INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

GRUPO DE INVESTIGACIÓN FICB-PG

CREACIÓN DE POLITICAS DE SEGURIDAD PARA CORMAGDALENA

PRESENTA:

JAIME ANDRES OCHOA CASTAÑEDA 1622010108

LINA MARIA VELA FORIGUA 1411980609

MSC:

JAIMES FERNANDEZ WILMAR

ABRIL 2018

ÍNDICE GENERAL

RESUMEN

Este trabajo trata de como ayudaremos con esta investigación que realizamos a la empresa Cormagdalena a implementar un excelente esquema de políticas de seguridad, ya que por ser una empresa del estado cuenta con muchas falencias en sus políticas de seguridad por el ahorro de costos, es así como llegamos a visualizar en esta investigación que la mayoría de compañías por el avanzan sin límites de la tecnología, las empresas asumen riesgos como perder un negocio o arriesgarse a ser hackeadas; en ocasiones estas políticas de seguridad son utilizadas incorrectamente provocando daños de grandes dimensiones.

Se realiza esta investigación para explicar la creación de políticas de seguridad de la información para la empresa Cormagdalena y adicional poder dejar una guía para todo aquel que lea este trabajo pueda tener una serie de indicadores que ayunen a crear nuevos proyectos.

Queremos con lo investigado y plasmado aquí que las personas vean la seguridad de la información como algo muy importante en el proceso y desarrollo de las compañías y no como una parte incómoda para la alta gerencia o un obstáculo para el crecimiento como algunos lo ven, más bien insistir en que si se realiza una excelente política de seguridad la compañía va a tener un crecimiento asegurado y con excelente calidad.

ABSTRACT

This work deals with how we will help with this research that we made to the company Cormagdalena to implement an excellent security policy scheme, since being a state company has many flaws in its security policies for cost savings, this is how as we came to see in this research that most companies are advancing technology without limits, companies take risks like losing a business or risking being hacked; Sometimes these security policies are used incorrectly causing large damages.

This research is carried out to explain the process of creation of information security policies for the company Cormagdalena and additionally to leave a guide for everyone who reads this work can have a series of indicators for the realization of future research projects

We want with the research and reflected here that people see the security of information as something very important in the process and development of companies and not as an uncomfortable part for top management or an obstacle to growth as some see it, more Well insist that if an excellent security policy is carried out the company will have an assured growth and with excellent quality.

PALABRAS CLAVE

Cormagdalena: Empresa que se encarga del tratamiento y cuidado del rio magdalena, Empresa escogida para realizar el trabajo,

Seguridad de la información: grupo de reglas que se hacen para prevenir incidentes y que las organizaciones utilizan para proteger y resguardar la información, tanto física como visual.

Políticas de seguridad: medidas que se toman para afrontar y mitigar riesgos de seguridad en una empresa.

KEY WORDS

User, Password, internet, hacker, hacked.

1. NOMBRE DEL PROYECTO:

CREACIÓN DE POLITICAS DE SEGURIDAD PARA CORMAGDALENA.

2. INTRODUCCIÓN

En el siguiente trabajo expondremos los puntos de investigación sobre la realización y creación de políticas de seguridad de la información, con la finalidad de que se pueda realizar paso a paso con la guía del tutor asignado.

En primer lugar, se presentarán lo puntos del inicio de la investigación que se presentaron con el Anteproyecto abordando las opciones que elegimos para definir el problema o factor principal sus actores y como estos influyen en el pro o contra del problema para la búsqueda final de la posible solución de este.

Basándonos en los diferentes materiales y guías de todas las materias vistas más los que debemos realizar en este módulo para así poder obtener un excelente trabajo investigativo.

El objetivo es poder realizar un trabajo claro y conciso que permitan poder aportar los puntos a mejorar y así poder terminarlo.

Tomamos como referencia la empresa Cormagdalena, la cual no cuenta con unas políticas establecidas de seguridad de la información, poniendo en Gran riesgo los activos informáticos y la información almacenada el ellos ya que el personal no se encuentra capacitado sobre el adecuado uso de la información y la seguridad que esta requiere, así el impacto que tendrá la mejora de esta situación será el poder que la empresa Cormagdalena sea ejemplo para las demás empresas del estado que tienen las mismas falencias; evitando así reprocesos en el sistema y la protección del Rio magdalena que es el objetivo primordial de la compañía.

Dando que la investigación es factible ejecutarla en el tiempo establecido el cual es un año, para generar los cambios establecidos para la compañía y así poder

llegar al objetivo final, que es la protección de los activos informáticos en Cormagdalena.

3. SITUACIÓN DE INTERÉS

El presente trabajo describe la creación de unas políticas de seguridad de la información para Cormagdalena. La cual requiere del diseño estructurado para la elaboración de unas políticas de seguridad de la información sólidas y así poder salvaguardar su activo más importante, la información. Velando en todo momento por mantener La confidencialidad, integridad y disponibilidad de la información. De esta manera, las políticas de seguridad de la información son el instrumento para demostrar la importancia de proteger la información de situaciones críticas, de fallas, debilidades, y así poder proteger los activos más importantes de Cormagdalena.

4. JUSTIFICACION

La seguridad de la información es uno de los mecanismos que hoy por hoy ha tomado fuerza dentro de las organizaciones debido a los avances tecnológicos que trae consigo riesgos que pueden afectar de manera directa e indirecta a la corporación.

