Fecha de elaboración: dd.mm.aaaa [del RAI]			
Tipo de documento	TID:	Obra Creación:	Proyecto Investigación: X
Título	**Lineamientos de seguridad de la información para los documentos electrónicos en la empresa Latinoamericana de Construccione**s		
Autor(es)	**Aristizábal Castro Juan José**		
Tutor(es)	**González Mendieta Fabio Antonio**		
Fecha de finalización	24/04/2023		
Temática	**Trabajo de grado enfocado en generar lineamientos para el manejo adecuado de los documentos electrónicos y garantizar la seguridad de la información.**		
Tipo de investigación	**Estudio de caso**		

Resumen

El estudio de caso se realiza en la entidad Latinoamericana de Construcciones, una empresa dedicada a la infraestructura vial. El objetivo principal del desarrollo de este busca establecer recomendaciones o lineamientos de seguridad de la información basados en las normas ISO y las políticas de seguridad. Este trabajo se desarrollará mediante una investigación cualitativa que describe la situación actual de la compañía respecto a las prácticas de seguridad de la información, esto con la finalidad de generar recomendaciones para el proceso del manejo de la información sobre todo los documentos electrónicos de archivo que se generan en la compañía, teniendo en cuenta que ha sido víctima de ataques informáticos que han puesto en riesgo estos datos.

Palabras clave

Seguridad, Información, Documentos, Informática, Vulnerabilidad, Amenaza, Ataques, Hacker, Hackeo, Metadatos, Base De Datos, Redes, Wifi, Servidores, Software, Hardware, Confidencialidad, Integridad, Disponibilidad.

Planteamiento del problema

La empresa Latinoamericana de Construcciones, es una empresa que se dedica a la infraestructura vial a lo largo del territorio colombiano. La compañía lleva 28 años de vida institucional, en los cuales ha desarrollado diferentes proyectos de

infraestructura vial. En cuanto a la información, se genera en diferentes proyectos, por lo que no se cuenta con un sistema centralizado el cual garantice la seguridad de la información en todos los proyectos. En los últimos años, la compañía se ha encaminado a la producción y almacenamiento de toda su información digital, por lo que genera un reto mayor a la hora de establecer lineamientos y estrategias para garantizar la seguridad de la información.

"*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".* (Romero Castro, y otros, 2018)

Para la empresa Latinco (Latinoamericana de Construcciones), este activo no suele ser el más importante, por lo que en ocasiones se ha vulnerado notablemente, esto genera grandes problemas para cumplir los tres pilares de la información (autenticidad, integridad y disponibilidad). La situación actual genera grandes retos para la empresa pues como lo exponen los autores (Romero Castro, y otros, 2018)", los usuarios son considerados el eslabón más débil de la cadena, concepto que aplica severamente en la organización pues el gran problema de las vulnerabilidades se centra en los usuarios.

Este problema se permea desde la alta dirección hasta todos los usuarios administrativos, pues desde la gerencia no se ha visto la necesidad de invertir en procesos los cuales garanticen la seguridad de la información[1] y para el caso de los usuarios administrativos, tampoco ven la necesidad de administrar adecuadamente este activo que es de vital importancia para la empresa.

Pregunta

¿Cómo construir la seguridad de la información en los documentos electrónicos de archivo de la empresa, mediante procesos establecidos de ciberseguridad basados en las normas ISO y políticas de seguridad de información, para que la compañía cumpla con los tres pilares de la información disponibilidad, integridad y confidencialidad?

Objetivos

- Realizar un diagnóstico de las vulnerabilidades de seguridad de la información de la empresa.
- Analizar las vulnerabilidades encontradas mediante el diagnóstico.
- Priorizar los riesgos encontrados.
- Establecer lineamientos mediante la estandarización y gestión del riesgo en seguridad de la información.

Marco teórico

Resuma únicamente los principales referentes teóricos o artísticos que siguió su trabajo. Señale los números de las páginas de su documento en los que se encuentra la información completa.

Entendemos que los SGDEA tienen unas características muy específicas que las expone la teoría archivística. Después de tener claro lo que es dicho sistema, las entidades deberían empezar con su implementación, es decir que las instituciones no deben empezar por la implementación del sistema sin aún entender los requisitos que este debe poseer, para garantizar la adecuada gestión de documentos electrónicos, se podría decir que un sistema debe tener un planeación adecuada a las necesidades de cada entidad, para este caso en específico la empresa ya posee con un SGDEA, pero aún no cumple con todas sus necesidades.

Según la ISO 15489-1, los documentos electrónicos de archivo, deben contar con unos requisitos mínimos para la gestión adecuada, los cuales son los siguientes:

- Utilización de metadatos.
- Accesos y permisos en el SGDEA.
- Permitir la consulta de los registros.

- La interoperabilidad para apoyar la interacción con otros sistemas.
- Seguridad de la información (Backup), esto para permitir la continuidad del negocio.
- Captura de la información.

Según estos criterios expuestos anteriormente, la gestión electrónica de documentos de archivo, debe contar con unas fases para su implementación, las cuales garantizarán que el SGDEA se hará tal cual las necesidades de la entidad.

El diseño para la gestión electrónica de documentos, debe tener en cuenta diferentes fases, las cuales se deben adaptarse a las necesidades de la entidad.

Fase de diseño: se trata de intervenir en el diseño de los documentos y de los procesos en los que se insertan para garantizar la incorporación de requisitos archivísticos, que en buena medida trascienden más allá. (Mundet, 2003)

Fase de utilización: en la que los documentos fiables, auténticos, íntegros y accesibles deben conservar estas características inalteradas mediante fórmulas de autentificación, limitando el acceso a los individuos que han de intervenir en un proceso, sea como meros consultantes, sea para incorporar datos. Además, el uso de los documentos implica otros requisitos archivísticos. (Mundet, 2003)

Fase de conservación: a diferencia de los documentos no electrónicos, que conservan su autenticidad si se les mantiene en la misma forma y estado de transmisión en el que han sido creados, recibidos o guardados, los electrónicos conservan su autenticidad mediante la renovación constante y la migración periódica.

Por otro lado debemos tener en cuenta la seguridad de la información, la cual va ligada a la gestión electrónica de documentos, esto debido a los grandes riesgos que se corren a la hora de usar los documentos electrónicos de archivo. Es por esto que empresa debe “garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto,

garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías". (ICONTEC, 2006) ver en página 10l

Método

Resuma únicamente los principales elementos metodológicos que empleó en su investigación. Señale los números de las páginas de su documento en los que se encuentra la información completa.

La metodología para utilizar en este estudio de caso es cualitativo enfocado en la observación, con sentido de indagar por el cómo ha sido el proceso con los documentos electrónicos en la empresa, ésta incluye los siguientes elementos: enfoque, método, técnicas e instrumentos. Dicha metodología se aplica para indagar inicialmente sobre la situación actual en la documentación electrónica, y así de este modo poder generar recomendaciones con el objeto de mejorar este proceso.

Con el desarrollo de dicha metodología se podrán establecer recomendaciones, las cuales puedan ser aplicadas en la entidad, esto en pro de mejorar el proceso que se lleva a cabo en cuanto a la gestión electrónica de documentos. La metodología desarrollada en la investigación se basa en el trabajo de campo, es decir, que se trata de adentrar lo mejor posible en la entidad, pudiendo estar reunido con varios funcionarios.

Alcance

Este proyecto tiene como alcance, definir los lineamientos de seguridad de la información para el manejo adecuado de los documentos electrónicos de la compañía Latinoamericana de Construcciones. El tipo de alcance de la

investigación será netamente descriptivo, el cual busca definir la problemática planteada en el estudio de caso.

