Maestría en Dirección Estratégica de la Información

Cohorte 2019 – 2020

Título del Trabajo Final:

"Plan Estratégico de Sistema de Gestión de Seguridad de la Información para el grupo CESIJO"

Autor: ***Ing. Martin Pires***
Legajo: ***1106192***

Director del Trabajo Final: ***Mg. Pablo Fernández***

Institución a la que pertenece: UADE Business School

Fecha de entrega: ***17/09/2019***

DEDICATORIA

Esta tesis está dedicada a mi madre por su apoyo constante, por llenar mi vida con valiosos consejos. Me ha hecho sentir seguro de mí mismo.

A mis hijos y mi mujer quienes con su amor, paciencia y aceptación me han permitido llegar a cumplir hoy un nuevo logro profesional.

Finalmente quiero dedicar esta tesis a todas las personas que fueron y son parte de mi vida, por apoyarme y por el amor brindado cada día.

AGRADECIMIENTOS

En primer lugar, agradezco a todos los docentes de la maestría Direcciones Estrategia de la Información, en especial a mi director de tesis, Mg Pablo Fernandez por haberme orientado en todos los momentos que necesité sus consejos y formar parte de otro objetivo personal alcanzado.

Agradezco a la Universidad Argentina de Empresa, por los valiosos conocimientos adquiridos en estos años posibilitando continuar desarrollarme como persona y profesional.

Finalmente, a mis padres, colegas y amigos que me brindaron su apoyo para obtener un nuevo logro profesional.

ABSTRACT

The main objective of this work focuses on the necessary actions for an organization to align with the ISO / IEC 27001: 2013 standard.

This allows correct security measure application in order to control status and usage of information, aiming for an adequate management of confidentiality, integrity and availability of information assets.

An exhaustive analysis was carried out on controls defined by the ISO/IEC 27002:2013 standard with the goal of identifying strategic plan guidelines. Result will be source of information to detect complex situations which an organization might face in relation to information security management.

In order to facilitate the budget planning process related to such projects, results are grouped in short, medium and long term sections.

RESUMEN

El presente trabajo centra su objetivo en las acciones necesarias para alinear una organización con los requerimientos de la norma ISO/IEC 27001:2013, lo que permitirá a la empresa gestionar y aplicar de forma adecuada las medidas de la seguridad mencionadas para controlar el estado y la utilización de la información, con el fin de gestionar adecuadamente la confidencialidad, integridad y disponibilidad de los activos de la información.

Para identificar los lineamientos del plan estratégico se realizó un análisis exhaustivo de todos los controles definidos por la ISO/IEC 27002:2013. El resultado obtenido será fuente de información para detectar situaciones complejas que enfrente la organización respecto a la gestión de la seguridad de la información.

El plan estratégico está compuesto por 14 proyectos, cada uno cubre los objetivos especificados en cada capítulo de la Norma ISO/IEC 27001:2013.

Con el fin de facilitar a la empresa la reserva de presupuestos para abordar los proyectos que componen dicho plan, se los planifico agrupándolos en proyectos a corto, mediano y largo plazo.

ÍNDICE

1. INTRODUCCIÓN 9
1.1. VISIÓN PLAN ESTRATÉGICO DE TI/SI 9
1.2. OBJETIVOS Y ALCANCES 9
2. MARCO METODOLÓGICO Y MARCO CONCEPTUAL 10
3. PLAN ESTRATÉGICO DE TI/SI: SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GRUPO CESIJO 11
3.1. CASE FOR ACTION 11
3.1.1. PROBLEMA 11
3.1.2. MERCADO 12
3.1.3. DIAGNÓSTICO 12
3.1.4. COSTO DE LA INACCIÓN 13
3.2. SITUACIÓN ACTUAL DE TI/SI – DIAGNÓSTICO 14
3.2.1. DESCRIPCIÓN DE GRUPO CESIJO 14
3.2.2. ORGANIGRAMA UNIDADES DE NEGOCIO 16
3.2.3. NEGOCIOS FORESTALES 17
3.2.4. ORGANIGRAMA EMPRESA FORESTAL 17
3.2.5. PROCESO PRODUCTIVO FORESTAL 18
3.2.6. PROCESO COSECHA 19
3.2.7. ETAPAS DE LA COSECHA 21
3.2.8. ÁREAS COORPORATIVAS DE GRUPO CESIJO 21
3.2.9. ORGANIGRAMA ÁREAS CORPORATIVAS 22
3.2.10. ÁREA CORPORATIVA DE SISTEMAS 22
3.2.11. ORGANIGRAMA DE SISTEMAS 23
3.2.12. MAPA DE APLICACIONES DE SISTEMAS 23
3.2.13. INFRAESTRUCTURA Y SEGURIDAD 27
3.2.14. GESTIÓN DE LA SEGURIDAD 29
3.2.15. INVERSIONES EN SISTEMAS 29
3.2.16. ANÁLISIS DE CONTROLES ISO 27002 30
3.2.17. FODA 33
3.3. NUEVOS PROYECTOS DE TI/SI QUE COMPONEN EL PLAN ESTRATÉGICO 38

3.3.1. PROYECTOS DEL PLAN ESTRATÉGICO. 39
3.3.2. PLAN DE ACCIÓN A CORTO PLAZO 39
Proyecto: MARCO NORMATIVO DE SEGURIDAD 41
Proyecto: CRIPTOGRAFÍA 43
Proyecto: ORGANIZACIÓN DE LA SEGURIDAD 45
Proyecto: GESTIÓN DE ACTIVOS 47
Proyecto: SEGURIDAD EN LAS COMUNICACIONES 50
3.3.3. PLAN DE ACCIÓN A MEDIANO PLAZO 52
Proyecto: SEGURIDAD DE LOS RECURSOS HUMANOS 53
Proyecto: SEGURIDAD FISICA 55
Proyecto: CONTROL DE ACCESO 58
Proyecto: SEGURIDAD DE LAS OPERACIONES 60
Proyecto: SEGURIDAD EN DESARROLLO DE SISTEMAS 62
Proyecto: GESTIÓN DE INCIDENTES DE SEGURIDAD 65
3.3.4. PLAN DE ACCIÓN A LARGO PLAZO 68
Proyecto: RELACIONES CON LOS PROVEEDORES 69
Proyecto: GESTIÓN DE CONTINUIDAD DE NEGOCIO 70
Proyecto: CUMPLIMIENTO 73
PROGRAMA DE CAPACITACIÓN Y CONCIENTIZACIÓN 76
3.3.5. EVOLUCIÓN DE LA SEGURIDAD POR PLAZOS 77
3.4. ESTRATEGIA DE MANAGEMENT 78
3.4.1. GESTIÓN DE PROYECTOS 78
3.4.2. GESTIÓN DE RECURSOS HUMANOS 81
3.4.3. GESTIÓN DE PROVEEDORES 83
3.5. PLAN DE IMPLEMENTACIÓN 84
3.6. PRESUPUESTO 88
4. CONCLUSIONES 89
4.1. ASPECTOS DE IMPLEMENTACIÓN 90
4.2. FUTURAS LÍNEAS 91
5. BIBLIOGRAFÍA 91
6. ANEXOS 92
6.1. ANEXO 1: ENTREVISTA DIRECTOR FORESTAL 92
6.2. ANEXO 2: ENTREVISTA GERENTE FORESTAL 93

6.3. ANEXO 3: ENTREVISTA GERENTE FORESTAL 94
6.4. ANEXO 4: ENTREVISTA SUPERVISOR DE COSECHA 95
6.5. ANEXO 5: ENTREVISTA GERENTE DE TECNOLOGÍA 95
6.6. ANEXO 6: CUMPLIMIENTO DE CONTROLES DE SEGURIDAD 96
6.7. ANEXO 7: CURRICULUM VITAE 102

1. INTRODUCCIÓN

Grupo CESIJO es un conjunto de empresas de capitales argentinos comprometido con el desarrollo del país en proyectos de largo plazo. Las áreas de negocio son Ciencias de la Vida, Agronegocios, Información & Cultura y Naturaleza & Diseño. Adicionalmente a las áreas descriptas, Grupo CESIJO cuentas con áreas corporativas que dan soporte transversal a las distintas empresas que conforman el grupo. Éstas son: Recursos Humanos, Legales, Finanzas, Sistemas, I+D y Comunicaciones.

El Plan Estratégico surge a partir del cambio de CEO de Grupo CESIJO, el cual se produce en el mes de octubre del 2018. En el inicio de la nueva gestión, se solicita la generación de un plan Estratégico de Sistema de Gestión de Seguridad de la Información, con el objetivo de gestionar adecuadamente los activos de información de la empresa.

Dicho sistema, basado en la norma ISO 27001, permite que las empresas gestionen de manera eficiente los activos de información, para asegurar la integridad, confidencialidad y disponibilidad de los mismos.

1.1. VISIÓN PLAN ESTRATÉGICO DE TI/SI

Gestionar adecuadamente la confidencialidad, integridad y disponibilidad de los activos de información utilizados, cumpliendo con el estándar internacional de seguridad de la información ISO/IEC 27001:2013. Se establece como meta el alcance del 60% del Modelo de Madurez de Capacidad (Nivel 3 CMMI).

1.2. OBJETIVOS Y ALCANCES

El objetivo principal de este trabajo es alinear la organización con los requerimientos de la norma ISO/IEC 27001:2013. Por lo cual se propone desarrollar un Plan Estratégico de Sistema de Gestión de Seguridad de la Información (SGSI) en Grupo CESIJO, para el período 2019-2021. Teniendo como meta conseguir el 60% de madurez del Modelo de Madurez de Capacidad (Nivel 3 CMMI), de manera que permita gestionar adecuadamente la confidencialidad, integridad y disponibilidad de los activos de información.

Para el logro de dicho objetivo, se implementarán los controles especificados en el anexo A de la norma ISO/IEC 27001:2013 en el Sistema de Planificación de Recursos Empresariales (ERP) de la empresa Forestal con sede en Argentina. El alcance del mismo estará fijado en el proceso de Cosecha, se centrará el análisis en la información soportada en formato digital.

El resto de los procesos de la empresa Forestal, así como las empresas restantes que conforman el grupo CESIJO serán integradas al Plan Estratégico en una etapa posterior.

2. MARCO METODOLÓGICO Y MARCO CONCEPTUAL

En función de los objetivos propuestos, se opta por utilizar el enfoque mixto.

Los aspectos del enfoque cuantitativo adoptados consistirán en el uso de datos numéricos, los cuales serán analizados con criterios estadísticos, permitiendo identificar el cumplimiento de los distintos controles establecidos, así como procedimientos estandarizados y aceptados por la comunidad científica (controles definidos en el anexo A de la norma ISO/IEC 27001:2013). En lo que respecta al enfoque cualitativo, se utilizarán métodos de recolección de datos no estandarizados, para identificar la existencia y el uso de normas y procedimientos establecidos en la organización.

Se usarán fuentes primarias y secundarias de recolección de datos.

Las técnicas a utilizar como fuentes primarias son:

- Entrevistas y Encuestas: se realizarán entrevistas y encuestas a las distintas personas que intervienen en el proceso de cosecha, con el objetivo de determinar el nivel de cumplimiento de los controles establecidos en el anexo A de la norma ISO/IEC 27001:2013.
- Normas ISO:
  - ISO/IEC 27001. 2013 - *Information technology. Security techniques. Information security management systems. Requirements*. Ginebra, Suiza, 2013.
  - ISO/IEC 27002. 2013, *Information technology - Security Techniques - Code of practice for information security controls*. Ginebra, Suiza, 2013.

En lo que respecta a las fuentes secundarias, se usarán:

- Investigaciones sobre la utilización del Sistemas de Gestión de la Seguridad de la Información.
- Artículos afines y sitios en Internet.
- Estudio de documentación: en el caso de contar con documentos que describan el proceso de cosecha se analizará si la misma está alineada a algunos de los 14 dominios definidos por la norma.

El tipo de diseño utilizado será el descriptivo. Se observarán los procesos estandarizados e informales, el nivel de uso y la aceptación por parte del grupo CESIJO. Adicionalmente, se indagará el grado de cumplimiento de los procedimientos establecidos.

3. PLAN ESTRATÉGICO DE TI/SI: SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GRUPO CESIJO

3.1. CASE FOR ACTION

3.1.1. PROBLEMA

Se destaca como problema nodular la ausencia de una cultura organizacional de seguridad de la información. Grupo CESIJO no la considera como un factor relevante, por lo cual no existen recursos destinados exclusivamente para su gestión.

No cuenta con políticas ni procedimientos formales relacionados con la seguridad de la información, como tampoco acuerdos de confidencialidad con los empleados y proveedores.

Se identificaron responsabilidades incompatibles dentro del área de sistemas lo que podría generar accesos o modificaciones no autorizadas, no intencionales o simplemente el incorrecto uso de los activos de la información.

3.1.2. MERCADO

La superficie forestal argentina está conformada por 33,1 millones de hectáreas de monte nativo y aproximadamente 1,2 millones de hectáreas de monte implantado. Existen más de 42 mil hectáreas destinadas a la producción, lo cual implica que aproximadamente el 2% del Producto Bruto Interno Nacional (PBI) corresponde a la industria forestal. [1]

La Argentina es una de las regiones del mundo con mayores ventajas naturales por el rápido crecimiento de sus plantaciones y su potencial productivo.

En relación a las perspectivas del sector, de acuerdo a las asociaciones de productores forestales se prevé que, la Argentina posee potencial disponible para alcanzar una superficie de 5 millones de hectáreas forestadas y que, de lograr esta expansión, el país podría triplicar sus exportaciones; pasar de los 800 millones exportados en 2012 a superar los 3000 millones de dólares en un lapso aproximado de 10 años.

3.1.3. DIAGNÓSTICO

Según fuentes consultadas en la investigación, los directivos del Grupo CESIJO no consideran necesario invertir en recursos especializados en el área de seguridad de la información, ni en destinar una partida presupuestaria para tratar adecuadamente los activos de información. Las únicas inversiones, en relación a la seguridad, se centran en la compra de equipamiento informático específico para proteger los activos de la empresa.

La seguridad de la información e informática es administrada por el área de Tecnología. No existe un equipo de profesionales que se dedique específicamente a gestionarla. El personal encargado de la seguridad es el mismo que define y controla la utilización de los activos de información.

[1] SERVICIO NACIONAL DE SANIDAD Y CALIDAD AGROALIMENTARIA VIRTUAL [en línea]. [consulta 8 feb. 2019]. <http://www.senasa.gob.ar/senasa-comunica/noticias/bosques-argentinos-actividad-forestal-y-economias-regionales>

Las empresas que conforman el grupo presentan una cultura informal, donde no existen procedimientos normalizados, ni se realizan acciones de concientización respeto al uso de la tecnología ni de los riesgos asociados al uso de la misma.

3.1.4. COSTO DE LA INACCIÓN

En la actualidad la transformación digital atraviesa el funcionamiento en general. Se produce un mayor uso de herramientas de tecnologías de información y comunicación para realizar labores comunes y cotidianas, que benefician en términos de tiempo y esfuerzo. Sin embargo, aunque existen numerosas ventajas, también existen riesgos que necesariamente deben ser tenidos en cuenta para evitar problemas con los activos de información.

La información que maneja Grupo CESIJO es uno de sus principales activos, la protección del mismo de posibles ataques de seguridad, internos o externos a la empresa, es algo imprescindible.

Un problema de integridad por alteración indebida de datos, afectaría directamente los ingresos provenientes de la venta, por ejemplo, la modificación del pesaje de los troncos que van a transportar los camiones. Otro factor significativo podría ser que, empleados sin derechos de acceso, puedan manipular información confidencial del área de recursos humanos o finanzas.

Se presentan tres escenarios que demuestran la importancia de gestionar adecuadamente la seguridad en los activos de información de la empresa:

1- Problemas de Integridad por alteración de datos.
El precio de la tonelada del tronco paraíso tiene un costo de U$S 170. Un camión soporta una carga máxima de 30 toneladas. De esta forma cada camión transporta un importe total de U$S 5.100. Si el operador del sistema de pesaje por error o adrede modifica la cantidad de toneladas de troncos a transportar alteraría el importe total de la carga, generando cuantiosas pérdidas.

2- Problema de disponibilidad.

El promedio de la facturación diaria de la empresa forestal es U$S 8.500, la no disponibilidad de los sistemas utilizados durante el proceso de cosecha puede generar grandes implicancias al negocio.

3- Acceso no autorizado.

Divulgación de información confidencial del área de RRHH, como nómina de pagos, beneficios específicos por buen desempeño, etc. podría generar conflictos entre los empleados de la empresa.

Es necesario implementar las medidas necesarias para asegurar el cumplimiento de los conceptos de la seguridad de la información: confidencialidad, integridad y disponibilidad.

3.2. SITUACIÓN ACTUAL DE TI/SI – DIAGNÓSTICO

3.2.1. DESCRIPCIÓN DE GRUPO CESIJO

Grupo CESIJO es un conjunto de empresas de capitales argentinos comprometido con el desarrollo del país en proyectos de largo plazo. Las áreas de negocio son Ciencias de la Vida, Agronegocios, Información & Cultura, Naturaleza & Diseño y Energía renovable.

Las áreas de negocio son:

CIENCIA DE LA VIDA

La industria farmacéutica es la principal actividad, se especializa en la producción de principios activos y productos biológicos. Cuenta con dos plantas de producción, ubicadas en la provincia de Buenos Aires, Argentina. Por medio de la utilización de biorreactores de última tecnología se garantiza la pureza y calidad de los medicamentos bajo los más estrictos estándares internacionales de calidad.

AGRONEGOCIOS

El sector agro-forestal se desarrolla en distintos puntos de Argentina y Paraguay. Las principales actividades están orientadas a agregar valor en la producción primaria, con un fuerte anclaje en investigación, desarrollo y producción sustentable.

Las actividades agrícolas y ganaderas se desarrollan en siete establecimientos distribuidos en cinco provincias: Los Tumos en Chubut, El Perdido y San Andrés en Buenos Aires, El Retiro en San Luis, Zamuchos y Puerto Lavale en Corrientes, y La Malena y San Jorge en Córdoba.

En la agricultura, el foco es la producción de granos. A través de la utilización del sistema de siembra directa y la rotación de cultivos, se optimiza el rendimiento y la preservación de los suelos.

En lo que respecta a la ganadería, el ganado bovino se utiliza tanto para la producción de animales Pedigree, como para tambo y recría, lo que permite que sea una producción sustentable en el tiempo.

El área forestal, se dedica a la obtención de madera sólida de alta calidad. Las plantaciones incluyen una diversidad de especies, entre las que se destacan: Eucalyptus, Pino, Corymbia y Grevillea. Este proceso forestal contempla: la preparación del terreno, técnicas de plantación, control de malezas, las podas (remoción de ramas) y los raleos (reducción del número de árboles por unidad de área) y por último la cosecha. Estas actividades se llevan a cabo en Argentina en las provincias de Corrientes y Misiones, y en Paraguay en los departamentos de Alto Paraná y Caazapa.

INFORMACIÓN Y CULTURA

El grupo tiene una productora de cine, una editorial, la edición Cono Sur de un diario francés y la publicación bimestral de una revista.

La productora de cine realiza producciones nacionales y brinda servicios de producción a compañías internacionales.

La editorial, ofrece publicaciones que abordan desde diferentes ángulos temáticas como ciencia, política, literatura, filosofía, deporte y psicología.

Se publica mensualmente la edición de un diario francés que ofrece análisis y opiniones documentadas sobre política, cultura y actualidad mundial para el cono sur, con una mirada puesta en los países del Mercosur.

NATURALEZA Y DISEÑO

En el área de naturaleza y diseño, con un hotel boutique, una marca de marroquinería de lujo sostenible y un programa de conservación y aprovechamiento sustentable de caimanes.

ENERGIA SUSTENTABLE

El grupo posee una planta de generación de energía sustentable de fuentes renovables. La que produce 40 MW de energía eléctrica, a tal fin utiliza chips, aserrín, cortezas de pino y eucalipto y biomasa proveniente de bosques renovables.

3.2.2. ORGANIGRAMA UNIDADES DE NEGOCIO

3.2.3. NEGOCIOS FORESTALES

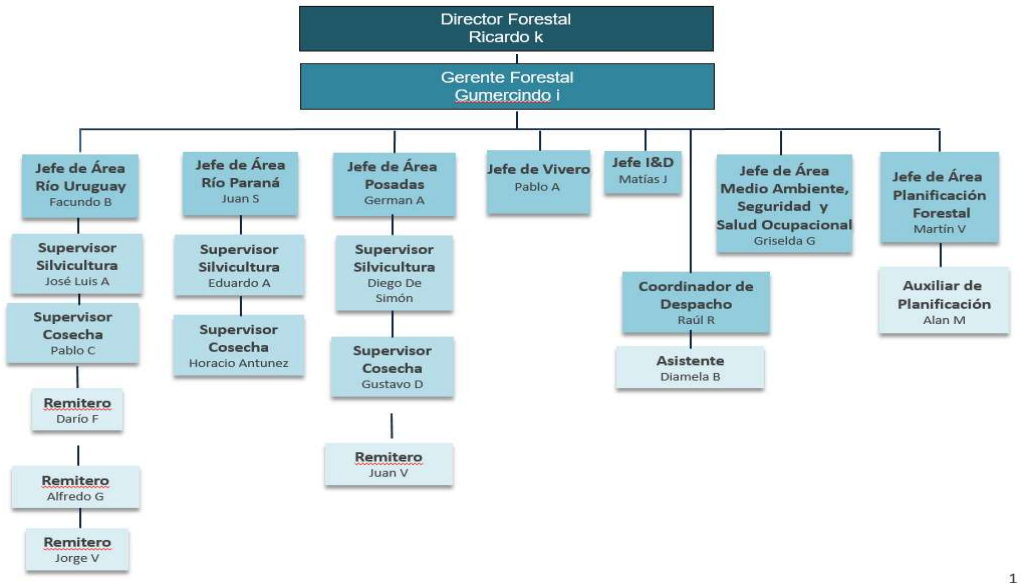
Dentro del área de agronegocios se encuentran la empresa Pomera.