La creación de unas políticas para la seguridad de la información se realiza para minimizar los riesgos a los que se pueda estar expuesta la organización por un mal manejo de información o recursos tecnológicos.

Con este proyecto y una buena planificación del trabajo, se verán reflejados una serie de beneficios como: mayor competencia y desarrollo de la corporación, mayor conocimiento y solución de situaciones problema que se puedan presentar a nivel de seguridad de la información.

5. OBJETIVOS

OBJETIVO GENERAL

Proporcionar a todos los empleados y usuarios de Cormagdalena los recursos informáticos y políticas de seguridad de fácil acceso para que conozcan las normas de seguridad de la informácion de la entidad, y con el cual sea compromiso institucional la seguridad de la información.

OBJETIVOS ESPECIFICOS

- Analizar como se encuentra la entidad, con relación a las políticas de Seguridad de la Información.
- Establecer los roles y la responsabilidad en cuanto a las políticas de Seguridad de la Información.
- Estudiar las necesidades y exigencias de las partes interesas de la corporación con relación a la creación de las políticas de Seguridad de la Información.
- Determinar la metodología para la identificar y clasificar los activos de la corporación y así poder valorar y dar un adecuado tratamiento de riesgos.
- Catalogar los activos de Tecnología de la Corporación, analizar sus riesgos y definir los planes de tratamiento, en base a la metodología fijada.
- Determinar un modelo para gestionar los incidentes de seguridad.

6. ESTADO DEL ARTE O MARCO TEORICO

A medida que va pasando el tiempo, la tecnología ha ido avanzando cada

día más, todos hemos tenido que irnos adaptando a estos avances para poder estar al día y poder proteger nuestra información, se ha visto la necesidad de crear manuales, normas o políticas que puedan servir a realizar controles que ayuden a prevenir y corregir problemas que puedan llegar afectar los sistemas de la corporación.
La política de seguridad de información no es un estándar, por lo cual no indica cómo se realiza una labor o control de manera específica, NO indica herramientas para su uso. Es un documento de gran importancia que indica un objetivo a cumplir por parte del encargado y la corporación.[1]

El avance tecnológico también hace que aumenten los delincuentes informáticos y las intrusiones no autorizadas a las empresas para robo de información, secuestro de información o sabotaje, lo que ha obligado a que todas las empresas realicen un manual de políticas de información para poder detectar, prevenir o mitigar cualquier ataque que pueda sufrir la empresa que pueda perjudicar su activo más valioso que es la información.
El riesgo de seguridad se da cuando se une una amenaza con una vulnerabilidad. Esto trae como consecuencia la pérdida o daño de datos, la falta de privacidad, fraude, tiempo de no servicio y la caída de confianza de los clientes.[2]
“Aunque anteriormente la seguridad de la información estaba entendida como la aplicación de un conjunto de medidas de orden físico y lógico a los sistemas de información, para evitar la pérdida de esta, siendo ésta una tarea de responsabilidad exclusiva de los departamentos de informática de las organizaciones”.[3]

Para la creación de soluciones de problemas de seguridad, debemos identificar las posibles opciones para determinar cuál de ellas es la más acertada para alcanzar los objetivos de la organización.[4]
ese proceso lo podemos crear con unas políticas de seguridad de la información solidas que permitan detectar a tiempo las amenazas, y si alguna

se llegase a concretar, tener un manual con los pasos para mitigarla de una forma rápida y adecuada.

Es obligación de todas las organizaciones capacitar a todo el personal sobre los riesgos tecnológicos y de comunicacion, que conozcan la importancia de los activos de la corporación, dar a conocer los riesgos que amenazan la información, las trampas de la ingeniería social de la que se aprovechan los delincuentes para atentar contra la seguridad de la organización. “aspectos que exigen el trabajo en equipo entre los diferentes actores para consolidar un sistema eficaz de gestión de la seguridad de la información” [3]

Debemos crear conciencia en todas las empresas, para que vean la importancia de tener unas políticas de seguridad de la información completas y sólidas para lograr un buen uso de los sistemas informáticos, infraestructura e información de la empresa y así poder mitigar en gran medida las amenazas que se puedan presentar.

7. ESTRATEGIA METODOLÓGICA

A continuación, se explican las técnicas utilizadas para lograr una solución al problema de falta de Políticas de Seguridad de la Información para CORMAGDALENA, en base a los objetivos y el alcance que se propusieron en esta investigación.

La metodología propuesta busca la realización de los objetivos específicos que fueron definidos para lograr el objetivo general del proyecto, por tanto, en esta metodología se tendrá en cuenta la norma ISO/IEC 27002[2] que hace referencia a los controles y tareas que se deberán desplegar para realizar el diseño de las política de Seguridad de la Información.

INSTRUMENTOS DE RECOLECCION DE INFORMACION

Para desarrollar este trabajo, se emplearon instrumentos para la recolección

de información, los cuales se relacionan a continuación:
Cuestionario.
Observaciones.
Reuniones con funcionarios y con la Dirección tecnológica de Cormagdalena.
registro en el sistema de calidad de Cormagdalena.
Teniendo en cuenta las exigencias de la norma ISO/IEC 27002 para el diseño de las Políticas de Seguridad de la Información, se crearon las siguientes fases para el desarrollo de la investigación:

FASE 1: evaluación de las Políticas de seguridad para
determinar el grado de madurez inicial de Cormagdalena, teniendo en cuenta las normas que plantea la ISO/IEC 27002.