Enfoque

El enfoque de investigación que se toma en este caso es el cualitativo, debido a que el propósito del proyecto es hacer un diagnóstico que nos permita identificar las características del procesamiento y al igual las cualidades que se da en los documentos electrónicos en dicha entidad, en este caso sería analizar el proceso que se lleva a cabo con estos documentos en la empresa Latinoamericana de Construcciones, este enfoque es elegido desde la metodología descrita en los seminarios de investigación. Ver en página 15

Resultados, hallazgos u obra realizada

Presente el resumen de los principales resultados o hallazgos de su investigación o una sinopsis de la obra creada. Señale los números de las páginas de su documento en los que se encuentra la información completa.

En varios momentos se ha evidenciado problemas en la compañía por motivo de virus, como se expresa en el siguiente caso, esta información es tomada de la mesa de ayuda de la compañía:

En la organización se cuenta con un almacenamiento de información en la nube, mediante la cual se garantiza la seguridad de dicha información mediante backups continuos. Esta nube se conecta en cada uno de los equipos de la organización para realizar el almacenamiento de la información generada por cada uno de los colaboradores. El pasado mes (enero 2023), el equipo de informática de la organización evidencia que cierta información de la nube se encontraba encriptada mediante un ransomware tipo .pouu en el cual no había recuperación de las versiones anteriores debido a que este encripta la versión actual y sus anteriores, por lo que en ese caso no funcionaba el modelo de recuperación de la información inicial. Por lo que fue necesario acudir a otro medio de recuperación de información que se tiene previsto para estos casos denominado Spanning Backup, de esta forma fue posible recuperar la información.

La compañía cuenta con un software desactualizado el cual se instala en el año 2017 y hasta la fecha no cuenta con ninguna actualización de ningún tipo, lo cual ha hecho que se dificulte nuevos desarrollos y que se garantice su seguridad pues el código de desarrollo se encuentra totalmente obsoleto, esto hace que la rotación del personal de soporte del mismo sea muy frecuente lo que hace que no se tenga un soporte constante y efectivo, esto hace que la compañía tenga un sistema sin garantías el cual solo sirve como motor de base de datos, pero con funcionalidades escasas.

Capacitación de usuarios

Teniendo en cuenta los resultados de los instrumentos, como lo fue la entrevista, hay que realizar un plan de capacitación para todos los usuarios con el objetivo de dar a conocer las generalidades de la seguridad de la información y las buenas prácticas con el objetivo de mitigar el riesgo humano en la filtración de la información de la compañía.

Clasificación de la información

Como se expone en la teoría archivística, mediante los diferentes autores, se recomienda que todo sistema de información cuente con una clasificación adecuada, pues la compañía en este caso cuenta con un repositorio que garantiza el backup pero la información pierde la característica de la disponibilidad, pues no se encuentra clasificada adecuadamente, tampoco cuenta con la integridad, pues no tiene un mecanismos de autenticidad de la misma, lo que hace que la consulta de esta información se dificulte. De este modo se hace importante ejecutar instrumentos archivísticos para la clasificación de la información, garantizando la adecuada descripción y disposición de la misma. Ver en página 22

Conclusiones

Presente el resumen de las conclusiones a las que llegó. Señale los números de las páginas de su documento en los que se encuentra la información completa.

Productos derivados Referencie los artículos, libros, capítulos de libro, ponencias, etc., que fueron resultado de su proceso investigativo.

Lineamientos de seguridad de la información para los documentos electrónicos en la empresa Latinoamericana de Construcciones

JUAN JOSÉ ARISTIZÁBAL CASTRO
Cod. 12226019

CORPORACION UNIVERSITARIA UNITEC

Escuela de ingenierías

Especialización en seguridad de la información

Bogotá, Distrito Capital

24 de abril de 2023

Lineamientos de seguridad de la información para los documentos electrónicos en la empresa Latinoamericana de Construcciones

JUAN JOSÉ ARISTIZÁBAL CASTRO
Cod. 12226019

FABIO ANTONIO GONZÁLEZ MENDIETA
Director
CORPORACION UNIVERSITARIA UNITEC

CORPORACION UNIVERSITARIA UNITEC

Escuela de ingenierías

Especialización en seguridad de la información

Bogotá, Distrito Capital

24 de abril de 2023

Tabla de contenido

Índice de Tablas

Tabla de ilustraciones

Resumen

El presente estudio de caso se realiza en la entidad Latinoamericana de Construcciones, una empresa dedicada a la infraestructura vial. El objetivo principal del desarrollo de este busca establecer recomendaciones o lineamientos de seguridad de la información basados en las normas ISO y las políticas de seguridad. Este trabajo se desarrollará mediante una investigación cualitativa que describe la situación actual de la compañía respecto a las prácticas de seguridad de la información, esto con la finalidad de generar recomendaciones para el proceso del manejo de la información sobre todo los documentos electrónicos de archivo que se generan en la compañía, teniendo en cuenta que ha sido victima de ataques informáticos que han puesto en riesgo estos datos.

El boom de las tecnologías de la información ha traído grandes retos para la seguridad de la información, pues al crecer la producción de información se requirieren sistemas los cuales soporten la seguridad de estos datos que se generan, además de estrategias las cuales garanticen la autenticidad y disponibilidad de la información producida digitalmente, llevando a cabo todos los procesos que establece la seguridad informática. Teniendo en cuenta esta problemática, la empresa Latinoamericana de Construcciones, se encuentra sin procesos adecuados para el tratamiento de la información electrónica, por lo que es esencial generar dichos lineamientos de seguridad y recomendar herramientas las cuales ayuden a la gestión del riesgo en la compañía.

Palabras clave

Amenaza, Ataques, Base Confidencialidad, Datos, De Disponibilidad. Documentos, Hackeo, Hacker, Hardware, Información, Informática, Integridad, Metadatos, Redes, Seguridad, Servidores, Software, Vulnerabilidad, Wifi.

1. Planteamiento del problema

1.1 Contexto entidad

La empresa Latinoamericana de Construcciones, es una empresa que se dedica a la infraestructura vial a lo largo del territorio colombiano. La compañía lleva 28 años de vida institucional, en los cuales ha desarrollado diferentes proyectos de infraestructura vial. En cuanto a la información, se genera en diferentes proyectos, por lo que no se cuenta con un sistema centralizado el cual garantice la seguridad de la información en todos los proyectos. En los últimos años, la compañía se ha encaminado a la producción y almacenamiento de toda su información digital, por lo que genera un reto mayor a la hora de establecer lineamientos y estrategias para garantizar la seguridad de la información.

"*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".* (Romero Castro, y otros, 2018)

Para la empresa Latinco (Latinoamericana de Construcciones), este activo no suele ser el más importante, por lo que en ocasiones se ha vulnerado notablemente, esto genera grandes problemas para cumplir los tres pilares de la información (autenticidad, integridad y disponibilidad). La situación actual genera grandes retos para la empresa pues como lo exponen los autores (Romero Castro, y otros, 2018)", los usuarios son considerados el eslabón más débil de la cadena, concepto que aplica severamente en la organización pues el gran problema de las vulnerabilidades se centra en los usuarios.

Este problema se permea desde la alta dirección hasta todos los usuarios administrativos, pues desde la gerencia no se ha visto la necesidad de invertir en

procesos los cuales garanticen la seguridad de la información[2] y para el caso de los usuarios administrativos, tampoco ven la necesidad de administrar adecuadamente este activo que es de vital importancia para la empresa.

