destruir o modificar datos confidenciales[7].

WAREHOUSE

Es un sistema que agrega y combina información de diferentes fuentes en un almacén de datos único y centralizado; consistente para respaldar el análisis empresarial, la minería de datos, inteligencia artificial (IA) y Machine Learning. Data Warehouse permite a una organización o empresa ejecutar análisis potentes en grandes volúmenes (petabytes y petabytes) de datos históricos de formas que una base de datos estándar simplemente no puede[8].

---

[5] Forcepoint. [En línea]. Texas, 2021. [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.forcepoint.com/es/why-forcepoint/our-approach

[6] Network. [En línea]. Ciudad de México, 2021 [Fecha de consulta: 08 mayo 2021]. Disponible en: https://sistemas.com/network.php#

[7] Vulnerabilidad en Seguridad Informática. [En línea]. Lima, 2020. [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.hostdime.com.pe/blog/que-es-una-vulnerabilidad-en-seguridad-informatica-ejemplos/

[8] Data Warehouse. [En línea]. California, 2021. [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.oracle.com/co/scm/logistics/warehouse-management/

RESUMEN

La siguiente investigación monográfica aborda el tema de los DLP - Protección de la Perdida de Datos, como estrategia de seguridad ante los evidentes problemas presentados en las organizaciones con la perdida y filtración de información. Por tal motivo, el objetivo principal que se estableció con la investigación fue describir el impacto que genera en las organizaciones él no establecer mecanismos de seguridad para la protección de la información, identificando los factores que influyen en la fuga de datos y conocer sobre las medidas que se pueden adoptar para proteger su integridad. Para tal fin, se toma un enfoque metodológico cualitativo basado en la indagación de material académico investigativo tecnológico como: libros de informática, bibliotecas virtuales, revistas científicas, Informes corporativos. Entre los principales resultados se busca plantear a los DLP como una herramienta que permite dar una solución para el monitoreo y control de la filtración de datos, conocer su efectividad ante los eventos de fuga de información e identificar los factores que influyen para que la filtración de información se materialice. De acuerdo con el análisis realizado, se concluye que la información es el activo más importante en cualquier organización y su valor es directamente proporcional con los mecanismos de seguridad que se empleen, así mismo se verá reflejada su confidencialidad.

Palabras clave: Filtración de información, fuga de datos, impacto y factores, mecanismos de seguridad, protección de la información.

ABSTRACT

The following monographic research addresses the topic of DLP - Protection of data loss, as a security strategy in the face of the obvious problems presented in organizations with the loss and leakage of information. Therefore, the main objective that was established with the research was to describe what is generated in organizations by not establishing security mechanisms for the protection of information, identifying the factors that influence data leakage and knowing about the measures that are they can adopt to protect their integrity. For this purpose, a qualitative methodological approach is taken based on the investigation of technological research academic material such as: computer science books, virtual libraries, scientific journals, corporate reports. Among the main results, it seeks to propose DLP as a tool that allows to provide a solution for the monitoring and control of data leakage, to know its effectiveness in the event of information leakage and to identify the factors that influence the leakage of data. information to materialize. According to the analysis carried out, it is concluded that the information is the most important asset in any organization and its value is directly proportional to the security mechanisms used, as well as its confidentiality.

Keywords: Information leakage, data leakage, impact and factors, security mechanisms, information protection.

1. DEFINICIÓN DEL PROBLEMA

La tecnología ha sido un factor muy importante e influyente en los tiempos de pandemia que actualmente se presenta, las empresas y organizaciones han tenido que modificar su forma de trabajar para que su actividad económica continúe con su rumbo de sostenibilidad y crecimiento, para esto, ha sido necesario cambiar un poco la metodología de trabajo enviando a los empleados a sus hogares para que desde allí ejerzan las funciones que generalmente se realizaban desde las oficinas, esto ha conllevado a que se haga uso de herramientas que no son tan habituales como medios de comunicación de video llamada para hacer seguimiento de los logros obtenidos por determinada meta asignada u presentación de informes de cualquier otra índole, otro de los medios que no carece de menos importancia son las conexiones por medio de VPN para lograr tener acceso a los servicio de red de la organización. Estos son por nombrar algunos, los medios que son más necesarios para poder realizar actividades como si se estuviera en su lugar de trabajo. Que si bien son herramientas muy útiles como alternativa de comunicación también representan un riesgo de seguridad sino se tienen políticas y lineamientos de seguridad apropiados.

1.1 ANTECEDENTES DEL PROBLEMA

Las empresas han optado por replantear su esquema de trabajo y adaptarlo a las necesidades que actualmente se presentan, en medio de este proceso de cambio se ha adoptado por el modelo de home office, donde el recurso humano y tecnológico efectuaran labores netamente empresariales en lugares que no se encuentran del todo adecuados para esta labor, refiriéndonos sobre todo en el aspecto de seguridad informática, los recursos tecnológicos se encontraran en un ecosistema potencialmente vulnerable en el cual los controles son mínimos, el personal que los opera en la mayoría de los casos no cuenta con la concienciación y asesoría sobre cuales con los riesgos a los cuales están expuestos ni cómo afrontarlos. Debido a esta problemática las grandes organizaciones están muy interesadas en estudiar cual es el impacto que genera el trabajo remoto en lo que concierne a protección de la información.

Un estudio realizado por IPSOS para Samsung “afirma que un 36% de los españoles ha puesto en práctica la modalidad del teletrabajo y han valorado de forma positiva esta opción porque produce ahorro de tiempo y costes, pero

también se menciona que un 78% del capital humano tubo que proporcionar su propio recurso tecnológico"[9].
Estas acciones no brindan las garantías ni de productividad y con un gran riesgo de pérdida de información ya sea por el mal manejo por parte de los usuarios o por los carentes mecanismos de seguridad establecidos en los dispositivos. Es por esto por lo que las empresas deben de alinearse con los avances tecnológicos y fortalecer su infraestructura tecnológica como de talento humano capacitado para que se esté a la vanguardia de todos los sucesos que pueden beneficiar o perjudicar los activos de información.

Según los datos de Cisco, "el acceso seguro es el principal reto para el trabajo remoto (62% de los consultados), seguido por la privacidad de datos (55%) y el control y reforzamiento de las políticas (50%). Así, el 85% de las organizaciones consideran la ciber-seguridad más importante que antes de la pandemia, y el 66% están aumentando su inversión frente a esta demanda".

Las organizaciones han avanzado con la implementación de tecnología para que sus procesos sean más dinámicos y seguros, a través del tiempo surgen herramientas que generan un gran aporte a estos aspectos, tal es la importancia de sistemas como los servidores, firewalls, IDS, IPS y muchos más, los cuales administran variedad de servicios que contribuyen a la gestión de políticas y lineamientos que son ajustados de acuerdo con las necesidades de las empresa u organización. Aunque son herramientas de gran importancia para la filtración de datos entrantes y salientes de una red aun requieren ser complementadas especialmente con recurso humano que ofrezca nuevas alternativas para llevar estas y nuevas herramientas a otro nivel, si bien hay personal especializado en el área de la seguridad informática las empresas consideran este factor como una inversión de alto costo, y en la mayor de las ocasiones se enfocan en adquirir equipos sin darles un buen uso o explotar verdaderamente su funcionalidad[10].

[9] Teletrabajas pero, ¿cuentas con las herramientas necesarias?[En linea]. Madrid: 05 de marzo de 2021. [Fecha de consulta: 06 marzo 2021]. Obtenido de: https://revistabyte.es/noticias/teletrabajar-herramientas/.
[10] Garcia, V. (). Cómo ir hacia un trabajo inteligente. [En linea].Madrid: 05 de marzo de 2021. [Fecha de consulta: 06 de marzo 2021]. Obtenido de: https://revistabyte.es/tema-de-portada-byte-ti/trabajo-inteligente-digital-workspace/.

Como menciona Reyes[11], en su análisis se identificó que desde el 2014 a la fecha a nivel regional en Suramérica no se ha avanzado mucho en el enfoque a la seguridad informática, los sistemas de clasificación de información y seguridad son muy deficientes, en la mayoría de los casos no hay, la información se encuentra dispersa en múltiples sistemas lo cual evidencia la falta de estrategias para la protección de la información. (Referencia).

Esto no es más que una realidad que actualmente se ve más evidente, no hay estrategias definidas para que a los usuarios se les supervise el manejo de los datos, estos son transferidos por diferentes medios sin ningún tipo de control que a su vez generan una gran amenaza. Los controles no son aplicados en dispositivos externos, en carpetas de red compartidas, sistemas de correo electrónico, en información que en muchas ocasiones es compartida en redes sociales siendo este una problemática adicional debido a que un mal uso de la publicación de información puede generar un impacto importante ya que esta es visualizada por una cantidad considerable de personas.

[11] Reyes F, *Seguridad y ciberseguridad ¿Qué hemos aprendido en esta decada?¿Cúales son los retos a 2030?[En linea]. Bogota DC:* 31 de diciembre de 2020*. [Fecha de consulta:* 01 de marzo de 2021*]*.Obtenido de: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjNjZaZlprvAhXYcn0KHcviDms4ChAWMAN6BAgGEAM&url=https%3A%2F%2Fsistemas.acis.org.co%2Findex.php%2Fsistemas%2Fissue%2Fdownload%2F14%2F11&usg=AOvVaw1hD0kAT38prJTV86Zj65iN.

2. FORMULACIÓN DEL PROBLEMA

¿Cómo puede incidir la fuga de información confidencial en los sistemas de comunicación y cuál es el impacto que esto genera en las organizaciones?

3. JUSTIFICACIÓN

La información es considerada como uno de los factores sino el factor más importante en una organización, los datos que allí se procesan tienen un gran valor por tratarse de que son la columna vertebral de cómo funciona la empresa, es aquí donde adquiere gran relevancia del cómo se administran estos datos. Por lo general, las organizaciones tienden a implementar dispositivos que sirven como muro para filtrar los datos que ingresan o salen de su zona perimetral, esto con el propósito de evitar el acceso no autorizado de contenido malicioso, hasta este punto las medidas tomadas brindan una estabilidad importante que aportan al monitoreo, análisis, contención y mitigación de cualquier acceso no consentido.

La información no solo requiere ser monitoreada para que factores externos no accedan a los sistemas y se apropien de ella, también ha tomado gran relevancia gestionar la forma en que esta es administrada, es decir, se debe saber cuáles son los datos más confidenciales, quienes pueden acceder a ellos, cuáles son los medios por los cuales se pueden transferir y cuáles son los medios de almacenamiento. Para tener en cuenta todos estos aspectos, es necesario replantear o crear unas políticas de seguridad para protección de la información, acompañando este factor con instrumentos que permitan evitar cualquier fuga de datos que se encuentra internamente en la organización, si tenemos en cuenta la amenaza puede estar en el mismo lugar de trabajo y puede estar representada por el mismo empleado.

El trabajo remoto siempre ha representado un riesgo para la seguridad de las empresas y las vuelve vulnerable ante cualquier evento que atente con su bienestar. Es aquí donde los DLP – Prevención de Perdida de Datos, toman una gran importancia debido a que aportan una seguridad adicional y se integra al ecosistema de toda la red para brindar una garantía sobre todos los datos que se encuentran en el entorno.

Las empresas van a ser el sector directamente beneficiado con la implementación de esta solución tecnológica, debido a la importancia y el alto flujo de información que administran y procesan periódicamente, podrán gestionar de una manera más efectiva y eficiente ´los recursos asignados para tal propósito, tendrán un control sobre las acciones que los empleados ejecuten sobre la información, no permitirá que la información sea dirigida por canales que no son los autorizados, tales como: correos electrónicos, memorias USB, identifica que información puede ser impresa y cual no, bloquea los acceso a dispositivos que pueden generar algún tipo de vulnerabilidad. Como protección adicional genera un cifrado en el medio donde se almacenen los datos, aporta a la formación y concienciación del usuario generando unas alertas cuando se identifique una actividad inusual o restringida, la herramienta DLP puede ser configurada de acuerdo con las necesidades que la

empresa considere necesarias. Con esta investigación se pretende que se conozca una alternativa que ayuda a resolver en gran medida el mal uso de las herramientas de trabajo que administran la información, teniendo un control y monitoreo de todo lo que se desenvuelve en ellas.

4. OBJETIVOS

4.1 OBJETIVOS GENERAL

Crear una estrategia de seguridad empresarial a partir de DLP Data Loss Prevention para la detección de pérdida de datos en los sistemas de comunicación evitando la filtración de información.

4.2 OBJETIVOS ESPECÍFICOS

Examinar las vulnerabilidades y amenazas de seguridad presentes en los dispositivos remotos empresariales que pueden generar afectaciones en la información al momento de su procesamiento, almacenamiento y transferencia.

Establecer los distintos sistemas DLP con relación a sus características, funcionalidad, efectividad y su uso en las organizaciones como solución de seguridad informática.

Estructurar una estrategia de seguridad de información basada en la aplicación DLP, apoyada con controles que se puedan implementar para prevenir la fuga de información en las organizaciones.

5. MARCO TEÓRICO

5.1 DEFINICIÓN DE DLP, PREVENCIÓN DE LA PÉRDIDA DE DATOS.

La prevención frente a la pérdida de datos (DLP por sus siglas en inglés) es un elemento básico para detener las filtraciones de datos accidentales y malintencionadas, ya se trate de información de clientes, datos financieros, propiedad intelectual o secretos comerciales. Las empresas actuales deben ser capaces de identificar todos los datos confidenciales, realizar un seguimiento de estos y protegerlos, tanto si están almacenados, en uso o en tránsito. Esta tarea resulta cada vez más complicada debido a los crecientes factores de riesgo, como la movilidad de los trabajadores y el uso generalizado de las unidades USB, el correo Web, la mensajería instantánea y los CD/DVD[12].

5.2 FUNCIONAMIENTO DE UN DLP.

De acuerdo con INCIBE, "Un DLP es una herramienta que tiene como finalidad prevenir las fugas de información cuyo origen está dentro de la propia organización, de una manera activa y sin perder productividad. Estas herramientas suelen incorporar inteligencia artificial que les permite aprender sobre el tipo de documentos confidenciales que se utilizan y qué acciones llevan a cabo los usuarios sobre los mismos, para volverse cada vez más efectivas en la prevención de fugas de información"[13].

5.3 CARACTERÍSTICAS DE UN DLP.

- Prevención completa de fugas de información.

- protege todos los canales de fuga de información y es muy fácil de instalar y poner en funcionamiento.

- Perfiles de tendencias y productividad: Avisa a los administradores de la empresa en caso de cambios repentinos en el rendimiento del empleado y muestra los cambios de productividad por departamento en una gráfica temporal. Estos cambios son indicaciones de posibles riesgos de seguridad.

[12] TrendMicro; Data Loss Prevention. [Sitio web]. Una completa solución de prevención frente a la pérdida de datos que reduce los riegos y mejora la visibilidad. Madrid. [03 marzo 2021]. Disponible en: https://www.trendmicro.es/media/ds/data-loss-prevention-datasheet-es.pdf.
[13] Instituto Nacional de Ciberseguridad España. Guía gestión de fuga de la información. Madrid.: INTECO, 2016.

- Informe de actividad: Descubre los riesgos de seguridad en muchos frentes revisando todas las actividades de los usuarios en busca de signos de un posible peligro, incluso antes de la transferencia misma de la información.

- Prevención de fugas por correo electrónico: Garantiza que la información protegida no se envía a la cuenta de correo equivocada. Registra dónde se han enviado los archivos con información sensible y almacena esta información para futuros informes.

- Control de aplicaciones con reglas de tiempo: Permite un paquete seleccionado de aplicaciones relacionadas con el trabajo y bloquea otras para conseguir un entorno más seguro. Puede establecerse que las aplicaciones estén disponibles solo durante un período determinado de tiempo.

- Filtro web: Permite aplicar fácilmente las Políticas de uso aceptable en la empresa con categorías seleccionadas cuidadosamente y filtro de palabras clave.

- Control de impresión: Limita qué puede ser impreso y por quién con cuotas para usuarios y departamentos.

- Control de dispositivos: Evita que los empleados puedan conectar dispositivos no autorizados en el trabajo. Los puertos comunes pueden activarse para ciertos dispositivos o bloquearse para todos.

- Administración del cifrado: Ofrece cifrado total del disco o cifrar particiones enteras y crear unidades virtuales locales o de red para almacenar los archivos con seguridad.

- Clasificación de información en tránsito: Protege la nueva información inmediatamente después de crear o recibir un archivo clasificado.

- Consola de administración unificada: Permite la gestión y creación de informes completos de seguridad, integra toda la protección de información de la empresa y las políticas de informes y bloqueo.

- Inspección SSL/HTTPS: Revisa y protege las líneas de comunicación securizadas incluyendo las páginas web que utilizan el protocolo HTTPS, las aplicaciones IM con conexiones y las transmisiones seguras por correo electrónico[14].

[14] NOD32; Safetica DLP. [Sitio web]. Características principales Barcelona. [Consulta: 28 febrero 2021]. Disponible: https://www.antivirusnod32.es/dlp-prevencion-de-fugas-de-informacion/safetica-dlp/.

5.4 PRINCIPALES BENEFICIOS

- Protección de la privacidad: identifica, supervisa y evita la pérdida de datos confidenciales (tanto dentro como fuera de la red).

- Protección de la propiedad intelectual: identifica, supervisa y protege los activos empresariales básicos (tanto dentro como fuera de la red).

- Cumplimiento de normativas: implemente controles para mejorar la protección, la visibilidad y la aplicación.

- Formación de usuarios: personalice diálogos interactivos para informar a los empleados cuando exista un comportamiento peligroso y exija justificación de los usuarios cuando sea necesario.

- Detección de datos: detecte datos confidenciales en equipos portátiles, equipos de sobremesa y servidores.

- Detección de malware que roba datos: identifique redes robot, procesos de FTP ocultos, aplicaciones de registro de pulsaciones, spyware y troyanos que intenten recopilar y enviar datos[15].

5.5 ECOSISTEMAS DE APLICACIÓN DE DLP.

5.5.1 Network DLP

Proporciona el punto de aplicación crítico para detener el robo de datos en movimiento que se produce a través del correo electrónico y la web. La solución ayuda a identificar y prevenir la exfiltración de datos y la pérdida accidental de datos causada por ataques externos o producidos como resultado de la amenaza interna. El reconocimiento de caracteres ópticos (OCR) reconoce datos dentro de imágenes. El análisis identifica la DLP para detener el robo de datos con un registro por vez y otros comportamientos de usuarios de alto riesgo[16].

5.5.2 DLP – Discovery

Identifica y protege datos confidenciales de distintos servidores de datos, SharePoint (en las instalaciones y en la nube), Exchange (en las instalaciones y

[15]TrendMicro; Data Loss Prevention; Una completa solución de prevención frente a la pérdida de datos que reduce los riegos y mejora la visibilidad. [Sitio web]. Madrid. [05 marzo 2021]. Disponible en: https://www.trendmicro.es/media/ds/data-loss-prevention-datasheet-es.pdf.

[16] Forcepoint. Forcepoint Data Loss Prevention (DLP). Protección de datos en un mundo sin perímetros. Austin. 2020. p. 5.

en la nube), y brinda capacidades de detección dentro de bases de datos como SQL Server y Oracle. La tecnología de localización (fingerprinting) identifica los datos regulados y la propiedad intelectual inactivos, y protege esos datos al aplicar la encriptación y los controles correspondientes. Discovery también incluye reconocimiento de caracteres ópticos (OCR) que brinda visibilidad a datos en imágenes[17].

5.5.3 Cloud Applications

Los controles de almacenamiento de información en la nube requieren toda la atención, este es uno de los medios que fácilmente se puede extraer información, es por esto por lo que Cloud Applications es una herramienta que respalda la seguridad de la información mediante políticas que definen que servicios se pueden acceder y en qué condiciones.

De acuerdo con Forcepoint "Amplía el control único y análisis avanzado de Forcepoint DLP a aplicaciones sancionadas en la nube, como Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack y muchas más"[18].

5.5.4 Endpoint DLP

Proporciona protección integral para todos los posibles canales de fuga de datos, como dispositivos de almacenamiento extraíbles, la nube, correo electrónico, mensajería instantánea, Web, material impreso, portapapeles, capturas de pantalla, aplicaciones para compartir archivos, etc.

Sus principales características son:

- Integración con análisis de comportamientos de usuarios (UEBA) de terceros.

- Clasificación manual.

- Análisis y reparaciones iniciados por el usuario.
- Clasificación flexible, que ofrece diccionarios, expresiones regulares y algoritmos de validación.

- Una exclusiva tecnología de etiquetado para identificar los documentos según su origen, que impide que la información sensible que manejan las aplicaciones web, las aplicaciones de red y los recursos compartidos de red se duplique, renombre o salga de las instalaciones de la empresa.

[17] Ibid., p. 6.
[18] Ibid., p.7.

- Compatibilidad con tecnologías de virtualización para proteger equipos de sobre mesa remotos y soluciones VDI[19].

Este servicio de monitoreo supervisa e impide la fuga de datos en la oficina, desde otro lugar y en la nube. Supervisa rápidamente los eventos en tiempo real, aplique directivas de seguridad que se administran de manera centralizada y genere detallados informes forenses y de proliferación, sin que se vean afectadas las operaciones cotidianas.

- Crea directivas de protección de datos para comunicar las infracciones. De esta forma, facilita la información necesaria para saber cómo se desplazan los datos en la organización y permite la aplicación de reglas de bloqueo.

- Crea pantallas informativas para que los usuarios conozcan las directivas de protección de datos cuando realicen transferencias de datos cotidianas. Estos cuadros emergentes informativos y personalizables son extremadamente útiles y reducen los riesgos en las transferencias de datos realizadas por los empleados.

- Consulta el Administrador de incidentes para identificar las propiedades de los datos que se transfieren a ubicaciones no autorizadas; por ejemplo, cómo y quién realiza las transferencias.

- Activa el bloqueo de transferencias de datos no autorizadas.

- Permite las clasificaciones manuales, para que los usuarios puedan clasificar los documentos que hayan creado. Ellos que son los propietarios podrán entender mejor su nivel de confidencialidad.

- Permite a las aplicaciones autorizadas transferir datos confidenciales, pero se limita el acceso a esos datos a las aplicaciones no verificadas o maliciosas[20].

[19] CCN; Guía de Seguridad de las TIC CCN-STIC 1503; Procedimiento de empleo seguro McAfee Data Loss Prevention 11.1 con ePolicy Orchestrator 5.10. [Sitio web]. Madrid. [Consulta: 08 marzo 2021]. Disponible en: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/1000-procedimientos-de-empleo-seguro/5729-ccn-stic-1503-pes-mcafee-data-loss-prevention-11/file.html.