Es una empresa Forestal líder en la producción de madera sólida de alta calidad. Cuenta con más de 45.500 hectáreas forestadas propias en el norte de la Argentina y en Paraguay.

La superficie forestada, la calidad de los bosques, la edad de las plantaciones y los volúmenes de producción convierte a Pomera en una de las principales empresas del sector foresto-industrial del mercado argentino. En Paraguay, es líder en plantaciones de madera sólida. Fue pionera en la implementación de mejores prácticas y buen manejo forestal con un fuerte compromiso ambiental. De esta forma certificó sus prácticas forestales con el estándar Forest Stewardship Council® (FSC®), la más exigente validación internacional que garantiza un manejo responsable de los bosques y de la cadena de custodia.

Según la entrevista realizada al Director Forestal (Anexo 1), Pomera cuenta con 37.000 hectáreas forestadas en la provincia de Misiones y Corrientes. Esto representa el 5,09% del total de las 725.661 hectáreas forestadas en Misiones y Corrientes

3.2.4. ORGANIGRAMA EMPRESA FORESTAL



1

3.2.5. PROCESO PRODUCTIVO FORESTAL

En la entrevista realizada al Gerente Forestal (Anexo 2), se ha identificado que el ciclo forestal es el conjunto de actividades que incluyen todas las etapas de la actividad desde el desarrollo, en laboratorios y viveros, de las plantas que serán trasladadas al bosque hasta la comercialización de los productos de la madera.

Los procesos productivos del sector forestal, comienzan con la reproducción de semillas y plantas que se llevan a cabo en viveros, donde se busca asegurar las características genéticas de interés, con la finalidad de obtener mejores rendimientos, fustes más rectos, menores defectos, etc.

Actividades reproducción de semillas y plantas
Fuente primaria información de Pomera Madera.

El siguiente paso se refiere al desarrollo y cuidado de los árboles, proceso de Silvicultura. Se realizan las tareas de cuidado de plantas y árboles ante el ataque de diversos agentes patógenos. Se hacen controles químicos y biológicos. Se mejoran las condiciones del terreno, mediante fertilizaciones periódicas y raleos.

Actividades del proceso de Silvicultura
Fuente primaria información de Pomera Madera.

Una vez finalizado el desarrollo de las especies, se procede a la etapa de cosecha. La cual consiste en un conjunto de actividades relacionadas con cortar, procesar y extraer los troncos u otras partes aprovechables de los árboles.

Por último, la etapa de transporte es fundamental en este tipo de procesos, consiste en hacer llegar las trozas de árboles (o árbol completo) a las distintas plantas, aserraderos o centros de acopio.

Actividades del proceso productivo forestal
Fuente primaria información de Pomera Madera.

3.2.6. PROCESO COSECHA

Según entrevista realizada al Gerente Forestal (Anexo 3), se identificó que el proceso de cosecha inicia con una Solicitud de Venta, donde se definen los datos del cliente, las cantidades y tipo de árbol, el importe por tonelada de rollos o por cantidad de postes que serán vendidos y especificación sobre la inclusión del flete en la venta, si así fuera detalla su costo.

Posteriormente, se genera un Acta de Intervención. En ésta se declaran los datos de la empresa tercerizada (contratista) que ha de realizar el proceso de cosecha. Se especifica: el lote donde se realizan las tareas, el importe a pagar por tonelada, si la mercadería es por rollo o por poste y el costo pertinente.

Una vez finalizado dicho proceso, el camión con el producto se dirige a una báscula. Allí, se registra en el Software de Báscula el pesaje de los rollos (descontando el peso del camión) o la cuantificación de postes, el precio del flete, los datos del contratista

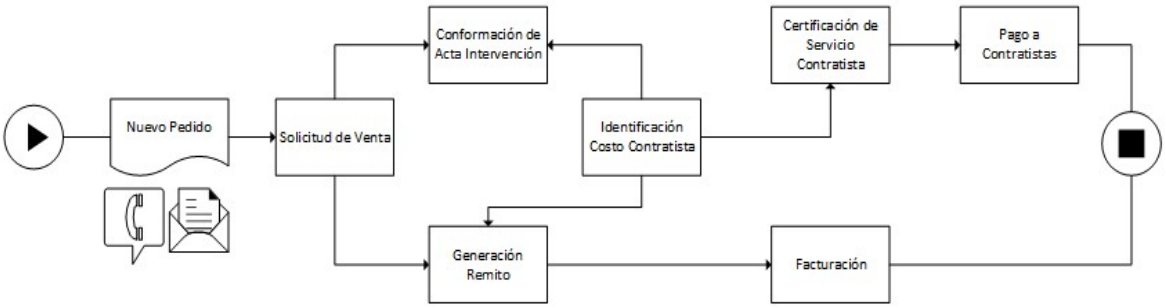
que realizó el proceso de cosecha y del cliente. Con esta información se genera el Remito.

Por medio de una interface, los remitos generados en el sistema de básculas son registrados en el sistema ERP.

Los días viernes, en dicho sistema se ejecuta un proceso automatizado donde se asocia el acta de intervención con los remitos correspondientes. Este procedimiento genera la facturación correspondiente a la Solicitud de Venta, y permite determinar el importe a pagar a los contratistas creando un Certificado de Elaboración. Esto es posible, por los datos brindados tanto en el acta de intervención (importe pactado por tonelada o cantidad de postes) como en el remito (contratista que realizó la tarea de cosecha, el peso de los rollos/cantidad de postes).

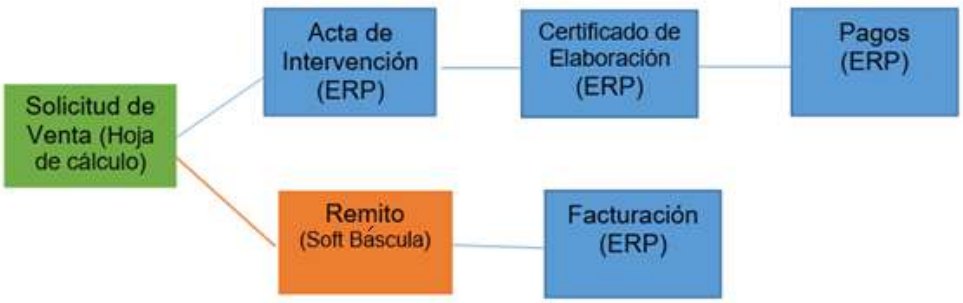
El certificado de elaboración es entregado a los contratistas para que realicen la factura por los servicios prestados.

DIAGRAMA DE PROCESO COSECHA



Fuente: elaboración propia

SOFTWARE QUE INTERVIENEN EN EL PROCESO DE COSECHA



Fuente: elaboración propia.

3.2.7. ETAPAS DE LA COSECHA

Según entrevista realizada al Supervisor Forestal (Anexo 4), se identifican cinco etapas durante el proceso de cosecha.

Estas comienzan con el apeo, donde se cortan los árboles utilizando distintos mecanismos, cada uno de ellos dependerá de las características del lote. Se busca dirigiendo la caída de los árboles en un mismo sentido, a fin de permitir una rápida extracción y reducir el posterior tránsito de maquinaria sobre el lote. La altura del tocón deberá ser la menor posible, de acuerdo a las características del terreno, las máquinas y el árbol. Continúa con el desrame donde se quita las ramas de los árboles que fueron cortados, con el fin de dejar el tronco lo más limpio posible. Posteriormente se procede con la extracción a borde de camino o a un punto específico que se determina según las particularidades del lote. La extracción se realiza con maquinaria y requiere de ciertos cuidados para no dañar la masa forestal remanente y conseguir la mayor productividad posible en el proceso. Luego se realiza la medición y clasificación de los troncos. Esta tarea es muy importante dado que se definen las clases de productos que se obtendrá del bosque, por lo tanto, es necesario procurar la máxima utilización del fuste y respectar las clases indicadas por el Supervisor. Por último, se realiza la carga en el camión para el traslado.

3.2.8. ÁREAS COORPORATIVAS DE GRUPO CESIJO

Adicionalmente a las áreas de negocios descriptas, Grupo CESIJO cuentas con áreas corporativas que dan soporte transversal a las distintas empresas que conforman el grupo. Estas son: Recursos Humanos, Legales, Finanzas, Sistemas y Comunicaciones

3.2.9. ORGANIGRAMA ÁREAS CORPORATIVAS

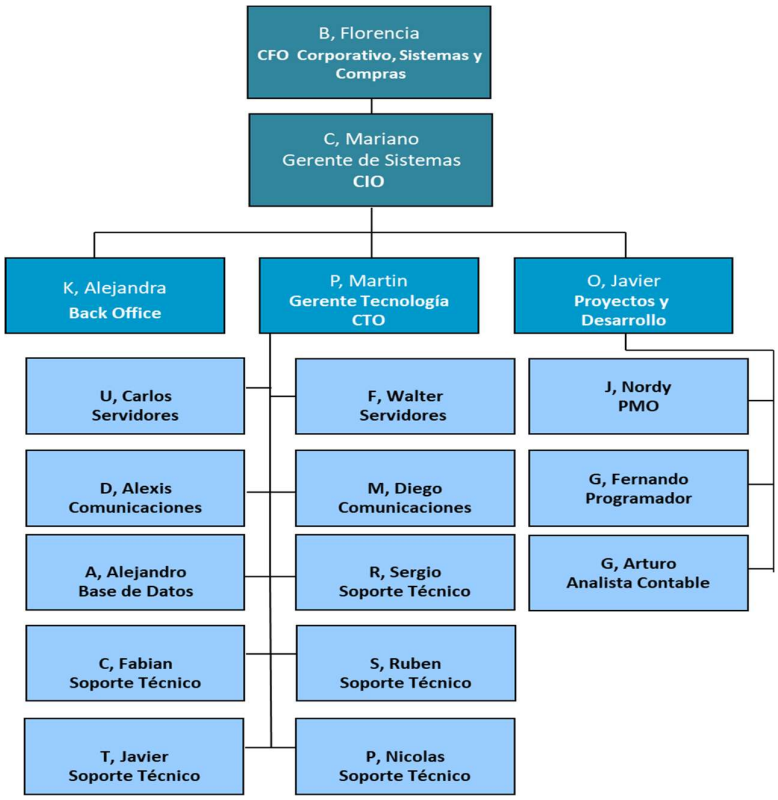
3.2.10. ÁREA CORPORATIVA DE SISTEMAS

El Departamento de Sistemas cuenta con cinco centros de cómputos. Están ubicados en Argentina y Paraguay, donde se procesa y brinda servicio a todas las unidades de negocios del grupo, así como a las áreas corporativas.

El centro de cómputos principal, donde están el 90% de los servicios informáticos está situado en la calle Paraguay 1500, CABA. El resto de los centros de cómputos están ubicados en Argentina, en la provincia de Misiones y Corrientes y en Paraguay en el departamento de Alto Paraná.

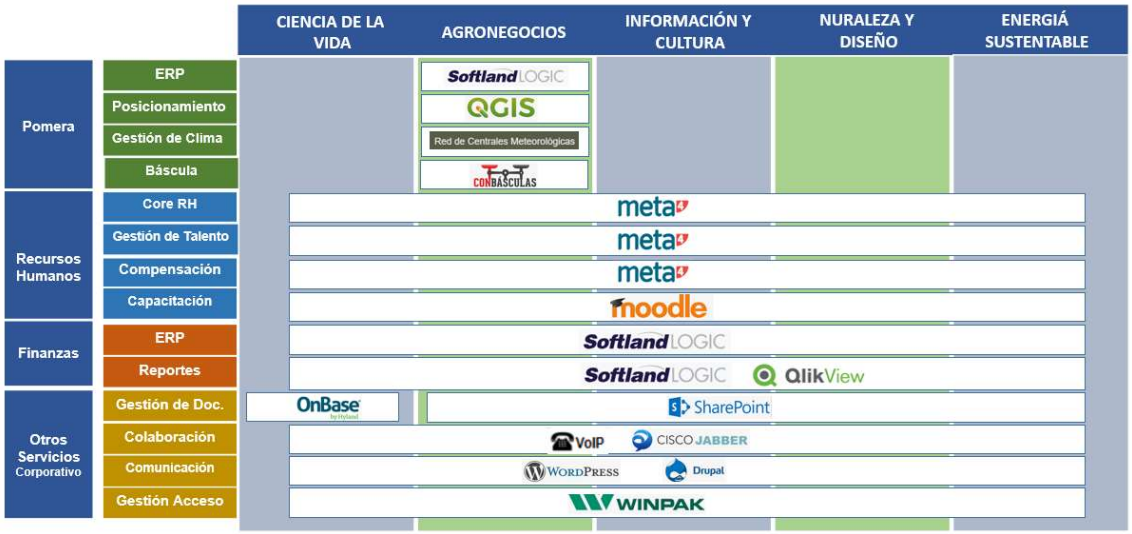
El Departamento de Sistemas está dividido en tres áreas: Infraestructura y Seguridad, Desarrollo, y Gestión de ERP. Cada área tiene un responsable y reporta al gerente de sistemas, quien a su vez reporta a la directora de finanzas. A continuación, se presenta el organigrama del área de sistemas:

3.2.11. ORGANIGRAMA DE SISTEMAS



3.2.12. MAPA DE APLICACIONES DE SISTEMAS

A continuación, se presenta un mapa de las aplicaciones utilizadas por las distintas áreas corporativas y por la empresa Pomera.



Fuente: elaboración propia

El área de Recursos Humanos utiliza el software Meta4 para gestionar los siguientes temas:

Módulo Core RH	Organización	Proporciona las herramientas necesarias para establecer relaciones jerárquicas y funcionales entre los diferentes integrantes de los grupos de trabajo, así como reflejar de forma dinámica su evolución.
	Administración de Personal	Permite identifica al trabajador y reconoce sus habilidades más importantes: el rol que desempeña, sus competencias y las relaciones que mantiene con el resto de los individuos.
Módulo Gestión de Talento	Selección	Permite gestionar todo el proceso de selección, desde la identificación de vacantes, el registro de los candidatos, la fase de evaluación hasta los costos y decisiones finales.
	Evaluación	Fija el funcionamiento de los procesos de evaluación, especificando criterios, plazos y acciones de seguimiento.
Módulo de Compensación	Selección	Permite gestionar el proceso de selección, desde la identificación de vacantes, el registro de los candidatos, la fase de evaluación hasta los costos y decisiones finales.
	Evaluación	Fija el funcionamiento de los procesos de evaluación, especificando el tipo, criterios, plazos, etapas y acciones de seguimiento
Módulo de Nómina	Nómina	Proporciona un completo motor de cálculo de nómina con el que llevar a cabo todas las tareas de administración de personal.

Se utiliza el software Moodle para digitalizar y estandarizar el proceso de integración al grupo, así como la realización de cursos online y la evaluación de los mismos.

El área de finanzas y administración corporativa y las específicas de las distintas unidades de negocio utilizan como software de planificación de recursos empresariales el software Softland Logic. Se detallan los módulos utilizados:

Módulo Gestión Contable y Dirección	Herramienta de registración y reporting muy potente. Cubre los requerimientos de la contabilidad formal y de gestión (multidimensional), facilita eventuales auditorías externas. Los informes gerenciales, ofrecen a la estructura de Dirección y Control de Gestión, la posibilidad de generar múltiples reportes orientados al análisis de la información para la toma de decisiones. Control Presupuestario, es una eficaz herramienta para el análisis y control presupuestario de los diferentes sectores. Permite analizar en detalle los desvíos entre la contabilidad real y la presupuestada. La información, recuperada de los módulos transaccionales, es agrupada según la estructura del control presupuestario definido.
Módulo Gestión Financiera	Administración y gestión de todas las operaciones relacionadas con el manejo de fondos. Conciliación Bancaria cubre las necesidades operativas de la Tesorería en relación con la conciliación de las operaciones de las cuentas bancarias. Cash Flow ofrece a los cuadros directivos la posibilidad de generar reportes orientados al análisis de la situación financiera de la compañía.
Módulo Gestión de Ventas y Cuentas a Cobrar	Cuentas a Cobrar – Facturación de Productos y Servicios administra y gestiona todas las instancias asociadas al circuito comercial. A su vez, genera información de gestión, impositiva y de control relacionada con los clientes. Por otro lado, Facturación y Seguimiento de Contratos administra procesos de facturación automáticos con una frecuencia periódica (abonos, alquileres, liquidación de expensas, etc.). Finalmente, Gestión de Cobranzas facilita la gestión y el seguimiento de las cobranzas. Toda transacción registrada en Cuentas a Cobrar, Facturación de productos y servicios, Facturación de contratos y Tesorería es recuperada por este módulo para apoyar la gestión de la cartera de cobranzas.

Módulo de Billing	Herramienta que permite administrar y gestionar grandes volúmenes de facturación recurrente. El proceso genera distintos informes para análisis global o individual pudiendo también activar alarmas sobre desvíos previamente diseñados.
Módulo de Punto De Venta	Aplicación especialmente diseñada para atender las necesidades de un punto de venta ágil y dinámico, administrando promociones y descuentos mediante un motor especialmente preparado para la gestión diaria de estas operaciones.
Módulo de Gestión de Compras y Cuentas a Pagar	Administra y gestiona todas las instancias asociadas al circuito de compras. Genera información de gestión, impositiva y de control relacionada con los proveedores. Importaciones, administra, gestiona y da seguimiento de todas las compras al exterior. Activo Fijo es una herramienta para la administración de los inventarios de activos fijos, el cálculo y la contabilización automática de las amortizaciones producidas sobre dichos activos.

En lo que respecta a reportes se utiliza el módulo Generador de Reportes de Softland Logic, el cual cubre las necesidades de generación, ejecución e impresión de listados, formularios y consultas en todo el Sistema de Gestión ERP.

Como software de inteligencia de negocio (Business Intelligence) se utiliza qlikview, que permite optimizar el proceso de toma de decisiones en las distintas empresas del grupo.

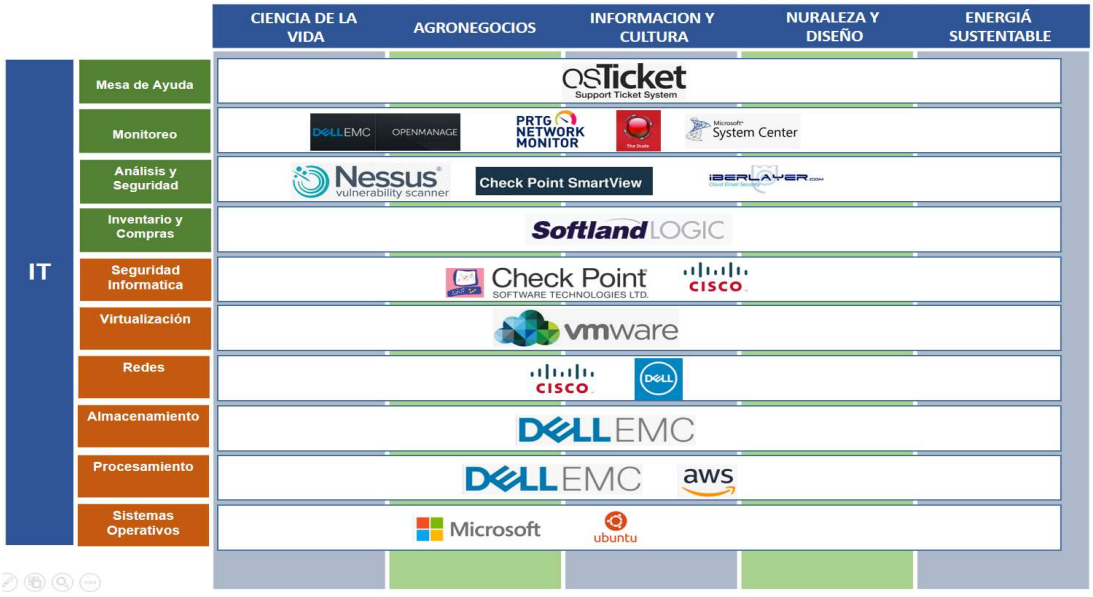
El grupo maneja un conjunto de servicios corporativos que permiten dar soporte a la gestión de documentos, herramienta de colaboración, plataformas de comunicación y gestión de seguridad de acceso a las distintas zonas del edificio corporativo.