1.2 Justificación

Durante los últimos años el auge en los crímenes digitales o ciberataques ha puesto en jaque a los usuarios de internet, sitios web, empresas y corporaciones, generando pérdidas por miles de millones de dólares al año con tendencia al alza, debido a que cada día los cibercriminales mejoran o evolucionan sus métodos para lograr acceder a la información personal y confidencial de las víctimas y con ello poder obtener un lucro económico. (Gamboa Suarez, J. L. 2020).

Teniendo en cuenta esta premisa, se hace necesario que las personas y entidades generen estrategias y soluciones que ataquen las vulnerabilidades y protejan su información. En este caso más específico se toma como estudio de caso la entidad Latinoamericana de Construcciones (Ver contexto entidad). Esta organización ya sufrió de un ataque en el cual afortunadamente no perdió la información gracias a los backups que tenía, pero tuvo que reestructurar totalmente sus sistemas, esto hace que se vuelva aún más importante establecer lineamientos los cuales garanticen la autenticidad, integridad y disponibilidad de la información, esto con el objetivo de que no se repita un ataque similar o de mayor escala.

Además de esto, se debe establecer recomendaciones para la seguridad informática, teniendo en cuenta el antecedente que la compañía ha sido victima de ataques informáticos que ponen en riesgo la información de la organización, lo que podría hacer que la compañía deba incurrir en gastos para recuperarla o simplemente perder el recurso más importante hoy en día.

[2] Es el conjunto de medidas preventivas y reactivas que permiten resguardar o proteger la información, manteniendo la confidencialidad, integridad y la autenticación de los datos, tanto en el almacenamiento como en el tránsito. Cabe aclarar que el término seguridad de información difiere a seguridad informativa, debido a que el primero abarca un rango más amplio, llegando a tener una importancia global en otros aspectos que no involucran a la Ciberseguridad. Gamboa Suarez, J. L. (2020).

1.3 Pregunta problematizadora

¿Cómo construir la seguridad de la información en los documentos electrónicos de archivo de la empresa, mediante procesos establecidos de ciberseguridad basados en las normas ISO y políticas de seguridad de información, para que la compañía cumpla con los tres pilares de la información disponibilidad, integridad y confidencialidad?

1.4 Objetivos

Objetivo general

Establecer los lineamientos de seguridad de la información, mediante procesos establecidos de ciberseguridad basados en las normas ISO y políticas de seguridad de información, con el objetivo de que la empresa cumpla con la disponibilidad, integridad y confidencialidad de la información

Objetivos específicos

- Realizar un diagnóstico de las vulnerabilidades de seguridad de la información de la empresa.
- Analizar las vulnerabilidades encontradas mediante el diagnóstico.
- Priorizar los riesgos encontrados.
- Establecer lineamientos mediante la estandarización y gestión del riesgo en seguridad de la información.

2. Marco teórico y estado del arte

Los documentos electrónicos de archivo se definen como:

El conjunto de documentos producidos, recibidos o reunidos por una persona física o jurídica de modo involuntario, natural y espontáneo en el transcurso, y como apoyo, de su actividad de la que es testimonio, haciendo uso de la electrónica, que se conservan y transmiten también mediante medios electrónicos en depósitos de conservación permanente tras efectuar una selección a partir de la identificación y valoración de las series, con medidas de autentificación y de preservación adecuadas y con una organización respetuosa con su modo de producción, con el fin de garantizar su valor informativo, legal y cultural así como de permitir su acceso y uso también mediante las tecnologías de la información. (Navarro, 2001)

Con esta definición, se podría decir que los documentos electrónicos de archivo tienen un trato específico, es decir, que se debe cumplir con las características de los procesos documentales tal cual como se implementan en los documentos de formato físico. En las últimas décadas, los documentos electrónicos de archivo han aumentado su producción debido a que las empresas lo ven como una gran ventaja para cumplir con sus funciones. El problema se basa en que dicho cambio de formato no fue estructurado y aún sigue muy inmaduro en lo que se refiere a la entidad presentada.

Los sistemas que soporten dichos documentos no deben ser estáticos y deben de contar con unas características específicas, como lo expone el Decreto 2609 de 2012.

“Interoperabilidad. Los sistemas de gestión documental deben permitir la

Interoperabilidad con los otros sistemas de información, a lo largo del tiempo, basado en el principio de neutralidad tecnológica, el uso de formatos abiertos y estándares nacionales o internacionales adoptados por las autoridades o instancias competentes”.

- “Seguridad. Los sistemas de gestión documental deben mantener la información administrativa en un entorno seguro”.

- “Metadescripción. Se debe procurar la generación de metadatos normalizados, sean manuales o automatizados, desde los mismos sistemas y aplicativos”.

- “Adición de contenidos. El sistema de gestión documental debe permitir que sean agregados nuevos contenidos a los documentos, en forma de metadatos, sin que se altere la autenticidad, valor de evidencia e integridad de los documentos”.

- “Diseño y funcionamiento. La creación y captura de documentos en el sistema debe ser de fácil manejo para los usuarios, haciéndola tan simple como sea posible”.

- Gestión Distribuida. Los sistemas de gestión documental deben ofrecer capacidades para importar y exportar masivamente los documentos (series, subseries y expedientes y metadatos asociados desde y hacia otros sistemas de gestión documental).

- Disponibilidad y acceso. Un sistema de gestión de documentos electrónicos (SGDE) debe asegurar la autenticidad, integridad, inalterabilidad, accesibilidad, interpretación y comprensión de los documentos electrónicos en su contexto original, así como su capacidad de ser procesados y reutilizados en cualquier momento.

- Neutralidad tecnológica. El Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible.

Las entidades deben tener muy en cuenta las características anteriormente expuestas, debido a que son esenciales a la hora de implementar un adecuado

Sistema de Gestión Electrónica de Documentos de Archivo, este sistema es el que permitirá que los documentos electrónicos de archivo cumplan su ciclo vital, desde su producción, hasta su disposición final.

Es así como deberíamos mencionar que el ciclo de vida de los documentos electrónicos debe ser como se expone en la teoría archivística, el cual contiene las fases de archivo (gestión, central e histórico).

Los documentos electrónicos poseen un ciclo de vida similar al de los documentos en papel, mas como quiera que tienen mayor dependencia de la forma física y de la tecnología, hace falta una gestión más activa para asegurar el acceso durante todo el ciclo de vida del documento. (Mundet, 2003)

De tal modo tendríamos definir lo que es un SGDEA, pues es el sistema base para la adecuada gestión de documentos electrónicos y es el apoyo para cumplir con dicho ciclo de vida de los documentos electrónicos al igual que todos los procesos documentales.

La gestión de documentos electrónicos de archivo es compleja y exige la correcta aplicación de una gran variedad de funciones. Es obvio que el sistema –un SGDEA– que colme tales necesidades precisa software especializado, que puede consistir en un módulo especializado, en varios módulos integrados, en software desarrollado a la medida del usuario o en una combinación de varios tipos de programas informáticos. En todos los casos, siempre tendrán que existir procedimientos y políticas que complementen la gestión de forma manual. La naturaleza del SGDEA variará según la organización. La presente especificación no presupone la naturaleza de las soluciones individuales de los SGDEA. Los usuarios de la especificación tendrán que decidir cómo llevar a la práctica la funcionalidad de un SGDEA de forma que responda a sus necesidades. (CECA-CEE-CEEA, Bruselas, 2001)

De este modo entendemos que los SGDEA tienen unas características muy específicas que las expone la teoría archivística. Después de tener claro lo que es dicho sistema, las entidades deberían empezar con su implementación, es decir

que las instituciones no deben empezar por la implementación del sistema sin aún entender los requisitos que este debe poseer, para garantizar la adecuada gestión de documentos electrónicos, se podría decir que un sistema debe tener un planeación adecuada a las necesidades de cada entidad, para este caso en específico la empresa ya posee con un SGDEA, pero aún no cumple con todas sus necesidades.