[20] McAfee; Cómo evitar las fugas de datos en su empresa; McAfee DLP Endpoint. [Sitio web]. Madrid. [Consulta: 08 marzo 2021]. Disponible en: https://www.mcafee.com/enterprise/es-mx/assets/solution-briefs/sb-quarterly-threats-sep-2016-2.pdf.

6. FILTRACIÓN DE DATOS EN LAS EMPRESAS.

6.1 FACTORES DE FUGA DE INFORMACIÓN.

La no valoración de la información conlleva a que en las empresas se presente considerables fugas de información no dimensionando el riesgo y la afectación que esta falencia les genera, el desconocimiento del valor de los activos es el reflejo de los deficientes controles de seguridad tanto técnicos como humanos, como no hay una valoración, no hay unos controles y en consecuencia es una entidad inestable que no genera confianza, que no solo está en constante riesgo de fracaso sino que también esta conllevado a que empresas aliadas sientan este impacto negativo.

De acuerdo con lo mencionado por García, "Las fugas de datos seguirán ocurriendo y, como no existe el 100% de seguridad absoluta, es necesario enfocarse en la reducción de riesgos, es decir, que las empresas conozcan y detecten las amenazas que enfrentan o podrían enfrentar y se preparen proactivamente. Para ello deben combinar la tecnología con políticas que prevengan las amenazas, las identifiquen y les permitan responder tan rápido como sea posible"[21].

Las fugas de información generalmente se presentan por la ausencia de mecanismos y herramientas de control que permitan establecer unos lineamientos de seguridad que estén continuamente monitoreando los procesos y eventos que se presentan en la organización.

> Según INCIBE, La mayoría de las causas, organizativas o técnicas, por lo general, implican la ausencia de algún tipo de medida de seguridad, procedimiento, herramienta, etc. La ausencia supone la falta de control y esta aumenta de forma significativa la probabilidad de que se produzca un incidente de fuga de información.

6.1.1 Factor Organizativo

- Clasificación de la información: esta debe ser seleccionada de acuerdo con el nivel de confidencialidad, como son el valor que tiene para la organización, el impacto público que puede generar su difusión, su nivel de sensibilidad o si se trata de información personal o no.

- Desconocimiento del valor de la información: este factor influye debido a que no será posible diseñar y seleccionar las medidas de protección adecuadas.

[21] ¿Qué hacer después de una fuga de datos? [en línea]. Ciudad de México, 2014-. [Fecha de consulta: 02 marzo 2021]. Disponible en: https://www.forbes.com.mx/que-hacer-despues-de-una-fuga-de-datos/.

- Falta de conocimiento y formación: Por un lado, el empleado debe utilizar los recursos que la organización pone a su disposición de forma responsable, como en el caso del uso del correo electrónico, la navegación Web u otros servicios y por otro lado, debe disponer de ciertos conocimientos y formación en relación con su actividad diaria, siendo responsabilidad de la organización proporcionar la información y la formación necesaria de manera que el empleado pueda desempeñar su función adecuadamente.

- Establecimiento de políticas: que indiquen claramente cuáles son los límites dentro de los cuales deberán desempeñar su actividad y, por otro lado, los procedimientos para aquellas actividades de especial importancia o riesgo, de manera que se sigua un proceso controlado y las tareas se realicen de la forma más segura posible.

- Nivel de disuasión: durante el proceso de contratación de un empleado, se solicite por escrito la conformidad con diversas normas internas, como la política de confidencialidad o de seguridad, entre otras, de manera que el futuro empleado, deja por escrito la aceptación de las condiciones correspondientes[22].
  Con el propósito de conocer los desafíos que afrontan las empresas con la protección de la información confidencial, Cisco encargó a InsightExpress para que realizara este estudio. El cual se realizó en 10 países: Estados Unidos, Reino Unido, Francia, Alemania, Italia, Japón, China. La investigación descubrió que a pesar de las políticas, procedimientos y herramientas de seguridad actualmente en uso, los empleados de todo el mundo exhiben conductas arriesgadas que ponen en peligro los datos personales y empresariales. Tales conductas incluyeron:

- Uso de aplicaciones no autorizadas: el 70% de los profesionales de TI cree que el uso de programas no autorizados fue responsable de hasta la mitad de los incidentes de pérdida de información en sus empresas.

- Uso indebido de computadoras de la empresa: el 44% de los empleados comparte dispositivos de trabajo con otras personas sin supervisión.

- Acceso no autorizado tanto físico como a través de la red: el 39% de los profesionales de TI afirmó que ha debido abordar el acceso no autorizado por parte de un empleado a zonas de la red o de las instalaciones de la empresa.

- Seguridad de trabajadores remotos: el 46% de los empleados admitió haber transferido archivos entre computadoras del trabajo y personales al trabajar desde el hogar.

[22] Instituto Nacional de Ciberseguridad España. Guía gestión de fuga de la información. Madrid.: INTECO, 2012. p.8.

- Uso indebido de contraseñas: el 18% de los empleados comparte contraseñas con sus colegas. El porcentaje aumenta al 25% en China, India e Italia.

  Para reducir la fuga de datos, las empresas deben integrar la seguridad en su cultura empresarial y evaluar constantemente los riesgos de cada interacción con redes, dispositivos, aplicaciones, datos y, por supuesto, otros usuarios.

- China presenta tal nivel de abuso tecnológico que los responsables de tomar decisiones de TI auditan las computadoras en busca de contenido no autorizado.

- En Japón, el 65% de los usuarios finales no acata de manera constante las políticas de TI de su empresa, y el estudio indica que el abuso tecnológico por parte de los usuarios finales está en aumento.

- Los usuarios finales en India tienden a emplear el correo electrónico y la mensajería instantánea para fines personales y modifican la configuración de seguridad de TI en las computadoras empresariales para poder ver sitios web no autorizados[23].

- Los empleados en Brasil utilizan las computadoras empresariales para fines de comunicación personal y para actividades como descargar música.

- Los usuarios de Francia tienen la tasa más baja de cumplimiento de políticas de TI de todos los países encuestados, ya que sólo el 16% de los empleados afirmó cumplir de manera constante las políticas de seguridad.

6.1.2 Factores técnicos:

El cambio de modalidad de trabajo ha puesto en evidencia falencias en los métodos de seguridad en especial el de la protección de la información, métodos o lineamientos que deberían estar implementados en los dispositivos que estarán fuera de los lugares de trabajo corporativos, esto no solo sucede con empresas que su impacto comercial no están relevante o su tamaño aun no es lo suficientemente importante, aunque sin importar estos aspectos la seguridad debería ser prioridad para cualquier organización. Las grandes compañías, aunque tienen esquemas de seguridad importantes tanto en infraestructura como en los dispositivos de trabajo, estos están enfocados en prevenir y corregir amenazas potenciales externas que quieran vulnerar estos controles, pero el enfoque requiere más que estos controles, la información no solo es del interés de cibercriminales, la amenaza puede estar internamente, las personas que administran la información o tiene acceso a ella de forma directa o indirecta

[23] Ibib., p.10.

pueden ser los causantes de que la información sea extraída con fines que no son propiamente el interés de la empresa.

- Uno de los mayores peligros del código malicioso, es que permite automatizar una buena parte del proceso relacionado con la fuga de información y, además, el diseño de muchos de estos programas incluye técnicas que permiten mantener oculto el código en un sistema, mientras recoge y envía información.

- El acceso no autorizado a sistemas e infraestructuras es otra de las causas detrás del robo de información. Ya sea como parte de una campaña de desprestigio, con el acceso no autorizado a una página web de una organización con cierta relevancia pública, o con motivo de sustraer información sobre secretos industriales.

- Servicio de actualizaciones se considera parte fundamental de una buena aplicación, puesto que aporta mayor seguridad y denota un trabajo de mejora continua, que redunda en beneficio para la aplicación y por extensión, para el usuario.

  Según lo anunciado por la BBC, “En 2008, una memoria USB cargada de software maligno (conocido como malware) posiblemente encontrada en un estacionamiento de una base militar en el extranjero, sacudió a Washington. El programa informático a unos piratas penetrar en sistemas militares estadounidenses clasificados que se suponía que debían mantenerse fuera de línea”[24].

  De acuerdo con lo analizado por Assolini “Muchas compañías mantienen Java desactualizado porque existen soluciones específicas como sistemas de contabilidad que dejan de funcionar con las últimas versiones de sus aplicaciones y sistemas internos”.

  Según estudio realizado por Kaspersky, “La clasificación mundial de ataques de phishing está encabezada por Brasil, seguido de Venezuela. Otros países de América Latina incluidos en el Top 20 de ataques de phishing son Chile, en séptimo lugar; Ecuador, octavo sitio, Guatemala, décimo lugar; Panamá, onceavo; Honduras doceavo lugar; México que ocupa la posición número 13 y Argentina en la posición 14” [25].

[24] Corera Gordon. transformaron la ciberseguridad en Estados Unidos. [Sitio web]. Londres, 20 diciembre 2020. [Consulta: 12 marzo 2021]. Disponible en: https://www.bbc.com/mundo/noticias-internacional-55381892.
[25] Instituto Nacional de Ciberseguridad España. Guía gestión de fuga de la información. Madrid.: INTECO, 2012. p.9.

Julio de 2018 y julio de 2019, los usuarios latinoamericanos de teléfonos inteligentes recibieron seis intentos de ataque de malware móvil por minuto. Entre los países más atacados de la región se encuentran Brasil (6º en el ranking mundial), México (9o), Colombia (22o), Perú (37o), Chile (38o), Ecuador (41o) y Argentina (46o)[26].

De acuerdo con estadísticas generadas por la Policía Nacional de Colombia[27], el ciber crimen muestra indicativos de alza a partir del 2015, los registros indican que a partir de este año se registraron 7.523 casos, en el 2016 11.225, 2017 15.840, 2018 22.524, 2019, 17531. Las ciudades con mayor afectación y el sector donde se enfocó esta actividad delictiva fue el de las PYMES, entidades financieras y grandes compañías. En Bogotá se registraron 5.308 casos, seguido por Cali con 1.190, Medellín con 1.186 casos, Barranquilla 643 casos y Bucaramanga con 397 casos.

Según informe de la policía Nacional[28], Los delitos que más incidencia tuvieron en el 2019 estuvieron relacionados con los correos electrónicos, en la modalidad de correos Spacer Phishing con un 80%, Spoofing con 53%, suplantación de identidad 60%, en cuanto a los ataques por Ransonware Colombia recibió el 30 % de los ataques en Latinoamérica. 170 empresas reportaron ataques de DDoS, el Malware presento un crecimiento de los años 2018 con 99 casos reportados por las empresas, para el periodo 2019 se registraron 705 casos.

6.2 IMPACTO DE LA PÉRDIDA DE DATOS.

Un estudio realizado por The Economist Intelligence Unit, “reveló que 1 de cada 3 clientes de empresas que sufrieron una fuga de datos en el último año, dejó de hacer transacciones comerciales con ellas “por la fuga””.

De acuerdo con Investigación realizada por ESET, “Tan solo en Londres, durante el primer mes de cierre se registró un aumento del 72% en las pérdidas financieras derivadas del ciberdelito, ya que los delincuentes aprovecharon el cambio al trabajo desde casa”[29].

---

[26] Forbes; En América Latina se registran 45 ataques cibernéticos por segundo. [Sitio web]; Ciudad de México, 2019. [Consulta: 12 marzo 2021]. Disponible en: https://www.forbes.com.mx/en-america-latina-se-registran-45-ataques-ciberneticos-por-segundo/.

[27] Policía Nacional de Colombia. Tendencias Cibercrimen Colombia 2019-2020. Bogotá DC. 2020. p. 8-10.

[28] Ibid., p. 14-20-28.

[29] ESET. La cuarentena por coronavirus o el cibercrimen: ¿Cuál es la mayor amenaza para las empresas? [Sitio web]. Asunción. [Consulta: 15 marzo 2021]. Disponible en: https://www.eset.com/py/acerca-de-eset/por-que-eset/.

- Daño de imagen. Son aquellas consecuencias que generan impacto negativo en la imagen de la compañía o de la organización y que además generan pérdida de confianza.
- Consecuencias legales. Son aquellas consecuencias que se enmarcan en el ámbito legal, que podrían conllevar sanciones económicas o administrativas.

- Consecuencias económicas: Son aquellas que afectan o suponen un impacto negativo a nivel económico, en forma de sanciones, disminución de la inversión, negocio, etc.

- Otras consecuencias. Son aquellas que afectan o supone un impacto negativo en ámbitos muy diversos, como, por ejemplo, el ámbito político, diplomático, institucional, o gubernamental, entre otros. En general se trata de consecuencias que no están englobadas en los otros tres tipos[30].

6.2.1 Tratamiento de datos corporativos.

A través del tiempo los datos han sido un activo de gran importancia para cualquier sector de la economía mundial, la humanidad los ha valorado y aplicado variedad de mecanismos para su protección, cuando no se contaba con equipos de comunicación se empleaban métodos de cifrado rústicos pero muy efectivos, los papiros se destacaron por contar con una única seguridad la cual era conocida solo por el remitente y el emisor, esta técnica se ha venido empleando a través del tiempo pero con tecnologías y técnicas mucho más sofisticadas y efectivas.

Esto en el sector empresarial conlleva a que como menciona Agustina, “Cuando los datos sensibles son identificados correctamente como tal, las organizaciones construyen confianza con sus clientes y socios”.

Según estudio realizado por Dell EMC, Global Data Protection Index. Para elaborar este estudio se ha contado con las opiniones de 2.200 profesionales de los departamentos de tecnología de organizaciones públicas y privadas con más de 250 empleados de 11 sectores de actividad en 18 países del mundo.

- Según el informe del Dell EMC, es frecuente que las empresas sufran incidentes en los que se interrumpe el normal acceso a los datos, sin embargo, lo más alarmante es el aumento de incidentes en los que los datos se pierden para siempre. Así, un:

[30] Instituto Nacional de Ciberseguridad España. Guía gestión de fuga de la información. [Sitio web]. Madrid.: INTECO, 2015. p.13. [Consulta: 14 marzo 2021]. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/Formacion/EstudiosInformes/guia_gestion_fuga_informacion.pdf

- 76% de los encuestados dice haber sufrido algún tipo de incidente en los últimos 12 meses y un 27% afirma haber perdido datos que nunca se llegaron a recuperar, casi el doble (14%) que en 2016[31].

- El 95% afirman encontrarse con algún reto en su estrategia de protección de datos. Los tres grandes desafíos que se repiten en todo el mundo son:

- La complejidad de la configuración del software/hardware de protección de datos (46%) y los costes cada vez mayores del almacenamiento y la gestión de las copias de Backus, debido al gran crecimiento.
- La escasez de soluciones de protección de datos para tecnologías emergentes (45%).
- Garantizar que se cumple con regulaciones como GDPR (41%).
- Más de la mitad (51%) de las organizaciones que tratan de encontrar soluciones de protección de datos adecuadas para las tecnologías más nuevas afirmaron no haber sido capaces de encontrar soluciones de protección de datos adecuadas para inteligencia artificial y aprendizaje automático.
- Un 47% trata de encontrar soluciones de protección apropiadas para aplicaciones nativas cloud y un 40% para aplicaciones IoT.

- Sólo el 16% de los encuestados piensa que sus actuales soluciones de protección de datos serán capaces de afrontar los desafíos futuros de sus negocios.
  De acuerdo con estudio realizado por SEMANA, “Uno de los hallazgos más preocupantes del estudio es que 24.424 organizaciones públicas y privadas no han puesto en marcha una política de protección para el acceso remoto a la información personal, es decir, no cuenta con mecanismos eficientes para proteger los datos de sus usuarios de accesos no autorizados o incidentes de seguridad”.

  Al comparar los resultados del más reciente estudio con los de 2019, en términos generales, se encontró una mejoría del 12,73 % en el nivel promedio de cumplimiento de medidas de seguridad. No obstante, persiste un alto nivel de incumplimiento respecto a los temas evaluados.

  La medición de este año halló los siguientes resultados:

- Número de organizaciones evaluadas: 33.596.

[31]Agustina Sanllehi, José R. Delito en la empresa. Estrategias de prevención de la criminalidad intra-empresarial y deberes de control empresario. [Sitio web]. Barcelona: Atelier Libros, 2010. p.103. ISBN. 8415929234, 9788415929239. [Consulta: 15 marzo 2021]. Disponible en: https://books.google.com.co/books/about/Delito_en_la_empresa_Estrateg%C3%ADas_de_pre.html?id=V5O05Mt9KlIC&printsec=frontcover&source=kp_read_button&hl=es&redir_esc=y#v=onepage&q&f=false

- No tienen una política de protección para acceso remoto a la información personal: 72,7 %.
- No cuenta con mecanismos de monitoreo de consulta de las bases de datos: 69,3 %.
- No ha implementado un procedimiento de auditoría de los sistemas de información: 71,3 %.
- No tiene implementado un sistema de gestión de seguridad o un programa integral de gestión de datos: 67,5 %[32].
- No ha implementado medidas especiales para proteger datos sensibles: 61,3 %.
- No ha implementado una política de seguridad para el intercambio físico o electrónico de datos: 66.1 %.
  No tiene política de auditoría de seguridad de la información: 63,6 %
- No tiene controles de seguridad en la tercerización de servicios para el tratamiento de datos:61 %.
- No implementa medidas apropiadas y efectivas de seguridad: 50,7 %
- No cuenta con herramientas de gestión de datos: 46,9 %.
- No tiene políticas y procedimientos de gestión de incidentes de seguridad: 52,6 %
- Promedio de incumplimiento respecto de los ítems evaluados: 62,3 %.
- Las conclusiones surgen de la información suministrada por 33.596 organizaciones responsables del tratamiento de datos que registraron sus bases de datos en la entidad desde el año 2015 hasta el 30 de septiembre de 2020"[33].
  Es claro que, aunque la información es el activo más importante de cualquier organización y a un existiendo las herramientas y mecanismos para su protección a un no se establecen las políticas necesarias para que esta se encuentra debidamente custodiada. Hace falta más concienciación para que se le preste la atención requerida, Se requiere personal especializado en el área de seguridad para que se alinee la empresa con las nuevas tecnologías y oriente al personal corporativo instruyéndolo sobre las medidas y acciones que se deben tener en cuenta para que los procesos que involucran la administración de información tengan el manejo y uso adecuado.

[32] El manejo de datos por parte de las empresas creció un 569% desde 2016. [en línea]. Madrid, 2019 [Fecha de consulta: 21 marzo 2021]. Disponible en: https://www.computerworld.es/tecnologia/el-manejo-de-datos-por-parte-de-las-empresas-crecio-un-569-desde-2016

[33] El 73 % de empresas no cuenta con mecanismos eficientes para proteger datos de sus usuarios. [en línea]. Bogotá, 2021. [Fecha de consulta: 15 marzo 2021]. Disponible en: https://www.semana.com/economia/empresas/articulo/el-73-de-empresas-no-cuenta-con-mecanismos-eficientes-para-proteger-datos-de-sus-usuarios/202137/.

7. ADMINISTRACIÓN DE DATOS CORPORATIVOS

Como menciona Heredero[34] Los datos generalmente fueron almacenados de manera centralizada lo cual generaba un acumulado de información considerable presentando un riesgo para su integridad es por esto por lo que, se hizo necesario crear nuevas tecnologías como Datawarehouse y datamining.

De acuerdo con lo enunciado por ESAN, "Actualmente, la mayoría de las compañías reúnen gran cantidad de datos tanto de clientes, usuarios de sus plataformas o de los colaboradores a nivel interno. La gestión de dicha información permite obtener patrones, tendencias o factores que ayuden a la organización a generar una comunicación eficaz. En este contexto, en la actualidad existen diversas herramientas para el manejo de datos; entre las más importantes están el Data Warehouse y el Data Mining"[35].

7.1.1.1 Warehouse

De acuerdo con el análisis realizado por la empresa de ciber seguridad. La función principal de un data Warehouse es la de contener los datos necesarios o útiles para una organización y así poder utilizarlos en un futuro para extraer información ventajosa para la compañía y sus clientes. De esta forma, en estos almacenes los datos están organizados en una base especialmente diseñada para favorecer su análisis y solo se entregará la información a la persona indicada en el momento óptimo y en el formato adecuado utilizando Sistemas de Soporte a Decisiones[36].

Citado por: Inmon, "Entre las características distintivas de los data Warehouse se encuentra la orientación al tema, la integración, la no volatilidad de los datos y su denominación de tiempo variante, esto es, que facilitan el uso de datos históricos para el análisis de tendencia debido a que el horizonte de tiempo es significativamente más largo que en el sistema operacional"[37].

---

[34] Heredero Carmen de Pablos, Hermoso Agius José Joaquín López, Romo Romero Santiago Martín, Medina Salgado Sonia. Organización y transformación de los sistemas de información en la empresa. 4 ed. Madrid: ESIC, 2019. ISBN. 8417513744, 9788417513740.

[35] De Molina Alonso. El impacto del Data Warehouse y Data Mining en la nueva comunicación empresarial [en línea]. Lima, 2018. [Fecha consulta: 17 marzo 2021]. Disponible en: https://www.esan.edu.pe/apuntes-empresariales/2018/05/el-impacto-del-data-warehouse-y-data-mining-en-la-nueva-comunicacion-empresarial/#:~:text=En%20este%20contexto%2C%20en%20la,se%20depuran%20los%20datos%20innecesarios.

[36] ¿Qué es un Data Warehouse? [En línea]. Madrid, 2015. [Fecha de consulta: 17 marzo 2021]. Disponible en: https://directortic.es/tecnologia-2/que-es-un-data-warehouse-2015022413162.htm#:~:text=La%20funci%C3%B3n%20principal%20de%20un,la%20compa%C3%B1%C3%ADa%20y%20sus%20clientes.

[37] Gorbea Portal Salvador, Madera Jaramillo María de Jesús. Características del data Warehouse. **En:** Diseño de un data Warehouse para medir el desarrollo disciplinar en instituciones académicas. [Sitio web]. 72 ed. México: BIBLIOTECOLÓGICA, 2017. P.167. [Fecha consulta: 17 marzo 2021].

Como menciona ESAN, “Gracias a esto se obtienen diversos beneficios. Por ejemplo, la mejora de decisiones corporativas, el almacenamiento y posterior consulta de datos trascendentales. Por supuesto, también se logra un mejor conocimiento del público interno y externo a quienes irán dirigidos los mensajes empresariales. La comunicación con el Data Warehouse es mucho más confiable entre las distintas áreas de la compañía a nivel comercial”[38].

7.1.1.2 Datamining

Según Palma, “Consiste en un conjunto de metodologías estadísticas y computacionales que, junto a un enfoque desde las ciencias de conducta, permite el análisis de datos y la elaboración de modelos matemáticos descriptivos y predictivos de la conducta del consumidor”[39].