La unidad de negocio Pomera, adicionalmente a los servicios descriptos anteriormente utiliza un Sistema de Información Geográfica denominado QGIS para especificar los ambientes de los lotes y analizar la densidad. Utiliza una aplicación meteorológica para analizar las distintas variables climáticas, las cuales afectas de manera directa en determinadas tareas realizadas en los distintos procesos forestales.

Por último, se utiliza un sistema de básculas, desarrollado por personal del Departamento de Sistemas. Este sistema se utiliza para generar los remitos, a partir de los cuales se realiza la facturación a los clientes y el pago de los contratistas que realizan el proceso de cosecha.

3.2.13. INFRAESTRUCTURA Y SEGURIDAD

En lo que respecta al área de infraestructura y seguridad, se presenta un mapa de servicios y empresas aliadas, las cuales integran el centro de procesamiento de datos corporativo.



Fuente: elaboración propia.

El área de sistemas utiliza como sistema de gestión de incidentes para todas las unidades de negocio un producto llamado OSTicket. Por medio de este software, se registran los incidentes, se asignan tiempos de resolución según la categoría de los mismos, se obtienen reportes de efectividad, entre otros indicadores.
El monitoreo de toda la infraestructura corporativa se realiza por medio de las siguientes herramientas:

DELL-EMC Open Manager: destinado a monitorear los equipos de almacenamiento, procesamiento y redes. Permite, ante la falla de algún componente físico de un equipo, se solicite de manera automática su remplazo. Otras de las funciones, es identificar vencimientos de garantía, versiones de softwares instalados y actualizaciones de componentes.

Para el análisis de la infraestructura de red se utiliza el producto PTRG Network Monitor. Permite identificar distintos flujos de datos, así como la salud de los distintos equipos de comunicaciones.

El producto The Dude alerta si un servicio no está operativo, los avisos son enviadas por correo electrónico a los distintos responsables según el tipo de incidente. Este software se utiliza en conjunto con el producto PTRG Network Monitor de esta forma se aumenta la consistencia del monitoreo de los servicios de IT.

En lo que respecta al monitorio, se utiliza el producto System Center de la empresa Microsoft para monitorear e identificar el estado de los distintos servidores y de la plataforma virtual.

El análisis de vulnerabilidades en la seguridad informática se centra en los siguientes productos y servicios:

1. Nessus: para la prevención de ataques de red, identificación de vulnerabilidades y detección de problemas de configuración que utilizan los hackers para ingresar a la red.

2. Check Point SmartViwer: es un sistema de análisis de seguridad y redes de alto rendimiento. Proporciona una interfaz única y central para monitorear la actividad de la red y el rendimiento de los dispositivos de seguridad Checkpoint distribuidos

en las distintas redes. Otra funcionalidad significativa es el establecimiento de hábitos de trabajo basados en patrones de recursos.

3. Iberlayer: servicio de filtrado y bloqueo en la Nube. Brinda protección contra múltiples amenazas existentes en el correo electrónico: Spam, Malware, Phishing, CrytoLockers, ataques DDoS, y campañas de marketing, entre otras.

El área de sistemas, al igual que las distintas empresas del grupo, utiliza el software SoftLand Logic para gestionar los activos informáticos y las compras de equipamiento informático.

3.2.14. GESTIÓN DE LA SEGURIDAD

La seguridad de la información e informática es gestionada por el Área de Infraestructura y Seguridad. No existe un equipo de profesionales que se dediquen específicamente a gestionarla. Las personas que mantienen la seguridad son los que definen y controlan la utilización de los activos de información.
Se destaca la ausencia de auditorías de seguridad de los principales activos de información.

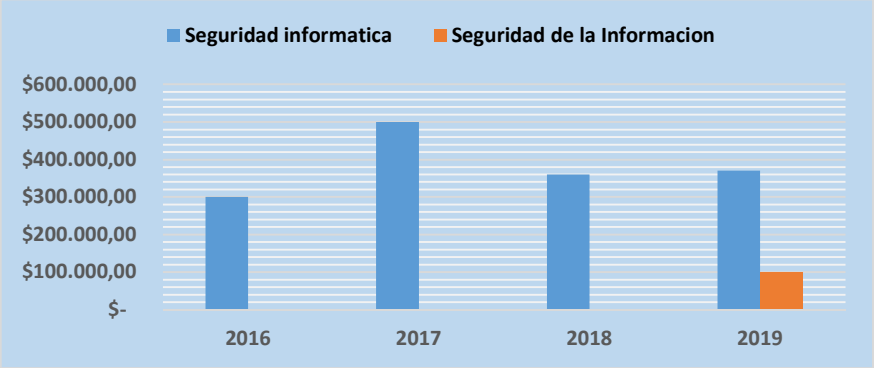
3.2.15. INVERSIONES EN SISTEMAS

Según entrevista realizada al Gerente de Tecnología (Anexo 5), se ha identificado que, durante los últimos 4 años, se ha incrementado los recursos financieros destinados al área de sistemas. En lo que respecta a Infraestructura y Seguridad, las inversiones han sido destinadas a la adquisición de equipamiento y software. No se aprobaron recursos para gestionar la seguridad de la información.

A partir del corriente año, tras el cambio de CEO del grupo, se otorga una partida presupuestaria para comenzar la alineación de los procesos del negocio con la norma internacional ISO/IEC 27001:2013

PRESUPUESTO ÁREA DE TECNOLOGÍA

Año	Infraestructura	Seguridad informatica	Seguridad de la Informacion
2016	$ 300.000,00	$ 15.000,00	$ -
2017	$ 500.000,00	$ 45.000,00	$ -
2018	$ 360.000,00	$ 35.000,00	$ -
2019	$ 370.000,00	$ 37.000,00	$ 100.000,00



Fuente: elaboración propia.

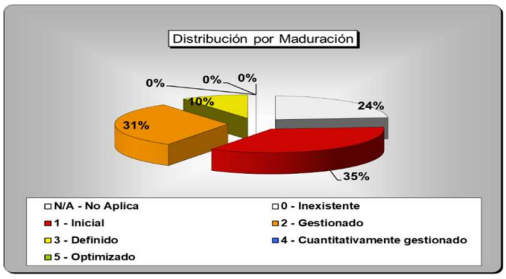
3.2.16. ANÁLISIS DE CONTROLES ISO 27002

Se utiliza el Modelo de Madurez de Capacidades (CMM) para clasificar el complimiento de los controles de seguridad de la información establecidos por la norma ISO/IEC 27001:2013.

El modelo descripto define 6 niveles para medir la capacidad de los procesos:

0. Incompleto: El proceso no se realiza, o no se consiguen sus objetivos.
1. Ejecutado: El proceso se ejecuta y se logra el objetivo.
2. Gestionado: Además de ejecutarse, el proceso se planifica, se revisa y se evalúa para comprobar que cumple los requisitos, pero las definiciones no aplican a nivel corporativo, ni existe normalización.
3. Definido: La organización entera participa en el proceso. Existen métodos y planillas definidos, y documentadas.
4. Cuantitativamente gestionado: Además de ser un proceso definido se controla utilizando técnicas cuantitativas.
5. Optimizado: hace foco en la mejora continua. Se comprende donde detectar la mejora y actuar al respecto, con el objetivo de conseguir una mayor eficiencia del proceso.

Según análisis realizado (Anexo 6), se identifica que el 24% de los controles establecidos por la norma ISO/IEC 27002:2013 son inexistentes. El 35% se encuentra en estado Iniciado, el cumplimiento de los mismos se basa en el esfuerzo personal de los empleados. El 31% de los controles se encuentran en estado Gestionado, se normalizan las buenas prácticas en base a la experiencia y no aplican a nivel corporativo. Sólo el 10% cumple con el objetivo especificado en el plan estratégico.

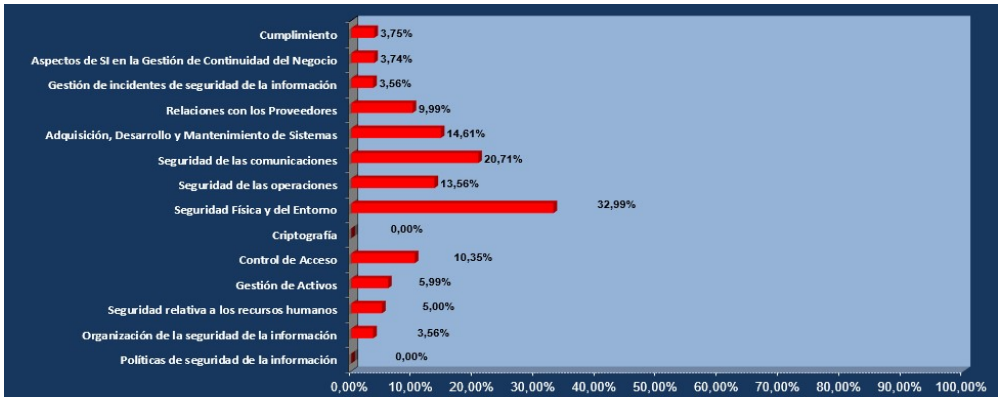


Fuente: elaboración propia

Se considera importante destacar que, de los 114 controles analizados por la norma ISO/IEC 27002:2013, solo 27 no son gestionados por la organización y en 40 el cumplimiento se reduce al esfuerzo personal de los empleados, puesto que no existe normalización ni se aplican a nivel corporativo.

MADURACIÓN	TOTAL
N/A - No Aplica	0
0 - Inexistente	27
1 - Inicial	40
2 - Gestionado	36
3 - Definido	11
4 - Cuantitativamente gestionado	0
5 - Optimizado	0

RESUMEN CUMPLIMIENTO DE LOS 14 DOMINIOS



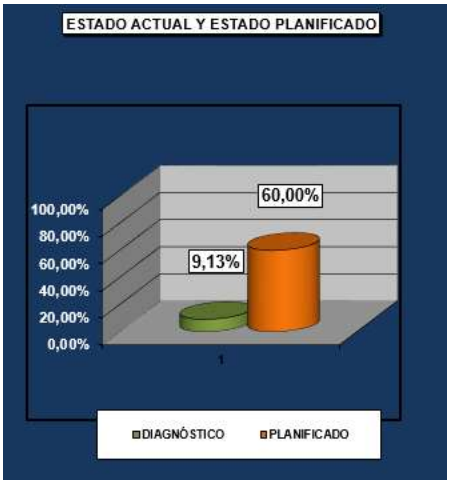
Fuente: elaboración propia.

RELACIÓN ENTRE EL DIAGNÓSTICO Y LA PLANIFICACIÓN

MATERIA FUNDAMENTAL	ESTADO ACTUAL		ESTADO DESEABLE	
	DIAGNÓSTICO	MADURACIÓN	PLANIFICADO	MADURACIÓN
Políticas de seguridad de la información	0,00%	0 - Inexistente	60,00%	3 - Definido
Organización de la seguridad de la información	3,56%	0 - Inexistente	60,00%	3 - Definido
Seguridad relativa a los recursos humanos	5,00%	1 - Inicial	60,00%	3 - Definido
Gestión de Activos	5,99%	1 - Inicial	60,00%	3 - Definido
Control de Acceso	10,35%	1 - Inicial	60,00%	3 - Definido
Criptografía	0,00%	0 - Inexistente	60,00%	3 - Definido
Seguridad Física y del Entorno	32,99%	2 - Gestionado	60,00%	3 - Definido
Seguridad de las operaciones	13,56%	1 - Inicial	60,00%	3 - Definido
Seguridad de las comunicaciones	20,71%	2 - Gestionado	60,00%	3 - Definido
Adquisición, Desarrollo y Mantenimiento de Sistemas	14,61%	1 - Inicial	60,00%	3 - Definido
Relaciones con los Proveedores	9,99%	1 - Inicial	60,00%	3 - Definido
Gestión de incidentes de seguridad de la información	3,56%	0 - Inexistente	60,00%	3 - Definido
Aspectos de SI en la Gestión de Continuidad del Negocio	3,74%	0 - Inexistente	60,00%	3 - Definido
Cumplimiento	3,75%	0 - Inexistente	60,00%	3 - Definido
TOTAL	9,13%	1 - Inicial	60,00%	3 - Definido

Fuente: elaboración propia.

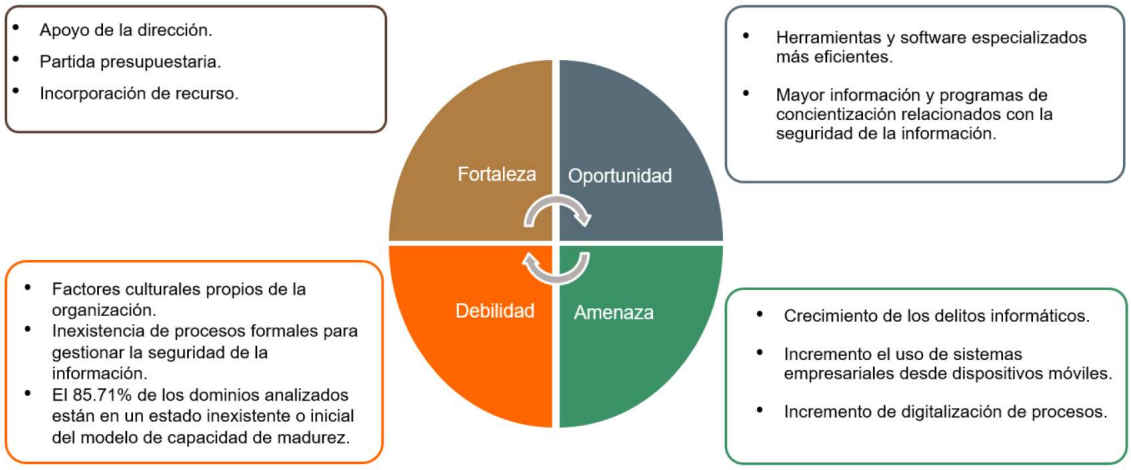
Según lo descripto, se puede indentifica que el complimiento de los controles establecidos por la norma es de 9,13%.



Fuente: elaboración propia.

3.2.17. FODA

Del análisis realizado se pudieron identificar las siguientes Fortalezas, Oportunidades, Debilidades y Amenazas

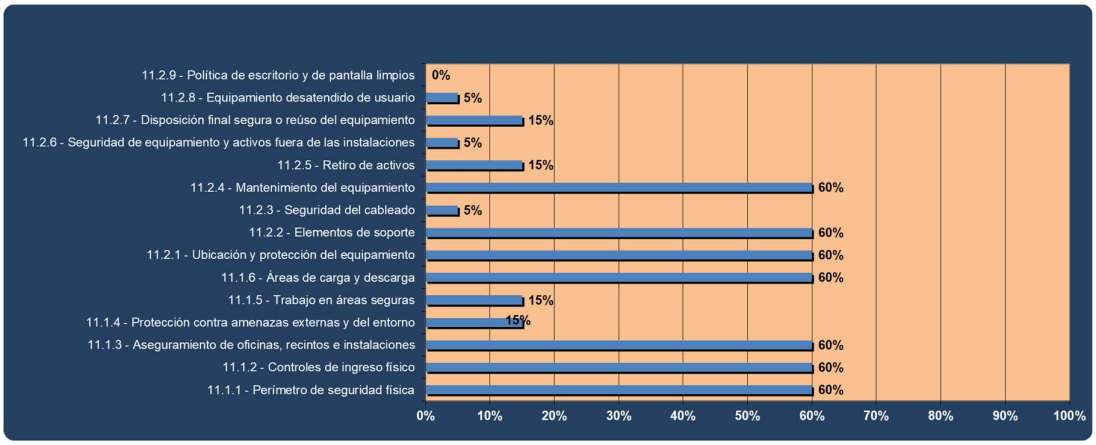


A continuación, se detallarán cada uno de estos puntos:

Fortalezas:

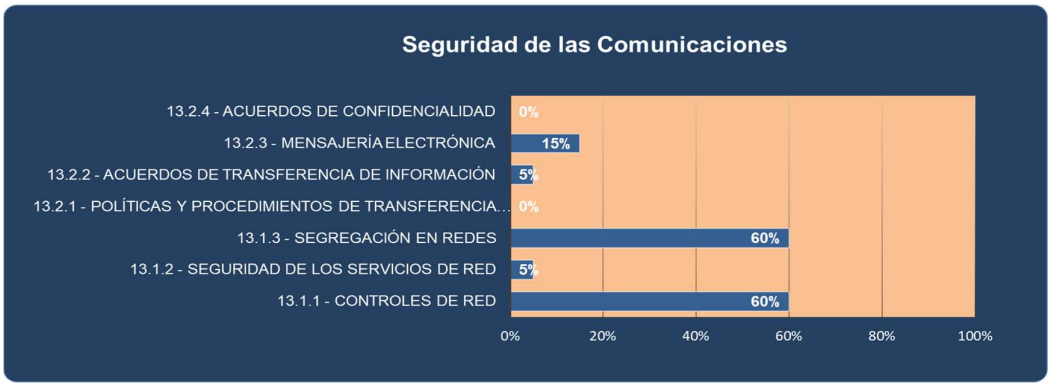
- Apoyo de la dirección: el CIO de grupo CESIJO solicitó alinear los procesos de negocio con normas internacionales de seguridad de la información. Especificó a los directores de las unidades de negocios y las áreas corporativas colaborar activamente en los proyectos relacionados con mejoras de seguridad.
- Partida presupuestaria propia para proyectos de seguridad de la información: por primera vez en la historia del grupo, se asignó una partida presupuestaria específica para el área de seguridad de la información.
- Incorporación de recurso técnico especializado en nómina: se autorizó incorporar un recurso especializado en seguridad de la información.
- Luego del análisis realizado se identificaron los dominios de Seguridad de las Comunicaciones, y Seguridad Física y del Escritorio. Se encuentran es un estado Gestionado, nivel 2 dos del modelo de capacidad de madurez.

  El dominio de seguridad física y del escritorio está compuesto por quince controles, de los cuales siete cumplen con el objetivo establecido de alcanzar el 60% de complimiento del modelo de capacidad de madurez.



Fuente: elaboración propia.

El dominio de seguridad de las comunicaciones está compuesto por siete controles, de los cuales dos cumplen con el objetivo establecido de alcanzar el 60% de complimiento del modelo de capacidad de madurez



Fuente: elaboración propia.

Oportunidades:

- Herramientas y software especializados más eficientes en lo que respecta a la seguridad de la información e informática.
- Mayor información y programas de concientización relacionados con la seguridad de la información.

Debilidades:

- Factores culturales propios de la organización: cultura informal, inexistencia de procedimientos formales y falta de concientización a los empleados respecto al uso tecnología.
- El área de sistemas no utiliza procesos formales para gestionar la seguridad de la información.

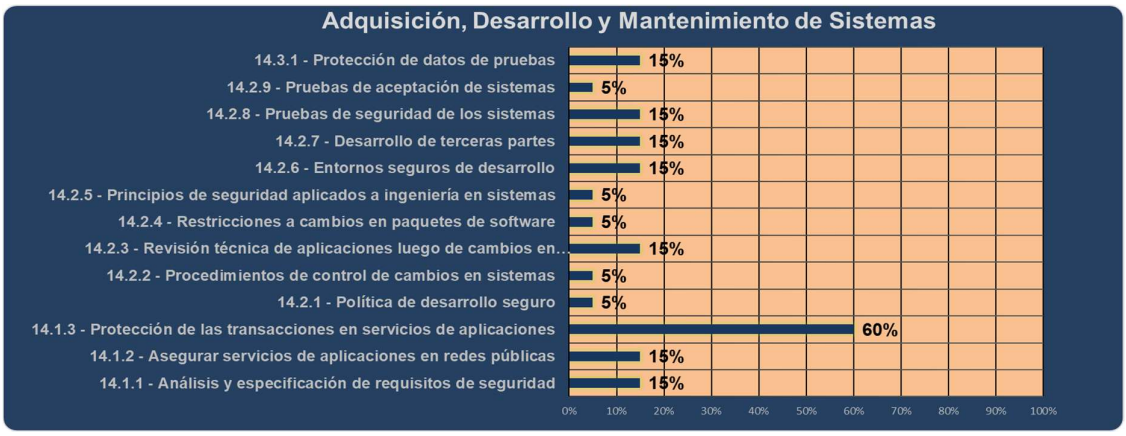
- Luego del análisis realizado se identificaron doce de los catorce dominios establecidos por la norma ISO 27001 que se encuentran en un estado inexistente o inicial del modelo de capacidad de madurez.