Según la ISO 15489-1, los documentos electrónicos de archivo, deben contar con unos requisitos mínimos para la gestión adecuada, los cuales son los siguientes:

- Utilización de metadatos.
- Accesos y permisos en el SGDEA.
- Permitir la consulta de los registros.
- La interoperabilidad para apoyar la interacción con otros sistemas.
- Seguridad de la información (Backup), esto para permitir la continuidad del negocio.
- Captura de la información.

Según estos criterios expuestos anteriormente, la gestión electrónica de documentos de archivo, debe contar con unas fases para su implementación, las cuales garantizarán que el SGDEA se hará tal cual las necesidades de la entidad.

El diseño para la gestión electrónica de documentos, debe tener en cuenta diferentes fases, las cuales se deben adaptarse a las necesidades de la entidad.

Fase de diseño: se trata de intervenir en el diseño de los documentos y de los procesos en los que se insertan para garantizar la incorporación de requisitos archivísticos, que en buena medida trascienden más allá. (Mundet, 2003)

Fase de utilización: en la que los documentos fiables, auténticos, íntegros y accesibles deben conservar estas características inalteradas mediante fórmulas de autentificación, limitando el acceso a los individuos que han de intervenir en un

proceso, sea como meros consultantes, sea para incorporar datos. Además, el uso de los documentos implica otros requisitos archivísticos. (Mundet, 2003)

Fase de conservación: a diferencia de los documentos no electrónicos, que conservan su autenticidad si se les mantiene en la misma forma y estado de transmisión en el que han sido creados, recibidos o guardados, los electrónicos conservan su autenticidad mediante la renovación constante y la migración periódica.

Por otro lado se debe tener en cuenta la seguridad de la información, la cual va ligada a la gestión electrónica de documentos, esto debido a los grandes riesgos que se corren a la hora de usar los documentos electrónicos de archivo. Es por esto que empresa debe "garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías". (ICONTEC, 2006)

Si se analiza la situación de la entidad más a fondo, podremos evidenciar que el uso del documento electrónico de archivo se realiza de forma inadecuada debido a la falta de conocimiento de los mismos usuarios, debido a que su validez jurídica es desconocida. Para evacuar dicho pensamiento es necesario exponer los principios por los cuales todo documento electrónico de archivo posee valores jurídicos.

La Ley 527 de 1999 en su artículo segundo describe los mensajes de datos como: "la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el tele-grama, el telex o el telefax". (Flórez, 2014)

Si llevamos este concepto al contexto actual, todo documento mencionado anteriormente es válido, debido a que los documentos electrónicos cuentan con dichas características, es debido a esto que no se debe tener un concepto erróneo a la hora de realizar el almacenamiento de los documentos electrónicos de archivo como si fueran un simple documento de apoyo.

A modo de conclusión, la teoría archivística en cuanto a los documentos electrónicos de archivo tiene unos pasos básicos para su construcción, estos son expuestos a partir de diferentes fuentes, también vale la pena mencionar que existe el MOREQ: modelo de requisitos para la gestión de documentos electrónicos de archivo, el cual es instrumento utilizado para diferenciar los requisitos mínimos que debe tener la gestión electrónica de documentos.

3. Método

La metodología para utilizar en este estudio de caso es cualitativo enfocado en la observación, con sentido de indagar por el cómo ha sido el proceso con los documentos electrónicos en la empresa, ésta incluye los siguientes elementos: enfoque, método, técnicas e instrumentos. Se busca implementar dicha metodología con el objetivo de indagar inicialmente sobre la situación actual en la documentación electrónica, y así de este modo poder generar recomendaciones con el objeto de mejorar este proceso, tal como se tiene planteado en los objetivos de la investigación.

El resultado de esta metodología propuesta, se quiere generar algunas recomendaciones, las cuales puedan ser aplicadas en la entidad, esto en pro de mejorar el proceso que se lleva a cabo en cuanto a la gestión electrónica de documentos. La metodología que será desarrollada en la investigación se basa en el trabajo de campo, es decir, que se trata de adentrar lo mejor posible en la entidad, pudiendo estar reunido con varios funcionarios.

3.1. Alcance

Este proyecto tiene como alcance, definir los lineamientos de seguridad de la información para el manejo adecuado de los documentos electrónicos de la

compañía Latinoamericana de Construcciones. El tipo de alcance de la investigación será netamente descriptivo, el cual busca definir la problemática planteada en el estudio de caso.

3.2. Enfoque

El enfoque de investigación que se toma en este caso es el cualitativo, debido a que el propósito del proyecto es hacer un diagnóstico que nos permita identificar las características del procesamiento y al igual las cualidades que se da en los documentos electrónicos en dicha entidad, en este caso sería analizar el proceso que se lleva a cabo con estos documentos en la empresa Latinoamericana de
Construcciones, este enfoque es elegido desde la metodología descrita en los seminarios de investigación.

La observación permitirá colectar datos y de este modo ayudar a entender cuál es el estado actual, pues de allí resultan las cualidades y el porqué del problema que se define en el procesamiento de los documentos electrónicos y la falta de importancia que muestran los usuarios hacia éste. Con la generación de nuevos conocimientos a partir del análisis de la información recolectada, se buscará establecer recomendaciones que nos ayuden a mejorar el uso de los documentos electrónicos de archivo.

Toda la metodología desarrollada se realizó con el sentido de plasmar la situación actual de la entidad en cuanto a los documentos electrónicos de archivo, este al ser un tema muy nuevo en Colombia, se logra evidenciar que hace mucha falta nuevas estrategias las cuales nos ayuden a afrontar las tecnologías de la información de una forma más adecuada, pues estamos en el momento el cual se hace más uso de un equipo o máquina que de los métodos tradicionales.

3.3. Metodología de investigación

El método seleccionado es la observación, esto a fin de verificar el proceso que se lleva a cabo en este estudio de caso, puesto que se desarrollará una recopilación de información de lo que expone la teoría del deber ser con el

proceso de los documentos electrónicos de archivo, esto con el sentido de dar las recomendaciones dependiendo del resultado del diagnóstico y comparando éste con la teoría archivística.

3.4. Técnicas

Para la indagación, se utilizarán técnicas como la observación y la recopilación documental, éstas permiten generar un contexto amplio y especifico, garantizando un mejor análisis del diagnóstico y de la situación de los documentos electrónicos.

El diagnóstico, se llevará a cabo mediante la observación del proceso y además de realizar preguntas a los encargados del uso de los documentos electrónicos en la entidad, debido a que éstas nos brindarán una visión de lo que perciben los usuarios de la información, además que permitan indagar el tema del uso de los documentos electrónicos y la importancia que se tiene hacia el documento electrónico en la organización.

3.5. Instrumentos

Para este caso y como se ha expresado anteriormente, el principal instrumento a aplicar sería el diagnóstico integral, este instrumento nos brindará información clara, de cómo ha sido el proceso y como es su situación actual, para posteriormente cumplir con el objeto de la investigación, el cual será para generar los lineamientos adecuados para el manejo de dichos documentos.

El uso de los instrumentos se hará en campo, es decir que el diagnóstico se aplicara en la entidad por medio de preguntas a los encargados de los documentos electrónicos de archivo de la entidad, posteriormente dichas respuestas se llevarán a los diagnósticos los cuales nos ayudaran a establecer punto por punto cuál es la problemática que se evidencia en cada proceso y cada paso hacia la gestión electrónica de documentos adecuada.