FASE 2: preparación de las políticas.
Entender el contexto de la entidad para definir el alcance y las políticas que se van a crear.

FASE 3: Planificación de las Políticas.
Estimar riesgos de seguridad y determinar procedimientos para el tratamiento.
Crear el marco de políticas y sus lineamientos para su debido tramite.

Fase I - Diagnostico.
Pertenece a las actividades para reconocer el nivel inicial que posee Cormagdalena, en relación con el modelo de seguridad planteado por la norma ISO/IEC 27002.
Para la recoger la información se utilizarán los siguientes métodos:
realización de cuestionarios para verificar el nivel de cumplimiento de Cormagdalena con relación a la norma ISO/IEC 27002.
Que documentación hay en el sistema de calidad de Cormagdalena relacionada con seguridad de la información.

Información externa, como encuestas que se encuentran disponibles en línea por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Fase II - Preparación

son las actividades que se van a desarrollar para crear las políticas de Seguridad, las cuales son:

Estudiar la organización, para definir las observaciones internas y externas de Cormagdalena, que son concernientes para implementar las Políticas de Seguridad.

“Definir el alcance del Políticas de seguridad de la Información, en el cual se establece los límites y la aplicabilidad del Sistema de Políticas de Seguridad de la Información”[2].

Definir la Política de Seguridad de la Información.

Definir la estructura organizacional de Cormagdalena que contiene los roles y responsabilidad de las Políticas de seguridad.

Fase III – Planificación.

Se apreciarán las actividades que se conecten con:

determinar los activos de información tecnológicos para su posterior clasificacion dependiendo de su criticidad.

valorar los riesgos de seguridad informática teniendo en cuenta el alcance de las Políticas de seguridad.

Determinar e incluir planes de acción para los controles que se van a implementar con el propósito de disminuir los riesgos que puedan ser identificados en el proceso de calcular los riesgos. se tomará como base los objetivos y controles de la norma ISO/IEC 27002.

Elaborar la declaración de aplicabilidad, que corresponde a un documento que contiene los objetivos de control y controles seleccionados de la norma ISO/IEC 27002, su nivel de cumplimiento y los motivos para su elección o exclusión.

Crear un manual de políticas de seguridad, que contenga los objetivos que se darán a cumplir en Cormagdalena y así poder asegurar la confidencialidad, disponibilidad e integridad de toda la información.

ROLES Y RESPONSABILIDADES

DIRECTOR EJECUTIVO
DEPARTAMENTO: DIRECCION EJECUTIVA
RESPONSABILIDADES CON LAS POLITICAS DE SEGURIDAD DE LA INFORMACION
Planear y controlar todas las actividades administrativas, financieras y de las Políticas de seguridad de la información de Cormagdalena. Además de realizar actividades de mercadeo y supervisión. Realizar la revisión por la dirección a las Políticas de seguridad de la información. Establecer y realizar revisión a las políticas y los objetivos de la Corporación. Analizar los datos arrojados por el análisis de riesgos y tomar las decisiones necesarias para garantizar el mantenimiento y mejoramiento del sistema. Asignar los recursos necesarios a los procesos de las políticas de seguridad de la información Reportar e identificar los riesgos, incidentes o eventos de seguridad de la información que se generen en las actividades desarrolladas a su cargo y/o al de sus compañeros. Velar por la eficaz comunicación al interior de la organización. Garantizar el logro de la política y objetivos de Seguridad de la Información. Reportar e identificar actos y condiciones inseguras durante el desarrollo de las actividades. Cumplir con el plan mínimo de capacitación definido. Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad). Implementar las mejoras identificadas para las políticas de seguridad de la información.

SUBDIRECTOR EJECUTIVO
DEPARTAMENTO: DIRECCION EJECUTIVA
RESPONSABILIDADES CON LAS POLITICAS DE SEGURIDAD DE LA INFORMACION
Verificar y coordinar el cumplimiento del funcionamiento de las Normas ISO Reportar e identificar actos y condiciones inseguras durante el desarrollo de las actividades. Cumplir con el plan mínimo de capacitación definido en las políticas de seguridad de la información. Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad). Implementar las mejoras identificadas en las políticas de seguridad de la información. Cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en Cormagdalena.

SUBDIRECTOR COMERCIAL
DEPARTAMENTO: DIRECCION EJECUTIVA
RESPONSABILIDADES CON LAS POLITICAS DE SEGURIDAD DE LA INFORMACION
Cumplir y hacer cumplir los principios de seguridad de la información en el procedimiento establecido para comercial. Reportar e identificar actos y condiciones inseguras durante el desarrollo de las actividades. Cumplir con el plan mínimo de capacitación definido en las políticas de seguridad de la información. Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad). Implementar las mejoras identificadas en las políticas de seguridad de la información. Cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la Cormagdalena.

ENCARGADO AREA DE LAS TIC
DEPARTAMENTO: SECRETARIA GENERAL
RESPONSABILIDADES CON LAS POLITICAS DE SEGURIDAD DE LA INFORMACION
Velar por el correcto uso y administración de los recursos informáticos de Cormagdalena. Cronograma de mantenimiento de equipos Inventarios de activos Participar en la elaboración del programa de capacitación de las políticas de seguridad de la información y velar por su cumplimiento. Reportar e identificar actos y condiciones inseguras durante el desarrollo de las actividades. Cumplir con el plan mínimo de capacitación definido en las políticas de seguridad de la información. Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad). Implementar las mejoras identificadas las políticas de seguridad de la información. Cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la organización.