  Dominios en estado inexistente:

  - Políticas de seguridad de la información
  - Organización de la seguridad de la información
  - Criptografía
  - Gestión de incidentes de seguridad de la información
  - Aspectos de seguridad de la información en la Gestión de Continuidad del Negocio
  - Cumplimiento

  Dominios en estado inicial:

  - Adquisición, Desarrollo y Mantenimiento de Sistemas:

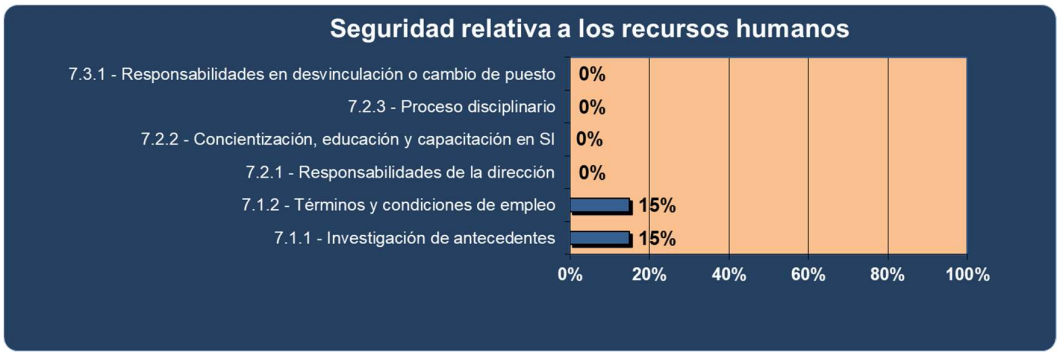


Fuente: elaboración propia.

  - Relaciones con los Proveedores

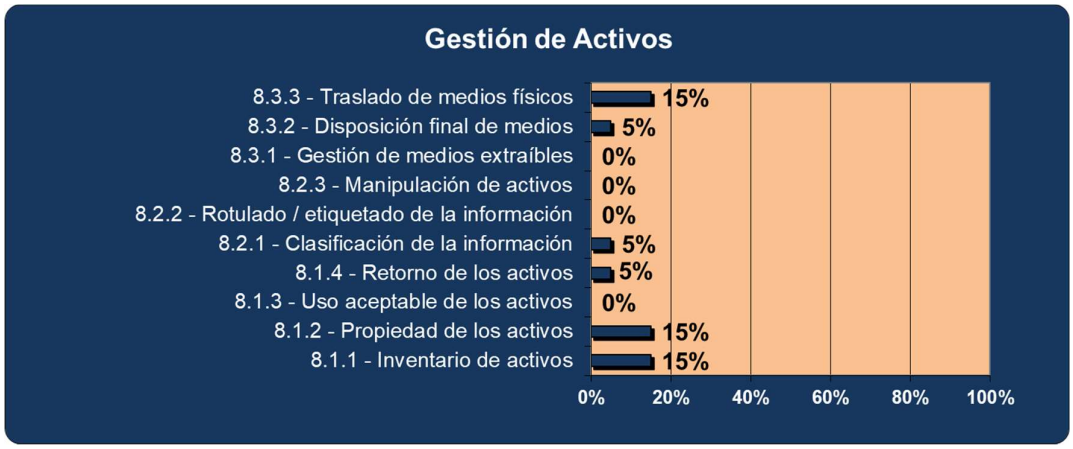
Fuente: elaboración propia.

- Seguridad relativa a los recursos humanos: este dominio está compuesto por seis controles, de los cuales en sólo dos se realizan actividades básicas para gestionarlos.



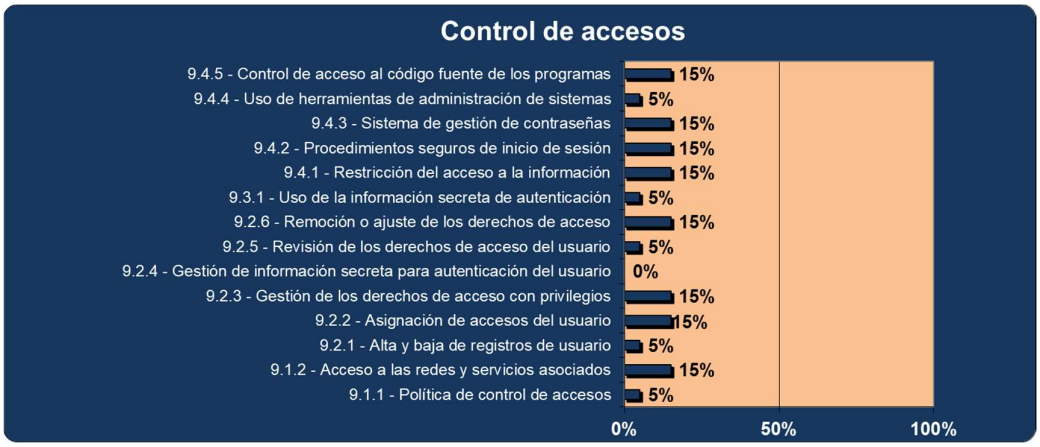
Fuente: elaboración propia.

- Gestión de Activos



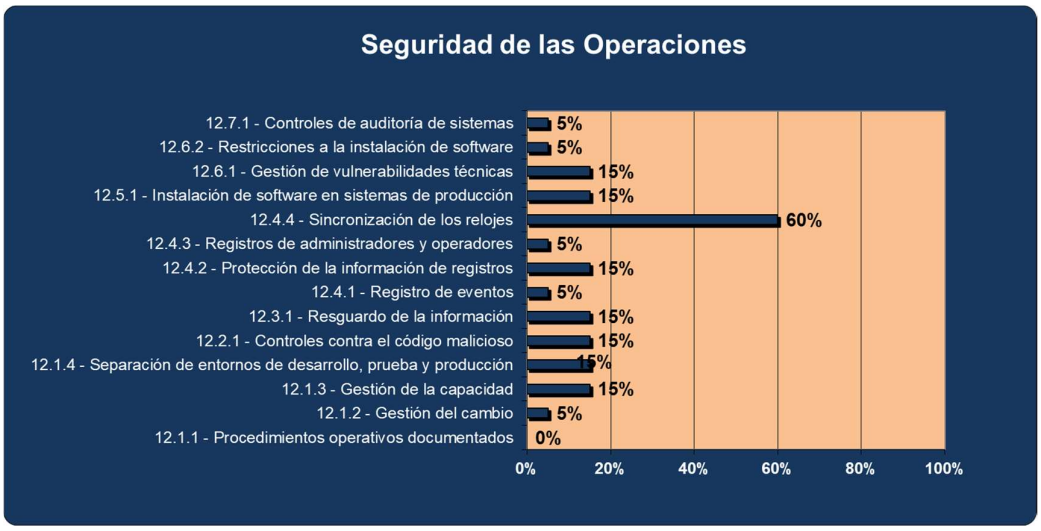
Fuente: elaboración propia.

- Control de Acceso



Fuente: elaboración propia.

- Seguridad de las operaciones



Fuente: elaboración propia.

Amenazas:

El gran crecimiento de los delitos informáticos ha comprometido a las organizaciones por medio de ataques, ya sean dirigidos o como daños colaterales. Es cada vez más común que sucedan incidentes de seguridad en la infraestructura informática.

A partir de esta problemática, es necesario entender que la confidencialidad, la integridad y la disponibilidad de los datos son aspectos centrales para toda organización.

Las siguientes son algunas de las fuentes más comunes de amenazas de seguridad para una empresa:

- Dispositivos móviles: la mayoría de los empleados llevan consigo al trabajo un dispositivo móvil. Estos son fáciles de robar y pueden ser atacados desde dispositivos cercanos, o incluso a través de mensajes de texto.
- Error humano: muchas infracciones son el resultado de un error humano. Contraseñas demasiado simples, dispositivos perdidos y ordenadores desatendidos. Todos los sistemas, tanto online como locales, deben estar protegidos con un acceso que dependa del rol de usuario. Por otro lado, todos los empleados deben estar al tanto de las posibles consecuencias de sus acciones.

- Fraude interno: sin controles internos adecuados, cualquier empleado puede tener acceso a información no autorizada.
- El incremento de dispositivos conectados a internet (sistemas de alarma, sistema de aire acondicionado, entre otros equipos) trae muchas ventajas, así como también puede ocasionar problemas de seguridad. Es necesario utilizar controles para gestionar y mitigar estos posibles problemas.

3.3. NUEVOS PROYECTOS DE TI/SI QUE COMPONEN EL PLAN ESTRATÉGICO

Concluidas las tareas del análisis de la situación actual y diagnóstico sobre la Norma ISO/IEC 27001:2013, se realizará un Plan de Acción que contendrá diferentes proyectos. De acuerdo al tiempo de inicio de ejecución, serán clasificados en:

- Proyectos a Corto Plazo: inmediatos a iniciar en los 12 próximos meses.
- Proyectos a Medio Plazo: a iniciar en el periodo comprendido entre los 12-24 meses desde la fecha actual.
- Proyectos a Largo Plazo: a iniciar en el periodo comprendido entre los 24-32 meses desde la fecha actual.

Esta división de tiempo se ha realizado teniendo en cuenta la posibilidad de ejecutar proyectos en paralelo, así como la de facilitar a la empresa la reserva de presupuestos para abordar los mismos.

Cada proyecto será identificado con la siguiente información:

- Proyecto
- Descripción
- Objetivos
- Alcance
- Beneficios
- Dependencias
- Clasificación del Proyecto
- Plazo
- Equipos del Proyecto y Duración
- Costo
- Controles Relacionados

3.3.1. PROYECTOS DEL PLAN ESTRATÉGICO.

El plan estratégico está compuesto por 14 proyectos, cada uno cubre los objetivos especificados en cada capítulo de la Norma ISO/IEC 27001:2013.

1. Proyecto de Marco Normativo de Seguridad
2. Proyecto de Organización de la seguridad de la información
3. Proyecto de Seguridad de Recursos Humanos
4. Proyecto de Gestión de Activos
5. Proyecto de Control de Acceso
6. Proyecto de Criptografía
7. Proyecto de Seguridad Física
8. Proyecto de Seguridad de las operaciones
9. Proyecto de Seguridad de las Comunicaciones
10. Proyecto de Seguridad en Desarrollo de Sistemas
11. Proyecto de Relaciones con los Proveedores
12. Proyecto de Gestión de incidentes de seguridad de la información
13. Proyecto de Gestión de Continuidad del Negocio
14. Proyecto de Cumplimiento

Adicional a los proyectos descriptos se realizaría un programa de capacitación y concientización una vez finalizados los proyectos. El objetivo de este programa es garantizar que todo el personal este notificado y comprenda la importancia del cumplimiento de las políticas, normas y procedimientos establecidos.

3.3.2. PLAN DE ACCIÓN A CORTO PLAZO

Los proyectos que se detallan a continuación, han sido identificados como necesarios para elevar el nivel de Seguridad en el corto plazo alcanzando el **32,75%** de cumplimento acumulado, respecto de la Norma ISO/IEC 27001:2013.

PROYECTOS A CORTO PLAZO

- Proyecto Marco Normativo de Seguridad
- Proyecto de Criptografía
- Proyecto de Organización de la seguridad

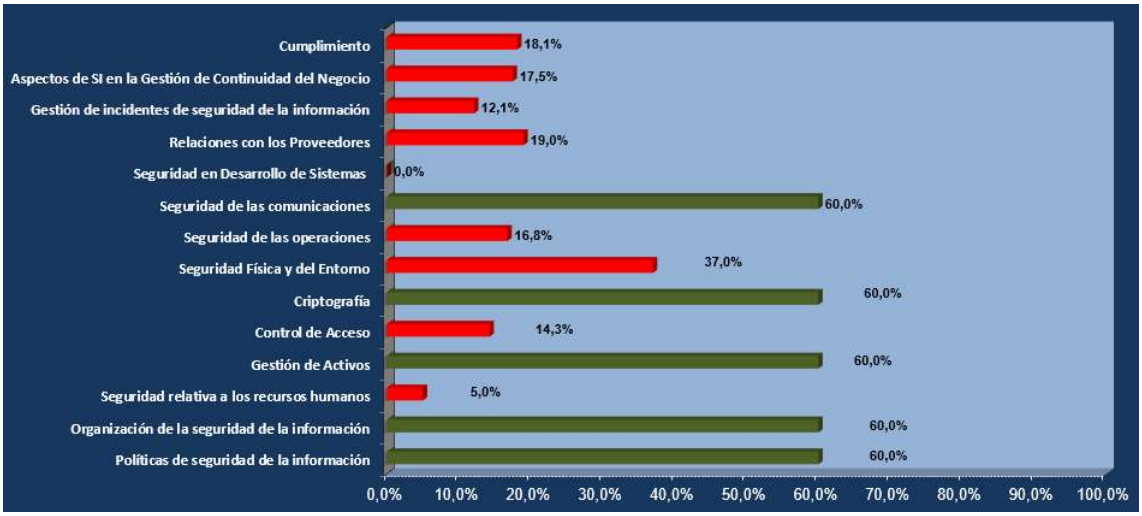
- Proyecto de Gestión de Activos
- Proyecto de Seguridad en las Comunicaciones

La ejecución de los proyectos aporta a la seguridad un 23,62% de cumplimento, respecto de la Norma ISO/IEC 27001:2013.

A continuación, se detalla el aporte de cada uno de los proyectos.

Fuente: elaboración propia.

Nivel de cumplimiento de los capítulos de la Norma ISO/IEC 27001:2013 luego de la finalización de los proyectos de corto plazo



Fuente: elaboración propia.

Proyecto: MARCO NORMATIVO DE SEGURIDAD

Descripción

En este proyecto se establecerá el Marco Normativo necesario, elaborando aquellos documentos determinados en el alcance.

En función de las necesidades detectadas se definirá el conjunto de Normas, Procedimientos, Guías y Estándares para establecer un adecuado proceso de normalización, tomando como base de referencia la ISO/IEC 27002:2013.

Objetivos

Elaborar la Política General de Seguridad y el conjunto de Normas, Guías y Estándares que se consideren necesarias para establecer un adecuado proceso de normalización, tomando como base de referencia la serie ISO/IEC 27000.

Alcance

El alcance del proyecto abarca lo siguiente:

- Redacción o revisión de la Política de Seguridad de la Información para toda la organización.
- Desarrollo del conjunto de documentos necesarios para que la organización disponga de un marco normativo acorde la Norma ISO/IEC 27002:2013.
- Aunque no es posible indicar de forma precisa el número exacto de documentos a desarrollar; se prevé que el alcance del marco normativo abarque la totalidad de los temas y apartados referenciados por la Norma ISO/IEC 27001:2013, contemplando un máximo de 45 documentos.

Beneficios

Los beneficios del proyecto son los siguientes:

- Obtener un Marco Normativo de Seguridad que acompañe a las directrices esenciales definidas para el desarrollo del negocio de la organización.
- Proporcionar orientación y apoyo a la gestión de seguridad de la información.
- Establecer una guía y facilitar la toma de conciencia por parte de los empleados en relación a las buenas prácticas de seguridad.
- Adecuar a la organización a los lineamientos de la Norma ISO/IEC 27001:2013, en relación con la documentación de sus sistemas de información

Dependencias

La ejecución del mismo no depende de otros proyectos predecesores.

Clasificación del Proyecto

El presente proyecto se clasifica como “seguridad organizativa”.

Plazo

Realización en el corto plazo.

Equipos del proyecto y duración

El proyecto estará liderado por el Responsable de Seguridad de la Información.

La realización del mismo llevara una fuerte participación de personal interno para la definición, revisión y aprobación de los documentos generados.

Las áreas descriptas tendrás una relación directa durante la realización del proyecto.

Equipos del Proyecto	Perfil	Disponibilidad %
Interno	Responsable de Seguridad de la Información	100%
	Gerente de Sistemas	20%
	Gerente de Tecnología	50%
Externo	Un Consultor SR	100%
	Un Consultor SSR	100%
Áreas involucradas en el Proyecto	Dirección General	
	Dirección unidad de negocio Forestal	
	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
Duración	La duración estándar del proyecto es de 44 jornadas laborales.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por un consultor sr y un consultor ssr.

Costo del Proyecto		
Consultoría	$	8.360,00
Software	$	-
Adquisición de equipos	$	-
Costo Total del proyecto U$	$	8.360,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

5.1.1 - Existencia de políticas de SI

5.1.2 - Revisión de las políticas de SI

6.2.1 - Política de uso de dispositivos móviles

9.1.1 - Política de control de accesos

11.1.1 - Perímetro de seguridad física

11.2.9 - Política de escritorio y de pantalla limpios

12.5.1 - Instalación de software en sistemas de producción

13.2.1 - Políticas y procedimientos de transferencia de información

14.2.1 - Política de desarrollo seguro

15.1.1 - Política de SI para relación con proveedores

16.1.1 - Responsabilidades y procedimientos

17.1.2 - Implementación de la continuidad de la SI

18.1.2 - Derechos de propiedad intelectual

Proyecto: CRIPTOGRAFÍA

Descripción

Establecer una política de uso de controles criptográficos e implementar mecanismos que permitan el cifrado de la información sensible en aquellos sistemas que así lo requieran. El cifrado de la información en tránsito o a nivel repositorio puede ser necesario por cuestiones legales, regulatorias o de negocio.

Objetivos

Identificar la información que requiera cifrarse tanto por razones legales, regulatorias o de negocio.

Analizar soluciones técnicas de cifrado de información (a nivel tránsito y repositorio) y elaborar un plan de implantación de dichas soluciones.

Alcance

El proyecto se circunscribe a las aplicaciones críticas que son propiedad de la empresa, excluyendo las aplicaciones de terceros. El análisis de las soluciones técnicas aplicará a aquellos sistemas que almacenen información de procesos de autenticación no cifrada.

Beneficios

Los beneficios asociados a este proyecto son:

- Proteger información en tránsito o en almacenamiento y que por diversas cuestiones debe salvaguardarse su valor confidencial.
- Confidencialidad de los datos sensibles almacenados en la red interna y que podrían ser accedidos ilegalmente.
- Confidencialidad de los datos sensibles en tránsito y que podrían ser accedidos ilegalmente.

Dependencias

La ejecución del mismo no depende de proyectos predecesores.

Clasificación del Proyecto

El presente proyecto se clasifica como “seguridad lógica”.

Plazo

Realización en el corto plazo.

Equipos del proyecto y Duración

El proyecto estará liderado por el Responsable de Seguridad de la Información.

Las áreas descriptas tendrás una relación directa durante la realización del proyecto.

Equipos del Proyecto	Perfil	Disponibilidad %
Interno	Responsable de Seguridad de la Información	50%
	Gerente de Tecnología	30%
Externo	Un Consultor SR	100%
	Dirección General	
	Dirección unidad de negocio Forestal	
Áreas involucradas en el Proyecto	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
Duración	La duración estándar del proyecto es de 15 jornadas laborales.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por un consultor sr.

No requerirá realizar gastos de infraestructura. Se utilizaran recursos existentes en el centro de datos.

Costo del Proyecto		
Consultoría	$	1.650,00
Software	$	10.000,00
Adquisición de equipos	$	-
Costo Total del proyecto U$	$	11.650,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

10.1.1 - Política de uso de los controles criptográficos

10.1.2 - Gestión de claves

18.1.5 - Regulación de los controles criptográficos

Proyecto: ORGANIZACIÓN DE LA SEGURIDAD

Descripción

Este proyecto está dividido en 4 secciones:

- Elaborar una propuesta de estructura organizativa y jerárquica enfocada en los distintos roles que participan en la gestión de la seguridad, contemplando la implantación, mantenimiento y control. Establecer el proceso de asignación de los propietarios de los activos se definirán los roles y responsabilidades de los mismos.
- Definir procedimientos que especifiquen cuándo y a qué autoridades se contactará, y cómo se informarán los incidentes de seguridad de la información identificados de manera oportuna.
- Integrar la seguridad de la información en los métodos de administración de proyectos de la organización para identificar y abordar los riesgos de seguridad de la información como parte de un proyecto.
- Implementar la protección necesaria para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada por estos dispositivos.

Objetivos

Los objetivos del proyecto son los siguientes:

- Establecer una estructura organizativa para la gestión de la seguridad de la información.
- Asignar eficientemente los roles y responsabilidades relativos a la seguridad de la información.
- Concientizar a la organización para que la responsabilidad sobre la seguridad de la información no recaiga solamente sobre el Responsable o el Área de Seguridad.
- Definir perfiles estándar para la realización de las tareas relativas a la seguridad de la información, evitando solapamientos en sus funciones.
- Establecer los contactos adecuados con grupos de intereses especiales o empresas de seguridad.
- Integrar la seguridad de la información en la administración de proyectos.
- Garantizar la seguridad del teletrabajo y dispositivos móviles.

Alcance

El proyecto se circunscribe a los sistemas de información de la empresa; a las áreas y personal involucrado en el proceso de cosecha.

Beneficios

Los beneficios del proyecto son los siguientes:

- Gestionar la seguridad de la información de forma efectiva.
- Alcanzar la máxima eficiencia en materia de seguridad de la información, reaccionando rápidamente ante la aparición de incidentes de seguridad y controlando y minimizando los riesgos.
- Concientizar a la organización en todo lo relacionado con la seguridad de la información y a la protección de sus activos.
- Definir y asignar las responsabilidades de seguridad entre los directores de departamentos, usuarios finales y los que tienen día a día, la posesión de la información (funciones y roles de seguridad).
- Garantizar que en todos los proyectos se tengan en cuenta aspectos de la seguridad de la información.
- Garantizar la seguridad del teletrabajo y dispositivos móviles.

Dependencias

El presente proyecto tiene relación con otros proyectos predecesores. La ejecución del mismo podrá realizarse una vez finalizadas las tareas agrupadas en el proyecto “Marco Normativo de Seguridad” y “Criptografía”.