Como se logra ver en el desarrollo del primer objetivo, se aplican los instrumentos, los cuales son un diagnóstico y una guía de observación de los puntos críticos de la entidad en cuanto a la gestión electrónica de documentos. La

observación también es documental y sobre todo se basa en identificar las falencias que se tienen en el proceso a la hora de gestionar adecuadamente los documentos del caso.

Una vez se apliquen los instrumentos, estos deberán ser analizados. Con la ayuda de la información recopilada y el análisis de la misma, se logrará realizar o priorizar los puntos más críticos de la entidad esto con el sentido de desarrollar el último objetivo de la investigación el cual es generar lineamientos que se especificarán al finalizar el proceso.

Tabla 1

Cronograma

Cronograma proyecto																
Actividad	**S 1**	**S 2**	**S 3**	**S 4**	**S 5**	**S 6**	**S 7**	**S 8**	**S 9**	**S 10**	**S 11**	**S 12**	**S 13**	**S 14**	**S 15**	**S 16**
Realizar diagnóstico situación actual entidad																
Recopilar información mediante los intrumentos definidos																
Análisis de la información recopilada																
Establecer vulnerabilidades en los documentos electrónicos																
Priorizar riesgos encontrados																
Contrastar riesgos vs teoría del deber ser																
Establecer lineamientos de seguridad de la información																

Cronograma elaboración propia

Tabla 2

Presupuesto

Presupuesto			
Recurso	**Cantidad**	**Duración**	**Valor**
Equipos de computo	1	4 meses	$ 3.000.000
Profesional Ciencias de Información	1	4 meses	$ 12.000.000
Conexión de red	1	4 meses	$ 320.000
		Total	$ 15.320.000

Presupuesto elaboración propia

3.6. Diagnóstico de la situación actual.

3.6.1. Observación

La empresa Latinoamericana de Construcciones cuenta con un área de informática, la cual cuenta con personal técnico y profesional. El personal no

cuenta con toda la capacidad para garantizar el funcionamiento de un Sistema de Seguridad de la Información para todos sus activos de información, en este caso con alcance a su sistema de Gestión Documental. Esta información es tomada mediante el análisis de la mesa de ayuda de la compañía y entrevistas a los usuarios, las cuales fueron aplicadas a la compañía en su oficina central con una población de 79 personas, dichas entrevistas fueron analizadas para obtener la información que se arroja en el caso de estudio a continuación. Además también se realiza observación y levantamiento de información mediante el manejo de los diferentes sistemas en campo, teniendo en cuenta que se hace ejercicio de investigación en campo verificando la usabilidad y errores en los diferentes aspectos para garantizar un ejercicio de análisis objetivo.