Se implementa a través de cuatro pasos. El primero es la fijación de metas, bajo las cuales se recopilará los datos. Por ejemplo, la finalidad será agrupar la información para impactar en la gestión comunicacional de la organización. En segundo lugar, está el procesamiento de datos, seguido del análisis y, por último, la recopilación de las evaluaciones y observaciones para usarlos en un plan corporativo”[40].

7.2 AGENTES DE AMENAZAS.

“No se realizó un estudio comprensivo de los sentimientos de la población. NO existe una base de datos decisiva, que compare los fraudes que se comente hoy en día con aquellos que se cometían en el pasado. Sin embargo, Los medios de

---

Disponible en: https://www.researchgate.net/publication/319362633_Diseno_de_un_data_warehouse_para_medir_el_desarrollo_disciplinar_en_instituciones_academicas.

[38] ¿Qué es un Data Warehouse? [Sitio web]. Madrid, 2015. [Fecha de consulta: 17 marzo 2021]. Disponible en : https://www.esan.edu.pe/apuntes-empresariales/2018/05/el-impacto-del-data-warehouse-y-data-mining-en-la-nueva-comunicacion-empresarial/#:~:text=En%20este%20contexto%2C%20en%20la,se%20depuran%20los%20datos%20innecesarios.

[39] Palma Claudio, Palma Wilfredo, Pérez Ricardo. Data Mining. El arte de anticipar. Santiago: [En línea]. RIL Editores, 2009. P.43. ISBN. 978-956-284-711-7. [Fecha de consulta: 17 marzo 2021]. Disponible en : https://www.studocu.com/ca-es/document/universitat-oberta-de-catalunya/mineria-de-datos/data-mining-el-arte-de-anticipar-by-claudio-palma-wilfredo-palma-ricardo-perez/19171612

[40] De Molina Alonso. El impacto del Data Warehouse y Data Mining en la nueva comunicación empresarial [en línea]. Lima, 2018. [Fecha consulta: 17 marzo 2021]. Disponible en: https://www.esan.edu.pe/apuntes-empresariales/2018/05/el-impacto-del-data-warehouse-y-data-mining-en-la-nueva-comunicacion-empresarial/#:~:text=En%20este%20contexto%2C%20en%20la,se%20depuran%20los%20datos%20innecesarios.

comunicación de masas. Los pleitos que suceden los tribunales y los distintos estudios que se han realizado apuntan hacia la extensión y el crecimiento del fraude de la sociedad norteamericana".

Esto ratifica que la sociedad esta permeada por querer obtener un beneficio propio sin importar en muchas ocasiones las consecuencias y la afectación que esto pueda generar ya sea de manera particular o singular. La cultura que se ha ido alimentando ha sido la del engaño y con el auge de las tecnologías este aspecto se ha visto reflejado en todas las culturas.

7.2.1 Características del agente amenaza.

La información se encuentra expuesta a variedad de amenazas y se vuelve a un más vulnerable cuando las empresas no implementan métodos de seguridad para que su infraestructura esté preparada ante cualquier evento que tenga la intención de afectar sus procesos internos[41].

8. SEGURIDAD EN EL TRABAJO REMOTO

Según datos de Adecco Group Institute, "Los países donde más se trabaja en remoto en el seno de la UE son Suecia (40,9%) y Holanda (40,1%), seguidos de Luxemburgo (37,5%) y Finlandia (33,5%). En Francia el porcentaje llega al 28,3% y en Portugal al 20,7%. Italia"[42].

Con la actual situación que se presenta mundialmente se evidencia el aumento de del desplazamiento del trabajo a modo remoto desde los hogares lo cual requerirá de la aplicación de una serie de políticas de seguridad para la protección de los dispositivos de cómputo y los procesos que desde allí se manejen.

De acuerdo con datos suministrados por Bellé, analista de IDG Research España "Este escenario ha hecho que surjan diversas preocupaciones en las empresas, como las referidas a la necesidad de dotar de herramientas a los empleados para trabajar en este nuevo entorno (84% de las organizaciones consultadas), el acceso y la conectividad de un modo seguro y sin perjuicio de la productividad (71%) o la manera de conocer de forma directa la experiencia del empleado (58%)"[43].

---

[41] DAMA International. Conocimiento Para La Gestión De Datos. 2 ed. : Technics Publications, 2010. ISBN 978-163-462-883-9.

[42] La pandemia consigue que teletrabaje el 14,5% de la población con empleo en España. [en línea]. Madrid, 2021. [fecha de consulta: 19 marzo 2021]. Disponible en: https://www.computerworld.es/tendencias/la-pandemia-consigue-que-teletrabaje-el-145-de-la-poblacion-con-empleo-en-espana.

[43] De las soluciones de urgencia al teletrabajo planificado. [en línea]. Madrid, 2021. [fecha de consulta: 19 marzo 2021]. Disponible en: https://www.computerworld.es/tendencias/de-las-soluciones-de-urgencia-al-teletrabajo-planificado.

IBM Security “Durante el último año en Latinoamérica hubo un incremento significativo de ciberataques en las industrias, con un 40% de aumento en malware de código abierto en 2020 y marcas falsificada herramientas para el distanciamiento social”[44].

Las consecuencias de no tener unas estrategias claras frente a la seguridad de todo el ecosistema tecnológico conlleva no solo a que se esté en constante zozobra por lo que pueda suceder con la fuga de información, sino que también se está en constante peligro por las amenazas externas, que en este caso se pueden materializar con ataques maliciosos los cuales no dudan en pensar si comenten o no el delito, cuando tienen un objetivo su único propósito es vulnerar el sistema y obtener lo que se proponen. De igual manera como contramedida, las empresas que ejercieron control en sus sistemas obtuvieron óptimos resultados de mitigación al momento de enfrentar ataques de seguridad[45].

Lo siguiente se ve reflejado en la Encuesta Mundial sobre Fraude y Delitos Económicos de PwC, donde se refleja que, “Casi la mitad de las organizaciones actuaron ante los delitos mediante la implementación y mejora de controles y el 60% afirmó que a sus organizaciones les iba mejor por ello. Los resultados de la encuesta señalan que “las compañías que ya contaban con un programa antifraude pudieron actuar de manera más rápida dispensando menos recursos, y abonaron un 16% menos en multas”.

“El informe revela que más del 60% de las organizaciones están empezando a utilizar tecnologías tales como inteligencia artificial y aprendizaje automático para combatir el fraude, la corrupción y otros delitos económicos, sin embargo, las inquietudes sobre su empleo se relacionan con los costos que implica su implementación, experiencia insuficiente y los recursos limitados. Adicionalmente a ello, el 28% opina que se les dificulta cuantificar su valor”[46].

---

[44] Se duplicaron ataques a industria por COVID-19: IBM. [en línea]. Ciudad de México, 2021. [fecha de consulta: 18 marzo de 2021]. Disponible en: https://esemanal.mx/2016/06/fortinet-detecta-riesgos-oportunidades/.

[45] PWC; Encuesta Global sobre Fraude y Delitos Económicos 2020; Las tasas globales de delitos económicos y fraude se mantienen en niveles altos: casi la mitad de las compañías informaron haber sufrido fraude en los últimos dos años; [sitio web]. Buenos Aires. [fecha de consulta: 18 marzo de 2021]. Disponible en: https://www.pwc.com.ar/es/prensa/encuesta-global-sobre-fraude-y-delitos-economicos-2020.html.

[46] Ibid., p. 2.

8.1 DISPOSITIVOS PERSONALES EN ENTORNOS LABORALES

El uso de dispositivos personales para la realización de actividades de carácter laboral se ha tornado en una constante y tomo más fuerza en los tiempos de pandemia por el COVID 19, la rápida expansión del virus de cierta forma obligo a las empresas a tomar decisiones inmediatas sin antes tener una preparación sobre cómo se iba a afrontar esta situación, en muchos casos se optó por dejar usar a los empleados equipos personales y extraer solo la información necesaria para lo laboral, esto con el fin de no exponer el total de la información que se contenía en los equipos corporativos para evitar pérdidas de información sobre todo la más confidencial. Aunque esta es una medida poco efectiva ya que la información siempre estará expuesta y más aún si los equipos son personales y no tienen los controles necesarios de seguridad.

Existen casos los empleados toman decisiones que creen son las más indicadas sin antes consultarlas con los directivos de la empresa y no asumen la responsabilidad de hacerse cargo de los equipos corporativos asignados, ya sea por evitar eventualidades como hurtos, averías por descuido que de alguna forma puede conllevar a sanciones económicas o disciplinarias, también se puede presentar que los dispositivos corporativos según el criterio de los funcionarios piensen que estos tienen un rendimiento menor que sus equipos personales y opten por utilizar estos últimos, aunque esta idea en parte puede ser cierta, es importante aclarar que los dispositivos corporativos estas diseñados para soportar largas duraciones de trabajo lo que en su mayoría los equipos personales no.

Algunas de las razones por las cuales el no control se ha convertido en un problema de seguridad muy importante se evidencia en el deterioro de los equipos corporativos, acceso a sitios web que representan una amenaza para la información, instalación de dispositivos externos de almacenamiento sin ningún tipo de seguridad aumentando el riesgo de transferencia de amenazas, cediendo los dispositivos a terceras personas para que realicen actividades con diferentes fines, conectando los dispositivos a redes sin protección.

“Las empresas reconocen que, si cambian su enfoque para mejorar el desempeño de las computadoras personales (particularmente cuando se maneja una forma de trabajo remota), no solo podrían aumentar la productividad de los empleados, sino también incrementar su nivel de compromiso. Estar comprometido y motivado constantemente para cumplir tareas laborales debido a una tecnología superior no solo es bueno para la productividad, sino también promueve un trabajo de mayor calidad” [47].

[47] INTEL. Según estudio la modernización de la computadora personal (PC) es esencial para el futuro del trabajo. [Sitio web]. [Consulta: 14 de mayo 2022]. Disponible en: https://newsroom.intel.la/news/segun-estudio-la-modernizacion-de-la-computadora-personal-pc-es-esencial-para-el-futuro-del-trabajo/.

Esta realización está impulsando a las más empresas a invertir en la administración de dispositivos basados en la nube y con ello tienen computadoras personales de mayor rendimiento y más seguras.
Concretamente, el 56% de los ITDM están invirtiendo en la administración de dispositivos basados en la nube, mientras que el 55% le está dando prioridad a chips más seguros, y el 48% invierten en chips de mayor rendimiento y velocidad.

La computadora personal sigue siendo la herramienta preferida de los empleados cuando desean centrarse en hacer su trabajo. Los resultados de Forrester son benéficos al ayudar a los departamentos de TI no solo a gestionar la crisis de COVID-19, sino a colocar las piezas necesarias para una fuerza laboral cada vez más remota en el futuro"[48].

"Quizás, muchas empresas todavía no lo saben, pero el riesgo es mucho más alto cuando los trabajadores se conectan a su empresa desde casa. Primero, porque se conecta desde su equipo personal, que muy probablemente no cuente con los estándares de seguridad exigidos, y segundo, porque no se conectará a través de una red 100% segura"[49].

Falta de controles de seguridad física: en ciertas ocasiones los dispositivos destinados al teletrabajo se utilizan en lugares fuera de la organización como por ejemplo en hoteles, cafeterías, en salas de conferencias, etc. Esta condición aumenta el riesgo de que los dispositivos se pierdan o sean robados, lo que lo convierte a su vez en una posible pérdida de datos corporativos si no están convenientemente protegidos. Es muy importante tener en cuenta este tipo de situaciones a la hora de aplicar las medidas de seguridad necesarias para este tipo de dispositivos y proteger la información de accesos no deseados.

Redes no seguras: las organizaciones no tienen control sobre las redes que usan sus empleados para teletrabajar. Es una práctica habitual utilizar redes abiertas e inseguras (aeropuertos, cafeterías, etc.) que un ciberdelincuentes podría aprovechar para acceder a la información que contiene el dispositivo utilizado para el trabajo en remoto.

Dispositivos infectados en redes corporativas: la inclusión del BYOD en el ámbito empresarial ha sumado factores de riesgo[50],

[48] Ibid., p. 3.
[49] CIBERNOS. Principales problemas de ciberseguridad en los puestos de teletrabajo. [Sitio web]. [Consulta: 14 de marzo 2022]. Disponible en: https://www.grupocibernos.com/blog/serie-problema-3-ciberseguridad-en-las-empresas-puestos-teletrabajo.
[50] INCIBE. Ciberseguridad en el teletrabajo. OBJETIVOS DE SEGURIDAD EN EL ACCESO REMOTO. [Sitio web]. [Consulta: 15 de marzo 2022]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf.

como el uso de dispositivos que están Infectados con algún tipo de malware a consecuencia del uso personal. El problema surge cuando una vez infectados se conectan a la red de la empresa, pudiendo propagar el malware a otros dispositivos.

Acceso remoto a los recursos internos: permitir el acceso externo a los recursos corporativos implica su exposición a nuevas amenazas, aumentando la posibilidad de que estos se vean comprometidos. Por este motivo, es necesario otorgar acceso a estos recursos solo a los empleados que lo necesiten para el desempeño de su trabajo.

Falta de formación: es habitual que la falta de formación o de conocimiento de las políticas de seguridad de la empresa por parte de los empleados pongan en riesgo la seguridad de la información[51].

8.2 MEDIDAS PARA LA PREVENCIÓN DE PÉRDIDA DE DATOS

Existen diferentes medidas para que una empresa pueda garantizar la seguridad de sus datos e información. A continuación, vamos a ver tres tipos de medidas muy recomendables:

8.2.1 Medidas técnicas

La empresa debe desarrollar funciones como el cifrado de la información, actualizaciones constantes de cortafuegos y del sistema en general o la utilización de herramientas o soluciones de prevención de pérdida de datos o DLP.

8.2.2 Medidas organizativas

Implantación de políticas de seguridad en las compañías, con el objetivo de que la información con la que se trabaja en la empresa no sea utilizada o compartida indebidamente. También se debe llevar a cabo acciones o políticas de concienciación a los propios trabajadores.

8.2.3 Medidas jurídicas

Instar a las personas que tengan cualquier actividad relacionada con la empresa a que firmen acuerdos de confidencialidad, donde se indicarán los aspectos referentes a la seguridad y la privacidad de los datos e información en la prestación de servicios, especificando los tipos de sanciones en caso de incumplimiento. Un aspecto muy relevante que debemos esclarecer y determinar

[51] Ibid., p. 9.

es el relacionado con la gestión de ficheros que contengan datos de carácter personal. Detallando estas medidas, no solo cumpliremos con las leyes, sino que también el cliente valorará nuestra preocupación porque sus datos permanezcan en la más estricta confidencialidad. De esta forma, la empresa también se asegura que en caso de que tenga lugar alguna fuga de información, tenga el apoyo legal necesario[52].

[52] Tuyu Technology; Gestión de prevención de pérdida de datos; Recomendaciones Para La Prevención De Pérdida De Datos. [Sitio web]. Madrid. [Consulta: 18 agosto 2017]. Disponible en: https://www.tuyu.es/prevencion-de-perdida-de-datos/#.

9. MARCO LEGAL

9.1 GDPR: LO QUE DEBES SABER SOBRE EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Los estados han están preocupados por el manejo que las empresas les están dando a la información de los ciudadanos y a raíz de la frecuente perdida de datos ya sea por ataques informáticos o por negocio entre las mismas organizaciones para el acaparamiento de clientes, se han tomado medias de persuasión mucho más rigurosas con las entidades que no cumplan con los requerimientos de protección de la información, las sanciones serán más rigurosas y los datos personales tuvieron una extensión de privilegios respecto al tipo de información que estaba protegida por las leyes Europeas.

En mayo de 2018, el Reglamento General de Protección de Datos de la Unión Europea (GDPR) entra en vigor para mejorar la protección de datos personales.

El GDPR va a tener un Impacto significativo para las organizaciones y su forma de manejar los datos, con sanciones potencialmente muy grandes para aquellas empresas que sufran una violación, llegando hasta un 4% de los ingresos globales.

El Reglamento General de Protección de Datos (GDPR) (Reglamento 2016/679) es un reglamento por el que el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea tienen la intención de reforzar y unificar la protección de datos para todos los individuos dentro de la Unión Europea (UE). También se ocupa de la exportación de datos personales fuera de la UE. El objetivo principal del GDPR es dar control a los ciudadanos y residentes sobre sus datos personales y simplificar el entorno regulador de los negocios internacionales unificando la regulación dentro de la UE.

Es responsabilidad del controlador asegurar que su procesador cumple con la ley de protección de datos y los procesadores deben respetar las reglas para mantener registros de sus actividades de procesamiento. Si los procesadores están involucrados en una violación de datos, son mucho más responsables bajo GDPR que estaban bajo la Ley de Protección de Datos.

La UE ha ampliado sustancialmente la definición de datos personales en el marco del GDPR. Para reflejar los tipos de organizaciones de datos que ahora recopilan sobre personas, los identificadores online, como las direcciones IP, ahora son considerados como datos personales. Otros datos, como la información económica, cultural o de salud mental, también se consideran información de identificación personal.

Los datos personales pseudónimos también pueden estar sujetos a las reglas de GDPR, dependiendo de lo fácil o difícil que sea identificar cuáles son los datos[53].

9.2 NORMATIVIDAD SOBRE DELITOS INFORMÁTICOS EN COLOMBIA

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones. 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para sí o para un tercero. 6. Con fines terroristas o generando riesgo

[53] Parlamento europeo, el Consejo de la Unión Europea y la Comisión Europea. Reglamento 679. (25, mayo, 2018). Reglamento General de Protección de Datos de la Unión Europea. GDPR.

para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información[54], además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales[55].

9.3 LEY ESTATUTARIA 1581 DE 2012

Entró en vigor la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

Aspectos claves de la normatividad:

- Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.

- Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

- Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.

- Crea una especial protección a los datos de menores de edad.

[54] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”. En: Diario Oficial. Marzo, 2021. Nro.51.609.
[55] Ibid,. p. 5.

- Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante[56].
- Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

- Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.

- Crea el Registro Nacional de Bases de Datos.
- Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos[57].

9.4 LEGISLACIÓN SOBRE DELITOS INFORMATICOS ESPAÑA

Artículos del Código Penal Español referentes a Delitos Informáticos (Ley-Orgánica 10/1995, de 23 de noviembre/BOE número 281, de 24 de noviembre de 1.995).

9.4.1 Artículo 197

1. El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier

[56] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1581. (17, octubre, 2012). Protección De Datos Personales. En: Sentencia C-748 de 2011 de la Corte Constitucional.
[57] Ibid,. p. 6.

medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero[58].

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

9.4.2 Artículo 199

1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

[58] ESTADO ESPAÑOL. CONGRESO DEL ESTADO ESPAÑOL. Ley-Orgánica 10. (23, noviembre, 1995). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado “referentes a Delitos Informáticos”. En: BOE. Noviembre, 1995.

9.4.3 Artículo 256

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses[59].

9.4.4 Artículo 270

Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización. Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

9.4.5 Artículo 278

1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

9.4.6 Artículo 536

La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías

[59] Ibib., p.2.

constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años[60].
Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses[61].

[60] Ibib., p.3.
[61] Ibib., p.4.

10. EXAMINAR VULNERABILIDADES Y AMENAZAS DE SEGURIDAD PRESENTES EN LOS DISPOSITIVOS REMOTOS EMPRESARIALES QUE PUEDEN GENERAR AFECTACIONES EN LA INFORMACIÓN AL MOMENTO DE SU PROCESAMIENTO, ALMACENAMIENTO Y TRANSFERENCIA.

El trabajo remoto es una modalidad que se desempeña en un lugar alternativo al sitio de trabajo empresarial ya sea de manera continua o alternancia, lo cual representa en parte un beneficio económico para la empresa por los gastos que se ahorran en manutención como servicios públicos por nombrar uno de los más importantes, pero visualizando otro tipo de aspectos como el de la productividad, administración de la información y seguridad, se evidencia la carencia de controles y capacitación de los funcionarios ante la presencia de amenazas que están al asecho continuamente en busca de hallar sistemas vulnerables o personal ingenuo que les permita lograr el objetivo propuesto que la mayoría de ocasiones es el secuestro o extracción de datos o colapso del sistema. . A continuación, veremos como el trabajo remoto es vulnerable e inseguro.

De acuerdo con un informe del "International Workplace Group, el 50% de los empleados del mundo ahora trabajan fuera de su sede principal. Además, El 80% de los encuestados indicaron que rechazarían ofertas de empleo si no permiten trabajo remoto. Otro 75% considera que el trabajo flexible será la nueva norma para los empleos tras la contingencia"[62].

"OpenVPN, por su parte, informó que el 90% de los profesionales de TI creen que el trabajo remoto no es seguro actualmente. Más del 70% de los encuestados piensa que el personal remoto representa un mayor riesgo para las empresas. Esto significa que los expertos están reconociendo los riesgos del trabajo remoto y ese es el primer paso para abordar el problema"[63].

Según un estudio de "CSO Online, el 83% de los ataques de phishing en 2019 tuvieron lugar fuera de los correos electrónicos. Específicamente, ocurrió desde plataformas como Facebook Messenger y WhatsApp y algunos juegos y servicios. Tus empleados podrían estar conectándose a una red no segura y los actores maliciosos pueden espiar fácilmente su conexión"[64].

"En América Latina, los registros son similares a lo que ocurre en el orbe, con un crecimiento de los ataques de fuerza bruta durante el tercer trimestre del 141%, tal

[62] Rivas Genesis. Trabajo Remoto: Conoce los Riesgos para tu empresa y cómo mitigarlos. Estadísticas del trabajo remoto. [Sitio web]. Madrid. 2020. [Consulta: 15 octubre 2021]. Disponible en: https://www.gb-advisors.com/es/trabajo-remoto-conoce-riesgos-empresa-mitigarlos/
[63] Ibib.,p.2.
[64] Ibib.,p.3.

como se muestra en la Imagen 1, donde incluso en algunos breves periodos las detecciones rebasaron los veinte millones de intentos diarios, según datos de la telemetría de ESET"[65].

Figura 1. Intentos de ataque mediante fu fuerza bruta al RDP.