Clasificación del Proyecto

El presente proyecto se clasifica como “seguridad organizativa”.

Plazo

Realización en el corto plazo.

Equipos del proyecto y Duración

El proyecto estará liderado por el Responsable de Seguridad de la Información.

Las áreas descriptas tendrás una relación directa durante la realización del proyecto.

Equipos del Proyecto		
	Perfil	Disponibilidad %
Interno	Responsable de Seguridad de la Información	100%
	Gerente de Sistemas	20%
	Gerente de RRHH	30%
Externo	Un Consultor SR	100%
	Un Consultor SSR	100%
	Dirección General	
Áreas involucradas en el Proyecto	Dirección unidad de negocio Forestal	
	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
Duración	La duración estándar del proyecto es de 44 jornadas laborales.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por un consultor sr y un consultor ssr.

Costo del Proyecto		
Consultoría	$	6.440,00
Software	$	-
Adquisición de equipos	$	-
Costo Total del proyecto U$	$	6.440,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

6.1.1 - Roles y responsabilidades de la SI

6.1.2 - Segregación de funciones

6.1.3 - Contacto con las autoridades

6.1.4 - Contacto con grupos de interés especial

6.1.5 - SI en la gestión de proyectos

6.2.2 - Teletrabajo

8.1.2 - Propiedad de los activos

Proyecto: GESTIÓN DE ACTIVOS

Descripción

Este proyecto está dividido en 4 secciones:

- Diseñar la estructura del inventario de activos de información. Éste contendrá los procesos de negocio, sus relaciones con las aplicaciones, el software

instalado, el hardware, la información que contiene o maneja y los responsables de todos estos activos.

- Establecer reglas para el uso aceptable y la devolución de los activos asociados a la información.
- Clasificar la información, asegurando que la misma reciba el nivel de protección adecuado de acuerdo su importancia. La información será clasificada en términos de requisitos legales, valor, criticidad y sensibilidad para la divulgación o modificación no autorizada.
- Implementar procedimientos para la administración de medios extraíbles de acuerdo a su clasificación permitiendo evitar divulgación, modificación, retiro o destrucción de información almacenada.

Objetivos

- Identificar los activos que componen el dominio, determinando sus características, atributos y tipificación.
- Establecer las dependencias entre los activos del inventario.
- Asegurar que la información reciba el nivel de protección adecuado según su importancia.
- Evitar la divulgación, modificación, retiro o destrucción de información almacenada en medios.

Alcance

El proyecto se circunscribe a los sistemas de información de la empresa; a las áreas y personal involucrado en el proceso de cosecha.

- Definición del modelo de datos y estructura del inventario de activos.
- Designación de los responsables del mantenimiento del inventario de activos.
- Implementación de las tareas de inventariado de activos de información.

Beneficios

- Adquirir la metodología de gestión de inventario de activos de información.
- Facilitará las tareas posteriores relacionadas con la gestión de riesgos y la clasificación y tratamiento de la información.
- Asegurará que la información reciba el nivel de protección adecuado según su importancia.
- Evitará la divulgación, modificación, retiro o destrucción de información almacenada en medios.

- Garantizará el uso aceptable y la devolución de los activos asociados a la información.

Dependencias

La ejecución del mismo no depende de proyectos predecesores.

Clasificación del Proyecto

El presente proyecto se clasifica como “seguridad lógica”.

Plazo

Realización en el corto plazo.

Equipos del proyecto y Duración

El proyecto estará liderado por el Responsable de Seguridad de la Información.

Las áreas descriptas tendrás una relación directa durante la realización del proyecto.

Equipos del Proyecto	Perfil	Disponibilidad %
Interno	Responsable de Seguridad de la Información	100%
	Gerente de Sistemas	20%
	Gerente de Tecnología	60%
Externo	Un Consultor SR	100%
	Un Consultor SSR	100%
	Dirección General	
Áreas involucradas en el Proyecto	Dirección unidad de negocio Forestal	
	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
Duración	La duración estándar del proyecto es de 44 jornadas laborales.	

Costo

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por un consultor sr y un cconsultor sr

Costo del Proyecto		
Consultoría	$	7.240,00
Software	$	-
Adquisición de equipos	$	-
Costo Total del proyecto U$	$	7.240,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

8.1.1 - Inventario de activos

8.1.3 - Uso aceptable de los activos

8.1.4 - Retorno de los activos

8.2.1 - Clasificación de la información

8.2.2 - Rotulado / etiquetado de la información

8.2.3 - Manipulación de activos

8.3.1 - Gestión de medios extraíbles

8.3.2 - Disposición final de medios

8.3.3 - Traslado de medios físicos

Proyecto: SEGURIDAD EN LAS COMUNICACIONES

Descripción

Diseñar la arquitectura de redes para proteger adecuadamente la información que transita por las redes dentro de la organización y asegurar la transferencia fehaciente de información entre la organización y partes externas.

Objetivos

- Garantizar la protección de la información en las redes y sus instalaciones de procesamiento de datos.
- Asegurar que la información transferida dentro de la organización y con cualquier entidad externa sea segura
- Cumplir con las normas de privacidad y confidencialidad.

Alcance

El alcance del proyecto se ajusta a las siguientes tareas:

- Definición e implementación de la arquitectura de redes.
- Actualización de la infraestructura de comunicaciones de la organización.
- Pruebas de las implementaciones.
- Documentación y formación a los administradores del entorno.

Beneficios

Los beneficios asociados a este proyecto son:

- Evitar la alteración indebida de la información en tránsito por las redes.
- Incrementar los niveles de seguridad dividiendo las redes en distintos dominios (recursos humanos, finanzas, legales entre otros).
- Establecer acuerdos y mecanismos de transferencia segura entre la organización y partes externas.
- La información involucrada en la mensajería electrónica estará correctamente protegida.

Dependencias

El presente proyecto tiene relación con otros proyectos predecesores. La ejecución del mismo podrá realizarse una vez finalizadas las tareas agrupadas en el proyecto "Marco Normativo de Seguridad".

Clasificación del Proyecto

El presente proyecto se clasifica como "seguridad lógica".

Plazo

Realización en el corto plazo.

Equipos del Proyecto y Duración

El proyecto estará liderado por el Responsable de Seguridad de la Información.

Las áreas descriptas tendrás una relación directa durante la realización del proyecto.

Equipos del Proyecto	Perfil	Disponibilidad %
Interno	Responsable de Seguridad de la Información	100%
	Gerente de Tecnología	50%
Externo	Un Consultor SR	100%
	Un Consultor SSR	100%
	Dirección General	
Áreas involucradas en el Proyecto	Dirección unidad de negocio Forestal	
	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
Duración	La duración estándar del proyecto es de 44 jornadas laborales.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por un consultor sr y un consultor ssr.

Se adquirirán softwares para realizar análisis de vulnerabilidades y monitoreo de trafico de red.

Sera necesario implementar equipamiento de infraestructura para segregar los grupos de servicios de información, usuarios y sistemas.

Costo del Proyecto		
Consultoría	$	6.440,00
Software	$	10.000,00
Adquisición de equipos	$	40.000,00
Costo Total del proyecto U$	$	56.440,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

13.1.1 - Controles de red

13.1.2 - Seguridad de los servicios de red

13.1.3 - Segregación en redes

13.2.2 - Acuerdos de transferencia de información

13.2.3 - Mensajería electrónica

13.2.4 - Acuerdos de confidencialidad

3.3.3. PLAN DE ACCIÓN A MEDIANO PLAZO

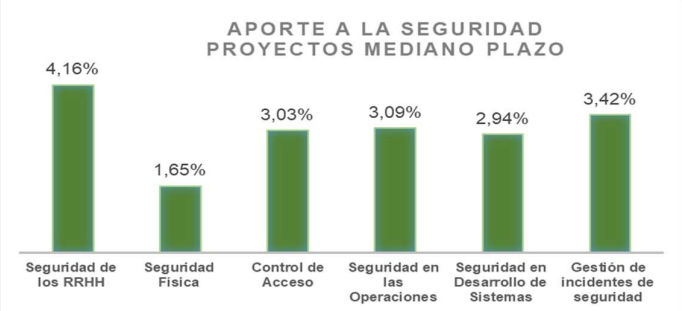
Los proyectos que en adelante se detallan, han sido identificados como necesarios para elevar el nivel de Seguridad en el mediano plazo alcanzando el **51,04%** de cumplimento acumulado, respecto de la Norma ISO/IEC 27001:2013.

PROYECTOS A MEDIANO PLAZO

- Proyecto de Seguridad de Recursos Humanos
- Proyecto de Seguridad Física
- Proyecto de Control de Acceso
- Proyecto de Seguridad de las Operaciones
- Seguridad en Desarrollo de Sistemas
- Gestión de Incidentes de Seguridad

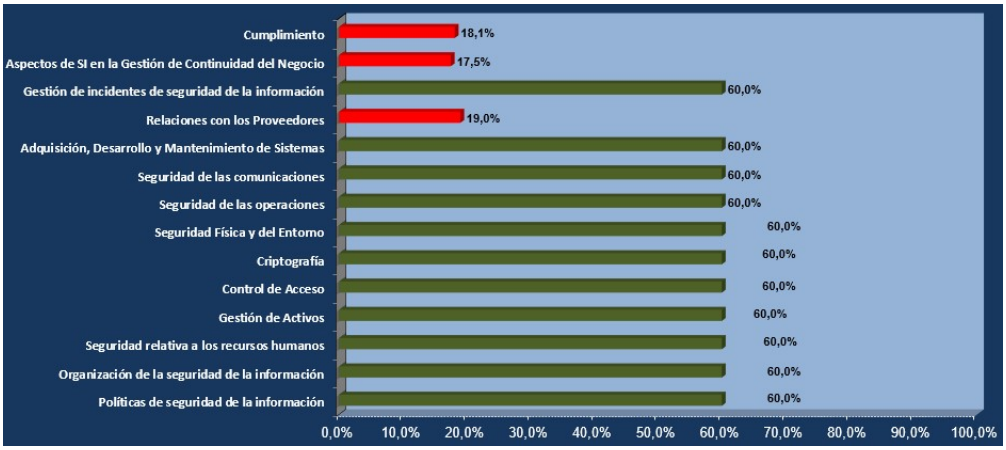
La ejecución de los proyectos aporta a la seguridad un 18,29 % de cumplimento, respecto de la Norma ISO/IEC 27001:2013.

A continuación, se detalla el aporte de cada uno de los proyectos.



Fuente: elaboración propia.

Nivel de cumplimiento de los capítulos de la Norma ISO/IEC 27001:2013 luego de la finalización de los proyectos de mediano plazo



Fuente: elaboración propia.

Proyecto: SEGURIDAD DE LOS RECURSOS HUMANOS

Descripción

Identificar y establecer cuáles son los requerimientos de seguridad relacionados con la captación y selección de nuevos miembros de la organización. Brindar formación especializada a los empleados y contratistas sobre la seguridad aplicada al ciclo de vida de un empleado.

Objetivos

- Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean idóneos para los roles para los cuales se los considera, y sean conscientes de sus responsabilidades con respecto a la seguridad de la información y las cumplan.
- Proteger los intereses de la organización como parte del proceso de desvinculación o cambio de puesto de sus empleados y contratistas.
- Establecer un programa de concientización sobre seguridad de la información dirigido a los empleados y, cuando sea pertinente a los contratistas.
- Definir un proceso disciplinario formal para aplicar a empleados ante transgresiones a la seguridad de la información. Será notificado a los empleados y contratistas.

Alcance

El alcance del proyecto se ajusta a los siguientes controles: medidas necesarias para controlar la seguridad de la información durante el ciclo de vida de los RRHH (antes, durante y después de la contratación) aplicable por las áreas de recursos humanos de la organización. Investigación de antecedentes, Términos y condiciones de empleo. Responsabilidades de la dirección. Concientización, educación y capacitación en seguridad de la información. Proceso disciplinario. Responsabilidades en la desvinculación o cambio de puesto.

Beneficios

- Los beneficios asociados a este proyecto son:
- Adecuar a la organización a los requisitos definidos por la Norma ISO/IEC 27001:2013.
- Garantizar que todos los recursos humanos (empleados, contratistas y terceros) vinculados con la organización, entiendan sus responsabilidades y posean las condiciones para desarrollarlas.
- Reducir riesgos de fraude y uso inadecuado de los activos de información de la organización.

Dependencias

El presente proyecto tiene relación con otros proyectos predecesores. La ejecución del mismo podrá realizarse una vez finalizadas las tareas agrupadas en el proyecto “Marco Normativo de Seguridad”.

Clasificación del Proyecto

El presente proyecto se clasifica como “seguridad organizativa”.

Plazo

Realización en el mediano plazo.

Equipos del Proyecto y Duración

El proyecto estará liderado por el Gerente de Recursos Humanos.

Las áreas descriptas tendrás una relación directa durante la realización del proyecto.

Equipos del Proyecto		
	Perfil	Disponibilidad %
Interno	Gerente de RRHH	20%
	Jefe de RRHH	60%
	Responsable de Seguridad de la Información	100%
Externo	Un Consultor SR	100%
	Un Consultor SSR	100%
	Dirección General	
Áreas involucradas en el Proyecto	Dirección unidad de negocio Forestal	
	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
Duración	La duración estándar del proyecto es de 20 jornadas laborales.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por un consultor sr y un consultor ssr

Costo del Proyecto		
Consultoría	$	3.000,00
Software	$	-
Adquisición de equipos	$	-
Costo Total del proyecto U$	$	3.000,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

7.1.1 - Investigación de antecedentes

7.1.2 - Términos y condiciones de empleo

7.2.1 - Responsabilidades de la dirección

7.2.2 - Concientización, educación y capacitación en SI

7.2.3 - Proceso disciplinario

7.3.1 - Responsabilidades en desvinculación o cambio de puesto

9.2.6 - Remoción o ajuste de los derechos de acceso

Proyecto: SEGURIDAD FISICA

Descripción

Definir controles de seguridad física que protejan los activos de información críticos ante accesos no autorizados, desastres naturales y daños intencionales contra la organización.

Objetivos

Adecuar el centro de datos, las salas técnicas y oficinas a la Norma ISO/IEC 27001:2013 en su capítulo referente a Seguridad Física. Definir controles que garanticen la protección adecuada de los elementos de la infraestructura crítica, permitiendo:

- Evitar acceso físico no autorizado, daños e interferencias a la información y a las instalaciones de procesamiento de datos.
- Evitar perdidas, daños, robos o situaciones que generen la interrupción de las operaciones de la empresa.

Alcance

Para la realización de las revisiones, se tendrán en cuenta las instalaciones de los Centros de Datos, Oficinas y Depósitos.

Beneficios

Los beneficios asociados a este proyecto son:

- Obtención de normas y directrices para la mejora de la seguridad física en la organización.
- Evitar el acceso no autorizado a las áreas que contienen información y a las instalaciones de procesamiento de datos sensibles o críticas.
- Garantizar la continuidad del negocio antes cortes de luz, falla de equipamiento y otras interrupciones provocadas por problemas en los servicios básicos.
- Realización del proyecto en base a buenas prácticas y normas que lleven a la organización al cumplimiento de los requerimientos de la Norma ISO 27001:2013.

Dependencias

El presente proyecto tiene relación con otros proyectos predecesores. La ejecución del mismo podrá realizarse una vez finalizadas las tareas agrupadas en el proyecto “Marco Normativo de Seguridad”.

Clasificación del Proyecto

El presente proyecto se clasifica como “seguridad física”.

Plazo

Realización en el mediano plazo.

Equipos del Proyecto y Duración

El proyecto estará liderado por el Responsable de Seguridad de la Información.

Las áreas descriptas tendrás una relación directa durante la realización del proyecto.

Equipos del Proyecto	Perfil	Disponibilidad %
Interno	Responsable de Seguridad de la Información	60%
	Jefe de Mantenimiento	50%
Externo	Un Consultor SR	100%
	Un Consultor SSR	100%
	Dirección General	
Áreas involucradas en el Proyecto	Dirección unidad de negocio Forestal	
	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
	Mantenimiento	
Duración	La duración estándar del proyecto es de 30 jornadas laborales.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por un consultor sr y un consultor ssr.

Costo del Proyecto		
Consultoría	$	4.100,00
Software	$	-
Adquisición de equipos	$	35.000,00
Costo Total del proyecto U$	$	39.100,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

11.1.2 - Controles de ingreso físico

11.1.3 - Aseguramiento de oficinas, recintos e instalaciones

11.1.4 - Protección contra amenazas externas y del entorno

11.1.5 - Trabajo en áreas seguras

11.1.6 - Áreas de carga y descarga

11.2.1 - Ubicación y protección del equipamiento

11.2.2 - Elementos de soporte

11.2.3 - Seguridad del cableado

11.2.4 - Mantenimiento del equipamiento

11.2.5 - Retiro de activos

11.2.6 - Seguridad de equipamiento y activos fuera de las instalaciones

11.2.7 - Disposición final segura o reúso del equipamiento

11.2.8 - Equipamiento desatendido de usuario

Proyecto: CONTROL DE ACCESO

Descripción

Definir controles de acceso que protejan los activos de información ante ingresos no autorizados. Brindar formación especializada y concientizar a los empleados respecto de la utilización de las contraseñas y la seguridad en los equipos puestos a su disposición.

Objetivos

- Crear controles que garanticen el acceso a la información, sistemas, aplicaciones e instalaciones de procesamiento de datos sólo al personal autorizado.
- Concientizar a los usuarios para que sean responsables de proteger su información de autenticación.

Alcance

El proyecto se circunscribe a los activos de información en formato digital de la empresa y a los empleados que interactúen con los mismos.

Beneficios

Los beneficios asociados a este proyecto son:

- Obtención de normas y directrices para la mejora de la gestión de accesos en la organización.
- Garantiza el acceso a la información, sistemas, servicios y a las instalaciones de procesamiento de datos únicamente al personal autorizado.
- La información de acceso a los activos de información estará protegida. Los usuarios serán conscientes de la importancia de mantener secretos los datos de autenticación para acceder a los distintos activos de información.

Dependencias

El presente proyecto tiene relación con otros proyectos predecesores. La ejecución del mismo podrá realizarse una vez finalizadas las tareas agrupadas en el proyecto “Marco Normativo de Seguridad” y “Gestión de Activos”

Clasificación del Proyecto

El presente proyecto se clasifica como “seguridad lógica”.

Plazo

Realización en el mediano plazo.

Equipos del Proyecto y Duración

El proyecto estará liderado por el Responsable de Seguridad de la Información.

Las áreas descriptas tendrás una relación directa durante la realización del proyecto.

Equipos del Proyecto	Perfil	Disponibilidad %
Interno	Responsable de Seguridad de la Información	100%
	Jefe de Proyectos y Desarrollo	50%
	Gerente de Tecnología	30%
Externo	Un Consultor SR	100%
	Un Consultor SSR	100%
	Dirección General	
Áreas involucradas en el Proyecto	Dirección unidad de negocio Forestal	
	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
Duración	La duración estándar del proyecto es de 30 jornadas laborales.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por un consultor sr y un consultor ssr.

Se adquirirán softwares para monitorear el acceso a los activos de información, estos serán instalados en el centro de procesamiento de datos. No es necesario adquirir equipamiento adicional.

Costo del Proyecto		
Consultoría	$	4.900,00
Software	$	20.000,00
Adquisición de equipos	$	-
Costo Total del proyecto U$	$	24.900,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

9.1.2 - Acceso a las redes y servicios asociados

9.2.1 - Alta y baja de registros de usuario

9.2.2 - Asignación de accesos del usuario

9.2.3 - Gestión de los derechos de acceso con privilegios

9.2.4 - Gestión de información secreta para autenticación del usuario

9.2.5 - Revisión de los derechos de acceso del usuario

9.3.1 - Uso de la información secreta de autenticación

9.4.1 - Restricción del acceso a la información

9.4.2 - Procedimientos seguros de inicio de sesión

9.4.3 - Sistema de gestión de contraseñas

9.4.4 - Uso de herramientas de administración de sistemas

9.4.5 - Control de acceso al código fuente de los programas

Proyecto: SEGURIDAD DE LAS OPERACIONES

Descripción

Analizar la infraestructura de TI e implementar mejoras en las operaciones tomando como base de referencia el apartado Seguridad de las Operaciones de la norma ISO/IEC 27002.

Documentar los procedimientos operacionales relacionados con la seguridad operacional, los que estarán disponibles para todas aquellas personas que los necesiten.

Objetivos

- Garantizar las correctas y seguras operaciones de las instalaciones de procesamiento de información.
- Asegurar que la información y las instalaciones de procesamiento de información estén protegidas contra software maliciosos.
- Registrar eventos y generar evidencias ante comportamientos anormales.
- Identificar rápidamente cualquier tipo de vulnerabilidades técnicas.

Alcance

El proyecto se circunscribe a las operaciones realizadas en el centro de procesamiento de datos y la información en formato digital utilizada por la empresa.

Beneficios

Los beneficios asociados a este proyecto son:

- Establecer los procedimientos operativos para las actividades operacionales según las buenas prácticas de seguridad.
- Gestionar los controles de cambios en las instalaciones, sistemas y procesamiento de datos.
- Identificar el uso de recursos actuales y proyectar las necesidades de los requisitos futuros para garantizar el rendimiento de los sistemas.