SOPORTE AREA DE LAS TIC
DEPARTAMENTO: SECRETARIA GENERAL
RESPONSABILIDADES CON LAS POLITICAS DE SEGURIDAD DE LA INFORMACION
Implementar procedimientos y técnicas para mejorar la eficiencia de la Red y el correcto funcionamiento de los equipos de cómputo bajo la supervisión del encargado de las TIC Hojas de vida de equipos. Cronograma de mantenimiento de equipos. Acciones correctivas y preventivas. Inventario de activos Reportar e identificar actos y condiciones inseguras durante el desarrollo de las actividades.

Cumplir con el plan mínimo de capacitación definido en las políticas de seguridad de la información. Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad). Implementar las mejoras identificadas en las políticas de seguridad de la información. Cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en Cormagdalena.

AREA CONTABLE
DEPARTAMENTO: SECRETARIA GENERAL
RESPONSABILIDADES CON LAS POLITICAS DE SEGURIDAD DE LA INFORMACION
Registrar hechos económicos, de tal modo que la información emanada de la contabilidad sea comprendida por todos los que la utilizan para tomar decisiones. Cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en Cormagdalena. Cumplir con el plan mínimo de capacitación definido en las políticas de seguridad de la información. Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad). Implementar las mejoras identificadas en las políticas de seguridad de la información.

ACTIVOS DE INFORMACION DE TECNOLOGIA				
No	**Nombre del Activo**	**Descripción del Activo**	**Tipo de activo**	**Contenedor**
A1	Centro Principal de Procesamiento	Centro Principal de procesamiento donde reside la infraestructura para soporta la operación del negocio	Instalaciones	Data Center del proveedor
A2	Centro Alterno de Procesamiento	Centro Alterno de procesamiento que contiene la infraestructura para la continuidad del negocio	Instalaciones	Data Center del proveedor
A3	Cuartos de comunicaciones	Instalación física donde residen los racks de comunicaciones	Instalaciones	Cuartos de rack