Ilustración 1

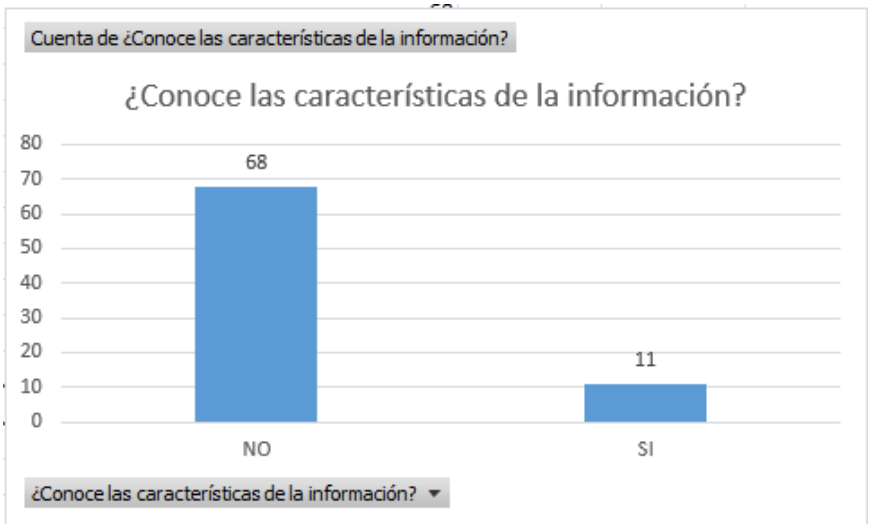

Ilustración elaboración propia

Ilustración 2

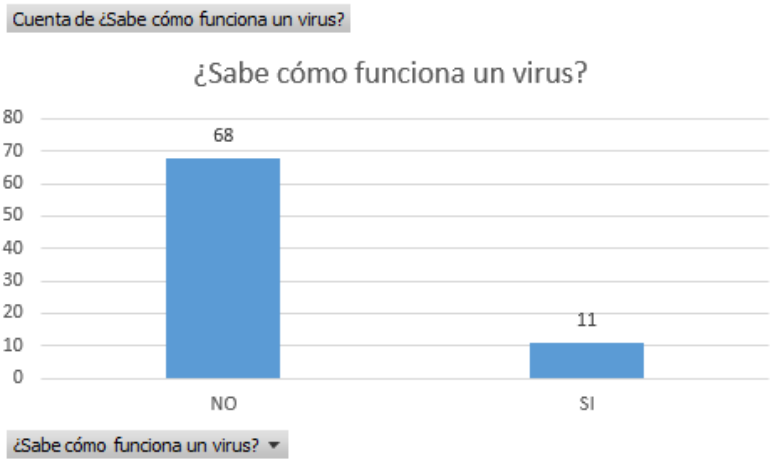

Ilustración elaboración propia

Ilustración 3

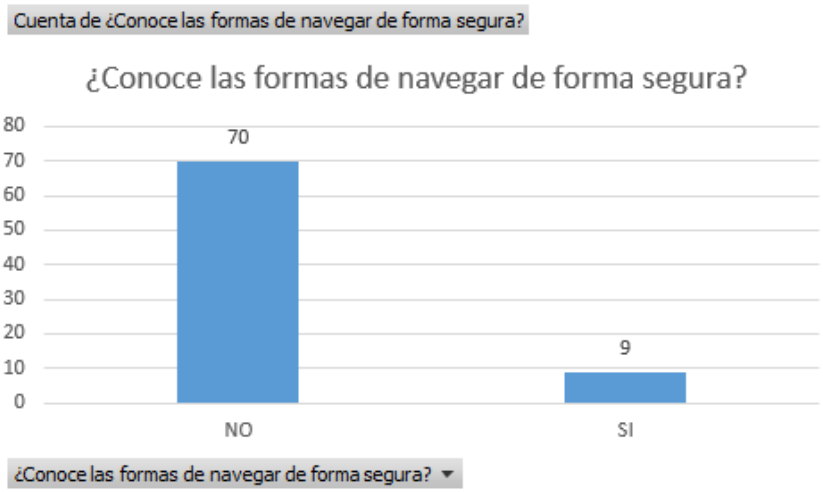

Ilustración elaboración propia

Ilustración 4

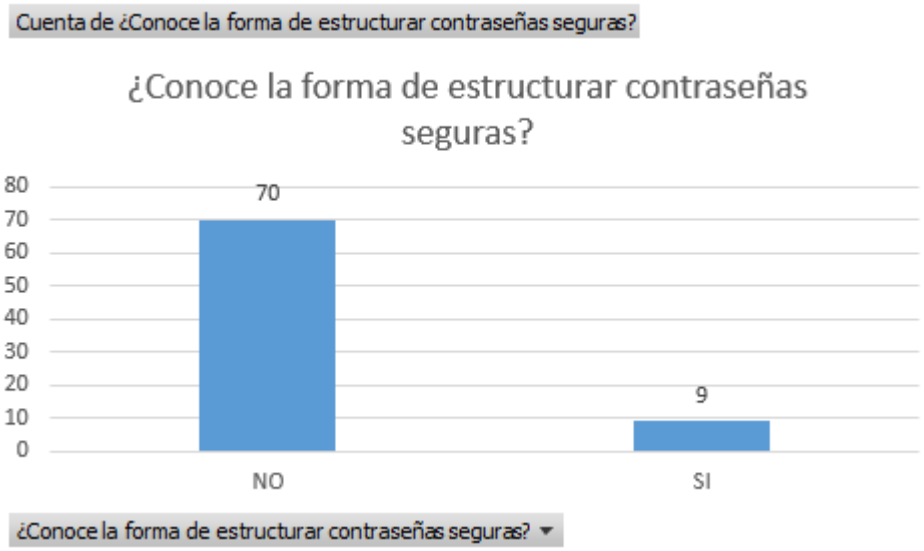

Ilustración elaboración propia

Ilustración 5

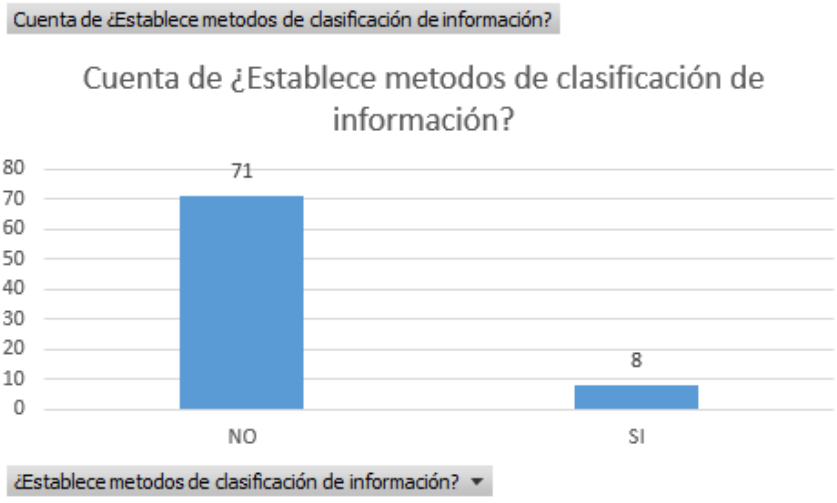

Ilustración elaboración propia

Ilustración 6

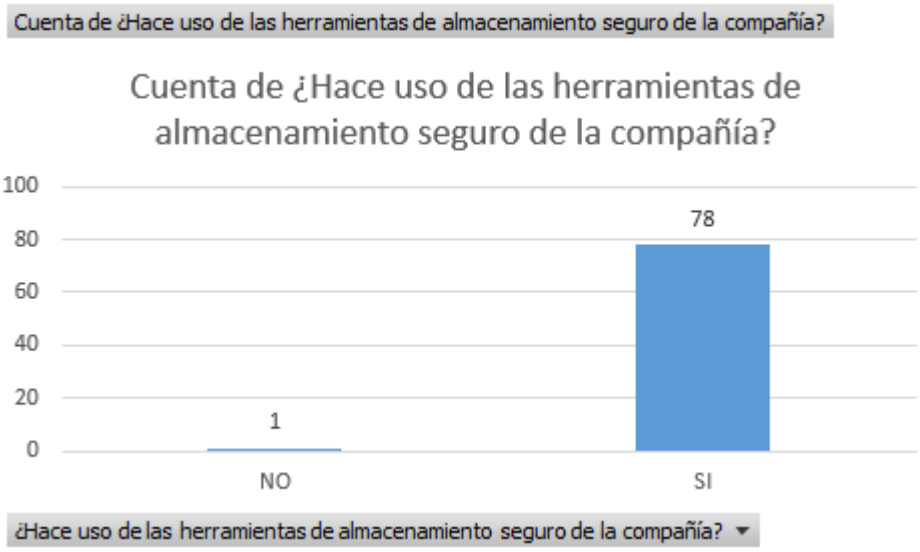

Ilustración elaboración propia

Teniendo en cuenta los resultados de las entrevistas, también se evidencia que los usuarios no poseen conocimientos sobre aspectos generales de la seguridad de la información, lo que hace que este sea un gran riesgo para la compañía pues hay que tener cuenta que por más controles que se tengan los usuarios son el mayor riesgo para las compañías.

3.6.2. Caso de estudio 1

En varios momentos se ha evidenciado problemas en la compañía por motivo de virus, como se expresa en el siguiente caso, esta información es tomada de la mesa de ayuda de la compañía:

En la organización se cuenta con un almacenamiento de información en la nube, mediante la cual se garantiza la seguridad de dicha información mediante backups continuos. Esta nube se conecta en cada uno de los equipos de la organización para realizar el almacenamiento de la información generada por cada uno de los colaboradores. El pasado mes (enero 2023), el equipo de informática de la organización evidencia que cierta información de la nube se encontraba encriptada mediante un ransomware tipo .pouu en el cual no había recuperación de las versiones anteriores debido a que este encripta la versión actual y sus

anteriores, por lo que en ese caso no funcionaba el modelo de recuperación de la información inicial. Por lo que fue necesario acudir a otro medio de recuperación de información que se tiene previsto para estos casos denominado Spanning Backup, de esta forma fue posible recuperar la información.

Investigando cómo ingresa este virus, el área evidencia que este fue contagiado mediante un equipo personal, por lo que no contaba con antivirus y tenía la información de la compañía sincronizada en dicho dispositivo, lo que no está permitido en la organización, de esta forma fue como se infectó la ruta a la cual tenía acceso dicho usuario.

3.6.2.1. Sistemas operativos de los servidores y servicios de almacenamiento

Estas bases de datos se encuentran almacenadas en servidores tercerizados lo que hace que dicha seguridad dependa de dicho proveedor, lo que es necesario que se implementen controles y se garanticen pruebas de intrusión en los mismos, pues estas no se realizan para que efectivamente la información se encuentre segura de cualquier ataque o vulnerabilidad, además de que se deben mantener los sistemas operativos actualizados con todos los paquetes con el objetivo de evitar vulnerabilidades por estas desactualizaciones.

Se ha evidenciado que el proveedor no realiza buen acompañamiento a la hora de realizar procesos en sus servidores, pues ellos deben garantizar que los demás proveedores que almacenan sus bases de datos en sus sistemas no hagan cambios que afecten la integridad de la información. (información tomada del contrato de servicio de servidores Cloud y entrevistas con el área TIC’S)

3.6.2.2. Seguridad del software de la compañía

La compañía cuenta con un software desactualizado el cual se instala en el año 2017 y hasta la fecha no cuenta con ninguna actualización de ningún tipo, lo cual ha hecho que se dificulte nuevos desarrollos y que se garantice su seguridad pues el código de desarrollo se encuentra totalmente obsoleto, esto hace que la rotación del personal de soporte del mismo sea muy frecuente lo que hace que no

se tenga un soporte constante y efectivo, esto hace que la compañía tenga un sistema sin garantías el cual solo sirve como motor de base de datos, pero con funcionalidades escasas. Además de esto los usuarios son una gran vulnerabilidad pues no tienen la cultura de la importancia que debe tener almacenar adecuadamente la información y gestionar sus contraseñas adecuadamente, lo que hace que se pueda vulnerar fácilmente con ingeniería social. (Esta información es recopilada mediante el contrato del software y la instalación en el servidor de aplicaciones).