- Evitar los cambios no autorizados en entornos de producción.
- Utilizar controles para la detección y prevención de software maliciosos.
- Asegurar la disponibilidad de copias de respaldo de los datos y servicios.
- Gestionar y resguardar los eventos generados por los sistemas y aplicaciones.
- Generar alertas ante comportamientos anormales.

Dependencias

El presente proyecto tiene relación con otros proyectos predecesores. La ejecución del mismo podrá realizarse una vez finalizadas las tareas agrupadas en el proyecto "Marco Normativo de Seguridad".

Clasificación del Proyecto

El presente proyecto se clasifica como "seguridad lógica".

Plazo

Realización en el mediano plazo.

Equipos del Proyecto y Duración

El proyecto estará liderado por el Responsable de Seguridad de la Información.

Las áreas descriptas tendrás una relación directa durante la realización del proyecto.

Equipos del Proyecto		
	Perfil	Disponibilidad %
Interno	Responsable de Seguridad de la Información	100%
	Gerente de Tecnología	50%
Externo	Un Consultor SR	100%
	Un Consultor SSR	100%
	Dirección General	
	Dirección unidad de negocio Forestal	
	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
Duración	La duración estándar del proyecto es de 40 jornadas laborales.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por un consultor sr y un consultor ssr.

Será necesario implementar equipamiento de infraestructura para mejorar e incrementar el tiempo de resguardo de la información y los sistemas utilizados.

Costo del Proyecto		
Consultoría	$	6.800,00
Software	$	-
Adquisición de equipos	$	30.000,00
Costo Total del proyecto U$	$	36.800,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

12.1.1 - Procedimientos operativos documentados

12.1.2 - Gestión del cambio

12.1.3 - Gestión de la capacidad

12.1.4 - Separación de entornos de desarrollo, prueba y producción

12.2.1 - Controles contra el código malicioso

12.3.1 - Resguardo de la información

12.4.1 - Registro de eventos

12.4.2 - Protección de la información de registros

12.4.3 - Registros de administradores y operadores

12.4.4 - Sincronización de los relojes

12.6.1 - Gestión de vulnerabilidades técnicas

12.6.2 - Restricciones a la instalación de software

12.7.1 - Controles de auditoría de sistemas

Proyecto: SEGURIDAD EN DESARROLLO DE SISTEMAS

Descripción

Definir una metodología de desarrollo seguro, contemplando la seguridad en cada una de las fases del ciclo de vida del desarrollo y para cada uno de los entornos y tecnologías empleadas.

Objetivos

Dotar a la organización de una metodología de desarrollo seguro de aplicaciones, mediante la cual se garantice la ejecución de los pasos necesarios que permitan disponer de un nivel aceptable de seguridad sobre todas las aplicaciones.

Para ello se hace necesario realizar una serie de acciones que, de forma resumida, serán:

- Tipificar los diversos modelos de aplicaciones y formalizar los requisitos y buenas prácticas de seguridad (normalización) para cada fase del ciclo de vida de desarrollo de aplicaciones.
- Definir el conjunto de pruebas necesarias para la aceptación y paso a producción de un sistema.
- Definir e implementar los mecanismos de selección y protección de los datos de prueba.
- Dotar a las aplicaciones de la seguridad necesaria a fin de prevenir los ataques de seguridad (Ej.: mediante el desarrollo de APIs de criptografía, auditoría, validación de datos, etc.).
- Concientizar a la organización e impartir formación continua a los desarrolladores, sobre la importancia de realizar desarrollos seguros, contemplando la seguridad en todas las fases del ciclo de desarrollo.
- Proteger la información de las aplicaciones que circulan por las redes públicas para evitar la transmisión incompleta, el enrutamiento incorrecto, la alteración, duplicación y divulgación no autorizadas.

Alcance

El alcance del proyecto se ajusta a las siguientes tareas:

- Realización de pruebas de seguridad con herramientas automáticas, y pruebas manuales con el objetivo de disponer una referencia del estado actual de seguridad de las aplicaciones existentes.
- Partiendo de la documentación y del conocimiento de las metodologías de desarrollo utilizadas por parte de la organización, se desplegará la política de desarrollo seguro y un conjunto de normas de seguridad, una por cada fase del ciclo de vida de desarrollo definido en la organización.
- Estandarizar los mecanismos de seguridad en el desarrollo de software por medio de la creación de cinco interfaces de programación de aplicaciones: validación de datos, criptografía, auditoria, control de sesión, identificación y autenticación.

Beneficios

Los beneficios asociados a este proyecto son:

- Elevar el nivel de seguridad de las aplicaciones.
- Obtener una visión global sobre la seguridad de las aplicaciones.

- Reducir los tiempos de desarrollo.
- Controlar de forma centralizada la seguridad de las aplicaciones.
- Definir y difundir normas, guías, recomendaciones y metodologías.
- Automatización de tareas y seguridad proactiva.
- Elevar la concientización de los equipos de desarrollo de software.

La adopción de una metodología de desarrollo seguro redundará en beneficio claro del negocio, aumentando notablemente el nivel de seguridad de las aplicaciones de la organización desde las fases iniciales del desarrollo, disminuyendo drásticamente los riesgos y ahorrando costos y tiempo.

Dependencias

El presente proyecto tiene relación con otros proyectos predecesores. La ejecución del mismo podrá realizarse una vez finalizadas las tareas agrupadas en el proyecto "Marco Normativo de Seguridad".

Clasificación del Proyecto

El presente proyecto se clasifica como "seguridad lógica".

Plazo

Realización en el mediano plazo.

Equipos del Proyecto y Duración

El proyecto estará liderado por el Responsable de Seguridad de la Información.

Las áreas descriptas tendrás una relación directa durante la realización del proyecto.

Equipos del Proyecto	Perfil	Disponibilidad %
Interno	Responsable de Seguridad de la Información	100%
	Gerente de Sistemas	20%
	Jefe de Proyectos y Desarrollo	80%
	Gerente de Tecnología	20%
Externo	Dos Consultores SR	100%
	Tres Consultores SSR	100%
Áreas involucradas en el Proyecto	Dirección General	
	Dirección unidad de negocio Forestal	
	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
Duración	La duración estándar del proyecto es de 44 jornadas laborales.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por dos consultores sr y tres consultores ssr.
Sera necesario adquirir equipamiento de infraestructura para incrementar la capacidad de memoria de acceso aleatorio de los servidores que componen el procesamiento de datos.

Costo del Proyecto		
Consultoría	$	20.240,00
Software	$	-
Adquisición de equipos	$	-
Costo Total del proyecto U$	$	20.240,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

14.1.1 - Análisis y especificación de requisitos de seguridad

14.1.2 - Asegurar servicios de aplicaciones en redes públicas

14.1.3 - Protección de las transacciones en servicios de aplicaciones

14.2.2 - Procedimientos de control de cambios en sistemas

14.2.3 - Revisión técnica de aplicaciones luego de cambios en producción

14.2.4 - Restricciones a cambios en paquetes de software

14.2.5 - Principios de seguridad aplicados a ingeniería en sistemas

14.2.6 - Entornos seguros de desarrollo

14.2.7 - Desarrollo de terceras partes

14.2.8 - Pruebas de seguridad de los sistemas

14.2.9 - Pruebas de aceptación de sistemas

14.3.1 - Protección de datos de pruebas

Proyecto: GESTIÓN DE INCIDENTES DE SEGURIDAD

Descripción

Asignar de forma oportuna los recursos necesarios y garantizar su uso adecuado, con el objeto de prevenir, detectar y corregir incidentes que afectan la seguridad de la información.

Objetivos

- Garantizar que las causas, el tratamiento y la solución de los eventos de seguridad de la información sirvan para la implementación de acciones correctivas y preventivas.

- Asegurar un enfoque coherente y eficaz para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación de los eventos y las vulnerabilidades de la seguridad.

Alcance

El proyecto se centra en la definición de un proceso de gestión de incidentes de seguridad de la información, mediante la ejecución de las siguientes tareas:

- Establecer un modelo de proceso que sirva de guía en el diseño y reingeniería y se ajuste a las siguientes tareas: definición del ciclo de vida de un incidente, definición de procedimientos, indicadores de gestión, concientización sobre los canales de comunicación de incidentes, vulnerabilidades y eventos de seguridad, priorización y tiempos de resolución de eventos.
- Diseñar un plan de acción, para integrar y adaptar aquellos procesos que requieran cambios o ajustes.
- Asistir y acompañar a la organización en la gestión y control de la implementación del plan de acción.
- Transferir conceptos y terminología básica a los principales participantes del proyecto.

Beneficios

Los beneficios asociados a este proyecto son:

- Mayor protección ante amenazas externas, internas y vulnerabilidades.
- Detectar tempranamente y reducir la probabilidad de incidentes.
- Respuesta a incidentes en forma sistemática.
- Facilitar la resolución rápida y eficiente de incidentes de seguridad, minimizando la pérdida de información e interrupción de servicios.
- Prevenir la ocurrencia reiterada de incidentes mediante el aprendizaje.
- Mejorar continuamente el marco de seguridad y el proceso de tratamiento de incidentes.
- Manejar correctamente los aspectos legales que pudieran surgir en el tratamiento de incidentes.

Dependencias

El presente proyecto tiene relación con otros proyectos predecesores. La ejecución del mismo podrá realizarse una vez finalizadas las tareas agrupadas en el proyecto “Marco Normativo de Seguridad”.

Clasificación del Proyecto

El presente proyecto se clasifica como “seguridad organizativa”.

Plazo

Realización en el mediano plazo.

Equipos del Proyecto y Duración

El proyecto estará liderado por el Responsable de Seguridad de la Información.

Las áreas descriptas tendrán una relación directa durante la realización del proyecto.

Equipos del Proyecto	Perfil	Disponibilidad %
Interno	Responsable de Seguridad de la Información	100%
	Gerente de Sistemas	10%
	Gerente de Comunicaciones	15%
	Gerente de Tecnología	30%
Externo	Un Consultor SR	100%
	Un Consultor SSR	50%
Áreas involucradas en el Proyecto	Dirección General	
	Dirección unidad de negocio Forestal	
	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
Duración	La duración estándar del proyecto es de 22 jornadas laborales.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por un consultor sr y un consultor ssr.

Costo del Proyecto		
Consultoría	$	3.300,00
Software	$	10.000,00
Adquisición de Hardware	$	-
Costo Total del proyecto U$	$	13.300,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

16.1.2 - Reporte de eventos de SI

16.1.3 - Reporte de debilidades de SI

16.1.4 - Evaluación y decisión sobre eventos de SI

16.1.5 - Respuesta a incidentes de SI

16.1.6 - Aprendizaje de los incidentes de SI

16.1.7 - Recolección de evidencias

3.3.4. PLAN DE ACCIÓN A LARGO PLAZO

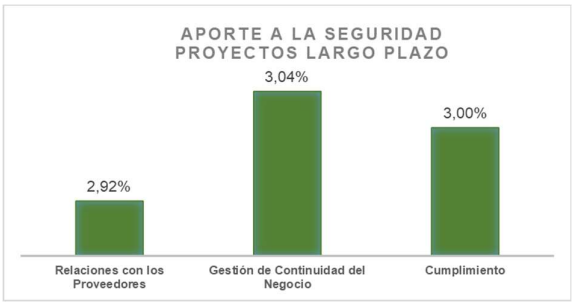
Los proyectos que en adelante se detallan, han sido identificados como necesarios para elevar el nivel de Seguridad a largo plazo alcanzando el **60%** de cumplimento, respecto de la Norma ISO/IEC 27001:2013.

PROYECTOS A LARGO PLAZO

- Proyecto de Relaciones con los Proveedores
- Proyecto de Gestión de Continuidad del Negocio
- Proyecto de Cumplimiento

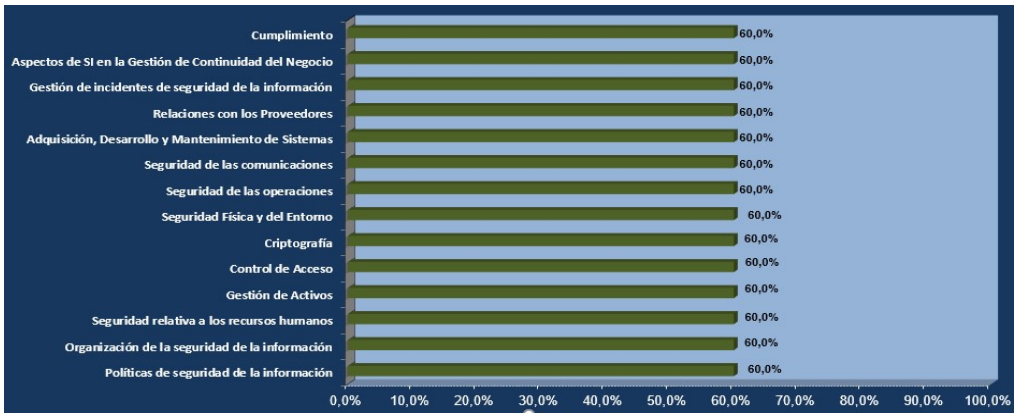
La ejecución de estos proyectos aporta a la seguridad un 8,96% de cumplimento, respecto de la Norma ISO/IEC 27001:2013. La realización de estos, permitirá alcanzar la meta especificada en el plan estratégico.

A continuación, se detalla el aporte de cada uno de los proyectos.



Fuente: elaboración propia.

Nivel de cumplimiento de los capítulos de la Norma ISO/IEC 27001:2013 luego de la finalización de los proyectos de largo plazo



Fuente: elaboración propia

Proyecto: RELACIONES CON LOS PROVEEDORES

Descripción

Establecer formalmente las condiciones de acceso de las empresas o personal externo a los sistemas de información y a los recursos que manejan activos de información. Supervisar el cumplimiento de los niveles de servicios acordados con los proveedores.

Objetivos

- Definir controles de acceso que protejan los activos de información utilizados por los proveedores.
- Gestionar los niveles establecidos con los proveedores respecto a la seguridad de la información y la prestación de los servicios.

Alcance

El proyecto se circunscribe a los proveedores que tengan acceso a los activos de la información o interactúen con cualquier recurso tecnológico o sistema de la empresa.

Beneficios

Los beneficios asociados a este proyecto son:

- Garantizar la protección de los activos de la organización, que sean accesibles por los proveedores.
- Mantener un nivel apropiado de seguridad de la información y la entrega del servicio acorde con los acuerdos por sus terceras partes.

Dependencias

El presente proyecto tiene relación con otros proyectos predecesores. La ejecución del mismo podrá realizarse una vez finalizadas las tareas agrupadas en el proyecto “Marco Normativo de Seguridad”.

Clasificación del Proyecto

El presente proyecto se clasifica como “seguridad organizativa”.

Plazo

Realización en el largo plazo.

Equipos del Proyecto y Duración

El proyecto estará liderado por el Responsable de Seguridad de la Información.

Las áreas descriptas tendrás una relación directa durante la realización del proyecto.

Equipos del Proyecto		
	Perfil	Disponibilidad %
Interno	Responsable de Seguridad de la Información	100%
	Gerente de Legales	20%
	Gerente de Sistemas	10%
	Gerente de RRHH	10%
Externo	Un Consultor SR	100%
Áreas involucradas en el Proyecto	Dirección General	
	Dirección unidad de negocio Forestal	
	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
Duración	La duración estándar del proyecto es de 22 jornadas laborales.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por un consultor sr.

Costo del Proyecto		
Consultoría	$	2.420,00
Software	$	-
Adquisición de Hardware	$	-
Costo Total del proyecto U$	$	2.420,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

15.1.2 - Tratamiento de la SI en acuerdos con proveedores

15.1.3 - Cadena de suministro en TI y comunicaciones

15.2.1 - Seguimiento y revisión en servicios de proveedores

15.2.2 - Gestión de cambios en servicios de proveedores

Proyecto: GESTIÓN DE CONTINUIDAD DE NEGOCIO

Descripción

Desarrollar un Programa de Gestión de la Continuidad de Negocio, que defina cuáles son los procesos críticos para el negocio en función de su valor de riesgo, y establezca las pautas de actuación ante desastres. Determinar los responsables de coordinar las acciones que deberá tomar la organización ante desastres, y los encargados de la evaluación y mantenimiento del plan.

Objetivos

Desarrollar el Programa de Gestión de la Continuidad de Negocio siguiendo los lineamientos definidos por la Norma ISO/IEC 27001:2013.

Garantizar que la organización disponga de capacidad de reacción frente a la interrupción de actividades de negocio causadas por la aparición de grandes fallos o desastres.

Para ello será necesario:

- Implantar un proceso de gestión de continuidad del negocio mediante la combinación de controles preventivos y de recuperación.
- Reducir a niveles aceptables la interrupción causada ante determinados incidentes o fallos, minimizando los tiempos de recuperación de los sistemas afectados.
- Asegurar la vuelta a la normalidad tras la activación de un proceso de recuperación.

El objetivo de la recuperación dentro del proceso de la continuidad, es permitir a la organización reanudar sus operaciones informáticas en un centro de datos secundario cuando se produce un desastre en el centro de datos principal, a causa del cual la infraestructura queda inutilizable.

Alcance

El alcance del proyecto se ajusta en el desarrollo del Programa de Gestión de la Continuidad de Negocio y la revisión y actualización de todos los planes de contingencia y recuperación de TI existentes dentro de la organización.

Beneficios

Los beneficios asociados a este proyecto son:

- Identificar los diversos eventos que podrían afectar la continuidad de las operaciones y su impacto sobre el negocio.
- Disponer de los mecanismos y procedimientos de recuperación necesarios que permitan afrontar una crisis que afecte a los sistemas de información, con el fin de asegurar la continuidad de la operación y consecuentemente minimizar el impacto en el negocio.
- Garantizar la disponibilidad de la información de negocio, en función de los niveles de riesgo establecidos en la Organización.

- Conocer los tiempos críticos de recuperación para volver a la situación anterior al desastre sin comprometer al negocio.
- Prevenir o minimizar las pérdidas para el negocio en caso de desastre.
- Clasificar los activos para priorizar su protección en caso de desastre.
- Aportar una ventaja competitiva frente a la competencia.

Dependencias

El presente proyecto tiene relación con otros proyectos predecesores. La ejecución del mismo podrá realizarse una vez finalizadas las tareas agrupadas en el proyecto "Marco Normativo de Seguridad".

Clasificación del Proyecto

El presente proyecto se clasifica como "seguridad organizativa".

Equipos del Proyecto y Duración

El proyecto estará liderado por el Responsable de Seguridad de la Información.

Las áreas descriptas tendrás una relación directa durante la realización del proyecto.

Equipos del Proyecto	Perfil	Disponibilidad %
Interno	Responsable de Seguridad de la Información	100%
	Gerente de Sistemas	20%
	Jefe de Proyectos y Desarrollo	30%
	Gerente de Tecnología	30%
Externo	Dos Consultor SR	100%
	Tres Consultores SSR	100%
Áreas involucradas en el Proyecto	Dirección General	
	Dirección unidad de negocio Forestal	
	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
Duración	La duración estándar del proyecto es de 66 jornadas laborales.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por dos consultores sr y tres consultores ssr.

Será necesario adquirir equipamiento de infraestructura y licencias de software para incrementar la capacidad de procesamiento en el sitio de contingencia.

Costo del Proyecto		
Consultoría	$	30.360,00
Software	$	15.000,00
Adquisición de Equipamiento	$	81.000,00
Costo Total del proyecto U$	$	126.360,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

17.1.1 - Planificación de la continuidad de la SI

17.1.3 - Verificación, revisión y evaluación de la continuidad de la SI

17.2.1 - Disponibilidad de las instalaciones

Proyecto: CUMPLIMIENTO

Descripción

Garantizar que la seguridad de la información sea implementada y operada de acuerdo con las políticas y procedimientos organizacionales. Evitar los incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con los requisitos de seguridad.

Objetivos

Los objetivos de este proyecto se centran en identificar de forma documentada todos los requisitos legales y contractuales que afecten a la organización y asegurar que los responsables de cada área revisen, den conformidad a los procedimientos y que éstos sean aplicados de acuerdo a los requisitos definidos.

Una vez establecidos los requisitos legales y contractuales que afecten a la organización se deberá:

- Establecer procedimientos que garanticen el uso del software de acuerdo a los derechos de propiedad Intelectual y utilizar productos de software propietario.
- Proteger los registros de información contra pérdidas, destrucción, falsificación, acceso no autorizado y publicación no autorizada de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.
- Garantizar la privacidad y la protección de la información personal identificable según se requiere en la legislación y las normativas pertinentes donde corresponda

- Utilizar controles criptográficos en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.

Alcance

El proyecto se circunscribe a todos los requisitos legales y contractuales que afecten a la organización y al cumplimiento de todos los proyectos que componen el plan estratégico.

Beneficios

Los beneficios asociados a este proyecto son:

- Evitar incumplimientos a las obligaciones legales, estatutarias, normativas o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.
- Garantizar que se implementa y opera la seguridad de la información de acuerdo a las políticas y procedimientos organizacionales.