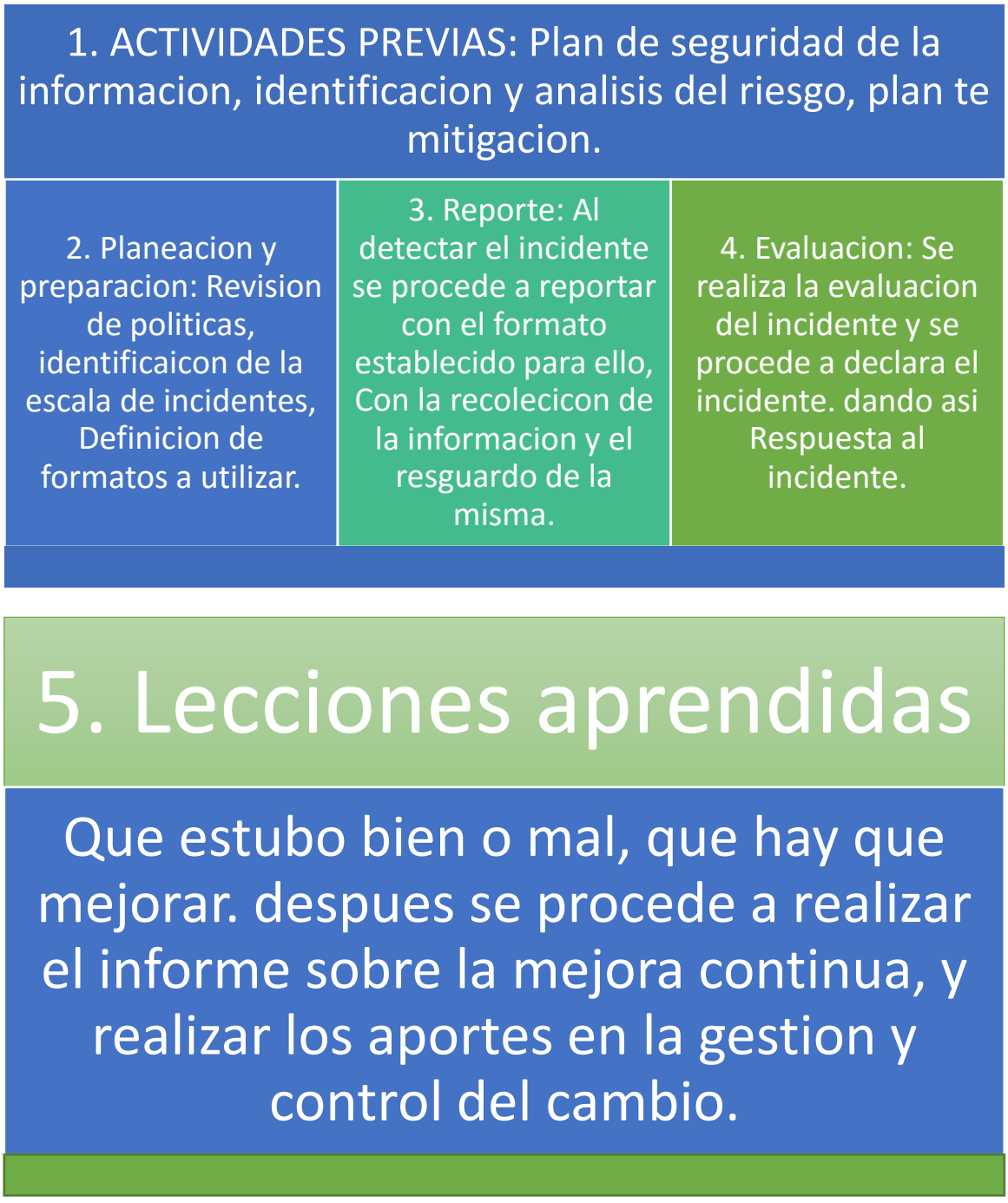
A4	Área administración de plataforma	Instalación física donde están ubicados los administradores de plataforma	Instalaciones	Área administración de plataforma
A5	Red LAN	Red LAN corporativa de la entidad	Redes de comunicaciones	Red LAN
A6	Red WAN	Red WAN de la entidad	Redes de comunicaciones	RED WAN
A7	Red WIFI corporativa	Red Wifi utilizada por los equipos móviles para acceder a los recursos de la red corporativa de la entidad	Redes de comunicaciones	Red LAN
A8	Red WIFI invitados	Red Wifi para invitados	Redes de comunicaciones	Red LAN
A9	Servidores de administración	Servidores que soportan los servicios bases de administración	Equipos informáticos	Data Center del proveedor
A10	Servidores de bases de datos de producción	Servidores de producción que soportan los motores e instancias de bases de datos	Equipos informáticos	Data Center del proveedor
A11	Servidores de aplicaciones de producción	Servidores de producción que soportan las aplicaciones y sistemas de información	Equipos informáticos	Data Center del proveedor
A12	Plataforma de Correo	Servidores que soportan la plataforma y servicio de correo corporativo	Equipos informáticos	Data Center del proveedor
A13	Servidores de Pruebas	Servidores que soportan los ambientes de prueba de la entidad	Equipos informáticos	Data Center del proveedor
A14	Servidores de Desarrollo	Servidores que soportan los ambientes de desarrollo de la entidad	Equipos informáticos	Data Center del proveedor
A15	SAN	Unidades de almacenamiento donde reside la información de la entidad	Equipos informáticos	Data Center del proveedor
A16	Solución de Backup	Solución de Backup para el respaldo de información del negocio	Equipos informáticos	Data Center del proveedor
A17	Dispositivos de red	Equipos y dispositivos de red activos (switch, router)	Equipos informáticos	Cuartos de rack
A18	Computadores Administradores	Computadores que utilizan los administradores de plataforma	Equipos informáticos	Área administración de plataforma
A19	Computadores de escritorio usuarios	Computadores de escritorio asignados a los colaboradores de la entidad	Equipos informáticos	Computadores
A20	Portátiles	Computadores portátiles de la entidad	Equipos informáticos	Portátiles
A21	Impresoras	Impresoras de la entidad ubicada en diferentes áreas	Equipos informáticos	Impresoras
A22	Equipos de seguridad perimetral	Equipos informáticos destinados a proteger la seguridad perimetral de la entidad	Equipos informáticos	Equipos de seguridad perimetral

Matriz con clasificación, evaluación y respuesta a los riesgos de Activos - Vulnerabilidades

No	Vulnerabilidad	Amenazas	Riesgo	Categoría
1.	**Hardware desactualizado.**	**Sistemas lentos, correos perdidos.**	**Servicio afectado**	**Hardware**
2.	**Datos en Bases desactualizados**	**Perdida de contenido o bases desactualizadas**	**Afectación a la seguridad de la empresa**	**Personal**
3.	**Hardware obsoleto**	**Desgaste**	**Reducir el funcionamiento óptimo del sistema.**	**Hardware**
4.	**Ubicación errada del centro de computo**	**Acceder fácilmente a él.**	**Fuga de la información.**	**Jefe Seguridad**
5.	**Equipos de segunda**	**Bajo rendimiento en los procesos**	**Afectación en el servicio**	**Personal**
6.	**Mal Proceso de selección**	**Personal contratado sin confirmar información**	**Perdida de información.**	**Personal**

MODELO PARA GESTIONAR LOS INCIDENTES DE SEGURIDAD.

Este se realizará con fases para una mejor claridad del modelo.



8. DESARROLLO E IMPLEMENTACIÓN

Se desarrollarán las fases que se definieron para diseñar las Políticas de Seguridad de la Información de CORMAGDALENA, las cuales tienen una secuencia que permite lograr el objetivo general.

Se relacionan los elementos y datos realizados para implementar las fases definidas para la creación de las Políticas de Seguridad de la Información de CORMAGDALENA.

- La información se recolecto por medio de las diferentes técnicas y que fueron utilizadas para analizar y diagnosticar.
- Las conclusiones de los análisis realizados.
- El resultado de la valoración de riesgos.
- La norma ISO/IEC 27002 que contiene las exigencias de las Políticas de seguridad que se deben realizar.

FASE I. DIAGNOSTICO

Se muestra la valoración que se realizo para poder obtener información inicial de la situación en que esta CORMAGDALENA en cara a las Políticas de Seguridad con base en la norma ISO/IEC 27002.