3.6.2.3. Análisis de información (autenticidad, integridad, disponibilidad)

La información que se almacena en las bases de datos de la compañía no cuenta con sistemas que garanticen su autenticidad pues si bien se tienen documentos digitales, estos no cuentan con ningún tipo de validación, estampa o firma digital la cual garantice que el documento es válido y no ha sido modificado, lo que también afecta la integridad de esta. La disponibilidad también es un tema que no se cumple, pues los usuarios no almacenan adecuadamente la información con los metadatos bien asociados lo que hace que no se encuentre disponible con facilidad para recuperarla. Además como se logró evidenciar en las entrevistas, los usuarios no cuentan con los conocimientos adecuados para el tratamiento de dicha información. (ver ilustraciones).

3.6.2.4. Seguridad física

La seguridad de la compañía en ocasiones puede verse vulnerada, pues sus instalaciones se encuentran en un centro comercial el cual tiene gran cantidad de visitantes, aunque sus oficinas cuentan con validación biométrica, no se cuenta con un control de ingreso para visitantes, además de que los equipos se encuentran constantemente desbloqueados y sin bloqueo de puertos USB lo que hace que se pueda robar información o ingresar algún tipo de software malicioso.

4. Resultados y hallazgos

4.1. Aspectos lógicos

- La compañía al tener usuarios de trabajo remoto debe garantizar que su política de seguridad de la información se cumpla a cabalidad, mediante las sanciones que sean necesarias.
- También se debe contratar servicios de software de control de dispositivos los cuáles garanticen el bloqueo de dispositivos desconocidos en los servicios de la entidad, como lo son el almacenamiento de información.
- Para el caso de los usuarios que trabajan en los proyectos de la compañía (se encarga de realizar proyectos de infraestructura vial), se debe garantizar el uso de equipos corporativos, la forma de realizar dicho bloqueo se podría hacer mediante la red, es decir que a la red corporativa no puedan acceder equipos personales, para esto podría generar dos canales uno corporativo y otro de invitados para evitar la conexión a la red de dispositivos personales.
- Realizar capacitación y difusión de la política de seguridad de la información, con el objetivo de mitigar el riesgo humano que se tiene en la compañía.
- Bloquear el acceso del correo corporativo en equipos diferentes a los de la organización, debido a que de esta forma no se podrá hacer uso del servicio de almacenamiento en la nube en el cual se encuentran todos los datos de la compañía.
- Realizar auditorías educativas a los usuarios, con el objetivo de verificar el cumplimiento de la política de seguridad de información de la compañía.
- Definir comités de seguridad, con el objetivo de verificar el estado de las redes y datos de la compañía.
- Realizar integración de los sistemas mediante los servidores que se tienen estipulados en el proceso de informática.
- Establecer los métodos de restauración y acceso a las bases de datos que se tendrán almacenadas en los servidores.

- Realizar configuración para administración de las redes mediante la gestión de los switches instalados, además de realizar bloqueos a los equipos que no son corporativos y navegan en la red corporativa.
- Establecer dos redes, una de ocio y otra corporativa, las cuales sean independientes, garantizando la seguridad mediante el tráfico de red a dispositivos desconocidos.
- Nivelar cargas de internet, para garantizar la estabilidad de la red en todos los pisos de la compañía.
- Establecer mecanismos de monitoreo y control de las redes de la compañía.
- Levantar la topología de red y marcación de cada uno de los Rack con el objetivo de garantizar el estándar establecido según los procedimientos del área de informática.
- Contar con red de contingencia en caso de que la red principal sufra caídas o problemas de conexión.
- Establecer una conexión en maya para cada uno de los switches, evitando que, al fallar un puente de fibra, existan puntos de desconexión, ya que al tener un anillo de conexión de fibra cerrado, se tendrá redundancia en la red.

4.2. Aspectos físicos

- Realizar aseguramiento de cada uno de los Rack en zonas donde no pueda acceder personal no autorizado.
- Instalar las redes y cableado estructurado, según los puestos de trabajo establecidos, garantizando conexión en los mismos.
- Restringir acceso a las zonas de administración de las redes, con el objetivo de evitar intrusiones mediante las redes de la compañía.
- Garantizar la contingencia en la energía mediante la UPS, con el objetivo de tener plan en caso de pérdida de electricidad y evitar daños en equipos o pérdida de información.
- Realizar demarcación de puntos de red y conexión en cada uno de los switches, garantizando que las puentes o conexiones se identifiquen adecuadamente.

4.3. Aspectos legales

- Garantizar el cumplimiento de la norma ISO 27001, con el objetivo de mantener el estándar de la seguridad informática.
- Cumplir con las leyes de tratamiento de datos personales.
- Establecer el cumplimiento de las leyes de archivo e información como lo son la ley general de archivo y los procedimientos para la preservación digital a largo plazo.

4.4. Infraestructura de Red

Al ser una empresa de construcción y tener varios proyectos por lo largo del país, se propone la siguiente estructura para garantizar la administración de las redes.

- Se tendrá en cada uno de los proyectos la red del proveedor de internet, se instala un RACK en el cual se va a contar con el switche para distribuir cada uno de los AP y los puntos de red.
- También se contará con una dream machine, con el objetivo de poder administrar cada uno de los switches de las obras desde la oficina central, además de realizar monitoreo de la red.
- Para la seguridad perimetral se cuenta con antivirus Bitdefender el cual se encarga de darnos seguridad desde esta perspectiva, teniendo en cuenta que todos los equipos corporativos cuentan con licencia de dicho antivirus y las redes se monitorean con el objetivo de que no se puedan conectar equipos no corporativos.
- En los proyectos más grandes adicional al switche, dream machine, se contará con un cortafuegos el cual ayude a tener una red más segura teniendo en cuenta que desde dichos proyectos ingresan a los software donde se almacena la información de la compañía, aunque también vale la pena mencionar que estos aplicativos se encuentran instalados en servidores cloud administrados por terceros los cuales garantizan backup de dicha información.

- Los puntos de red “AP”, también serán administrados desde la oficina central, con el objetivo de realizar bloqueos a los dispositivos que no cuenten con la política de administración de la compañía.
- Para el caso de los visitantes, se contará con una red diferente el cual garantice que navegan por otro canal y no podrán ingresar a ningún sistema de la red principal en caso de algún ataque.

4.5. Capacitación de usuarios

Teniendo en cuenta los resultados de los instrumentos, como lo fue la entrevista, hay que realizar un plan de capacitación para todos los usuarios con el objetivo de dar a conocer las generalidades de la seguridad de la información y las buenas prácticas con el objetivo de mitigar el riesgo humano en la filtración de la información de la compañía.

4.6. Clasificación de la información

Como se expone en la teoría archivística, mediante los diferentes autores, se recomienda que todo sistema de información cuente con una clasificación adecuada, pues la compañía en este caso cuenta con un repositorio que garantiza el backup pero la información pierde la característica de la disponibilidad, pues no se encuentra clasificada adecuadamente, tampoco cuenta con la integridad, pues no tiene un mecanismos de autenticidad de la misma, lo que hace que la consulta de esta información se dificulte. De este modo se hace importante ejecutar instrumentos archivísticos para la clasificación de la información, garantizando la adecuada descripción y disposición de la misma.