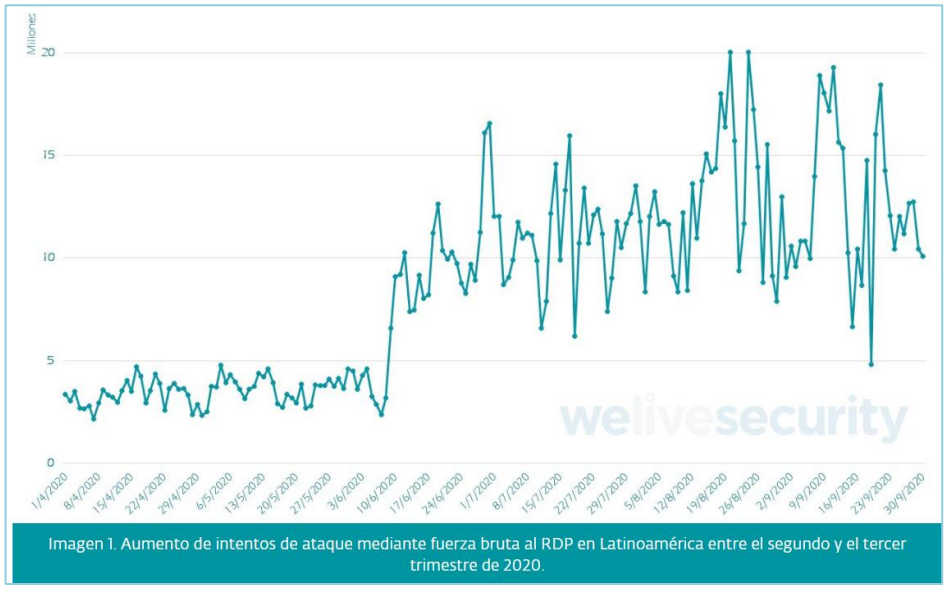


Imagen 1. Aumento de intentos de ataque mediante fuerza bruta al RDP en Latinoamérica entre el segundo y el tercer trimestre de 2020.

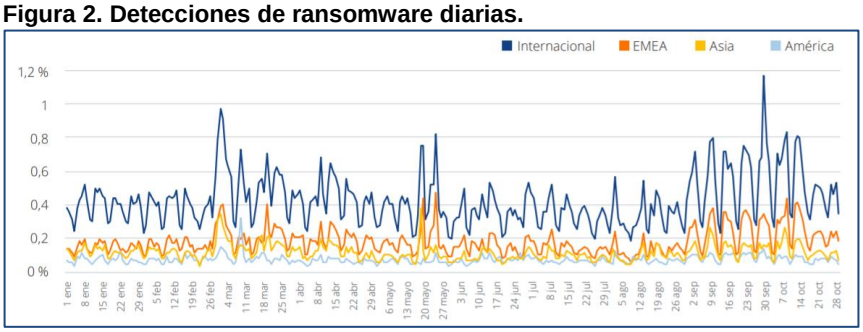
Fuente. Mendoza Miguel, Aumento de intentos de ataque mediante fuerza bruta al RDP en Latinoamérica entre el segundo y tercer trimestre de 2020. [En línea]. Welivesecurity. Madrid. Disponible en: https://www.welivesecurity.com/la-es/2020/11/30/aumentaron-ataques-fuerza-bruta-rdp-america-latina/

La pandemia del COVID ha provocado que los ciber atacantes encuentren oportunidades para ejecutar diversos métodos de vulneración a los sistemas informáticos y esto se debe en gran medida a los cambios de sitio de trabajo que naturalmente son utilizados para dichas labores. Las organizaciones por lo general tienen en su mayoría esquemas de seguridad implementados en sus locaciones, pero con grandes oportunidades en el esquema de seguridad en los dispositivos que son extraídos de las instalaciones de la empresa, además del replanteamiento de políticas con el uso de equipos de cómputo personales utilizados para actividades laborales que no cumplen con los esquemas de seguridad debidos para tal uso.

[65] Mendoza Miguel Ángel. Aumentaron 141% los ataques de fuerza bruta al RDP en América Latina. Aumento de ataques de fuerza bruta al RDP. [Sitio web]. Madrid: ESET. 2020. [Consulta: 15 octubre 2021]. https://www.welivesecurity.com/la-es/2020/11/30/aumentaron-ataques-fuerza-bruta-rdp-america-latina/

Según estudio realizado por “Acronis International Este año hemos observado un claro repunte global al inicio del confinamiento por la COVID-19 en marzo. Desde entonces, la actividad del ransomware ha seguido a un nivel más elevado de lo normal. En lo relativo a los sectores y zonas geográficas atacadas, no hay excepciones: los ciberdelincuentes atacan todos los sectores. En septiembre, comenzamos a ver otra ola de ataques de ransomware, en especial contra empresas de los sectores de educación y fabricación en América del Norte”[66].

Figura 2. Detecciones de ransomware diarias.



Fuente: Fuente: Fuente: IVANYUK Alexander. Ataques de Ransomware en el año 2020. [En línea]. Singapur.2020. Disponible en: https://dl.acronis.com/u/rc/WP-Acronis-Cyber-Threats-Report-2020-ES-ES-201203.pdf

Según informe de Acronis “Durante la pandemia, hemos observado un aumento de los ataques de phishing, en especial contra las herramientas de colaboración y los servicios de uso compartido de archivos que han ganado popularidad con el teletrabajo. Tras el pico inicial de marzo, los ataques de phishing se han normalizado. Algunos de los grupos de ciberdelincuentes parecen haber vuelto a utilizar adjuntos maliciosos. En julio, tras una ausencia de cinco meses, vimos incluso el regreso del célebre grupo Emotet, que repitió el envío de documentos maliciosos de Office.

[66] Ivanyuk Alexander. Tendencias de ciberseguridad de 2021, Amenaza de malware general. Berna: Acronis, 2020.p. 18. [Sitio web]. [Consulta: 15 octubre 2021]. Disponible en: https://dl.acronis.com/u/rc/WP-Acronis-Cyber-Threats-Report-2020-ES-ES-201203.pdf.

Figura 3. Sitios web maliciosos.

MES	PORCENTAJE DE USUARIOS que hicieron clic en URL maliciosas
Junio	5,5 %
Julio	5,1 %
Agosto	2,3 %
Septiembre	2,7 %
Octubre	3,4 %

Fuente: Fuente: IVANYUK Alexander. Porcentaje de usuarios que accedieron URL maliciosas en el segundo semestre del año 2020. [En línea]. Singapur.2020. Disponible en: https://dl.acronis.com/u/rc/WP-Acronis-Cyber-Threats-Report-2020-ES-ES-201203.pdf

El mayor porcentaje de URL maliciosas bloqueadas en el tercer trimestre de 2020 se registró en Estados Unidos, que alcanzó un 16,4 %, seguido de Alemania con un 14,1 % y de la República Checa con un 10,4 %. Sin embargo, el 51 % de las URL bloqueadas eran HTTPS cifradas, lo que dificultó su filtrado en la red. También hemos observado más grupos que captan tokens 2FA con phishing y los utilizan de inmediato con un script para iniciar sesión. Para que estas páginas de phishing sean más difíciles de detectar, normalmente se alojan en dominios de proveedores de servicios en la nube de confianza, como Azure o Google. Algunos agresores añaden incluso una página de CAPTCHA que el usuario debe resolver antes de llegar a la página de phishing final, una táctica que puede impedir que las soluciones de análisis automatizado examinen y bloqueen los sitios web de phishing"[67].

[67] Ibib.,p.22.

Figura 4. URL Bloqueadas por países.

CLASIFICACIÓN	PAÍS	PORCENTAJE DE URL BLOQUEADAS EN EL 3.ER TRIMESTRE DE 2020
1	Estados Unidos	16,4 %
2	Alemania	14,1 %
3	República Checa	10,4 %
4	España	8,3 %
5	Reino Unido	6,7 %
6	China	5,8 %
7	Sudáfrica	5,2 %
8	Hong Kong	3,6 %
9	Italia	3,4 %
10	Australia	2,4 %
11	Francia	2,1 %
12	Canadá	2 %
13	Perú	1,9 %
14	Noruega	1,9 %
15	Países Bajos	1,8 %
16	Japón	1,6 %
17	Suiza	1,6 %
18	Bulgaria	0,9 %
19	Singapur	0,8 %
20	Austria	0,7 %

Fuente: IVANYUK Alexander. Porcentaje de URL maliciosas bloqueadas en el tercer trimestre de 2020. [En línea]. Singapur. 2020. Disponible en: https://dl.acronis.com/u/rc/WP-Acronis-Cyber-Threats-Report-2020-ES-ES-201203.pdf

10.1 TIPOS DE VULNERABILIDADES

De acuerdo con lo mencionado por Martha Romero “una vulnerabilidad es un fallo en un sistema que puede ser explotada por un atacante generando un riesgo para la organización o para el mismo sistema”[68].

[68] *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades*. [Sitio web]. Universidad Estatal del Sur de Manabí. MANABI: Área de innovación y desarrollo, S.L. 2018, [Fecha de consulta: 20 octubre 2021]. primera edición. ISSN 9788494930614. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf.

10.1.1 Vulnerabilidades Físicas:

Son las que van a afectar la infraestructura de la organización de manera física y se pueden mencionar en este tipo de clasificación a los desastres naturales, como ejemplo se podría mencionar una vulnerabilidad alta de este tipo si se vive en una zona de alto riesgo de sismos, ya que puede presentarse una negación en el servicio, una afectación en la disponibilidad y a partir de ahí se podría empezar con problemas. Si la organización está en una zona que generalmente se inunda, se tiene también otro tipo de vulnerabilidad.

Otra de las opciones físicas con los controles de acceso, en muchas ocasiones se tiene los accesos a la infraestructura crítica y no se tienen los accesos pertinentes, cualquier persona podría abrir una puerta, podría entrar y constituye un gran riesgo para la organización porque cualquier usuario podría ingresar con una USB y copiar información, podría infectar la misma infraestructura.

10.1.1.1 Las vulnerabilidades Lógicas:

Son las que van a afectar directamente la infraestructura y el desarrollo de la operación de estos, estas pueden ser de[69]:

- Configuración inadecuada de los sistemas informáticos.
- Políticas de seguridad deficiente o inexistente[70].

10.1.1.2 Configuración inadecuada de los sistemas informáticos:

- La configuración inadecuada de los sistemas informáticas permite explotar determinadas vulnerabilidades, ya que las opciones que traen por defecto “de fábrica”, muchos dispositivos y Programas suelen ser poco seguras. Esta situación puede ser motivada, en parte, por una deficiente documentación sobre la configuración del sistema o dispositivo.

- Conviene destacar además la importancia de modificar las contraseñas predeterminadas por el fabricante, ya que éstas se suelen mantener en un porcentaje muy alto de dispositivos conectados a las redes (por ejemplo, en los puntos de acceso a redes inalámbricas o en los routers), seguramente por desinterés o por falta de una adecuada formación de los administradores y técnicos que los instalan.

[69] Ibid., p. 41.
[70] Ibid., p. 41.

- Ejecución de más servicios de los necesarios en los equipos, con cuentas de usuario que tienen privilegios excesivos para su función.

- Mantenimiento inadecuado de los sistemas: no se instalan y revisan los parches suministrados por el fabricante. En la actualidad podemos considerar que existe una auténtica competición entre los atacantes y usuarios maliciosos, por una parte, que descubren y tratan de explotar nuevos agujeros de seguridad, y los fabricantes de hardware y de software, por otra, que deben desarrollar e instalar los parches adecuados en los sistemas.

- Algunas aplicaciones informáticas presentan problemas de usabilidad de cara al usuario poco experimentado, que no es consciente de las opciones relacionadas con la seguridad. Así, se ha constatado que en muchos casos el usuario final desconoce cuáles son los cambios que pueden provocar la activación o desactivación de una determinada opción de seguridad en el programa que está utilizando.

- Módems con una configuración insegura que facilitan el acceso no autorizado de usuarios externos, mediante técnicas conocida como War dialing[71].

- Routers que utilizan protocolos de enrutamiento poco seguros (como el protocolo RIP), que no garantizan la integridad y autenticidad de los mensajes de control mediante los que se intercambian información sobre las rutas. Por este motivo, se recomienda utilizar protocolos de enrutamiento más avanzado, como OSPF o BGP, que incorporan funciones de autenticación y control de la integridad de los mensajes.

- Contar con excesivas relaciones de confianza entre redes y servidores, que facilitan el acceso a servidores sin requerir de autenticación, entre las que podríamos citar las siguientes:

- Dominios de confianza en sistemas Windows.

- Archivos ".rhosts" y "host.equiv" de UNIX/LINUX y los famosos comandos "" (rlogin, rcp, rsh...), que facilitan la confianza transitiva entre varios servidores (Host Equivalency o Trusted Host Access), de modo que un usuario o equipo se puede conectar a otros equipos sin tener que superar

[71] Gómez, Álvaro. Vulnerabilidad de los sistemas informáticos. En: Auditoría de Seguridad Informática (MF0487_3). [En línea]. Madrid: RA-MA, 2016. p. 18. [Fecha de consulta: 21 octubre 2021]. Disponible en: https://books.google.com.co/books?id=CI-fDwAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false.

un proceso de autenticación, simplemente porque su dirección IP se encuentra dentro de una lista de equipos de confianza"[72].

10.1.1.3 Políticas de seguridad deficiente o inexistente.

Muchas organizaciones no han definido e implantado de forma eficaz unas adecuadas Políticas y Procedimientos de Seguridad, de acuerdo con sus necesidades de seguridad de la información. Así, podríamos citar distintas situaciones que provocan vulnerabilidades en los sistemas informáticos que podrían ser aprovechadas por los atacantes:

- Política de contraseñas poco robusta: contraseñas que se pueden adivinar fácilmente y que no se cambian con frecuencia, contraseñas compartidas entre varios usuarios; usuarios que dejan sus contraseñas anotadas en su mesa o que se despreocupan de su seguridad (la comunican fácilmente a terceros); etcétera.

- Deficiente control de los intentos de acceso al sistema: las cuentas no se bloquean si se producen fallos de autenticación; no se registran los intentos reiterados de conexión en una misma cuenta; falta de seguimiento del tiempo de conexión de una sesión de usuario para detectar situaciones anómalas; etcétera[73].

- Escaso rigor en el control de acceso a los recursos: usuarios registrados en el sistema con permisos de acceso superiores a los que necesitan.

- Procedimientos inadecuados para la gestión de soportes informáticos o el control de equipos portátiles.
- Escaso control de las copias generadas en papel con información sensible: ausencia de vigilancia de las impresoras o de la documentación archivada en armarios y cajones. Conviene señalar, además, que el dumpster diving ("buceo en la basura") es una técnica de espionaje empresarial que, sorprendentemente, ha dado muy buenos resultados.

- Falta de control de los tratamientos realizados por terceros: éste sería el caso, por ejemplo, de las empresas de informática encargadas del mantenimiento de equipos y/o de programas.

- Deficiente o inexistente limitación del acceso físico a los equipos más sensibles, dispositivos de red y cableado.

[72] Ibid., p. 19.
[73] Ibid., p. 19.

- Instalación de programas poco fiables por parte de los usuarios sin contar con la autorización de los responsables de informática de la organización.

- Despreocupación por la instalación de parches y de nuevas versiones de software en servidores y otros equipos críticos. Desconocimiento de los posibles agujeros de seguridad que podrían afectar a cada sistema o equipo informático.

- Escasa protección de equipos portátiles que los usuarios pueden sacar de la red de la organización, y que podrían resultar vulnerables frente a virus, troyanos y otros códigos dañinos.

- Registros (logs) de los servidores y de los dispositivos de red sin activar, o activados con información insuficiente y/o que apenas son consultados por los responsables.

- Información sensible que se guarda sin cifrar en el sistema.

- Despreocupación por el adecuado almacenamiento de las copias de seguridad, o por los procedimientos implantados para su generación y verificación periódica.

- Transmisión de ficheros y mensajes de correo sin cifrar ni autenticar, sobre todo a través de redes públicas o redes basadas en enlaces de radio[74].

La pandemia de COVID-19 ha cambiado radicalmente el panorama de las amenazas, poniendo de manifiesto numerosos riesgos para la seguridad y la privacidad asociados al trabajo a distancia, como el acceso remoto a servidores internos de la empresa, las videoconferencias y la formación en seguridad para los teletrabajadores.

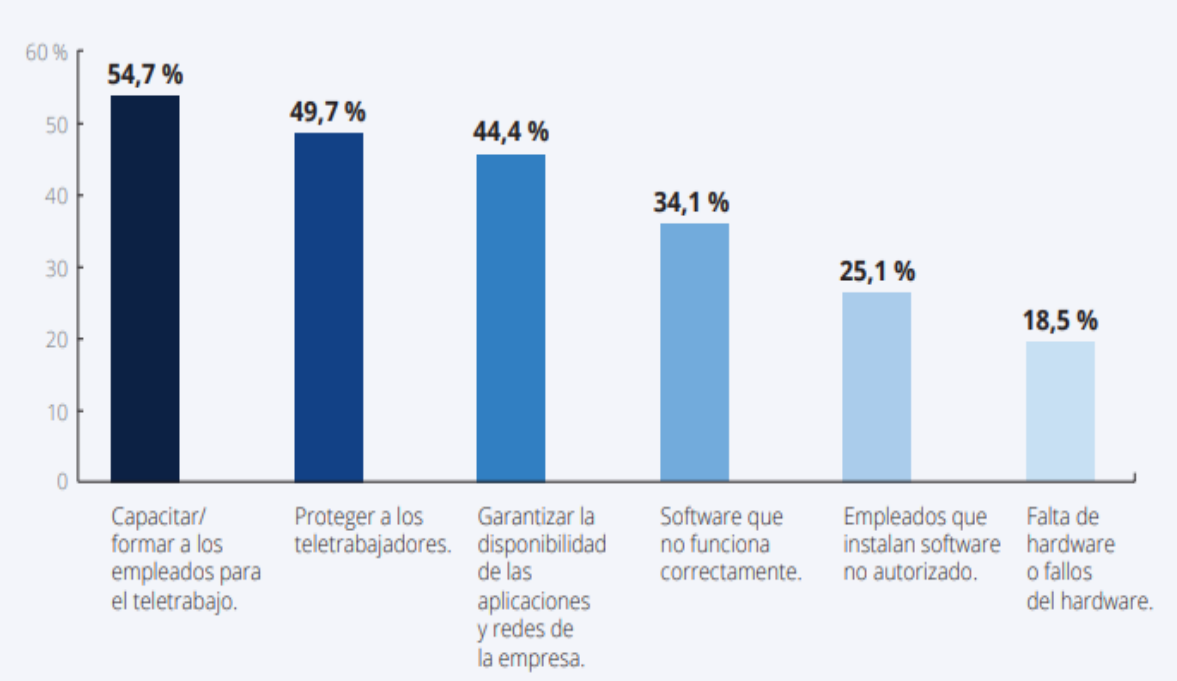
- Casi la mitad de todos los administradores de TI tienen problemas para formar y proteger a los teletrabajadores.
- El 31 % de las empresas internacionales sufren un ataque de ciberdelincuencia al menos una vez al día. Los tipos de ataques más habituales son intentos de phishing, ataques DDoS y ataques a sistemas de videoconferencia[75].

[74] Ibid., p. 20.

[75] Fuente: ACRONIS. Dificultades técnicas que ha encontrado para hacer frente al aumento de empleados que teletrabajo debido a la pandemia. [En línea]. Singapur.2020. P. 7. [Fecha de consulta: 20 mayo 2022]. Disponible en: https://dl.acronis.com/u/rc/WP-Acronis-Cyber-Threats-Report-2020-ES-ES-201203.pdf.

- El 92 % de las empresas internacionales tuvieron que adoptar nuevas tecnologías para cambiar al teletrabajo. Como resultado, el 72 % de las multinacionales han observado un incremento de costes de TI durante la pandemia.
- A pesar del aumento del gasto en tecnología, los ataques que consiguen sus objetivos siguen siendo frecuentes, ya que las empresas no priorizan de manera adecuada las funciones defensivas.
- El 39 % de todas las empresas denunciaron ataques a sistemas de videoconferencia durante la pandemia[76].

Figura 5. Informe sobre ciberpreparaciòn 2020.

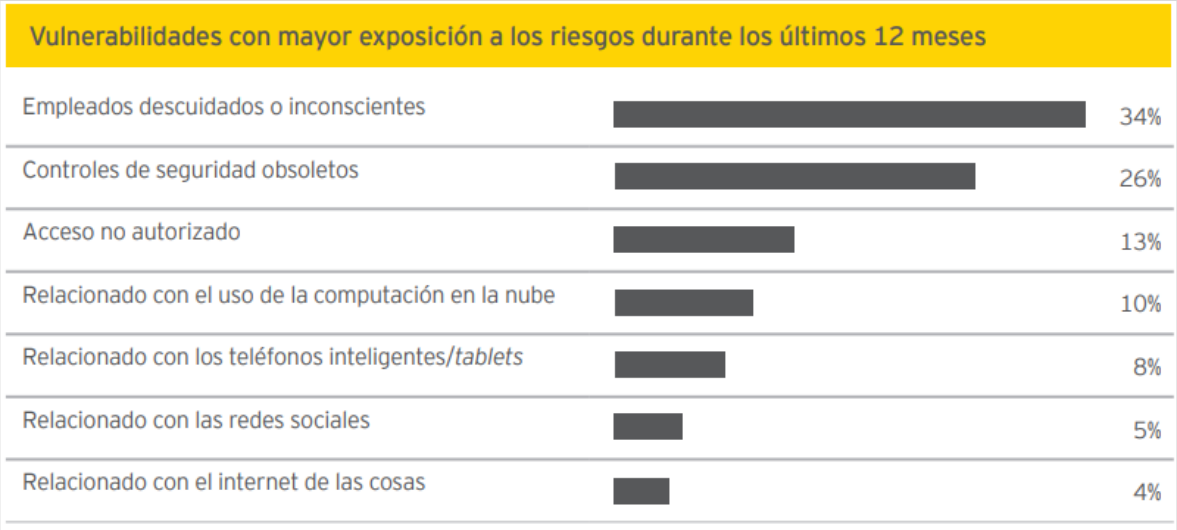


Fuente: ACRONIS. Dificultades técnicas que ha encontrado para hacer frente al aumento de empleados que teletrabajan debido a la pandemia. [En línea]. Singapur.2020. Disponible en: https://dl.acronis.com/u/rc/WP-Acronis-Cyber-Threats-Report-2020-ES-ES-201203.pdf.

[76] Ibid., p. 8.

“Las vulnerabilidades aumentan cuando se tratan de terceros. Solo el 15 % de las organizaciones han llevado a cabo los pasos básicos para protegerse de las amenazas de terceros; 36 % está al tanto de los riesgos a través de autoevaluaciones (22%) o evaluaciones individuales (14%); por lo que el 64% no tiene visibilidad sobre el tema. Esto aumenta hasta el 67% en las compañías más pequeñas.[77]”

Figura 6. Vulnerabilidades con mayor exposición a los riesgos.



Ernst & Young. ¿La ciberseguridad es algo más que protección? Encuesta Global de seguridad de la Información.[Sitio web].Lima.[Consulta: 23 de marzo 2022].Disponible en:https://assets.ey.com/content/dam/ey-sites/ey-com/es_co/topics/corporate-social-responsibility/ey- library-la-ciberseguridad-es-algo-mas-proteccion.pdf.