DIAGNOSTICO ESTADO ACTUAL DE LA SEGURIDAD

Se presenta un estudio completo de las situaciones que amenazan la seguridad de CORMAGDALENA, las cuales permiten detrminar que el problema es un Inadecuado o faltante Modelo de Políticas de Seguridad de

la Información.

Las situaciones identificadas son las siguientes:

Inadecuado tratamiento de Seguridad en CORMAGDALENA.

Falta de capacitación en temas de seguridad a las dependencias y funcionarios.

No hay una participación activa de Cormagdalena en controles de seguridad y evaluación de riesgos.

Los funcionarios no diferencian o reconocen la diferencia entre seguridad de la información y seguridad informática.

No hay un sistema adecuado para la gestión de riesgos de seguridad de la información.

No hay una valoración adecuada de riesgos de seguridad de la información.

FASE II. PREPARACION

Corresponde a las actividades que se desarrollaron para conformar las Políticas de Seguridad de la Información en Cormagdalena.

CONTEXTO DE LA ORGANIZACION

La norma ISO/IEC 27001:2013 recalca la importancia de conocer las causas externas e internas de la organización, que pueden ser afectados o afectar de manera positiva o negativa por la implementación de las políticas de Seguridad.

Por este caso, la norma ISO/IEC 27001:2013 tiene el capítulo “4. CONTEXTO DE LA ORGANIZACIÓN”, donde dice que la corporación debe decidir que situaciones o factores internos y externos la rodean y que son concernientes para crear las políticas de Seguridad.

FASE III. PLANIFICACION

En esta fase se realizaron las actividades necesarias para poder que el

diseño de las Políticas de Seguridad, pueda cumplir los objetivos propuestos, como la identificación de los riesgos y las acciones correspondientes para poderlos mitigar.

Las actividades que se realizaron en la clasificación de los activos identificando su valoración de riesgos, fueron desarrollados de la siguiente manera:

Identificación de activos: se realizó teniendo en cuenta el alcance de las Políticas de Seguridad, los cuales solo consideran el proceso de tecnología.

Metodología para la clasificación y valoración de sus riesgos. las actividades fueron desarrolladas identificando y clasificando los activos y con la respectiva valoración de los riesgos, para esto se utilizó la metodología de las MINTIC[7]

Quedando el documento presentado al área así:

POLITICAS DE SEGURIDAD CORMAGDALENA.

1. Los elementos de la corporación son de uso exclusivo de ella, cualquier cambio en la normatividad, será expresada y adecuada como política de seguridad en este documento.
2. La corporación CORMAGDALENA nombrará un comité de seguridad, que dará alcance al cumplimiento de la normativa de las políticas de seguridad de la información, así:

    a. Gestión y procedimiento de la información
    b. Aplicación de sanciones
    c. Cumplimiento de políticas
    d. vigilar la seguridad de los activos informáticos
    e. Capacitación de trabajadores en temas de seguridad
    f. Establecer un plan de contingencia, para dar solución al problema de seguridad dentro de Cormagdalena.

g. Orientar planes necesarios para mitigar cualquier eventualidad que se pueda presentar.

Este comité estará integrado por: Gerencia, Gestor de seguridad y Administrador.

3. Los trabajadores en cada cargo asignado serán los únicos responsables de las actividades que resulten de sus acciones.
4. El jefe del área de sistemas es el encargado de que los servidores del sistema permanezcan siempre activos y en buen estado.
5. Los usuarios de cargos que lo especifique en el manual de procesos y funciones, tendrán acceso a la red, siempre y cuando cumplan con el mínimo de seguridad para poder acceder al servicio. Siguiendo las normas de los encargados del área de sistemas.

1.2 EXCEPCIONES DE RESPONSABILIDAD

2. pueden estar exentos de cualquier responsabilidad, debido a su cargo, o por alguna situación que lo amerite. estas excepciones deberán ser solicitadas por escrito al encargado el cual dará su aprobación después de analizar la situación e informará a la gerencia para una decisión final.

2. **CLASIFICACION Y CONROL DE ACTIVOS**

RESPONSABILIDADES.

1. En cada área habrá un responsable por los activos de mayor importancia para la Cormagdalena.
2. Se encargará de salvaguardar los activos físicos como: (hardware y medios magnéticos, computadores, impresoras.), activos de

información (Bases de Datos, Archivos, programas, software).

3. El área de sistemas son los responsables de la custodia y seguridad de estos activos.

2.1 **CLASIFICACION DE LA INFORMACION**

1. De manera individual los departamentos de CORMAGDALENA son los encargados, de clasificar según el nivel de importancia, la información que en ella se procese.
2. Los niveles son:
   a. Publica
   b. Interna
   c. Confidencial

2.2 SEGURIDAD PARA EL PERSONAL

1. En cuanto a los contratos se le entregara, la documentación que sea necesaria para realizar sus labores dentro Cormagdalena.
2. La información que se maneje por acción de su trabajo, será de propiedad y uso exclusivo de CORMAGDALENA.

2.2. CAPACITACION A USUARIOS.

1. Los empleados estarán en constante capacitación de seguridad, según las funciones y actividades que estos desarrollen dentro de Cormagdalena.
2. Se tendrán en cuenta todas las medidas necesarias de seguridad, para capacitar personal ajeno a la corporación.