Dependencias

El presente proyecto tiene relación con todos los proyectos descriptos en el plan estratégico. La ejecución del mismo podrá realizarse una vez finalizados los proyectos:

- Marco Normativo de Seguridad
- Organización de la seguridad de la información
- Seguridad de Recursos Humanos
- Gestión de Activos
- Control de Acceso
- Criptografía
- Seguridad Física
- Seguridad de las operaciones
- Seguridad de las Comunicaciones
- Seguridad en Desarrollo de Sistemas
- Relaciones con los Proveedores
- Gestión de incidentes de seguridad de la información
- Gestión de Continuidad del Negocio

Clasificación del Proyecto

El presente proyecto se clasifica como “seguridad organizativa”.

Plazo

Realización en el largo plazo.

Equipos del Proyecto y Duración

El proyecto estará liderado por el Responsable de Seguridad de la Información.

Las áreas descriptas tendrán una relación directa durante la realización del proyecto.

La duración del mismo está prevista en 20 jornadas laborales. Posterior a esto se realizarían validaciones de complimiento, mensualmente, a cargo del equipo interno.

Equipos del Proyecto	Perfil	Disponibilidad %
Interno	Responsable de Seguridad de la Información	100%
Externo	Un Consultor SR	100%
Áreas involucradas en el Proyecto	Dirección General	
	Dirección unidad de negocio Forestal	
	RRHH	
	Legales	
	Sistemas	
	Finanzas	
	Comunicaciones	
Duración	La duración estándar del proyecto es de 20 jornadas laborales.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo.

El equipo externo estará conformado por un consultor sr.

Costo del Proyecto		
Consultoría	$	1.600,00
Software	$	-
Adquisición de Equipamiento	$	-
Costo Total del proyecto U$	$	1.600,00

Controles Relacionados

Los siguientes controles de la Norma ISO/IEC 27001:2013, están directamente relacionados con el aporte a la seguridad del proyecto:

18.1.1 - Identificación de la legislación aplicable

18.1.3 - Protección de los registros de información

18.1.4 - Privacidad y protección de información personal

18.2.1 - Revisión independiente de la SI

18.2.2 - Cumplimiento de políticas y normas de SI

18.2.3 - Revisión de cumplimiento técnico

PROGRAMA DE CAPACITACIÓN Y CONCIENTIZACIÓN

Descripción

Garantizar que todo el personal este notificado y comprenda la importancia del cumplimiento de las políticas, normas y procedimientos establecidos.

Generar talleres de capacitación y concientización respecto a la importancia de la seguridad de la información.

Objetivos

Los objetivos de este proyecto se centran en que:

- Los usuarios comprendan la importancia del cumplimiento de las políticas, normas y procedimientos establecidos.
- Los usuarios conozcan y hagan uso de las herramientas relacionadas con la seguridad de la información.

Alcance

El proyecto se circunscribe a todos los empleados de la empresa Pomera.

Beneficios

Los beneficios asociados a este proyecto son:

- Garantizar que los usuarios comprendan y conozcan la importancia del cumplimiento de las políticas, normas y procedimientos establecidos.
- Asegurar el correcto uso de las herramientas relacionadas con la seguridad de la información.

Dependencias

El presente proyecto tiene relación con todos los proyectos descriptos en el plan estratégico.

La ejecución del mismo se realizaría una vez que finalice cada uno de los proyectos que componen el plan estratégico.

Equipos del Proyecto y Duración

El proyecto estará liderado por el Gerente de Recursos Humanos.

Equipos del Proyecto	Perfil	Disponibilidad %
Interno	CEO	10%
	Director de Negocios Forestales	10%
	Geremte de Recursos Humanos	100%
	Gerente de Comunicaciones	100%
	Gerente de Sistemas	100%
	Responsable de Seguridad de la Información	100%
Duración	La duración estándar del proyecto es de 26 encuentros de 3hs.	

Costos

Por políticas de la empresa el costo interno de los recursos asignados al proyecto no serán asociados al mismo. Por lo tanto, este proyecto no tiene asociado ningún costo.

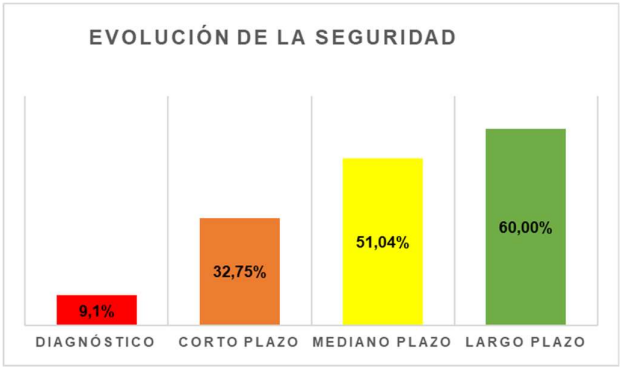
3.3.5. EVOLUCIÓN DE LA SEGURIDAD POR PLAZOS

Se expone en detalle el plan de acción requerido para alcanzar el 60% de madurez de conformidad de acuerdo a cada capítulo de la Norma ISO/IEC 27001:2013 en función de los plazos planificados (corto, medio y largo).

La siguiente tabla permite visualizar el plan de acción requerido, considerando el aporte acumulado de cada plazo, es decir la proyección escalonada que permitirá alcanzar el objetivo definido en el plan estratégico.

Capítulo de la Norma ISO/IEC 27001:2013	Evolución de la Seguridad			
	Diagnóstico	Corto Plazo	Mediano Plazo	Largo Plazo
Políticas de seguridad de la información	0,0%	60,0%	60,0%	60,0%
Organización de la seguridad de la información	3,6%	60,0%	60,0%	60,0%
Seguridad relativa a los recursos humanos	5,0%	5,0%	60,0%	60,0%
Gestión de Activos	6,0%	60,0%	60,0%	60,0%
Control de Acceso	10,3%	14,3%	60,0%	60,0%
Criptografía	0,0%	60,0%	60,0%	60,0%
Seguridad Física y del Entorno	33,0%	37,0%	60,0%	60,0%
Seguridad de las operaciones	13,6%	16,8%	60,0%	60,0%
Seguridad de las comunicaciones	20,7%	60,0%	60,0%	60,0%
Adquisición, Desarrollo y Mantenimiento de Sistemas	14,6%	18,8%	60,0%	60,0%
Relaciones con los Proveedores	10,0%	19,0%	19,0%	60,0%
Gestión de incidentes de seguridad de la información	3,6%	12,1%	60,0%	60,0%
Aspectos de SI en la Gestión de Continuidad del Nego	3,7%	17,5%	17,5%	60,0%
Cumplimiento	3,7%	18,1%	18,1%	60,0%
Meta según objetivo	9,1%	32,75%	51,04%	60,00%

Fuente: elaboración propia.



Fuente: elaboración propia.

3.4. ESTRATEGIA DE MANAGEMENT

3.4.1. GESTIÓN DE PROYECTOS

La dirección del grupo estará involucrada y apoyará públicamente la ejecución de los proyectos que componen el plan estratégico, buscando de esta forma conseguir el compromiso de los empleados.
Para ésto, la dirección participará en el inicio de cada uno de los proyectos y formará parte del comité encargado de tomar decisiones del plan estratégico.

EQUIPO DE TRABAJO

El equipo de trabajo estará compuesto por:

- El equipo interno: formado por distintos empleados de la empresa.
- El equipo externo: conformado por consultores expertos en seguridad de la información, con distintos niveles de experiencia.
- Usuarios claves: son usuarios específicos dentro de un área. Se los capacitará y participarán en las reuniones de avance de los proyectos. Serán el primer punto de contacto de los empleados ante consultas o sugerencias.

En los proyectos que amerite, se utilizará el concepto “train the trainers”. El equipo externo capacitará a los usuarios claves y posteriormente, ellos transmitirán el conocimiento adquirido a los demás usuarios.

Cada proyecto tendrá un líder de proyecto. Quien trabajara con el equipo de recursos internos y externos y el área de PMO.

A continuación, se detalla el equipo de trabajo de cada uno de los proyectos que componen el plan estratégico:

Proyectos / Equipo de Trabajo	Gerente de RRHH	Gerente de Sistemas	Gerente de Comunicaciones	Gerente de Legales	Responsable de Seguridad de la Información	Gerente de Tecnología	Jefe de RRHH	Jefe de Proyectos y Desarrollo	Jefe de Mantenimiento	Consultor SR	Consultor SSR	Lider del proyecto
Marco Normativo de Seguridad		x			x	x				x	x	Responsable de Seguridad de la Información
Criptografía					x	x				x		Responsable de Seguridad de la Información
Organización de la seguridad de la información	x	x			x	x				x	x	Responsable de Seguridad de la Información
Gestión de Activos		x			x	x				x	x	Responsable de Seguridad de la Información
Seguridad de las Comunicaciones					x	x				x	x	Gerente de Tecnología
Seguridad de Recursos Humanos	x				x		x			x	x	Gerente de Recursos Humanos
Seguridad Física					x				x	x	x	Responsable de Seguridad de la Información
Control de Acceso					x	x		x		x	x	Responsable de Seguridad de la Información
Seguridad de las Operaciones					x	x				x	x	Responsable de Seguridad de la Información
Seguridad en Desarrollo de Sistemas		x			x	x		x		x	x	Gerente de Sistemas
Relaciones con los Proveedores	x	x		x	x					x		Responsable de Seguridad de la Información
Gestión de incidentes de seguridad de la información		x	x		x	x				x	x	Responsable de Seguridad de la Información
Gestión de Continuidad del Negocio		x			x	x			x	x	x	Responsable de Seguridad de la Información
Cumplimiento					x					x		Responsable de Seguridad de la Información

Se creará un comité de seguridad, formado por los siguientes puestos:

El comité de seguridad garantizará una clara dirección y un apoyo manifiesto de las iniciativas de seguridad, mediante un adecuado compromiso y una apropiada asignación de responsabilidades.

Principales responsabilidades del comité de seguridad:

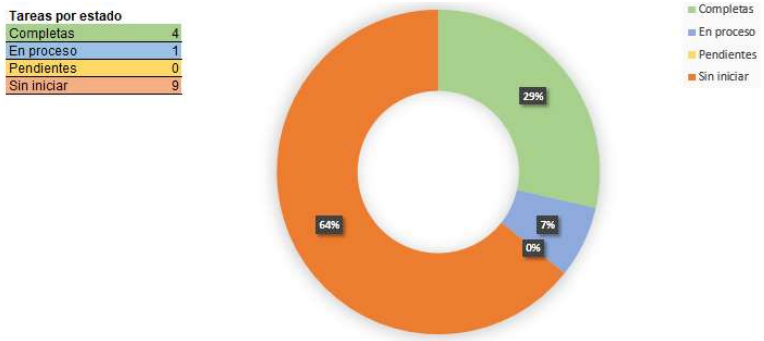
- Dentro del flujo de aprobación de las Políticas de Seguridad de la Información: es el primer nivel de aprobación, revisión, rechazo, modificación o eliminación de éstas.
- Aprobará normas y procedimientos de seguridad de la Información.
- Revisará y validará normas y procedimientos en general, a fin de verificar que se estén cumpliendo los aspectos de seguridad dentro de los procesos.
- Por medio del Comité de Seguridad de la Información se supervisa y controla el Plan de Seguridad de la Información.

- Velará por el cumplimiento de las políticas, normas, procedimientos y demás documentos relacionados en Seguridad de la Información dentro de la organización.

COMUNICACIÓN SOBRE EL AVANCE DE PROYECTO

El avance de los proyectos del plan estratégico, así como cualquier problema o desvío que surja será tratado en el comité de seguridad.

Los líderes asignados a cada proyecto son los responsables de comunicar el estado de los mismos al comité.
Se utilizará un documento llamado “Estado Plan Estratégico” para mostrar el estado de cada proyecto. El área de administración de proyectos será responsable de mantener el documento actualizado.



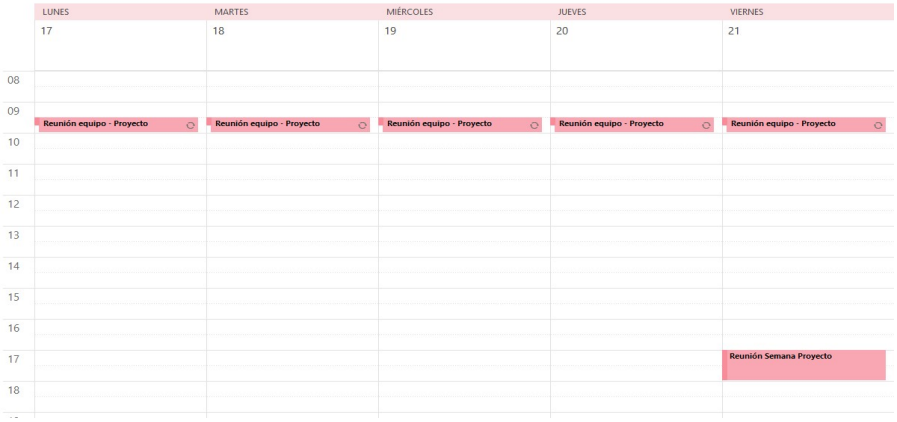
Estado	Fecha	Actividad	Nota	Responsable
Completas	30/4/2020	Marco Normativo de Seguridad		Responsable de Seguridad de la Información
Completas	1/5/2020	Criptografía		Responsable de Seguridad de la Información
Completas	2/5/2020	Organización de la Seguridad		Responsable de Seguridad de la Información
Completas	3/5/2020	Gestión de Activos	Pendiente aplicar configuración voice	Responsable de Seguridad de la Información
En proceso	4/5/2020	Seguridad en las Comunicaciones		Jefe de Infraestructura
Sin iniciar		Seguridad de los RRHH	Descarga ya habilitada por Copilot	Gerente de Recursos Humanos
Sin iniciar		Seguridad Física		Responsable de Seguridad de la Información
Sin iniciar		Control de Acceso		Responsable de Seguridad de la Información
Sin iniciar		Seguridad en las Operaciones		Responsable de Seguridad de la Información
Sin iniciar		Seguridad en Desarrollo de Sistemas		Gerente de Sistemas
Sin iniciar		Gestión de incidentes de seguridad	Pendientes pruebas de conectividad	Responsable de Seguridad de la Información
Sin iniciar		Relaciones con los Proveedores		Responsable de Seguridad de la Información
Sin iniciar		Gestión de Continuidad del Negocio		Responsable de Seguridad de la Información
Sin iniciar		Cumplimiento		Responsable de Seguridad de la Información

REUNIONES

Se realizarán reuniones diarias y mensuales con el equipo de trabajo de cada proyecto.
Las reuniones diarias tendrán una duración de 15 minutos, se concretarán al comienzo del día laboral. Las reuniones mensuales, se llevarán a cabo el último día de la semana por la tarde; la duración no será superior a 1 hora.

El comité de seguridad se reunirá una vez por mes o al finalizar un proyecto, horario y día a confirmar según disponibilidad de los integrantes

Agenda de reuniones diarias y mensuales:



3.4.2. GESTIÓN DE RECURSOS HUMANOS

La gestión de los recursos humanos estará centrada en dos líneas de acción:

- Motivación del personal involucrado en el plan estratégico
- Retención de los recursos humanos

MOTIVACIÓN

Se llevará a cabo un plan de motivación dirigido a todo el personal involucrado en el plan estratégico. Se desarrollarán acciones que permitan gestionar las motivaciones extrínsecas e intrínsecas.

MOTIVACIONES EXTRÍNSECAS

Se utilizará el siguiente modelo para clasificar el nivel de desarrollo profesional, el potencial y el riesgo de cambio laboral de cada uno de los principales empleados del plan estratégico. El resultante de este modelo determinará incrementos salariales y porcentaje de bonos.

Nombre	Nombre de puesto	Desempeño			Ocupante Clave	Riesgo vacante			Potencial			Antigüedad	Fecha Nacimiento	Edad	Nivel educativo
		Alto	Medio	Bajo		Alto	Medio	Bajo	Alto	Medio	Bajo				
	Gerente de RRHH														Universitario
	Gerente de Sistemas														Universitario
	Gerente de Comunicaciones														Universitario
	Gerente de Legales														Universitario
	Gerente de Tecnología														Universitario
	Responsable de Seguridad de la Información														Universitario
	Jefe de RRHH														Terciario
	Jefe de Proyectos y Desarrollo														Universitario
	Jefe de Mantenimiento														Terciario

Nombre y Puesto: se especificará el nombre del empleado y el puesto que ocupa actualmente.

Desempeño: analizando el desempeño a lo largo del plan estratégico, se identificarán los integrantes con desempeño sobresaliente, promedio o bajo

Ocupantes claves: corresponde a aquellos integrantes que contarán con información y/o experiencias clave.

Riesgo vacante: relacionado con la probabilidad de que un empleado deje la empresa en corto plazo, entre seis y doce meses.

Se considerará el atractivo del empleado en el mercado laboral, el grado de insatisfacción, situaciones particulares de su vida personal, etc.

La clasificación es:

- Riesgo bajo: ningún o pocos indicios de que la persona pudiera dejar la empresa en los próximos meses.
- Riesgo moderado: algunos indicios de que la persona pudiera dejar la empresa en los próximos meses.
- Riesgo alto: claros indicios de que la persona pudiera dejar la empresa en los próximos meses

Potencial:

- Potencial Alto: Describe a los empleados que pudieran ser promovidos a un puesto que implique mayor responsabilidad, de acuerdo a su desarrollo laboral.
- Potencial medio: describe aquellos empleados de los que se espera puedan ocupar otros puestos de mayor complejidad dentro de su mismo nivel organizacional. Esta categoría incluye a muchos empleados sobresalientes ("los mejores en su puesto").
- Potencial bajo: describe a aquellos empleados de los que se espera puedan continuar desarrollándose en su puesto actual. Esta categoría incluye a muchos empleados sobresalientes ("los mejores en su puesto"), así como a personas que no están interesadas en ser promovidas en este momento.

MOTIVACIONES INTRÍNSECAS

La motivación intrínseca será cubierta por medio de las siguientes acciones:

- Mayores responsabilidades y nuevos conocimientos a los empleados que demuestren mayor interés en el desarrollo del plan estratégico; se les asignará mayores responsabilidades, buscando mejorar su autoestima y aspiraciones de realización profesional y personal.
- Reconocimiento personal y potenciar los logros: se realizarán mensualmente publicaciones en el blog corporativo especificando los logros de los empleados. Se realizarán mensualmente actividades de media jornada laboral con el personal involucrado en los proyectos.

RETENCIÓN DEL PERSONAL

Junto con las acciones de motivación se desarrollará un plan de carrera profesional.
A medida que los empleados cumplan con los objetivos establecidos y exista una vacante en la estructura del plan de carrera desarrollado tendrán la opción de promocionar.
Los distintitos niveles definidos en el esquema de plan de carrera, tendrán asociado un conjunto de compensaciones preestablecidas.

3.4.3. GESTIÓN DE PROVEEDORES

En lo que respecta a la gestión de proveedores es de vital importancia establecer un acuerdo de confidencialidad con el equipo externo que colaborará a lo largo del plan estratégico. El cual tendrá acceso a información confidencial de la empresa y conocerá los procedimientos internos utilizados.

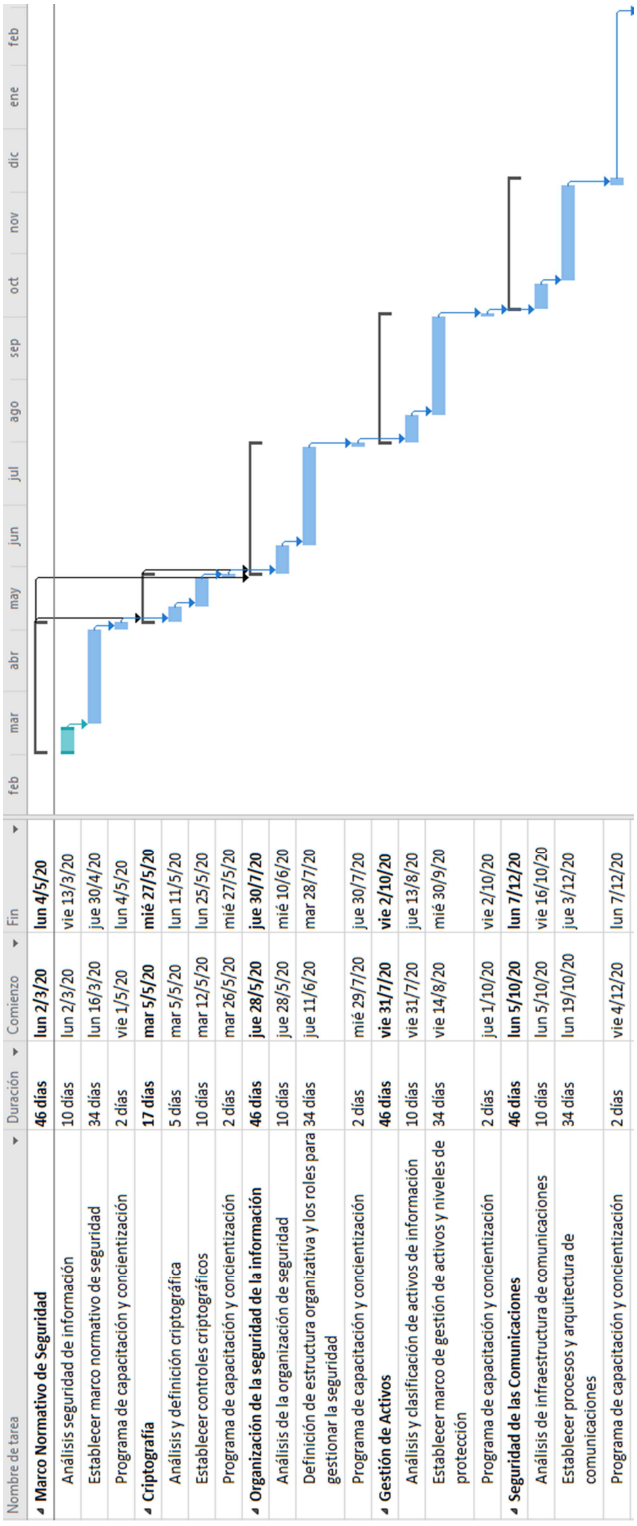
Se emplearán diferentes tecnológicas durante la ejecución de los proyectos. Al momento de adquirirlas se determinará los acuerdos de nivel de servicio y el modo de adquisición y nivel de soporte a utilizar.