[77] Ernst & Young. ¿La ciberseguridad es algo más que protección? Encuesta Global de seguridad de la Información. [Sitio web]. Lima. [Consulta: 23 de marzo 2022]. Disponible en: https://assets.ey.com/content/dam/ey-sites/ey-com/es_co/topics/corporate-social-responsibility/ey-library-la-ciberseguridad-es-algo-mas-proteccion.pdf.

11. ESTABLECER LOS DISTINTOS SISTEMAS DLP CON RELACIÓN A SUS CARACTERÍSTICAS, FUNCIONALIDAD, EFECTIVIDAD Y SU USO EN LAS ORGANIZACIONES COMO SOLUCIÓN DE SEGURIDAD INFORMÁTICA.

Las soluciones DLP Data Loss Prevención se han convertido en una herramienta necesaria e indispensable para las empresas que deseen dar un manejo en cuanto a seguridad y protección de la información, los datos son el activo más importante y por lo tanto requieren de mecanismos y políticas que garanticen su integridad, la legislación de protección de la información de cada estado así lo están requiriendo, por lo tanto, las nuevas tecnologías están al servicio para satisfacer estas necesidades. A continuación, se hace referencia a las soluciones DLP Data Loss Prevention.

De acuerdo con la argumentación de Arreola, “DLP son las siglas para los programas de Prevención de Pérdida de Datos (Data Loss Prevention), que se encarga de detectar potenciales brechas de datos/transmisión de datos y prevenirlos a través de monitoreo, detección y bloqueo de información sensible mientras está en uso, en movimiento o en reposo; que vienen a ser las tres condiciones en las que se pueden encontrar los datos en cualquier momento”[78].

11.1 SOLUCIONES DLP - PREVENCION DE PERDIDA DE DATOS

No es fácil determinar qué enfoque es mejor para los requisitos de una organización. Depende en gran medida de los tipos de datos que deben protegerse, la industria en la que opera la organización y las razones para proteger los datos.

11.1.1 DLP tradicional

Algunos de los proveedores del mercado ofrecen DLP tradicional, como Forcepoint, McAfee y Symantec. El enfoque tradicional que ofrecen estos proveedores también es múltiple: proporciona cobertura en la puerta de enlace de la red, en la infraestructura de almacenamiento, en los puntos finales y en la nube. Este enfoque fue lo suficientemente exitoso como para delinear el mercado DLP actual y fue el primero en hacerse con una parte importante de la cuota de mercado.

---

[78] Arreola Adolfo. Prevenir acceso no autorizado en su red privada en casa. En: Ciberseguridad: ¿Por qué es importante para todos? [En línea]. 1ª ed. Ciudad de México: Universidad Anáhuac, 2019. p. 95. . [Fecha de consulta: 21 octubre 2021]. Disponible en : https://books.google.com.co/books?id=ZqHDDwAAQBAJ&pg=PT4&dq=Arreola+Adolfo&hl=es&sa=X&ved=2ahUKEwi_1MDk-bn0AhWUtDEKHYHfDJ0Q6wF6BAgHEAE#v=onepage&q=Arreola%20Adolfo&f=false

Las soluciones tradicionales de DLP añaden aún más complejidad a la receta. Requieren varios dispositivos y software para ejecutar la solución completa. Estos podrían incluir dispositivos (virtuales o reales) y servidores.

La arquitectura de red de la organización debe integrar esos dispositivos, y esta integración debe incluir inspección del tráfico de la red, bloqueo de correo electrónico, etc. Una vez realizada la integración, surge otro nivel de complejidad en la gestión, que depende de cada proveedor[79].

11.1.2 Agente DLP

Utiliza agentes de punto final a nivel de kernel que monitorean toda la actividad del usuario y del sistema. Es por eso por lo que, las soluciones que encajan en este enfoque también se conocen como soluciones Endpoint DLP.

Las soluciones de agente DLP suelen ser menos complejas que las tradicionales, principalmente porque requieren poca o ninguna integración de red. Sin embargo, estas soluciones interactúan con el sistema operativo a nivel de kernel. Por lo tanto, se requiere un ajuste extendido para evitar conflictos con el sistema operativo y otras aplicaciones[80].

11.2 PROVEEDORES DE DLP TRADICIONAL Y ENDPOINT

11.3 FORCEPOINT

La fuga de datos puede tener consecuencias devastadoras, desde una reputación dañada hasta multas y sanciones reguladoras.

Forcepoint DLP le permite descubrir y proteger la información confidencial donde quiera que ésta se encuentre: en las terminales, en la nube o en las instalaciones. Adopte servicios de colaboración en la nube, como Microsoft Office 365 y Box, para promover la innovación y fomentar el crecimiento de su empresa. Proteja la información de importancia crítica en computadoras portátiles con Mac OS X y Microsoft Windows. Proteja información personal y de propiedad intelectual, cumpla rápidamente con los requisitos reglamentarios mediante una extensa biblioteca de políticas predeterminadas y haciendo uso de las capacidades únicas que Forcepoint pone a su alcance para para la prevención de la pérdida de datos (DLP, Data Loss Prevention) y detener el robo de datos.

---

[79] Las 6 mejores soluciones de prevención de pérdida de datos que podrían ahorrarle millones [en línea] Madrid, 2020. [Fecha de consulta: 20 abril 2021]. Disponible en: https://geekflare.com/es/data-loss-prevention-solutions/

[80] Ibid., p. 4.

11.3.1 Forcepoint DLP Discovery

Para proteger sus datos, debe encontrarlos donde quiera que se ubiquen. Forcepoint DLP Discovery le permite encontrar y proteger sus datos confidenciales en toda su red, así como datos confidenciales almacenados en la nube, tales como Microsoft Office 365 y Box. Al agregar Forcepoint DLP Endpoint, el poder de Forcepoint DLP Discovery se puede extender a dispositivos finales de Mac OS X y Microsoft Windows, dentro y fuera de la red[81].

11.3.2 Forcepoint DLP Network

La última oportunidad para detener el robo de datos se presenta cuando ya está circulando a través de los canales del correo electrónico y la web. Forcepoint DLP Network lo ayuda a identificar e impedir la pérdida accidental y malintencionada de datos a partir de ataques externos o de ataques producidos de la creciente amenaza interna. Responda a las técnicas de evasión de las amenazas avanzadas con un poderoso OCR que le permite reconocer datos dentro de una imagen. Use Drip DLP para detener el robo de datos con un registro a la vez y monitoree el comportamiento y las anomalías a fin de identificar usuarios de alto riesgo.

11.3.3 Forcepoint DLP Endpoint

Forcepoint DLP Endpoint extiende las capacidades de OCR, Drip DLP y otras capacidades de control de robo de datos a dispositivos finales de Mac OS X y Microsoft Windows, tanto dentro como fuera de su red. Forcepoint le permite compartir de forma segura los datos almacenados en dispositivos extraíbles usando encriptado de archivos basados en su política. Monitoree las descargas en la web, incluidos los HTTP, así como las descargas en la nube como Microsoft Office 365 y Box. Integración total con Outlook, Notes y clientes por correo electrónico, usando la misma interfaz que emplea para las soluciones de Forcepoint para datos, Web, correo electrónico y dispositivos finales.

11.3.4 Módulo de Análisis de Imágenes

Para cumplir con los requisitos reglamentarios en muchas partes del mundo, o simplemente para asegurar un entorno sin acoso, el Módulo de Análisis de Imágenes ofrece la capacidad de identificar imágenes explícitas, como las que contienen pornografía, que se encuentran almacenadas en la red de la organización o circulando por los canales del correo electrónico o la web[82].

---

[81] Forcepoint; Forcepoint DLP. [Sitio web]. Wisconsin. [Consulta: 22 abril 2021]. Disponible en: https://www.forcepoint.com/sites/default/files/resources/brochures/brochure_forcepoint_dlp_es.pdf

[82] Ibid., p. 4.

11.4 CISCO EMAIL SECURITY

11.4.1 Motor de DLP directa RSA

- Tiempo de actividad del correo electrónico.
- Prevención de amenazas.
- Análisis de correo electrónico.
- Aplicación de políticas[83].
- DLP integrada con la RSA Enterprise

- Definición de las políticas de riesgo.
- Flujo de trabajo avanzado ante incidentes.
- Huella digital.

11.4.1.1 Solución de DLP de RSA Enterprise, Cisco ESA proporciona:

- Flujo de correo ininterrumpido
- Visibilidad total del flujo de correo
- Detección y remediación integradas
- Menos sistemas que mantener y problemas que solucionar.

11.5 APLICACIÓN DE POLÍTICAS DE CIFRADO

Ajustes de TLS basados en correo electrónico de un usuario

- Aplicar las obligaciones contractuales.
- Impedir que los datos confidenciales se envíen en texto claro.
- Evitar que los partners mal configurados envíen datos confidenciales en texto claro.

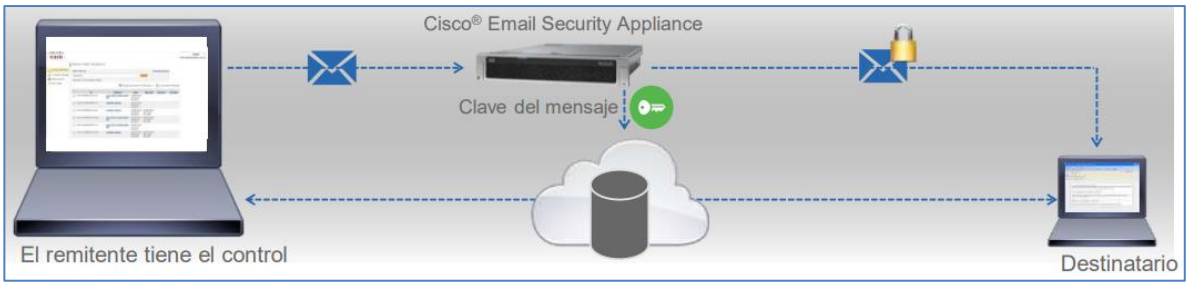
11.5.1 Cifrado de sobre de Cisco

Gestión de claves automatizada Sin requisitos de software para el equipo de escritorio Envío a cualquier dirección de correo electrónico de forma transparente Cifrado activado por + palabras clave, políticas, remitentes, destinatarios, etc.[84].

[83] Cisco; Cisco Email Security; DLP y cumplimiento. [Sitio web]. California: Cisco; [Consulta: 24 abril 2021]. Disponible en: https://www.cisco.com/c/dam/global/es_es/pdfs/SEC17Q4Cisco-Email-Security-Descripcion-general.pdf.

[84] Ibid., p. 25. p. 26. P.27.

Figura 7. Cifrado de sobre CISCO.



Fuente: BETTS Jeff. Aplicación de políticas de cifrado Ajustes de TLS basados en correo electrónico de un usuario. [En línea]. Cisco. Disponible en: https://www.cisco.com/c/dam/global/es_es/pdfs/SEC17Q4Cisco-Email-Security-Descripcion-general.pdf.

11.5.2 Autenticación de correo electrónico DKIM y SPF, DMARC.

- Evite la suplantación de sus mensajes
- Mejore su reputación
- Evite entrar en la lista negra
  Protéjase de la suplantación de identidad
- Mejore la reputación y la capacidad de entrega del remitente
- Visibilidad y control del correo electrónico enviado y de quién lo envía en su nombre[85]

11.6 MCAFEE DATA LOSS PREVENTION (DLP) PREVENT

Cuanto mayor sea el número de personas que comparten información de forma electrónica, mayor será la probabilidad de que alguien de manera involuntaria o intencionada envíe información confidencial a una persona no autorizada y ponga en riesgo los datos de la empresa. Ya sea a través del correo electrónico, la Web, la mensajería instantánea o FTP, la información puede salir de la empresa por medio de una gran variedad de canales. Algunos mensajes o transacciones están autorizados, pero deben cifrarse para garantizar la privacidad de los datos. Otros tipos de comunicaciones simplemente no son aceptables en ningún momento y deben bloquearse. La implementación de las directivas adecuadas en el momento justo es esencial para garantizar la seguridad de los datos, el cumplimiento de las normativas y la protección de la propiedad intelectual.

[85] Ibid., p. 29. P.30.

11.6.1 Totalmente integrado con el software McAfee ePolicy Orchestrator

McAfee DLP Prevent está completamente integrado con McAfee® ePolicy Orchestrator® (McAfee ePO™) y con McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint), con directivas, y gestión de incidentes y casos comunes. Los administradores pueden crear una única directiva de protección del correo electrónico y la Web en el software McAfee ePO y desplegarla en los endpoints y en la red. Además, McAfee DLP Endpoint y McAfee DLP Prevent comparten un motor de clasificación común, lo que facilita el empleo de una sola directiva para el correo electrónico y la Web[86].

11.6.2 Supervisión del correo electrónico de móviles

McAfee® DLP Prevent para el correo electrónico en móviles proporciona protección de contenido del correo electrónico en dispositivos móviles, interceptando los mensajes de correo electrónico que se han descargado en un dispositivo mediante un proxy ActiveSync con funciones de DLP. Además, puede interceptar ActiveSync tanto en Microsoft Exchange in situ como en Microsoft Office 365 Hosted Exchange.

11.6.3 Integración con proxies web y agentes de transferencia de mensajes (MTA)

McAfee DLP Prevent integra proxies web (que utilizan ICAP) y agentes MTA (que utilizan encabezados X) para llevar a cabo la acción adecuada. Al detener las transacciones no autorizadas a nivel de aplicación, en lugar de limitarse a interrumpir la sesión TCP (lo que no alteraría el comportamiento de las aplicaciones), McAfee DLP Prevent alerta a la aplicación de inicio de que se ha rechazado un transmisión debido a la infracción de una directiva. Esto garantiza una mayor protección de su organización ya que McAfee DLP Prevent "aprende" lo que debe protegerse e impide que la aplicación repita el mismo comportamiento.

11.6.4 Protección de la información confidencial conocida y desconocida

Gracias a la capacidad de clasificar más de 300 tipos de contenido distintos, McAfee DLP Prevent le ayuda a garantizar la seguridad de la información confidencial obvia (números de identificación personal y de tarjetas de crédito, y datos financieros).

[86] McAfee. McAfee DLP Prevent. Implemente directivas para proteger su información confidencial. [Sitio web]. México DF. McAfee. 2018. p. 1. [Consulta: 01 mayo 2021]. Disponible en: https://www.mcafee.com/enterprise/es-mx/assets/data-sheets/ds-dlp-prevent.pdf.

11.6.5 Aprovechamiento de la infraestructura existente

- Protege el correo electrónico de la empresa a través de la integración con gateways MTA que utilizan SMTP con encabezados X para bloquear, devolver, cifrar, poner en cuarentena y redireccionar.

- Proporciona control del tráfico a través de la integración de proxies web compatibles con el protocolo ICAP para impedir las infracciones de contenido a través de HTTP, HTTPS, mensajería instantánea, FTP y correo web.

11.6.6 Clasificación, análisis y corrección de fugas de datos

- Permite filtrar y controlar la información confidencial para disponer de protección contra los riesgos conocidos y desconocidos.

- Admite indexación e implementación de directivas de seguridad específicas para todos los tipos de contenido[87].
- Aplica directivas sobre el acceso a los recursos compartidos de archivos internos para impedir que los usuarios accedan a información o a repositorios sin autorización[88].

11.7 SYMANTEC DATA LOSS PREVENTION

Symantec ofrece un enfoque integral para la prevención de la pérdida de datos que cubre tanto los entornos locales como en la nube, así como los dispositivos móviles.

La oferta DLP de Symantec se expandió posteriormente para incluir muchos componentes diferentes, incluidos Symantec DLP para almacenamiento en la nube, Symantec DLP Cloud Prevent para Microsoft Office 365, Symantec Data Loss Prevention para Endpoint, Symantec Data Loss Prevention para dispositivos móviles, Symantec Data Loss Prevention Network y Symantec Data Loss Prevención para el almacenamiento.

En la actualidad, el producto está integrado con las capacidades de agente de seguridad de acceso a la nube de Symantec CloudSOC. La versión actual de Symantec Data Loss Prevention, 14.6, incluye integración con productos de Blue Coat Systems.

La arquitectura de Symantec Data Loss Prevention consta de servidores de detección de contenido y agentes de punto final, además de una plataforma de

[87] Ibid., p. 2.
[88] Ibid., p. 3.

administración unificada. La suite es escalable a cientos de miles de usuarios y dispositivos. También se puede implementar en las instalaciones, en entornos de nube híbrida y como un servicio administrado a través de un socio proveedor de servicios de seguridad administrado de Symantec.

La compatibilidad con Amazon Web Services (AWS) permite implementar servidores de detección de contenido DLP en la infraestructura de AWS. Esto permite a las organizaciones monitorear y proteger los datos confidenciales que se encuentran en instancias alojadas en AWS de Microsoft Exchange y SharePoint.

11.7.1 Protección móvil

La suite Symantec Data Loss Prevention también incluye monitoreo para dispositivos móviles y correo electrónico móvil a través de Symantec DLP for Mobile con Mobile Email Monitor y Mobile Prevent. Mobile Email Monitor es compatible con dispositivos Android e iOS y puede detectar cuándo los empleados descargan datos corporativos confidenciales a sus dispositivos móviles mediante el protocolo Microsoft Exchange ActiveSync[89].

11.7.2 Protección empresarial y de endpoints

Para el producto Symantec Data Loss Prevention for Endpoint, los módulos Symantec DLP Endpoint Discover y Symantec Endpoint Prevent controlan los datos en uso. Estos módulos realizan escaneo, detección y monitoreo local para máquinas macOS, Windows 7, Windows 8 y Windows 10.

En los puntos finales, estos módulos también monitorean y controlan las carpetas de sincronización de almacenamiento en la nube, los clientes de correo electrónico de Outlook y Lotus Notes, el tráfico de los protocolos HTTP / HTTPS y FTP, los medios de almacenamiento extraíbles, como USB, protocolo de transferencia de medios, CompactFlash y tarjetas SD, más eSATA y FireWire para unidades portátiles. Los módulos también monitorean y controlan escritorios virtuales, como Citrix, Microsoft Hyper-V y VMware.

Los datos en movimiento son tratados por Symantec DLP Network Monitor, Network Prevent para correo electrónico y Network Prevent para Web. Los datos en reposo se controlan mediante Symantec DLP Network Discover, Network Protect, Data Insight y el portal de autoservicio de Data Insight[90].

11.7.3 Funciones de la nube

[89] Hayes Bill. Symantec Data Loss Prevention. [En línea]. 2017. [Consultado: 03 de mayo 2021].
[90] Ibid., p. 2.

La suite admite implementaciones en la nube con Symantec DLP para Cloud Storage y Cloud Prevent para Microsoft Office 365.

Symantec DLP para almacenamiento en la nube es una herramienta de datos en reposo que analiza las cuentas de Box Business y Enterprise. Puede ayudar a determinar dónde se almacena la información confidencial, cómo se utiliza y quién la recibe. Se puede configurar para ayudar a los usuarios a corregir las infracciones de políticas colocando etiquetas visuales en los archivos de Box para que los usuarios puedan remediar las infracciones de políticas mediante el portal de autoservicio de Symantec DLP.

La función Cloud File Sync and Share evita que los usuarios sincronicen archivos de datos confidenciales desde su escritorio con sitios para compartir archivos en la nube como Box, Dropbox, Google Drive, Hightail, iCloud y Microsoft OneDrive.

Mientras tanto, Symantec DLP Cloud Prevent para Microsoft Office 365 supervisa y controla los correos electrónicos enviados desde instancias de Microsoft Office 365 de Microsoft Exchange Online. Funciona con las políticas actuales de Symantec DLP para Exchange, lo que permite a una organización migrar sus servidores Exchange a la nube[91].

La empresa consultora Gartner prevé que para el año 2022, el 60% de las organizaciones involucrarán a los propietarios de líneas de negocios cuando elaboren su estrategia de prevención de pérdida de datos (DLP). En comparación con el 15% actual.

Para 2020, el 85% de las organizaciones implementará al menos una forma de DLP integrado. Comparándolo con el 50% actual.

Para 2022, la mayoría de los ingresos del mercado de DLP estarán impulsados por productos DLP integrados, a diferencia de los sistemas DLP empresariales[92].

De acuerdo con predicciones de mercado realizadas por la empresa The Radicati Group “Las organizaciones de todos los tamaños continúan invirtiendo fuertemente en soluciones DLP para proteger los datos y garantizar el cumplimiento. Se espera que los ingresos mundiales de las soluciones DLP aumenten de más $ 1.2 mil millones en 2019, a casi $ 2.3 mil millones para 2023”[93].

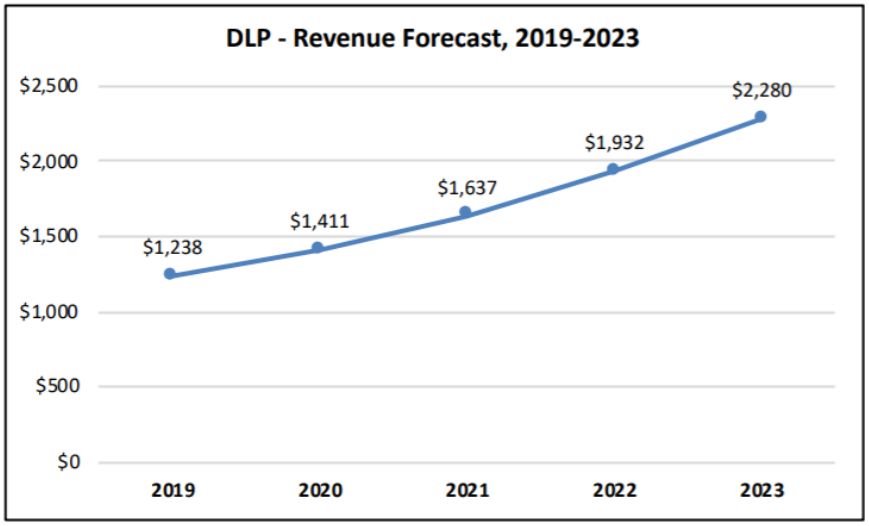
---

[91] Ibid., p. 3.

[92] TECNOZERO. Cuadrante de Gartner para Data Loss Prevention 2017. Predicciones de Data Loss Prevention según Gartner. [Sitio web]. Madrid. 2017. [Consulta: 06 mayo 2021]. Disponible en: https://www.tecnozero.com/dlp/cuadrante-de-gartner-para-data-loss-prevention-2017/

[93] THE RADICATI GROUP, INC. Data Loss Prevention--Market Quadrant 2019. MARKET SEGMENTATION – DATA LOSS PREVENTION. California. [Sitio web]. 2019. p.6. [Consulta: 06

Figura 8. Previsión de ingresos de DLP.