2.3. **RESPUESTAS A ANOMALIAS O INCIDENTES DE SEGURIDAD**.

1. Se realizarán backups de seguridad, diariamente, para los activos de mayor criticidad, uno semanal y uno mensual.
2. Estos respaldos serán guardados y se evitara utilizarlos a menos que sea estrictamente necesario.
3. Las fallas que se presenten por dos o más trabajadores en el área se trataran de inmediato para su solución.
4. El encargado del área de seguridad deberá dar un documento que elaborará explicando paso a paso para seguirlas en contratiempos a la seguridad con la explicación detalladamente.
5. Cualquier situación que este en contra de la seguridad de la compañía deberá ser documentada y posterior mente el área encargada deberá revisar los registros con el objetivo de dar respuesta congruentes y acordes con el problema.

2.1. CONTROL DE ACCESO.

1. El encargado del área de seguridad brindara la documentación que sea necesaria para poder utilizar de manera correcta y segura los sistemas, controles, guías y demás elementos que se llegasen a necesitar.
2. Siguiendo los canales de gestión formalmente establecidos, se deberá pasar cualquier petición de información, el no realizarlo dará:
   a. Negativa por parte del área, sin poder realizar

el cumplimiento de la acción.

b. Informe completo de la persona o el área que hizo caso omiso a la norma.
c. Sanciones impuestas por autoridades de otro nivel superior.

2.2. **ADMINISTRACION DE ACCESO DE USUARIOS**.

1. Son usuarios del sistema, los empleados de CORMAGDALENA los cuales sean de planta o estén por contratos de prestación de servicios.
2. Se asignará un usuario y un password para que puedan acceder a la intranet de la corporación, con sus respectivos permisos a los que este accederá.
3. El acceso a la red por parte de terceros está totalmente prohibido.
4. No se proporcionará el servicio solicitado sin antes haberse completado todos los procesos requeridos y autorizaciones necesarias.
5. Se dará una contraseña temporal en caso de que el usuario olvide o extravié su contraseña al que lo solicite presentando su identificación.
6. La longitud mínima de caracteres para las contraseñas será de 6. Los cuales tendrán una combinación alfanumérica con caracteres especiales.
7. La longitud máxima de caracteres para las contraseñas será de 8. Los cuales deberán tener una letra mayúscula.

2.3. RESPONSABILIDADES DEL USUARIO

1. El usuario es el responsable de tener a salvo su contraseña, ya que esta es personal e

intransferible.

2. El usuario se hará responsable del mal uso que haga en el acceso a los sistemas.
3. No se podrá guardar o escribir las contraseñas en papeles o superficies que puedan ser vistas por terceras personas.
4. Se deberá eliminar cualquier rastro de documentación o información que Cormagdalena proporcione y pueda ser vista por un tercero.
5. No se permitirá que se generen claves con alguna característica personales o relacionado con fechas de cumpleaños o fechas importantes.
6. se deberá proteger el equipo de trabajo, y no permitir que personas ajenas accedan a él.
7. Cualquier usuario que encuentre una falla en el sistema de seguridad está obligado a reportados a los administradores de inmediatamente.

4.1**. USO DE CORREO ELECTRONICO**.

1. El servidor de correo electrónico es de uso institucional únicamente, y se deberán cumplir todas las medidas de seguridad para su utilización.
2. El uso indebido del servidor de correo electrónico será motivo cierre temporal del correo.
3. El empleado se hará responsable de la información y archivos que se envíen desde su cuenta.

4.2. SEGURIDAD ACCESO A TERCEROS

1. Los permisos a terceros se darán siempre y cuando se cumplan con todos los requisitos de seguridad que estén establecidos en el contrato de trabajo.
2. Los usuarios externos, solo podrán utilizar el servicio que le fue asignado.

4.3. CONTROL DE ACCESO A LA RED.

1. El acceso a la red interna de Cormagdalena solo se permitirá cuando se cumplan todos los requisitos de seguridad.
2. Se eliminará cualquier acceso a la red que no haya sido permitida.
3. Cualquier anomalía del tráfico de red desde los dispositivos, se verificará inmediatamente y se hará una auditoria.
4. El departamento de informática deberá usar los dispositivos adecuados para el bloqueo y enrutamiento y así evitar el flujo de información no autorizado hacia la red de Cormagdalena.
5. Se prohibe el acceso a los dispositivos de red, utilizando archivos de registro.
6. Se ejecutará revisión de log de los dispositivos de acceso a la red en un tiempo predeterminado de 24 horas.

5.1. CONTROL DE ACCESO AL SISTEMA OPERATIVO.

1. Se cancelarán las cuentas de usuarios que ya no

laboren en Cormagdalena.

2. Al momento de terminar la jornada laboral, los trabajadores verificaran que sus equipos de trabajo queden apagados y que no haya dispositivos USB o discos duros con información conectados a estos.
3. En cuanto a los servidores, el acceso al sistema es autorizado únicamente al usuario administrativo.
4. cualquier programa instalado en los servidores, será ejecutado bajo cuentas que estén autorizadas.
5. Todas las aplicaciones tendrán que estar bien diseñadas, con acceso específico para cada usuario.
6. Se realizarán revisiones a las aplicaciones, antes de ponerlas en operación.
7. Los resultados de las aplicaciones en la red, tendrán que ser documentadas, y decir que terminal es el que deberá ejecutar la salida de información.
8. Se designará el nivel de permisos de las aplicaciones, teniendo en cuenta el nivel de criticidad y haciendo referencia a los derechos de escritura, ejecución, modificación o borrado de información.