5. Conclusiones

Realizando la conclusión del presente trabajo de investigación, mediante el análisis de los resultados, dando respuesta a la hipótesis o problema planteado, es importante que la compañía ejecute las recomendaciones presentadas en el presente documento, pues se evidencia que aún se tienen técnicas obsoletas a la hora de garantizar la seguridad de los documentos electrónicos, además que los usuarios no tienen conocimientos de las formas

adecuadas para el tratamiento de los mismos, lo que hace que la compañía se pueda tener un mayor riesgo de pérdida de información o fuga de la misma. Es importante recalcar las contribuciones más relevantes como lo son la capacitación de los usuarios, pues se evidenció en el estudio que la mayoría de la población evaluada no ha obtenido ninguna capacitación sobre el tema de seguridad informática y además de esto según el análisis de los casos que se han presentado en la organización, estos se han dado en su mayoría por desconocimiento de los usuarios a la hora de la manipulación o manejo de los sistemas de la compañía.

Se evidencia también que el trabajo descrito, tuvo ciertas limitaciones pues solo se logró hacer análisis de la población administrativa, pero también podría ser una fortaleza pues dicha población es la que interactúa en mayor parte con los sistemas de la compañía, pero es importante para futuros trabajos de investigación hacer ampliación tanto del objeto como del rastreo de información para obtener un resultado más preciso.

Haciendo un párelo con las investigaciones citadas, se logran evidenciar ciertas similitudes en cuanto a las afirmaciones de los autores a la hora de las buenas técnicas para el manejo de la información, con el objetivo de garantizar la confidencialidad, disponibilidad y seguridad de la información, además de que se llega a la conclusión de que si bien se podría tener un sistema totalmente seguro en cuanto a aspectos lógicos, siempre queda el riesgo que supone el manejo de los usuarios.

También vale la pena mencionar que dichas investigación o casos de estudio específicos, ayudan a que la profesión se mantenga actualizada, pues día a día se generan nuevos métodos de intrusión y también de protección lo que hace que al analizar las diferentes situaciones presentadas en las investigaciones planteadas, se puede mantener el conocimiento actualizado en pro de la seguridad no solo de las compañías sino también de la sociedad. Para terminar de concluir, es importante también que los profesionales de la informática, tengan una mayor relación con los profesionales en ciencias de la información, pues también se logra demostrar que la información requiere de

ambas profesiones pues por un lado está segura y por el otro lado se obtienen técnicas para el manejo de la misma en cuanto a su disponibilidad.

6. Bibliografía

Álvarez, A. (2013). Perspectivas actuales sobre la autenticidad y autentificación de los documentos electrónicos de archivo. Boletín del Archivo Nacional, 21, 7-26.

Archivo General de la Nación Jorge Palacios. (2014). Manual implementación de un Programa de Gestión Documental. AGN, 60.

Bofarull Mas, B., & Senar Rosell, M. À. (2008). Estudio de mejora de un sistema de backup.

Borja, J. L., Malagón, M. L., & Daza, N. J. P. (2017). Diseño de un Sistema de Gestión de Documentos Electrónicos de Archivo. Estudio de caso: Baker Mckenzie. Revista CODICES, 13(I), 38-38.

Castro, W. D. O., Barcia, J. E. A., & Pacheco, L. S. (2017). Manejo de los recursos didácticos informáticos y procesos de aprendizaje en el área de cableado estructurado para redes LAN. Dominio de las Ciencias, 3(2), 483-534.

CECA-CEE-CEEA, Bruselas. (2001). Modelo de requisitos para la gestión de documentos de Archivo. IDA, 156.

Chornet, V. G. (2014). Criterios ISO para la preservación digital de los documentos de archivo. Revista CODICES, 10(II), 16-16.

Fernández, L. G., & Álvarez, A. A. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. AENOR.

Flórez, G. D. (2014). La validez jurídica de los documentos electrónicos en Colombia a partir de sus evolución legislativa y jurisprudencial. Verba Iuris 3, 29.

García Pérez, A. (2001). La gestión de documentos electrónicos como respuesta a las nuevas condiciones del entorno de información. Acimed, 9(3), 190-200.

Gómez Domínguez, D., Ruiz Rodrigez, A. Á., & Peis Redondo, E. (2002). La gestión de documentos electrónicos: Requerimientos funcionales. Dialnet, 11.

ICONTEC. (2006). NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001. ICONTEC, 45.

Mundet, J. R. (2003). La gestión de los documentos electrónicos como función archivística. DIALNET.

Navarro, M. Á. (2001). Los Archivos de documentos electrónicos. DIALNET.

Presidencia de la Republica. (2012). DECRETO 2609 DE 2012. NA, 25.

Rivera Donoso, M. A. (2009). Directrices para la creación de un programa de preservación digital. Serie Bibliotecología y Gestión de Información, (43), 1-63.

Rodriguez, J. V. (1997). Documentos electrónicos y normalización . Dialnet, 13.

Romero Castro, M. I., Figueroa Morán, G. L., Vera, N. D., Alava Cruzatty, J. E., Parrales Anzúles, G. R., Alava Mero, C. J., . . . Castillo Merino, M. A. (17 de 10 de 2018). Google Scholar. Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Suarez, J. L. (17 de 10 de 2020). Google Scholar. Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8668/IMPORTANCIA%20DE%20LA%20SEGURIDAD%20INFORM%C3%81TICA%20Y%20CIBERSEGURIDAD%20EN%20EL%20MUNDO%20ACTUAL.pdf?sequence=1&isAllowed=y

Torres López, J. A. (2003). Análisis y soluciones en redes de cableado estructurado (Doctoral dissertation, Universidad Autónoma de Nuevo León).

Voutssas, J. (2010). Preservación documental digital y seguridad informática. Scielo.

Wong, B. I. Á. (2017). Los repositorios digitales para la conservación. Un acercamiento a la preservación digital a largo plazo. Ciencias de la Información, 48(2), 15-22.

Yanara Dorado, S., & Mena Mugica, M. (2009). Evolución de la cienca archivística. Scielo.

Por intermedio del presente documento en mi calidad de autor o titular de los derechos de propiedad intelectual de la obra que adjunto, titulada Lineamientos de seguridad de la información para los documentos electrónicos en la empresa Latinoamericana de Construcciones, autorizo a la Corporación universitaria Unitec para que utilice en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador o titular de la obra objeto del presente documento.

La presente autorización se da sin restricción de tiempo, ni territorio y de manera gratuita. Entiendo que puedo solicitar a la Corporación universitaria Unitec retirar mi obra en cualquier momento tanto de los repositorios como del catálogo si así lo decido.

La presente autorización se otorga de manera no exclusiva, y la misma no implica transferencia de mis derechos patrimoniales en favor de la Corporación universitaria Unitec, por lo que podré utilizar y explotar la obra de la manera que mejor considere. La presente autorización no implica la cesión de los derechos morales y la Corporación universitaria Unitec los reconocerá y velará por el respeto a los mismos.

La presente autorización se hace extensiva no sólo a las facultades y derechos de uso sobre la obra en formato o soporte material, sino también para formato electrónico, y en general para cualquier formato conocido o por conocer. Manifiesto que la obra objeto de la presente autorización es original y la realicé sin violar o usurpar derechos de autor de terceros, por lo tanto, la obra es de mi exclusiva autoría o tengo la titularidad sobre la misma. En caso de presentarse cualquier reclamación o por acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión asumiré toda la responsabilidad, y saldré en defensa de los derechos aquí autorizados para todos los efectos la Corporación universitaria Unitec actúa como un tercero de buena fe. La sesión otorgada se ajusta a lo que establece la ley 23 de 1982.

Para constancia de lo expresado anteriormente firmo, como aparece a continuación.

Firma

Nombre Juan José Aristizábal Castro
CC. 1036402220