Fuente: The Radicati Group, Inc. Ingresos mundiales de las soluciones DLP $ 1.2 mil millones en 2019, a casi $ 2.3 mil millones para 2023. [En línea]. THE RADICATI GROUP, INC. California. Disponible en: https://www.tecnozero.com/wp-content/uploads/2020/06/radicatti-dlp-2019.pdf

11.8 TENDENCIAS CLAVE DE LOS CUADRANTES DEL MERCADO

De acuerdo con un análisis de mercado realizado por The Radicati Group, Inc.

- "Los mejores jugadores en el mercado de prevención de pérdida de datos en la actualidad son Symantec, Digital Guardian, y McAfee.
- El cuadrante de los Trail Blazers incluye CoSoSys.
- El cuadrante de especialistas incluye Fidelis Cybersecurity, Clearswift, Zecurion, Safetica, SearchInform y Falcongaze.
- El cuadrante de jugadores maduros incluye Forcepoint"[94].

11.8.1 Symantec DLP

Cubre la nube, el Endpoint, la red y el almacenamiento, así como un Symantec DLP Enterprise Suite combinado.

---

mayo 2021]. Disponible en: https://www.tecnozero.com/wp-content/uploads/2020/06/radicatti-dlp-2019.pdf.

[94] Ibid., p.11.

FORTALEZAS

- Symantec ofrece una solución DLP sofisticada y completa que puede ayudar a cumplir con necesidades complejas de empresas de todos los tamaños.
- Symantec DLP ofrece un sólido conjunto de tecnologías de detección de contenido a través de capacidades como aprendizaje automático, huellas digitales, reconocimiento de imágenes y etiquetado.
- La solución DLP de Symantec incluye una serie de capacidades clave, como clasificación de datos, gestión de derechos digitales y cifrado, y análisis de comportamiento de entidades de usuario (UEBA).
- Symantec DLP está completamente integrado con componentes clave de la cartera de productos de Symantec, en particular, CloudSOC (CASB), seguridad de correo electrónico, seguridad de punto final y seguridad web.
- Los clientes pueden beneficiarse de una arquitectura y aplicación de políticas coherentes en múltiples canales de posible pérdida de datos.
- Las soluciones Symantec DLP están disponibles en todos los factores de forma, incluso en las instalaciones y administradas en la nube. Esto es importante para los clientes que es posible que no puedan migrar a la nube debido a requisitos reglamentarios y prefieren soluciones locales o soluciones híbridas.

DEBILIDADES

- Symantec puede ser algo más caro que otras soluciones DLP del mercado. Sin embargo, ofrece un amplio conjunto de funciones que, cuando se integra completamente con otros dispositivos de Symantec las soluciones de seguridad brindan importantes beneficios de protección.
- Si bien Symantec ofrece una amplia cartera de soluciones de seguridad de datos, puede ser algo complejo de administrar para organizaciones con menos recursos. Las empresas más pequeñas pueden confiar en servicios administrados ofrecidos a través de socios de Symantec.
- Si bien Symantec continúa innovando en este espacio y tiene un fuerte reconocimiento de marca, es percibido como más centrado en las necesidades de los clientes empresariales que los de los pequeños a clientes del mercado medio[95].

[95] Ibid., p.13.

11.8.2 Digital Guardian

Proporciona software de prevención de pérdida de datos destinado a detener amenazas internas y externas en dispositivos terminales, redes corporativas, servidores, bases de datos y basados en la nube Ambientes.

FORTALEZAS

- La plataforma de protección de datos de Digital Guardian protege los datos confidenciales contra las amenazas externas utilizando el mismo agente, dispositivo de red y consola de administración. También permite a las empresas marcar los datos como confidenciales en función del contexto en el que se crearon, y luego se basa en esta información contextual para 'seguir' los datos para que los controles apropiados puedan aplicarse para evitar la salida de información sensible.

- El agente de punto final de nivel de kernel de Digital Guardian está disponible para Windows, macOS y Linux.
- Digital Guardian ofrece una aplicación móvil para una visualización segura de documentos, a través de iTunes store, que permite a los usuarios ver documentos cifrados de MS Office, Apple iWork, texto o PDF en dispositivos iOS.
- Digital Guardian Endpoint DLP se basa en eventos, donde los agentes comienzan a recopilar información sobre el movimiento de datos en el momento de la implementación, en lugar de requerir políticas definidas que pueden ser más difícil de construir.
- Digital Guardian admite una amplia gama de integraciones, como SIEM, CASB, cifrado, fuentes de inteligencia de amenazas, entornos de prueba de red y, además de conectarse con la web y el correo electrónico pasarelas de seguridad a través de ICAP.
- Las capacidades UEBA de Digital Guardian mejoran aún más su capacidad para detectar riesgos o sospechas comportamiento del usuario[96].

DEBILIDADES

- Digital Guardian tiene capacidades limitadas de DLP móvil, por lo que los clientes deberían confiar en administración de dispositivos móviles (MDM) o administración de aplicaciones móviles (MAM) soluciones existentes.

[96] Ibid., p.16.

- Digital Guardian puede admitir el almacenamiento y la colaboración de archivos en la nube, pero solo para los proveedores como Box, Accellion, Citrix Share File, Office 365, One Drive y otros.
- El soporte para aplicaciones en la nube como Salesforce.com, está disponible actualmente solo a través de un Proveedor CASB. Digital Guardian se asocia e integra con soluciones CASB populares, incluidos Netskope y Bitglass.
- Mientras que Digital Guardian se integra con Microsoft Office 365 para ofrecer Azure de Microsoft Capacidad de gestión de derechos digitales de protección de la información, no ofrecen DRM nativo.
- El dispositivo DLP de red de Digital Guardian (de la adquisición de Code Green Networks) aún no se ha integrado completamente con su solución DLP de punto final, lo que requiere clientes de punto final y DLP de red para escribir políticas independientes.

MCAFEE

McAfee es una empresa de ciberseguridad de dispositivo a nube que ofrece soluciones y servicios de seguridad para organizaciones empresariales y consumidores. La empresa brinda soluciones que protegen endpoints, redes, servidores, nube y más.

FORTALEZAS

- McAfee DLP está integrado con McAfee MVISION Cloud (su oferta CASB), lo que ayuda Las organizaciones extienden fácilmente las políticas de DLP a la nube. Políticas comunes de protección de datos se puede crear en varios entornos, con las mismas etiquetas de clasificación de datos compartidas para que garantice una detección constante de pérdida de datos desde el dispositivo a la nube.
- McAfee ePolicy Orchestrator proporciona una gestión de flujo de trabajo de incidentes de panel único, así como también permite la administración de políticas comunes en los terminales, la red y la nube DLP.
- La base de datos de Capture incluida en la solución McAfee DLP registra todos los datos en movimiento y ofrece análisis valiosos a los administradores sobre cómo se utilizan y envían los datos. También es útil para fines forenses[97].

[97] Ibid., p.18.

- La solución McAfee DLP ofrece clasificación automática y manual por parte de los usuarios finales. La clasificación manual, que se incluye de forma gratuita en la licencia de DLP Endpoint, ayuda a aumentar conciencia de la protección de datos del usuario final y aliviar la carga administrativa.
- El paquete DLP incluido de McAfee, McAfee Total Protection for DLP, incluye todos los DLP componentes con descuento. Además, funciones como Clasificación manual y Prevención de DLP para el correo electrónico móvil se han agregado las licencias existentes de forma gratuita. McAfee Device Control es también se incluye en la licencia de McAfee DLP Endpoint.

DEBILIDADES

- Actualmente, McAfee DLP no ofrece soporte de agente para Linux.
- McAfee DLP no ofrece actualmente funciones específicas para la detección de DLP por goteo. Mientras tal la detección se puede configurar a través de reglas, los clientes con los que hablamos indicaron que es algo incómodo.
- Aunque ofrece un amplio conjunto de funciones, McAfee DLP requiere un equipo de TI experimentado para Instale y mantenga correctamente la solución de manera que aproveche al máximo sus capacidades.
- Si bien es rico en funciones, una implementación con todas las funciones de McAfee DLP tiende a ser algo más caro que las soluciones de la competencia[98].

FORCEPOINT

Forcepoint ofrece DLP, web, datos y correo electrónico seguridad de contenido, seguridad de acceso a la nube, firewall de próxima generación, análisis del comportamiento del usuario, información privilegiada detección de amenazas y soluciones de protección contra amenazas para organizaciones de todos los tamaños.

FORTALEZAS

- Forcepoint admite la implementación de componentes de clasificación de datos y administración de DLP en las instalaciones y en las nubes públicas (es decir, Microsoft Azure y Amazon AWS) [99].

[98] Ibid., p.19.
[99] Ibid., p.40.

- Además de Microsoft Windows, Forcepoint también ofrece soporte para Apple macOS y Sistemas Linux, incluida la detección de datos estructurados y no estructurados con huellas dactilares.
- La integración con Forcepoint CASB permite que las políticas de DLP se extiendan a la nube empresarial aplicaciones a través de un servicio alojado en la nube. Este enfoque híbrido permite incidentes y análisis forense. Los datos se protegerán en un centro de datos privado, mientras que la aplicación de políticas se puede realizar en la nube.
- Forcepoint proporciona detección de DLP por goteo en el punto final, la nube y la red DLP componentes.
- Forcepoint proporciona una solución de análisis de seguridad integrada que se utiliza para identificar altas interacciones de riesgo con datos confidenciales y presentar una vista priorizada de los casos de DLP con riesgo puntuaciones a los equipos de operaciones de seguridad.

DEBILIDADES

- Forcepoint OCR está actualmente limitado al descubrimiento de redes y datos en movimiento (es decir, web, correo electrónico e ICAP). Forcepoint planea extender el soporte de OCR a componentes DLP adicionales a medida que parte de su hoja de ruta.
- Las capacidades de Forcepoint DLP Endpoint para Linux no están actualmente tan desarrolladas como otros sistemas operativos.
- Forcepoint actualmente solo proporciona capacidades de cifrado integrado de datos en movimiento para media removible. También admite el cifrado de correo electrónico cuando se combina con Forcepoint Email Seguridad.
- Forcepoint ha perdido visibilidad en el mercado el año pasado y no se ve en acuerdos con tanta frecuencia como otros proveedores[100].

[100] Ibid., p.41.

12. ESTRATEGIA DE SEGURIDAD DE INFORMACIÓN BASADA EN LA APLICACIÓN DLP, APOYADA CON CONTROLES QUE SE PUEDAN IMPLEMENTAR PARA PREVENIR LA FUGA DE INFORMACIÓN EN LAS ORGANIZACIONES.

La principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando, pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad.

Como parte de la estrategia de seguridad es conveniente seguir unos lineamientos que permiten fortalecer los procesos que estén relacionados con los activos de información, para esto es importante estar orientado por las mejores normas y estándares de seguridad, es por esto por lo que la norma ISO 27001: 2013 cumple con las especificaciones necesarias que aportan a la seguridad que se pretende ejercer con el sistema DLP – Data Loss Prevention.

Para conocer que solución queremos implementar es necesario realizar una evaluación de riesgos de la seguridad de la información. Para esto, la norma ISO 27001 del 2013 nos indica que como paso inicial se debe definir el Sistema de Gestión de Seguridad de la información para identificar ¿qué información se requiere proteger? Paso que es muy importante para la implementación de un DLP – Data Loss Prevention, ya que permitirá definir las políticas y parámetros para que la información se encuentre custodiada, monitoreada y minimice su filtración.

12.1 EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

- “Identificamos nuestros activos de información determinando las salidas de información de esos activos.
- Clasifique información y establezca una prioridad sobre esa información. Por ejemplo, los registros financieros y las contraseñas se clasifican como “información confidencial”.
- Estos luego evalué la prioridad de cada tipo de información mediante una puntuación o valoración del riesgo.
- Finalmente defina los controles necesarios para asegurar la información que supere determinado nivel de riesgo establecido según los criterios de riesgo de la organización”[101].

[101] ISO27001. OPERACIÓN EN ISO 27001. Evaluación de Riesgos de Seguridad de la Información. [Sitio web]; Madrid. 2021. P.8. [Consulta: 12 mayo 2021]. Disponible en: https://normaiso27001.es/operacion-en-iso-27001/#h2.

12.1.1 CONTROL DE CAMBIOS

La norma nos pone ahora requisitos para controlar el cambio. En otras palabras, nos tenemos que pensar cómo vamos a manejar los cambios ya sean planificados o no. Para cumplir con el estándar, debe poder demostrar que ha identificado los efectos que el cambio puede tener en sus sistemas, que ha implementado algunas acciones para ayudar a disminuir cualquier impacto. ¡Y por supuesto todo hay que documentarlo!

Se trata de gestionar cualquier evento que se produzca dentro del ámbito de la seguridad de la información, cualquier cambio programado o no que pueda afectar a la seguridad de la Información (Actualizaciones etc.).

Para ello deberemos registrar o documentar

- Los procedimientos o procesos de cambios controlados
- Los eventos en la seguridad de la información
- Las auditorias y sus resultados
- Las reuniones para la revisión de los sistemas de información y objetivos del SGSI.

Manteniendo esta información al día estamos realmente recopilando las evidencias de cualquier evento en la seguridad de la información, lo que nos permitirá retroceder a través del tiempo lo que sea necesario para investigar las causas para identificar rápidamente cuando algo no funciona y hacer los cambios necesarios para estar al tanto de los requisitos del SGSI.

También será necesario mantener copias de seguridad de nuestros registros.

12.1.2 CÓMO CREAR Y GESTIONAR EL PROCESO DE TRATAMIENTO DEL RIESGO.

El plan de tratamiento de riesgos puede ser simplemente un documento donde se recoge la descripción de las actividades a realizar y donde se establezca la trazabilidad entre las medidas a implantar y los riesgos que cada una de ellas pretende mitigar.

Además, un plan de tratamiento de riesgos debe determinar no solo las actividades a realizar sino las acciones y los responsables de realizarlas junto con los indicadores o métodos para medir o evaluar el grado de cumplimiento de las acciones a emprender[102].

[102] Ibib., p.3.

Otro aspecto importante es la evaluación del esfuerzo necesario para obtener las medidas y registros. Para ello se recomienda ajustarse a un conjunto de métricas inicial que no suponga un esfuerzo no asumible para la organización y sea más un motivo de desánimo que una tarea asumida por la organización.

- Confidencialidad: reducir el número de incidentes con riesgo de fuga de información.
- Disponibilidad: porcentaje de disponibilidad de determinados equipos y sistemas.

Integridad: reducir los incidentes por información errónea.

12.2 CONTROL DE ACCESO

Las medidas de control de accesos de la norma ISO 27001 están orientadas a controlar y monitorizar los accesos a los medios de información de acuerdo con las políticas definidas por la organización.
Los propietarios de los activos son los que deben determinar estas normas o políticas de control de acceso de acuerdo con la política de seguridad de la información y el análisis de riesgos

El principio básico para la elaboración de estas reglas es:

- La asignación de la menor cantidad de privilegios posibles para llevar a cabo una tarea dentro de un sistema de información.
- La concesión de esos privilegios solamente por el tiempo que sea necesario para el desarrollo de las tareas.

Se deben asignar los permisos de acceso limitados solamente a la información necesaria para hacer un trabajo, tanto a nivel físico (accesos a instalaciones o soportes de información), como lógicos (Accesos a aplicaciones). Este control es la base de funcionalidad de las soluciones DLP es por esto por lo que los controles de acceso determinados por la norma ISO 27001 del 2013 son los lineamientos indicados para implementar en los sistemas DLP.

El objetivo de la política de control de acceso debería ser que todo está prohibido a menos que esté expresamente permitido y no al revés.

12.3 ASIGNACION DE ROLES

Los roles dentro de un sistema de Información nos informan de lo que un usuario está autorizado a hacer dentro de un sistema y de lo que no le está permitido[103].

[103] ISO 27001. CONTROL DE ACCESO. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO. [Sitio web]; Madrid. 2020.p.3. [Consulta: 12 mayo 2021]. Disponible en: https://normaiso27001.es/a9-control-de-acceso/.

Cada rol no solo tiene una serie de privilegios distintos, sino que además existe un mayor nivel de riesgo en un Rol de administrador que en un rol de colaborador. Es por ello por lo que el nivel de confianza juega un papel importante en los requisitos que deberemos exigir a dichas funciones en relación con la Seguridad de la Información.

De esta forma aplicando los principios sobre la asignación de privilegios deberemos hacernos estas preguntas antes de asignar privilegios a un usuario de sistemas de información:

- ¿Cuáles son los mínimos privilegios que puedo asignar a un puesto de trabajo con tal que le permita realizar sus tareas?
- ¿Durante cuánto tiempo es necesario que tenga estos privilegios?
- ¿Resulta pactico y es posible asignar estos privilegios solamente durante el tiempo que está realizando los trabajos?

12.4 GESTIÓN DE ACCESO A LOS USUARIOS

Se trata de un requisito para la gestionar la autorización de los usuarios que acceden a los recursos de red.

La política de “gestión de acceso de usuarios de red” debe determinar a qué información se puede acceder, los procedimientos de autorización, los controles de gestión para la protección de las redes, las conexiones de red permitidas (p. Ej., No mediante wifi), los requisitos de autenticación y la supervisión del uso.

Un proceso de control de acceso robusto pasa por los siguientes puntos realizados según la secuencia de:

Identificación: métodos para proporcionar un sujeto (entidad que solicita acceso) con una identidad reconocible (por ejemplo, ID usuario o cuenta de usuario, IVA, número de seguro social, pasaporte, etc.).

Autenticación: métodos para garantizar que un sujeto sea quien dice ser (por ejemplo, contraseña, token, huella digital, etc.). Autorización: métodos para controlar qué acciones puede realizar un sujeto en un objeto (entidad a la que se accede) (por ejemplo, lista de permisos de materia y lista de permisos de objetos).

Con respecto a los métodos de autenticación, los siguientes conceptos (o factores) se pueden usar, por separado o en combinación[104]:

- Algo que sabe un sujeto: por ejemplo, contraseñas y PIN. Este es el menos costoso de implementar y el menos seguro.

[104] Ibib., p.4.

- Algo que tiene un sujeto: por ejemplo, tarjetas inteligentes, fichas, llaves, etc. Caro, pero seguro.
- Algo que un sujeto es: por ejemplo, patrones de voz, retina, huella digital, etc. Este es el más costoso de implementar, y el más seguro.

La norma nos proporciona los elementos a considerar en la definición de la política de acceso de usuarios a la red.

La política debe identificar:

- La red y servicios a los cuales se accede.
- Los procedimientos de autorización.
- Que controles tienen estos procedimientos.
- Los medios por los cuales se accede (VPN, Wifi etc.).
- Los requisitos de autenticación.
- Como se supervisa el uso de los servicios de red.

De acuerdo con lo mencionado por escuela europea excelencia "El propósito inmediato es definir cuál es la información que la organización pretende proteger. Entonces, con este objetivo, no es necesario considerar el formato en el que se almacena la información, cuál es su ubicación ni si se resguarda en alguna instalación de la organización o en la nube"[105].

12.5 FRENTES DE SEGURIDAD INFORMATICA

Para garantizar una óptima protección de los sistemas de una organización es necesario conocer los eslabones donde se va a ejercer el control, identificando estos aspectos se procederá con el análisis, ejecución y aplicación de herramientas y estrategias que fortalezcan cada uno de estos medios.

12.5.1 Los usuarios

Son considerados como el eslabón más débil de la cadena, ya que a las personas es imposible de controlar, un usuario puede un día cometer un error y olvidar algo o tener un accidente y este suceso puede echar a perder el trabajo de mucho tiempo, en muchos casos el sistema y la información deben de protegerse del mismo usuario.

[105] ESCUELA EUROPEA DE EXCELENCIA, Cómo definir el alcance del Sistema de Gestión de Seguridad de la Información (SGSI), ¿Cuál es el propósito del alcance del Sistema de Gestión de Seguridad de la Información? [Sitio web]; Madrid, 2020. [Consulta: 15 mayo 2021]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2018/12/como-definir-el-alcance-del-sistema-de-gestion-de-seguridad-de-la-informacion-sgsi/

12.5.2 La información

Se considera como el oro de la seguridad informática ya que es lo que se desea proteger y lo que tiene que estar a salvo, en otras palabras, se le dice que es el principal activo.

12.5.3 La infraestructura

Este puede ser uno de los medios más controlados, pero eso no implica que sea el que corre menos riesgos, siempre dependerá de los procesos que se manejan. Se deben de considerar problemas complejos, como los de un acceso no permitido, robo de identidad, hasta los daños más comunes, por ejemplo, robo del equipo, inundaciones, incendios o cualquier otro desastre natural que puede tener el material físico del sistema de la organización[106].

Para potencializar la seguridad de estos tres aspectos es importante tener en cuenta las soluciones Data Loss Prevention (prevención de pérdida de datos), se emplean para prevenir y corregir las vulnerabilidades de un sistema cuando son diagnosticadas y reducir las amenazas vinculadas a la falta de seguridad informática. También te permiten definir políticas para que la data de carácter confidencial no salga de la compañía. Al respecto, existen tres tipos de soluciones DLP que debes conocer:

- Network DLP: Monitorea, rastrea y genera informes de todos los datos de tráfico en la red de la empresa. En términos generales, te permite saber qué información está siendo utilizado, por quién está siendo accedida y hacia dónde se dirige o de dónde proviene.

- Storage DLP: Te permite visualizar archivos confidenciales almacenados y compartidos por los colaboradores que tienen acceso a la red de la empresa. Así, puedes identificar puntos sensibles y prevenir las filtraciones de información.
- Endpoint DLP: Se instala en todas las estaciones de trabajo y dispositivos empleados por los colaboradores para supervisar e impedir la salida de datos sensibles en dispositivos de almacenamiento extraíbles, aplicaciones para compartir o áreas de transferencia[107].

---

[106] Romero Martha, Figueroa Grace Liliana. Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. [Sitio web]; Alicante: 3Ciencias, 2018. p. 14. ISBN 9788494930614. [Consulta: 17 mayo 2021]. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

[107] Seguridad informática para equipos de cómputo, dispositivos móviles, auditoría y DLP. [Sitio web]; Ciudad de México, D.F. 2019. [Consulta: 22 mayo 2021]. Disponible en: https://arrobasystem.com/pages/seguridad-informatica-para-equipos-de-computo-dispositivos-moviles-auditoria-y-dlp

En caso de un traslado de emergencia forzoso de personal para trabajar desde casa, es necesario encontrar soluciones simples y comprensibles lo antes posible que le permitan trabajar desde casa sin violar la seguridad de la red corporativa, sus recursos de información, la información que circula en el ordenador de casa, así como entre ella y red corporativa.