5.2. MONITOREO

1. Se inspeccionará y guardará toda actividad que provenga del uso de las aplicaciones y sistemas de información, así como el uso de la red, por medio de bitácoras.
2. Se realizará copia automática de los archivos de Log, y se enviará hacia otra terminal, para que no se guarde en el mismo terminal donde se genera dicha copia.

5.3. GESTION DE OPERACIÓN

1. La puesta en marcha de servicios, son normas

dadas por los encargados de informática, y el personal de comité de seguridad.

2. El personal a cargo de los servicios trasladará los archivos de registro de fallas de seguridad y los revisará de forma seguida.
3. El visto bueno del software se dará por la Gerencia de la Cormagdalena, previo estudio y una vez se hayan realizado pruebas por el personal encargado.

6.1. MEDIOS DE ALMACENAMIENTO.

1. el almacenamiento de información crítica o backups serán manejados solamente por el personal a cargo de dicha labor.
2. Toda unidad de almacenamiento que contenga información crítica será guardada en un sitio de seguridad cuyo acceso será dado únicamente a el encargado de seguridad o la gerencia de Cormagdalena.

9. RESULTADOS

Los resultados obtenidos con la implementación de las políticas para la seguridad de la empresa CORMAGDALENA, son favorables para los objetivos esperados por el proyecto realizado; ya que, con la ayuda de la información obtenida con los cuestionarios, entrevistas, documentación, y lo observado en la empresa se logra canalizar las fases del proyecto con satisfacción como lo fue poder realizar con la fase 1,2 y 3. Donde se recoge la información inicial para realizar las políticas de seguridad que es el tema central de este proyecto. A medida del desarrollo se fue corrigiendo cada

punto que está pendiente y así poder obtener el resultado que fue realizar las políticas de seguridad de la empresa CORMAGDALENA.

Quedando así que ahora la empresa esta adecuada en cuanto al gobierno de seguridad, ya que cuenta con la capacitación adecuada para todas las dependencias y funcionarios frente al tema de seguridad. Tanto sobre la seguridad informática y seguridad de la información. Logrando que toda la empresa participe activamente en la definición de los controles que se implementaron, así hablar un mismo idioma y presentando constantemente una evaluación del riesgo en cada área.
Teniendo así un canal de comunicación activo que hace parte del sistema de información para la gestión de riesgo de seguridad y su valoración.

La empresa CORMAGDALENA logra aumentar su productividad con estas políticas ya que la seguridad aumento totalmente, no hay perdida de datos, hoy cuenta con backups, copias de seguridad periódicas para la protección de sus datos.
Con los controles establecidos la empresa CORMAGDALENA pudo sopesar todas las fallas que estaban teniendo, dejando así un área de seguridad más sólida para el apoyo en cualquier eventualidad que se presente en la empresa.

10. DISCUSIÓN Y CONCLUSIONES.

La implementación de políticas para la compañía CORMAGDALENA es fundamental para su proceso vital y para que esta se consolide como una empresa que este a la vanguardia frente a las demás compañías que manejan la misma actividad económica; es así como vemos que la compañías en la que trabajamos presenta en sus resultados una gran mejora pues se sabe que las políticas de seguridad siempre ayudaran a que se resguarde la

información permitiendo que estas puedan ser renovadas cada vez que así lo requiera la empresa.

Para el área de TI, ha significado tener el control de esta área que tanto lo requería, con la finalidad de poder dar el valor agregado para la mejora constante de la compañía que lo necesitaba.
Es necesario que el área, realice algunas pruebas pertinentes para que el proceso de las políticas pueda ir en mejora constante ya que esto es lo bonito de realizar este tipo de trabajos, porque se está en constante aprendizaje y que este permita la creación de más políticas a favor de la seguridad de la compañía.

ANEXOS:

A. Documento ISO 27002- Controles de seguridad

B. Articles 5482_G7 Gestión de riesgo.

11. REFERENCIAS

[1] Mintic, “Seguridad Y Privacidad De La Información,” *Evid. Digit.*, no. 13, 2016.

[2] R. Perez, “Documento Normativo para la Implementación de Políticas de Seguridad en la ...: EBSCOhost,” *Rev. Técnica la Empres. Telecomunicaciones Cuba*, vol. 6, no. 2/3, pp. 66–72, 2009.

[3] A. Velasco, “EL DERECHO INFORMÁTICO Y LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN UNA PERSPECTIVA CON BASE EN LA NORMA ISO 27 001. (Spanish),” *Rev. Derecho*, no. 29, pp. 333–366, 2008.

[4] J. Areitio Bertolín, *Seguridad de la información : redes, informática y sistemas de información*. Paraninfo Cengage Learning, 2008.

[5] Colciencias, “Modelo de Medición de Grupos, de Investigación, Desarrollo Tecnológico o de Innovación y reconocimiento de investigadores del Sistema Nacional de Ciencia, tecnología e Innovación 2014.” 2014.

[6] Mintic, “Seguridad Y Privacidad De La Información,” Evid. Digit., no. 13, 2016.

[7] MINTIC, “Guía de gestión de riesgos,” Mintic, no. 7, p. 39, 2016.