Como aporte a la seguridad es importante la aplicación de herramientas que garanticen el flujo seguro de los datos cuando se requiera laborar en un entorno externo. Las redes privas virtuales son un apoyo significativo de seguridad y junto a los DLP contribuyen a que los procesos ejecutados se realicen con la mayor confidencialidad, integridad y seguridad[108].

12.6 CONTROLES DE SEGURIDAD

Los controles de seguridad de la información o acceso a los sistemas deben estar soportador por normas y herramientas que establezcan unos lineamientos y restricciones cuyo objetivo es su adecuada administración para que no llegue a fuentes que pudiesen con fines adversos a la misión o visión de la organización.

Dentro de las políticas para tener en cuenta la norma ISO 27001 del 2013 establece que se deben crear unas restricciones de control de acceso la autenticación. Este es un proceso que garantiza y confirma la identidad de un usuario. La autenticación es uno de los aspectos básicos en la seguridad de la información, junto con los tres pilares, a saber: la integridad, disponibilidad, y confidencialidad.

12.6.1 Autenticidad

La autenticación comienza cuando un usuario intenta acceder a la información. Primero, el usuario debe probar sus derechos de acceso y su identidad. Al iniciar sesión en una computadora, los usuarios comúnmente ingresan nombres de usuario y contraseñas con fines de autenticación. Esta combinación de inicio de sesión, que debe asignarse a cada usuario, autentica el acceso. Sin embargo, este tipo de autenticación puede ser evitado por los hackers.

Una mejor forma de autenticación, la biométrica, depende de la presencia del usuario y la composición biológica (es decir, la retina o las huellas dactilares). Esta tecnología hace que sea más difícil para los piratas informáticos ingresar en los sistemas informáticos.

[108] BYTE. Problemas de seguridad en el acceso remoto. [Sitio web]; Madrid, 2021. [Consulta: 22 mayo 2021]. Disponible en: https://revistabyte.es/ciberseguridad/seguridad-de-acceso-remoto/

El método de autenticación de la infraestructura de clave pública (PKI) utiliza certificados digitales para probar la identidad de un usuario. También hay otras herramientas de autenticación, como tarjetas de claves y tokens USB. Una de las mayores amenazas de autenticación ocurre con el correo electrónico, donde la autenticidad suele ser difícil de verificar[109].

La autenticidad es la seguridad de que un mensaje, una transacción u otro intercambio de información proviene de la fuente de la que afirma ser. Autenticidad implica prueba de identidad.

Podemos verificar la autenticidad a través de la autenticación. El proceso de autenticación usualmente involucra más de una "prueba" de identidad (aunque una puede ser suficiente).

12.6.2 DISPONIBILIDAD

Se refiere a la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto.
Cuando un sistema no funciona regularmente, la disponibilidad de la información se ve afectada y afecta significativamente a los usuarios. Además, cuando los datos no son seguros y no están fácilmente disponibles, la seguridad de la información se ve afectada. Otro factor que afecta la disponibilidad es el tiempo. Si un sistema informático no puede entregar información de manera eficiente, la disponibilidad se ve comprometida.

12.6.3 CONFIDENCIALIDAD

La confidencialidad, permite a los usuarios autorizados acceder a datos confidenciales y protegidos. Existen mecanismos específicos garantizan la confidencialidad y salvaguardan los datos de intrusos no deseados o que van a causar daño. La información o los datos confidenciales deben divulgarse únicamente a usuarios autorizados.

Las mejores prácticas utilizadas para garantizar la confidencialidad son las siguientes:

- Un proceso de autenticación, que garantiza que a los usuarios autorizados se les asignen identificaciones de usuario y contraseñas confidenciales. Otro tipo de autenticación es la biométrica.
- Se pueden emplear métodos de seguridad basados en roles para garantizar la autorización del usuario o del espectador. Por ejemplo, los niveles de

[109] ISO27001. Control de acceso en ISO 27002. Madrid. [Sitio web]; 2021. p.3. [Consulta: 25 mayo 2021]. Disponible en: https://normaiso27001.es/a9-control-de-acceso/

acceso a los datos pueden asignarse al personal del departamento específico.

- Los controles de acceso aseguran que las acciones del usuario permanezcan dentro de sus roles. Por ejemplo, si un usuario está autorizado para leer, pero no escribir datos, los controles del sistema definidos pueden integrarse[110].

Los controles de seguridad son medidas de seguridad técnicas o administrativas para evitar, contrarrestar o minimizar la pérdida o falta de disponibilidad debido a las amenazas que actúan por una vulnerabilidad asociada a la amenaza. En esto consiste un riesgo de seguridad.

Los controles administrativos son el proceso de desarrollar y garantizar el cumplimiento de las políticas y los procedimientos. Tienden a ser cosas que los empleados pueden hacer, o deben hacer siempre, o no pueden hacer. Otra clase de controles en seguridad que se llevan a cabo o son administrados por sistemas informáticos, estos son controles técnicos.

Los controles de la fase de actividad pueden ser técnicos o administrativos y se clasifican de la siguiente manera:

- Controles preventivos para evitar que la amenaza entre en contacto con la debilidad.
- Controles de detección para identificar que la amenaza ha aterrizado en nuestros sistemas.
- Controles correctivos para mitigar o disminuir los efectos de la amenaza que se manifiesta[111].

[110] Ibid., p.5.
[111] Ibid., p.14.

Figura 9. Controles Preventivos Detección Correctivos Compensación.

Preventivos	Detección	Correctivos	Compensación
Concienciación en la Seguridad	Sistemas de monitoreo de red	Actualización de Sistema Operativo	Copias de seguridad
Firewalls	IDS	Restaurar copias de respaldo	Servidor de respaldo en caliente
Anti virus	Anti virus	Anti virus	Aislamiento del servidor
Control de accesos	Detectores de Humos / Presencia	Mitigación de la vulnerabilidad	
IPS	IPS		

Fuente. normaiso27001.es. Definición de controles de compen-sación. Madrid. [En línea]. Disponible en: https://normaiso27001es/referencias -normativas-iso-27000/**.**

El primer paso es identificar los dispositivos y activos (incluyendo los datos) que deben ser protegidos y monitorearlos. No es posible proteger un activo si no sabemos que este existe, por ello es indispensable tener visibilidad de todos los activos que pertenecen a la organización y que tienen acceso a los recursos de esta. Esto nos ayudará a identificar la superficie de ataque que debemos proteger y cómo debemos hacerlo.

- Implementar sistemas de autenticación para garantizar que solo los dispositivos y usuarios autorizados tengan acceso a los recursos de la red.

- Monitorear el estado de la instalación de parches y actualizaciones de cada sistema/host.

- Implementar servicios y protocolos seguros (HTTPS, SSH, SCP o SFTP, DoH/DNSSEC, SMTP, POP3 o IMAP sobre SSL/TLS). Evitar protocolos que no fueron concebidos para ser seguros. Por ejemplo, HTTP, telnet, rsh, FTP o DNS.

- Prestar atención a servicios y puertos que permitan la administración de los sistemas en la red (RDP, SSH, VNC, webmin, portales web, concentradores VPN, routers y gateways) [112].

[112] WELIVESECURITY. Defensa en profundidad: cómo implementar esta estrategia de ciberseguridad. [Sitio web]; Bratislava, 2021. [Consulta: 23 mayo 2021]. Disponible en: https://www.welivesecurity.com/la-es/2021/03/26/defensa-profundidad-que-es-como-implementar-estrategia-ciberseguridad/

- Siempre que sea posible, implementar soluciones de autenticación centralizadas (Kerberos, RADIUS, TACACS) y soluciones de 2FA/MFA, sobre todo frente a servicios y activos que están expuestos directamente en Internet o en la DMZ.

- Monitorear los controles de acceso y el comportamiento de los usuarios con permisos administrativos.

- Utilizar contraseñas robustas y complejas (más de 12 caracteres alfanuméricos y símbolos).

- Configurar la vida máxima y expiración de las contraseñas (al menos cada 2 meses).
- Bloquear las cuentas de los usuarios luego de cierta cantidad de inicios de sesión fallidos (Ejemplo: 8 intentos).

- Agregar métodos de autenticación adicionales (MFA) siempre que sea posible: 2FA, llaves físicas, autenticación biométrica.

- No compartir las contraseñas y los accesos con ninguna otra persona.

- Asegurarse que los equipos y distintos servicios utilicen una verbosidad de logueo suficiente para que los eventos de seguridad registrados proporcionen información detallada.

- Deshabilitar consultas por métodos obsoletos como HTTP 1.0.

- Implementar SSL/TLS con suites de cifrado robustas y deshabilitar SSL v2 y v3[113].

De acuerdo con lo mencionado por escuela europea excelencia “El propósito inmediato es definir cuál es la información que la organización pretende proteger. Entonces, con este objetivo, no es necesario considerar el formato en el que se almacena la información, cuál es su ubicación ni si se resguarda en alguna instalación de la organización o en la nube”[114].

[113] Ibid., p. 1.
[114] ESCUELA EUROPEA DE EXCELENCIA, Cómo definir el alcance del Sistema de Gestión de Seguridad de la Información (SGSI), ¿Cuál es el propósito del alcance del Sistema de Gestión de Seguridad de la Información? [Sitio web]; Madrid, 2020. [Consulta: 23 mayo 2021]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2018/12/como-definir-el-alcance-del-sistema-de-gestion-de-seguridad-de-la-informacion-sgsi/

13. CONCLUSIONES

La investigación realizada logro dimensionar que las organizaciones tienen una seguridad aceptable en sus instalaciones físicas lo cual permite un funcionamiento seguro de los sistemas de comunicación en pro de los procesos que la conforman. En consecuencia, las falencias se hicieron notables en el periodo de pandemia donde se tuvo que optar por el trabajo remoto evidenciando que en esta otra forma de trabajo no se había establecido mecanismos ni lineamientos lo suficientemente seguros para la protección de los activos de información.

El principal problema que creo entornos inseguros en el trabajo remoto se vio relacionado además de los mínimos controles establecido por el área de IT, fue la no culturización de los empleados en cuanto a la administración de las herramientas que tenían bajo su responsabilidad, esto se pudo observar en el uso que se les dio fuera de lo laboral, realizando otras actividades que respectan a lo personal, accediendo a sitios web como redes sociales que en su momento eran el foco principal de los ciberatacantes que aprovechaban estos descuidos para iniciar ataques de ingeniería social, tomando control de los dispositivos para posteriormente sustraer información entre otras actividades delictivas.

Como solución de seguridad informática los DLP (Data Loss Prevention) quedo mostrado que son herramientas idóneas para el monitoreo y control de la información , la cual ofrece alternativas de acuerdo con las necesidades de las organizaciones en cuanto a seguridad de la información, con servicios que se integran con todo el sistema de comunicaciones, como infraestructura de almacenamiento, la nube, puntos finales y puertas de enlace de la red permitiendo una seguridad mucho más efectiva haciendo posible que haya un enfoque especial sobre la información, detectando y aplicando acciones de bloqueo de acuerdo con la confidencialidad del activo.

Las herramientas DLP además de que proporcionan mecanismos de seguridad para la filtración de la información, también tienen la funcionalidad de orientar al empleado a tomar las mejores decisiones en cuanto a la administración de la información, esto se pudo evidenciar cuando por medio de alertas informa cual es la opción más indicada de elegir al momento de que se haya realizado una acción que va en contra de los lineamientos corporativos de seguridad de la información. Se presenta como un guía que a la vez supervisa las acciones que no están al alcance de los controles sobre la información como la inserción de memorias USB, transferir información a servicios de la nube entre otros.

Teniendo en cuenta la investigación realizada se concluye que como estrategia de seguridad es importante la implementación de metodologías como la norma ISO 27001 del 2013 e ISO 27002, metodologías que describen como gestionar la seguridad de la información en una empresa por medio de la evaluación de riesgos y posterior aplicación de mitigación y control del riesgo, teniendo como ejes de seguridad la confidencialidad, integridad y disponibilidad de la información. Estos aspectos de seguridad son aplicables a herramientas de monitoreo y control del flujo de información, tal es el caso de las soluciones DLP (Data Loss Prevention), herramienta que por medio de políticas previamente estipuladas por las normas ISO fortalecen la seguridad de los activos de información ajustándose al objetivo de protección que requiere la empresa.

Las políticas de seguridad que se implementen en los DLP Data Loss Prevention, primero deben estar respaldadas por un estudio de los procesos que conforman la organización, esto con el fin de identificar los requerimientos de protección de la información que se requieren, es decir, se evalúa la importancia y ubicación de los activos que representan un mayor valor, esta implementación de políticas de protección de la información es posible con la integración de la norma ISO 27001 del 2013 la cual por medio del Sistema de Gestión de la Información otorga unos lineamientos de identificación y mitigación el riesgo.

14. RECOMENDACIONES

Las organizaciones deben identificar una metodología de estudio de los procesos que se ajuste a sus necesidades para que esta sea implementada en fin de conseguir el objetivo de seguridad de la información.

Para no permitir la filtración de información es importante que se tenga en cuenta el analizar las soluciones DLP (Data Loss Prevention) con las cuales se pretende ejercer políticas de seguridad en la organización teniendo en cuenta sus características, funcionalidad, efectividad.

Las organizaciones deben tener como objetivo la protección de la información tanto interna como externamente por esto es importante que se identifiquen potenciales amenazas y controles los cuales deben de ir acompañados de soluciones DLP Data Loss Prevention.

BIBLIOGRAFÍA

ACRONIS. Dificultades técnicas que ha encontrado para hacer frente al aumento de empleados que teletrabajo debido a la pandemia. [En línea]. Singapur.2020. P. 7. [Fecha de consulta: 20 mayo 2022]. Disponible en: https://dl.acronis.com/u/rc/WP-Acronis-Cyber-Threats-Report-2020-ES-ES-201203.pdf.

AGUSTINA SANLLEHI, JOSÉ R. Delito en la empresa. Estrategias de prevención de la criminalidad intra-empresarial y deberes de control empresario. Barcelona: Atelier Libros, 2010. p.103. ISBN. 8415929234, 9788415929239.

Arreola Adolfo. Prevenir acceso no autorizado en su red privada en casa. En: Ciberseguridad: ¿Por qué es importante para todos? [En línea]. 1ª ed. Ciudad de México: Universidad Anáhuac, 2019. p. 95. . [Fecha de consulta: 21 octubre 2021]. Disponible en : https://books.google.com.co/books?id=ZqHDDwAAQBAJ&pg=PT4&dq=Arreola+Adolfo&hl=es&sa=X&ved=2ahUKEwi_1MDk-bn0AhWUtDEKHYHfDJ0Q6wF6BAgHEAE#v=onepage&q=Arreola%20Adolfo&f=false

BYTE. Problemas de seguridad en el acceso remoto. [Sitio web]; Madrid, 2021. [Consulta: 22 mayo 2021]. Disponible en: https://revistabyte.es/ciberseguridad/seguridad-de-acceso-remoto/

CIBERNOS. Principales problemas de ciberseguridad en los puestos de teletrabajo. [Sitio web]. [Consulta: 14 de marzo 2022]. Disponible en: https://www.grupocibernos.com/blog/serie-problema-3-ciberseguridad-en-las-empresas-puestos-teletrabajo.

CISCO; Cisco Email Security; DLP y cumplimiento. [Sitio web]. California: Cisco; [Consulta: 24 abril 2021]. Disponible en: https://www.cisco.com/c/dam/global/es_es/pdfs/SEC17Q4Cisco-Email-Security-Descripcion-general.pdf.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”. En: Diario Oficial. Marzo, 2021. Nro.51.609.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1581. (17, octubre, 2012). Protección De Datos Personales. En: Sentencia C-748 de 2011 de la Corte Constitucional.

CN; Guía de Seguridad de las TIC CCN-STIC 1503; Procedimiento de empleo seguro McAfee Data Loss Prevention 11.1 con ePolicy Orchestrator 5.10. [Sitio web]. Madrid. [Consulta: 08 marzo 2021]. Disponible en: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/1000-procedimientos-de-empleo-seguro/5729-ccn-stic-1503-pes-mcafee-data-loss-prevention-11/file.html.

CORERA GORDON. Transformaron la ciberseguridad en Estados Unidos. [Sitio web]. Londres, 20 diciembre 2020. [Consulta: 12 marzo 2021]. Disponible en: https://www.bbc.com/mundo/noticias-internacional-55381892.

DEFENSA EN PROFUNDIDAD: cómo implementar esta estrategia de ciberseguridad. [En línea]. Bratislava, 2021. [Fecha de consulta: 03 de mayo 2021]. Disponible en: https://www.welivesecurity.com/la-es/2021/03/26/defensa-profundidad-que-es-como-implementar-estrategia-ciberseguridad/
Ibid., p. 1.

DAMA International. Conocimiento Para La Gestión De Datos. 2 ed.: Technics Publications, 2010. ISBN 978-163-462-883-9.

DATA WAREHOUSE. [En línea]. California, 2021. [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.oracle.com/co/scm/logistics/warehouse-management/

DE LAS SOLUCIONES DE URGENCIA AL TELETRABAJO PLANIFICADO. [En línea]. Madrid, 2021. [Fecha de consulta: 19 marzo 2021]. Disponible en: https://www.computerworld.es/tendencias/de-las-soluciones-de-urgencia-al-teletrabajo-planificado.

DATAMINING (Minería de datos). [En línea]. Coruña, 2021. [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.sinnexus.com/business_intelligence/datamining.aspx

DLP protege tus datos contra fugas de información. [En línea]. Madrid, 2019. [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/dlp-protege-tus-datos-fugas-informacion

De Molina Alonso. EL IMPACTO DEL DATA WAREHOUSE Y DATA MINING EN LA NUEVA COMUNICACIÓN EMPRESARIAL [en línea]. Lima, 2018. [Fecha consulta: 17 marzo 2021]. Disponible en: https://www.esan.edu.pe/apuntes-empresariales/2018/05/el-impacto-del-data-warehouse-y-data-mining-en-la-nueva-comunicacion-empresarial/#:~:text=En%20este%20contexto%2C%20en%20la,se%20depuran%20los%20datos%20innecesarios.

EL MANEJO DE DATOS POR PARTE DE LAS EMPRESAS CRECIÓ UN 569% DESDE 2016. [en línea]. Madrid, 2019 [Fecha de consulta: 21 marzo 2021]. Disponible en: https://www.computerworld.es/tecnologia/el-manejo-de-datos-por-parte-de-las-empresas-crecio-un-569-desde-2016

EL 73 % DE EMPRESAS NO CUENTA CON MECANISMOS EFICIENTES PARA PROTEGER DATOS DE SUS USUARIOS. [en línea]. Bogotá, 2021. [Fecha de consulta: 15 marzo 2021]. Disponible en: https://www.semana.com/economia/empresas/articulo/el-73-de-empresas-no-cuenta-con-mecanismos-eficientes-para-proteger-datos-de-sus-usuarios/202137/.

Ernst & Young. ¿La ciberseguridad es algo más que protección? Encuesta Global de seguridad de la Información. [Sitio web]. Lima. [Consulta: 23 de marzo 2022]. Disponible en: https://assets.ey.com/content/dam/ey-sites/ey-com/es_co/topics/corporate-social-responsibility/ey-library-la-ciberseguridad-es-algo-mas-proteccion.pdf.

ESCUELA EUROPEA DE EXCELENCIA, Cómo definir el alcance del Sistema de Gestión de Seguridad de la Información (SGSI), ¿Cuál es el propósito del alcance del Sistema de Gestión de Seguridad de la Información? [Sitio web]; Madrid, 2020. [Consulta: 15 mayo 2021]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2018/12/como-definir-el-alcance-del-sistema-de-gestion-de-seguridad-de-la-informacion-sgsi/

ESET. La cuarentena por coronavirus o el cibercrimen: ¿Cuál es la mayor amenaza para las empresas? [Sitio web]. Asunción. [Consulta: 15 marzo 2021]. Disponible en: https://www.eset.com/py/acerca-de-eset/por-que-eset/.

ESTADO ESPAÑOL. CONGRESO DEL ESTADO ESPAÑOL. Ley-Orgánica 10. (23, noviembre, 1995). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “referentes a Delitos Informáticos”. En: BOE. Noviembre, 1995.

FORBES; En América Latina se registran 45 ataques cibernéticos por segundo. [Sitio web]; Ciudad de México, 2019. [Consulta: 12 marzo 2021]. Disponible en: https://www.forbes.com.mx/en-america-latina-se-registran-45-ataques-ciberneticos-por-segundo/.

FORCEPOINT. Forcepoint Data Loss Prevention (DLP). Protección de datos en un mundo sin perímetros. Austin. 2020. p. 5.

FORCEPOINT. [En línea]. Texas, 2021. [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.forcepoint.com/es/why-forcepoint/our-approach

FORCEPOINT; Forcepoint DLP. [Sitio web]. Wisconsin. [Consulta: 22 abril 2021]. Disponible en: https://www.forcepoint.com/sites/default/files/resources/brochures/brochure_forcepoint_dlp_es.pdf

GARCÍA, V. (). Cómo ir hacia un trabajo inteligente. [En línea].Madrid: 05 de marzo de 2021. [Fecha de consulta: 06 de marzo 2021]. Obtenido de: https://revistabyte.es/tema-de-portada-byte-ti/trabajo-inteligente-digital-workspace/.

Gómez, Álvaro. Vulnerabilidad de los sistemas informáticos. En: Auditoría de Seguridad Informática (MF0487_3). [En línea]. Madrid: RA-MA, 2016. p. 18. [Fecha de consulta: 21 octubre 2021]. Disponible en : https://books.google.com.co/books?id=CI-fDwAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false.

GORBEA PORTAL SALVADOR, Madera Jaramillo María de Jesús. Características del data Warehouse. En: Diseño de un data Warehouse para medir el desarrollo disciplinar en instituciones académicas. 72 ed. México: BIBLIOTECOLÓGICA, 2017. P.167.

HAYES BILL. Symantec Data Loss Prevention. [En línea]. 2017. [Consultado: 03 de mayo 2021].

HEREDERO CARMEN DE PABLOS, Hermoso Agius José Joaquín López, Romo Romero Santiago Martín, Medina Salgado Sonia. Organización y transformación de los sistemas de información en la empresa. 4 ed. Madrid: ESIC, 2019. ISBN. 8417513744, 9788417513740.

INCIBE. Ciberseguridad en el teletrabajo. OBJETIVOS DE SEGURIDAD EN EL ACCESO REMOTO. [Sitio web]. [Consulta: 15 de marzo 2022]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf.

INSTITUTO NACIONAL DE CIBERSEGURIDAD ESPAÑA. Guía gestión de fuga de la información. Madrid.: INTECO, 2012.
Instituto Nacional de Ciberseguridad España. Guía gestión de fuga de la información. Madrid.: INTECO, 2012. p.8.
Ibib., p. 10.

INSTITUTO NACIONAL DE CIBERSEGURIDAD ESPAÑA. Guía gestión de fuga de la información. Madrid.: INTECO, 2012. p.9.
Instituto Nacional de Ciberseguridad España. Guía gestión de fuga de la información. Madrid.: INTECO, 2012. p.13.

INTEL. Según estudio la modernización de la computadora personal (PC) es esencial para el futuro del trabajo. [Sitio web]. [Consulta: 14 de mayo 2022]. Disponible en: https://newsroom.intel.la/news/segun-estudio-la-modernizacion-de-la-computadora-personal-pc-es-esencial-para-el-futuro-del-trabajo/.

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. Universidad Estatal del Sur de Manabí. MANABI: Área de innovación y desarrollo, S.L. 2018, primera edición. ISSN 9788494930614.

ISO 27001. CONTROL DE ACCESO. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO. [Sitio web]; Madrid. 2020.p.3. [Consulta: 12 mayo 2021]. Disponible en: https://normaiso27001.es/a9-control-de-acceso/.

ISO 27001. CONTROL DE ACCESO. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO. [Sitio web]. Madrid: ISO. [Consulta: 23 octubre 2021]. Disponible en: https://normaiso27001.es/a9-control-de-acceso/

ISO27001. Control de acceso en ISO 27002. [Sitio web]. Madrid, 2019. [Fecha de consulta: 24 octubre 2021]. Disponible en:https://normaiso27001.es/referencias-normativas-iso-27000/#def31

ISO27001. Control de acceso en ISO 27002. Madrid. [Sitio web]; 2021. p.3. [Consulta: 25 mayo 2021]. Disponible en: https://normaiso27001.es/a9-control-de-acceso/

ISO27001. OPERACIÓN EN ISO 27001. Evaluación de Riesgos de Seguridad de la Información. [Sitio web]; Madrid. 2021. P.8. [Consulta: 12 mayo 2021]. Disponible en: https://normaiso27001.es/operacion-en-iso-27001/#h2.

ISO 27001. OPERACIÓN EN ISO 27001. [Sitio web]. Madrid: ISO. [Consulta: 23 octubre 2021]. Disponible en: https://normaiso27001.es/operacion-en-iso-27001/

Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. [Sitio web]. Universidad Estatal del Sur de Manabí. MANABI: Área de innovación y desarrollo, S.L. 2018, [Fecha de consulta: 20 octubre 2021]. primera edición. ISSN 9788494930614. Disponible en : https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf.

Ivanyuk Alexander. Tendencias de ciberseguridad de 2021, Amenaza de malware general. Berna: Acronis, 2020.p. 18. [Sitio web]. [Consulta: 15 octubre 2021]. Disponible en: https://dl.acronis.com/u/rc/WP-Acronis-Cyber-Threats-Report-2020-ES-ES-201203.pdf.

LA PANDEMIA CONSIGUE QUE TELETRABAJE EL 14,5% DE LA POBLACIÓN CON EMPLEO EN ESPAÑA. [en línea]. Madrid, 2021. [Consulta: 19 marzo 2021]. Disponible en: https://www.computerworld.es/tendencias/la-pandemia-consigue-que-teletrabaje-el-145-de-la-poblacion-con-empleo-en-espana.

LAS 6 MEJORES SOLUCIONES DE PREVENCIÓN DE PÉRDIDA DE DATOS QUE PODRÍAN AHORRARLE MILLONES [en línea] Madrid, 2020. [Fecha de consulta: 20 abril 2021]. Disponible en: https://geekflare.com/es/data-loss-prevention-solutions/

Mendoza Miguel Ángel. Aumentaron 141% los ataques de fuerza bruta al RDP en América Latina. Aumento de ataques de fuerza bruta al RDP. [Sitio web]. Madrid: ESET. 2020. [Consulta: 15 octubre 2021]. https://www.welivesecurity.com/la-es/2020/11/30/aumentaron-ataques-fuerza-bruta-rdp-america-latina/

MCAFEE; Cómo evitar las fugas de datos en su empresa; McAfee DLP Endpoint. [Sitio web]. Madrid. [Consulta: 08 marzo 2021]. Disponible en: https://www.mcafee.com/enterprise/es-mx/assets/solution-briefs/sb-quarterly-threats-sep-2016-2.pdf.

McAfee. McAfee DLP Prevent. Implemente directivas para proteger su información confidencial. [Sitio web]. México DF. McAfee. 2018. p. 1. [Consulta: 01 mayo 2021]. Disponible en: https://www.mcafee.com/enterprise/es-mx/assets/data-sheets/ds-dlp-prevent.pdf.

NETWORK. [En línea]. Ciudad de México, 2021 [Fecha de consulta: 08 mayo 2021]. Disponible en: https://sistemas.com/network.php#

NOD32; Safetica DLP; Características principales. [Sitio web]. Barcelona. [Consulta: 28 febrero 2021]. Disponible: https://www.antivirusnod32.es/dlp-prevencion-de-fugas-de-informacion/safetica-dlp/

PALMA CLAUDIO, Palma Wilfredo, Pérez Ricardo. Data Mining. El arte de anticipar. Santiago: RIL Editores, 2009. P.43. ISBN. 978-956-284-711-7.
PARLAMENTO EUROPEO, el Consejo de la Unión Europea y la Comisión Europea. Reglamento 679. (25, mayo, 2018). Reglamento General de Protección de Datos de la Unión Europea. GDPR.

POLICÍA NACIONAL DE COLOMBIA. Tendencias Cibercrimen Colombia 2019-2020. Bogotá DC. 2020. p. 8-10.
Ibid., p. 14-20-28.

PWC; Encuesta Global sobre Fraude y Delitos Económicos 2020; Las tasas globales de delitos económicos y fraude se mantienen en niveles altos: casi la mitad de las compañías informaron haber sufrido fraude en los últimos dos años; [sitio web]. Buenos Aires. [Consulta: 18 marzo de 2021]. Disponible en: https://www.pwc.com.ar/es/prensa/encuesta-global-sobre-fraude-y-delitos-economicos-2020.html.
Ibid., p. 2.

PROBLEMAS DE SEGURIDAD EN EL ACCESO REMOTO. [En línea]. Madrid, 2021. [Fecha de consulta: 03 de mayo 2021]. Disponible en: https://revistabyte.es/ciberseguridad/seguridad-de-acceso-remoto/.

ROMERO MARTHA, Figueroa Grace Liliana. Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. Alicante: 3Ciencias, 2018. p. 14. ISBN 9788494930614.

Seguridad informática para equipos de cómputo, dispositivos móviles, auditoría y DLP. [Sitio web]; Ciudad de México, D.F. 2019. [Consulta: 22 mayo 2021]. Disponible en: https://arrobasystem.com/pages/seguridad-informatica-para-equipos-de-computo-dispositivos-moviles-auditoria-y-dlp

TECNOZERO. Cuadrante de Gartner para Data Loss Prevention 2017. Predicciones de data loss Prevention según Gartner. [Sitio web]. Madrid. 2017. [Consulta: 06 mayo 2021]. Disponible en: https://www.tecnozero.com/dlp/cuadrante-de-gartner-para-data-loss-prevention-2017/

THE RADICATI GROUP, INC. Data Loss Prevention--Market Quadrant 2019. MARKET SEGMENTATION – DATA LOSS PREVENTION. California. [Sitio web]. 2019. p.6. [Consulta: 06 mayo 2021]. Disponible en: https://www.tecnozero.com/wp-content/uploads/2020/06/radicatti-dlp-2019.pdf.

¿QUÉ ES UN ENDPOINT? Fundamental para Proteger a tu Empresa. [En línea]. México DF, 2020. . [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.accessq.com.mx/que-es-un-endpoint

¿QUÉ ES CLOUD? [En línea]. Madrid, 2021. [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.acens.com/partners/

¿QUÉ HACER DESPUÉS DE UNA FUGA DE DATOS? [en línea]. Ciudad de México, 2014-. [Fecha de consulta: 02 marzo 2021]. Disponible en: https://www.forbes.com.mx/que-hacer-despues-de-una-fuga-de-datos/.

¿QUÉ ES UN DATA WAREHOUSE? [En línea]. Madrid, 2015. [Fecha de consulta: 17 marzo 2021]. Disponible en: https://directortic.es/tecnologia-2/que-es-un-data-

warehouse-
2015022413162.htm#:~:text=La%20funci%C3%B3n%20principal%20de%20un,la%20compa%C3%B1%C3%ADa%20y%20sus%20clientes.

¿QUÉ ES UN DATA WAREHOUSE? [En línea]. Madrid, 2015. [Fecha de consulta: 17 marzo 2021]. Disponible en : https://www.esan.edu.pe/apuntes-empresariales/2018/05/el-impacto-del-data-warehouse-y-data-mining-en-la-nueva-comunicacion-
empresarial/#:~:text=En%20este%20contexto%2C%20en%20la,se%20depuran%20los%20datos%20innecesarios.

REYES F, Seguridad y ciberseguridad ¿Qué hemos aprendido en esta década? ¿Cuáles son los retos a 2030? [En línea]. Bogotá DC: 31 de diciembre de 2020. [Fecha de consulta: 01 de marzo de 2021].Obtenido de: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjNjZaZlprvAhXYcn0KHcviDms4ChAWMAN6BAgGEAM&url=https%3A%2F%2Fsistemas.acis.org.co%2Findex.php%2Fsistemas%2Fissue%2Fdownload%2F14%2F11&usg=AOvVaw1hD0kAT38prJTV86Zj65iN
Se duplicaron ataques a industria por COVID-19: IBM. [en línea]. Ciudad de México, 2021. [Consulta: 18 marzo de 2021]. Disponible en: https://esemanal.mx/2016/06/fortinet-detecta-riesgos-oportunidades/.

Rivas Genesis. Trabajo Remoto: Conoce los Riesgos para tu empresa y cómo mitigarlos. Estadísticas del trabajo remoto. [Sitio web]. Madrid. 2020. [Consulta: 15 octubre 2021]. Disponible en: https://www.gb-advisors.com/es/trabajo-remoto-conoce-riesgos-empresa-mitigarlos/

SEGURIDAD INFORMÁTICA PARA EQUIPOS DE CÓMPUTO, DISPOSITIVOS MÓVILES, AUDITORÍA Y DLP. [En línea]. Ciudad de México, D.F. [Fecha de consulta: 03 de mayo 2021]. Disponible en: https://arrobasystem.com/pages/seguridad-informatica-para-equipos-de-computo-dispositivos-moviles-auditoria-y-dlp.

TELETRABAJAS, PERO ¿CUENTAS CON LAS HERRAMIENTAS NECESARIAS? [En línea]. Madrid: 05 de marzo de 2021. [Fecha de consulta: 06 marzo 2021]. Obtenido de: https://revistabyte.es/noticias/teletrabajar-herramientas/.

TRENDMICRO; DATA LOSS PREVENTION; Una completa solución de prevención frente a la pérdida de datos que reduce los riegos y mejora la

visibilidad. [Sitio web]. Madrid. [03 marzo 2021]. Disponible en: https://www.trendmicro.es/media/ds/data-loss-prevention-datasheet-es.pdf.

TRENDMICRO; Data Loss Prevention; Una completa solución de prevención frente a la pérdida de datos que reduce los riegos y mejora la visibilidad. [Sitio web]. Madrid. [05 marzo 2021]. Disponible en: https://www.trendmicro.es/media/ds/data-loss-prevention-datasheet-es.pdf.

VULNERABILIDAD EN SEGURIDAD INFORMÁTICA. [En línea]. Lima, 2020. [Fecha de consulta: 08 mayo 2021]. Disponible en: https://www.hostdime.com.pe/blog/que-es-una-vulnerabilidad-en-seguridad-informatica-ejemplos/

WELIVESECURITY. Defensa en profundidad: cómo implementar esta estrategia de ciberseguridad. [Sitio web]; Bratislava, 2021. [Consulta: 23 mayo 2021]. Disponible en: https://www.welivesecurity.com/la-es/2021/03/26/defensa-profundidad-que-es-como-implementar-estrategia-ciberseguridad/

ANEXOS

ANEXO A. Intentos de ataque mediante fuerza bruta al RDP.

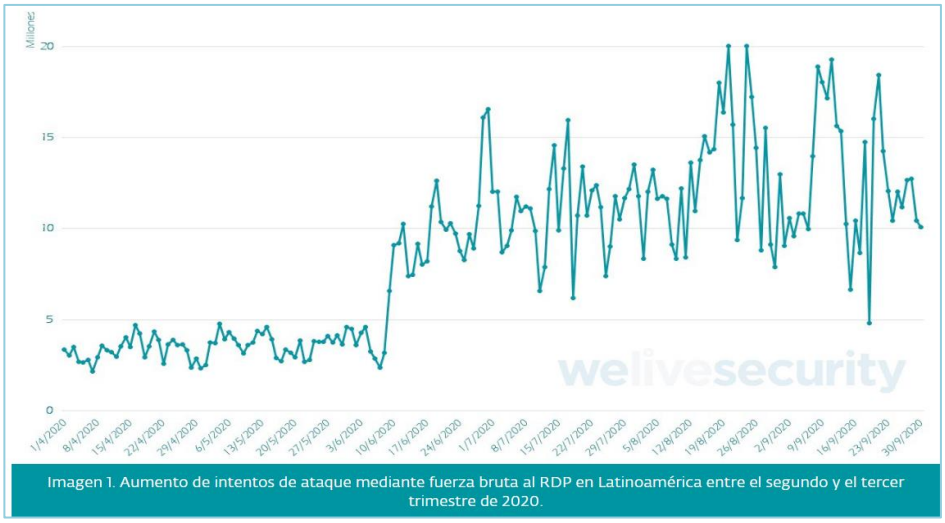
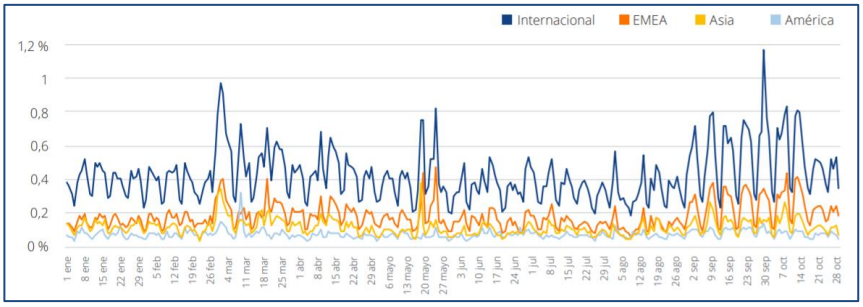


Imagen 1. Aumento de intentos de ataque mediante fuerza bruta al RDP en Latinoamérica entre el segundo y el tercer trimestre de 2020.

ANEXO B. Detecciones de ransomware diarias.



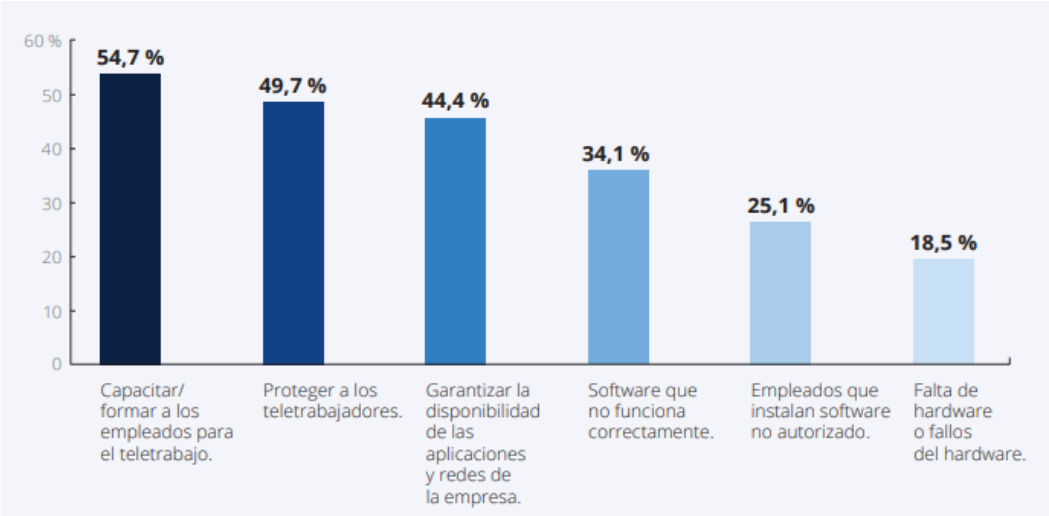
ANEXO C. Sitios web maliciosos.

MES	PORCENTAJE DE USUARIOS que hicieron clic en URL maliciosas
Junio	5,5 %
Julio	5,1 %
Agosto	2,3 %
Septiembre	2,7 %
Octubre	3,4 %

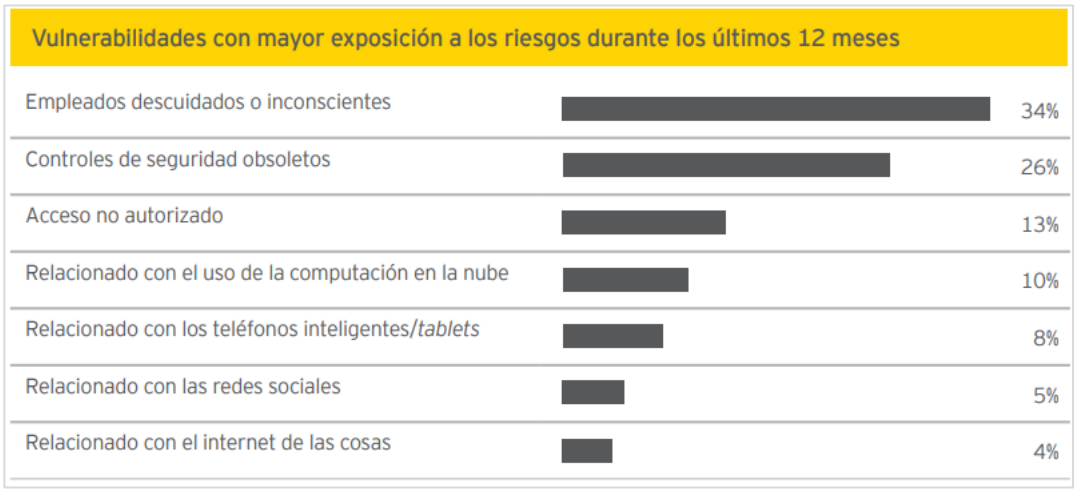
ANEXO D. URL Bloqueadas por países.

CLASIFICACIÓN	PAÍS	PORCENTAJE DE URL BLOQUEADAS EN EL 3.ER TRIMESTRE DE 2020
1	Estados Unidos	16,4 %
2	Alemania	14,1 %
3	República Checa	10,4 %
4	España	8,3 %
5	Reino Unido	6,7 %
6	China	5,8 %
7	Sudáfrica	5,2 %
8	Hong Kong	3,6 %
9	Italia	3,4 %
10	Australia	2,4 %
11	Francia	2,1 %
12	Canadá	2 %
13	Perú	1,9 %
14	Noruega	1,9 %
15	Países Bajos	1,8 %
16	Japón	1,6 %
17	Suiza	1,6 %
18	Bulgaria	0,9 %
19	Singapur	0,8 %
20	Austria	0,7 %

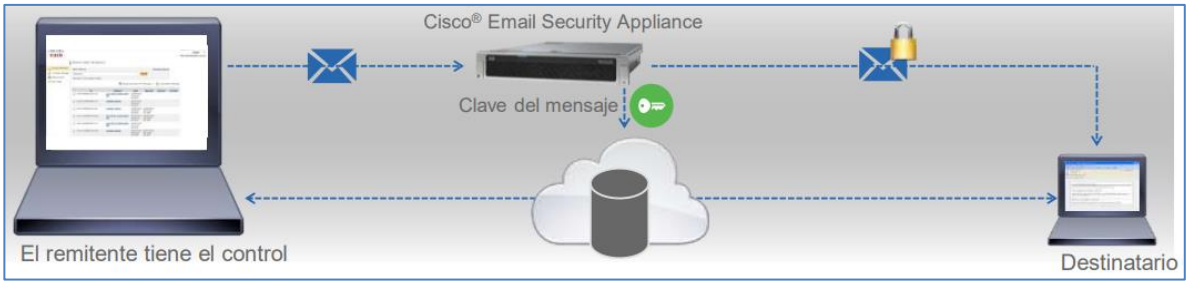
ANEXO E. Informe sobre ciberpreparaciòn 2020.



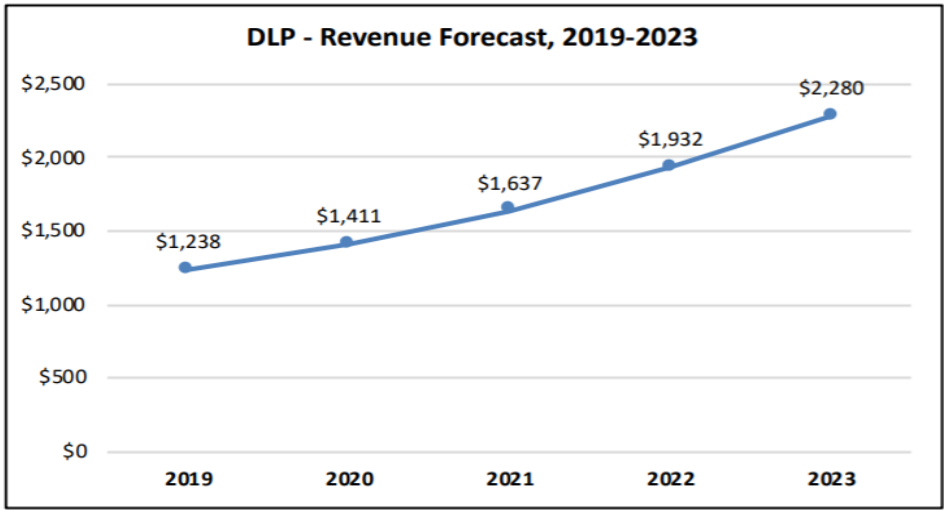
ANEXO F. Vulnerabilidades con mayor exposición a los riesgos.



ANEXO G. Cifrado de sobre de CISCO.



ANEXO H. Previsión de ingresos de DLP.



ANEXO I. Controles Preventivos Detección Correctivos.

Preventivos	Detección	Correctivos	Compensación
Concienciación en la Seguridad	Sistemas de monitoreo de red	Actualización de Sistema Operativo	Copias de seguridad
Firewalls	IDS	Restaurar copias de respaldo	Servidor de respaldo en caliente
Anti virus	Anti virus	Anti virus	Aislamiento del servidor
Control de accesos	Detectores de Humos / Presencia	Mitigación de la vulnerabilidad	
IPS	IPS		