3.5. PLAN DE IMPLEMENTACIÓN

Implementación de proyectos del plan estratégico.

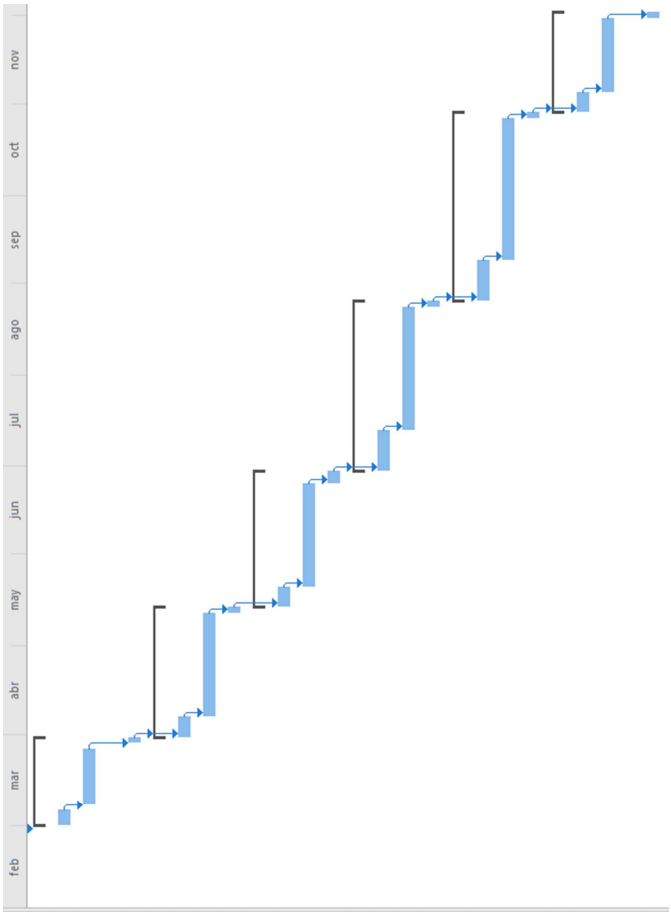
Nombre de tarea	Duración	Comienzo	Fin
Marco Normativo de Seguridad	**46 días**	**lun 2/3/20**	**lun 4/5/20**
Análisis seguridad de información	10 días	lun 2/3/20	vie 13/3/20
Establecer marco normativo de seguridad	34 días	lun 16/3/20	jue 30/4/20
Programa de capacitación y concientización	2 días	vie 1/5/20	lun 4/5/20
Criptografía	**17 días**	**mar 5/5/20**	**mié 27/5/20**
Análisis y definición criptográfica	5 días	mar 5/5/20	lun 11/5/20
Establecer controles criptográficos	10 días	mar 12/5/20	lun 25/5/20
Programa de capacitación y concientización	2 días	mar 26/5/20	mié 27/5/20
Organización de la seguridad de la información	**46 días**	**jue 28/5/20**	**jue 30/7/20**
Análisis de la organización de seguridad	10 días	jue 28/5/20	mié 10/6/20
Definición de estructura organizativa y los roles para gestionar la seguridad	34 días	jue 11/6/20	mar 28/7/20
Programa de capacitación y concientización	2 días	mié 29/7/20	jue 30/7/20
Gestión de Activos	**46 días**	**vie 31/7/20**	**vie 2/10/20**
Análisis y clasificación de activos de información	10 días	vie 31/7/20	jue 13/8/20
Establecer marco de gestión de activos y niveles de protección	34 días	vie 14/8/20	mié 30/9/20
Programa de capacitación y concientización	2 días	jue 1/10/20	vie 2/10/20
Seguridad de las Comunicaciones	**46 días**	**lun 5/10/20**	**lun 7/12/20**
Análisis de infraestructura de comunicaciones	10 días	lun 5/10/20	vie 16/10/20
Establecer procesos y arquitectura de comunicaciones	34 días	lun 19/10/20	jue 3/12/20
Programa de capacitación y concientización	2 días	vie 4/12/20	lun 7/12/20
Seguridad de Recursos Humanos	**22 días**	**lun 1/3/21**	**mar 30/3/21**
Análisis de procesos de RRHH	5 días	lun 1/3/21	vie 5/3/21
Establecer responsabilidades y acuerdos de seguridad de la información	15 días	lun 8/3/21	vie 26/3/21
Programa de capacitación y concientización	2 días	lun 29/3/21	mar 30/3/21
Seguridad Física	**32 días**	**mié 31/3/21**	**jue 13/5/21**
Análisis y definición de la seguridad física	5 días	mié 31/3/21	mar 6/4/21
Establecer procesos y controles de seguridad física	25 días	mié 7/4/21	mar 11/5/21
Programa de capacitación y concientización	2 días	mié 12/5/21	jue 13/5/21
Control de Acceso	**32 días**	**vie 14/5/21**	**lun 28/6/21**
Análisis de controles de acceso	5 días	vie 14/5/21	jue 20/5/21
Establecer marco de gestión y controles de acceso	25 días	vie 21/5/21	jue 24/6/21
Programa de capacitación y concientización	2 días	vie 25/6/21	lun 28/6/21
Seguridad de las Operaciones	**42 días**	**mar 29/6/21**	**mié 25/8/21**
Análisis y definición de las operaciones	10 días	mar 29/6/21	lun 12/7/21
Establecer procesos y controles de las operaciones	30 días	mar 13/7/21	lun 23/8/21
Programa de capacitación y concientización	2 días	mar 24/8/21	mié 25/8/21
Seguridad en Desarrollo de Sistemas	**46 días**	**jue 26/8/21**	**jue 28/10/21**
Análisis de Sistemas existentes	10 días	jue 26/8/21	mié 8/9/21
Generación de ambientes y procesos de desarrollo	34 días	jue 9/9/21	mar 26/10/21
Programa de capacitación y concientización	2 días	mié 27/10/21	jue 28/10/21
Gestión de incidentes de seguridad	**24 días**	**vie 29/10/21**	**mié 1/12/21**
Análisis de incidentes de seguridad	5 días	vie 29/10/21	jue 4/11/21
Establecer marco de gestión de incidentes de seguridad	17 días	vie 5/11/21	lun 29/11/21
Programa de capacitación y concientización	2 días	mar 30/11/21	mié 1/12/21
Relaciones con los Proveedores	**24 días**	**lun 7/3/22**	**jue 7/4/22**
Análisis y definición de accesos de proveedores	5 días	lun 7/3/22	vie 11/3/22
Establecer controles y niveles de acceso	17 días	lun 14/3/22	mar 5/4/22
Programa de capacitación y concientización	2 días	mié 6/4/22	jue 7/4/22
Gestión de Continuidad del Negocio	**68 días**	**vie 8/4/22**	**mar 12/7/22**
Análisis y planificación de la continuidad de negocio	15 días	vie 8/4/22	jue 28/4/22
Desarrollar el Programa de Gestión de la Continuidad de Negocio	51 días	vie 29/4/22	vie 8/7/22
Programa de capacitación y concientización	2 días	lun 11/7/22	mar 12/7/22
Cumplimiento	**20 días**	**mié 13/7/22**	**mar 9/8/22**
Identificar requisitos legales y contractuales	5 días	mié 13/7/22	mar 19/7/22
Garantizar el cumplimiento de los requisitos definidos	15 días	mié 20/7/22	mar 9/8/22

Proyecto: Implementación de proyectos de corto plazo



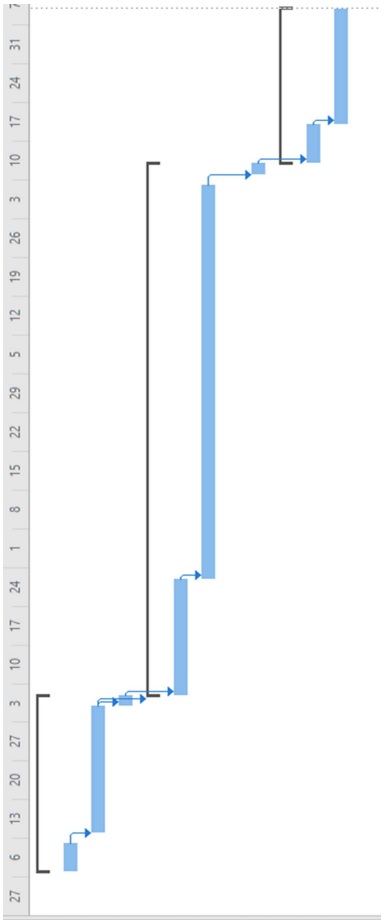
Nombre de tarea	Duración	Comienzo	Fin
Marco Normativo de Seguridad	**46 días**	**lun 2/3/20**	**lun 4/5/20**
Análisis seguridad de información	10 días	lun 2/3/20	vie 13/3/20
Establecer marco normativo de seguridad	34 días	lun 16/3/20	jue 30/4/20
Programa de capacitación y concientización	2 días	vie 1/5/20	lun 4/5/20
Criptografía	**17 días**	**mar 5/5/20**	**mié 27/5/20**
Análisis y definición criptográfica	5 días	mar 5/5/20	lun 11/5/20
Establecer controles criptográficos	10 días	mar 12/5/20	lun 25/5/20
Programa de capacitación y concientización	2 días	mar 26/5/20	mié 27/5/20
Organización de la seguridad de la información	**46 días**	**jue 28/5/20**	**jue 30/7/20**
Análisis de la organización de seguridad	10 días	jue 28/5/20	mié 10/6/20
Definición de estructura organizativa y los roles para gestionar la seguridad	34 días	jue 11/6/20	mar 28/7/20
Programa de capacitación y concientización	2 días	mié 29/7/20	jue 30/7/20
Gestión de Activos	**46 días**	**vie 31/7/20**	**vie 2/10/20**
Análisis y clasificación de activos de información	10 días	vie 31/7/20	jue 13/8/20
Establecer marco de gestión de activos y niveles de protección	34 días	vie 14/8/20	mié 30/9/20
Programa de capacitación y concientización	2 días	jue 1/10/20	vie 2/10/20
Seguridad de las Comunicaciones	**46 días**	**lun 5/10/20**	**lun 7/12/20**
Análisis de infraestructura de comunicaciones	10 días	lun 5/10/20	vie 16/10/20
Establecer procesos y arquitectura de comunicaciones	34 días	lun 19/10/20	jue 3/12/20
Programa de capacitación y concientización	2 días	vie 4/12/20	lun 7/12/20

Proyecto: Implementación de proyectos de mediano plazo



Nombre de tarea	Duración	Comienzo	Fin
Seguridad de Recursos Humanos	**22 días**	**lun 1/3/21**	**mar 30/3/21**
Análisis de procesos de RRHH	5 días	lun 1/3/21	vie 5/3/21
Establecer responsabilidades y acuerdos de seguridad de la información	15 días	lun 8/3/21	vie 26/3/21
Programa de capacitación y concientización	2 días	lun 29/3/21	mar 30/3/21
Seguridad Física	**32 días**	**mié 31/3/21**	**jue 13/5/21**
Análisis y definición de la seguridad física	5 días	mié 31/3/21	mar 6/4/21
Establecer procesos y controles de seguridad física	25 días	mié 7/4/21	mar 11/5/21
Programa de capacitación y concientización	2 días	mié 12/5/21	jue 13/5/21
Control de Acceso	**32 días**	**vie 14/5/21**	**lun 28/6/21**
Análisis de controles de acceso	5 días	vie 14/5/21	jue 20/5/21
Establecer marco de gestión y controles de acceso	25 días	vie 21/5/21	jue 24/6/21
Programa de capacitación y concientización	2 días	vie 25/6/21	lun 28/6/21
Seguridad de las Operaciones	**42 días**	**mar 29/6/21**	**mié 25/8/21**
Análisis y definición de las operaciones	10 días	mar 29/6/21	lun 12/7/21
Establecer procesos y controles de las operaciones	30 días	mar 13/7/21	lun 23/8/21
Programa de capacitación y concientización	2 días	mar 24/8/21	mié 25/8/21
Seguridad en Desarrollo de Sistemas	**46 días**	**jue 26/8/21**	**jue 28/10/21**
Análisis de Sistemas existentes	10 días	jue 26/8/21	mié 8/9/21
Generación de ambientes y procesos de desarrollo	34 días	jue 9/9/21	mar 26/10/21
Programa de capacitación y concientización	2 días	mié 27/10/21	jue 28/10/21
Gestión de incidentes de seguridad	**24 días**	**vie 29/10/21**	**mié 1/12/21**
Análisis de incidentes de seguridad	5 días	vie 29/10/21	jue 4/11/21
Establecer marco de gestión de incidentes de seguridad	17 días	vie 5/11/21	lun 29/11/21
Programa de capacitación y concientización	2 días	mar 30/11/21	mié 1/12/21

Proyecto: Implementación de proyectos de largo plazo



Nombre de tarea	Duración	Comienzo	Fin
Relaciones con los Proveedores	**24 días**	**lun 7/3/22**	**jue 7/4/22**
Análisis y definición de accesos de proveedores	5 días	lun 7/3/22	vie 11/3/22
Establecer controles y niveles de acceso	17 días	lun 14/3/22	mar 5/4/22
Programa de capacitación y concientización	2 días	mié 6/4/22	jue 7/4/22
Gestión de Continuidad del Negocio	**68 días**	**vie 8/4/22**	**mar 12/7/22**
Análisis y planificación de la continuidad de negocio	15 días	vie 8/4/22	jue 28/4/22
Desarrollar el Programa de Gestión de la Continuidad de Negocio	51 días	vie 29/4/22	vie 8/7/22
Programa de capacitación y concientización	2 días	lun 11/7/22	mar 12/7/22
Cumplimiento	**20 días**	**mié 13/7/22**	**mar 9/8/22**
Identificar requisitos legales y contractuales	5 días	mié 13/7/22	mar 19/7/22
Garantizar el cumplimiento de los requisitos definidos	15 días	mié 20/7/22	mar 9/8/22

3.6. PRESUPUESTO

El presupuesto total del plan estratégico es de USD 354.970.

Se detalla el presupuesto económico del plan estratégico:

Presupuesto del Plan Estratégico				
Proyecto	U$ Consultoría	U$ Software	U$ Adquisición de equipos	U$ por Proyecto
Marco Normativo de Seguridad	$ 8.360	$ -	$ -	$ 8.360
Criptografía	$ 1.650	$ 10.000	$ -	$ 11.650
Organización de la seguridad de la información	$ 6.440	$ -	$ -	$ 6.440
Gestión de Activos	$ 7.240	$ -	$ -	$ 7.240
Seguridad de las Comunicaciones	$ 6.440	$ 10.000	$ 40.000	$ 56.440
Seguridad de Recursos Humanos	$ 3.000	$ -	$ -	$ 3.000
Seguridad Física	$ 4.100	$ -	$ 35.000	$ 39.100
Control de Acceso	$ 4.900	$ 20.000	$ -	$ 24.900
Seguridad de las Operaciones	$ 6.800	$ -	$ 30.000	$ 36.800
Seguridad en Desarrollo de Sistemas	$ 20.240	$ -	$ 8.000	$ 28.240
Gestión de incidentes de seguridad	$ 2.420	$ -	$ -	$ 2.420
Relaciones con los Proveedores	$ 2.420	$ -	$ -	$ 2.420
Gestión de Continuidad del Negocio	$ 30.360	$ 15.000	$ 81.000	$ 126.360
Cumplimiento	$ 1.600	$ -	$ -	$ 1.600
			Total Plan Estrategico	$ 354.970,00

La ejecución del mismo será realizada en 3 etapas, las cuales se describen a continuación:

1- Los proyectos clasificados a corto plazo serán ejecutados con el presupuesto del año 2020.

Proyecto	U$ Consultoría	U$ Software	U$ Adquisición de equipos	U$ por Proyecto
Marco Normativo de Seguridad	$ 8.360	$ -	$ -	$ 8.360
Criptografía	$ 1.650	$ 10.000	$ -	$ 11.650
Organización de la seguridad de la información	$ 6.440	$ -	$ -	$ 6.440
Gestión de Activos	$ 7.240	$ -	$ -	$ 7.240
Seguridad de las Comunicaciones	$ 6.440	$ 10.000	$ 40.000	$ 56.440
			Partida presupuestaria 2020	$ 90.130

2- Los proyectos clasificados a mediano plazo serán ejecutados con el presupuesto del año 2021.

Proyecto	U$ Consultoría	U$ Software	U$ Adquisición de equipos	U$ por Proyecto
Seguridad de Recursos Humanos	$ 3.000	$ -	$ -	$ 3.000
Seguridad Física	$ 4.100	$ -	$ 35.000	$ 39.100
Control de Acceso	$ 4.900	$ 20.000	$ -	$ 24.900
Seguridad de las Operaciones	$ 6.800	$ -	$ 30.000	$ 36.800
Seguridad en Desarrollo de Sistemas	$ 20.240	$ -	$ 8.000	$ 28.240
Gestión de incidentes de seguridad	$ 2.420	$ -	$ -	$ 2.420
			Partida presupuestaria 2021	$ 134.460

3- Por último, los proyectos clasificados a lago plazo serán ejecutados con el presupuesto correspondiente al año 2022.

Proyecto	U$ Consultoría	U$ Software	U$ Adquisición de equipos	U$ por Proyecto
Relaciones con los Proveedores	$ 2.420	$ -	$ -	$ 2.420
Gestión de Continuidad del Negocio	$ 30.360	$ 15.000	$ 81.000	$ 126.360
Cumplimiento	$ 1.600	$ -	$ -	$ 1.600
			Partida presupuestaria 2022	$ 130.380

Con el objetivo de identificar los compromisos de pago, se detalla el presupuesto financiero del plan estratégico, el mismo esta expresado en dólares:

PPTO FINANCIERO 2020 - PLAN ESTRATÉGICO										
MESES	4	5	6	7	8	9	10	11	12	PPTO 2020
Marco Normativo de Seguridad	$ -	$ 8.360	$ -	$ -	$ -	$ -	$ -	$ -	$ -	
Criptografía	$ -	$ 10.000	$ -	$ 1.650	$ -	$ -	$ -	$ -	$ -	
Organización de la seguridad de la información	$ -	$ -	$ -	$ -	$ 6.440	$ -	$ -	$ -	$ -	$ 90.130
Gestión de Activos	$ -	$ -	$ -	$ -	$ -	$ -	$ 7.240	$ -	$ -	
Seguridad de las Comunicaciones	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 56.440	
PPTO FINANCIERO 2021 - PLAN ESTRATÉGICO										
MESES	4	5	6	7	8	9	10	11	12	PPTO 2021
Seguridad de Recursos Humanos	$ 3.000	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	
Seguridad Física	$ -	$ 39.100	$ -	$ -	$ -	$ -	$ -	$ -	$ -	
Control de Acceso	$ -	$ -	$ -	$ 24.900	$ -	$ -	$ -	$ -	$ -	$ 134.460
Seguridad de las Operaciones	$ -	$ -	$ -	$ -	$ -	$ 36.800	$ -	$ -	$ -	
Seguridad en Desarrollo de Sistemas	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 28.240	$ -	
Gestión de incidentes de seguridad	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 2.420	
PPTO FINANCIERO 2022 - PLAN ESTRATÉGICO										
MESES	4	5	6	7	8	9	10	11	12	PPTO 2021
Relaciones con los Proveedores	$ 2.420	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	
Gestión de Continuidad del Negocio	$ -	$ -	$ -	$ -	$ 126.360	$ -	$ -	$ -	$ -	$ 130.380
Cumplimiento	$ -	$ -	$ -	$ -	$ -	$ 1.600	$ -	$ -	$ -	

4. CONCLUSIONES

La mayoría de las personas supone que la seguridad de la información se trata de equipos informáticos y software antivirus. La adquisición e implementación de estas soluciones son sólo una parte de la seguridad de la información.

Los problemas de seguridad de la información generalmente surgen debido al comportamiento humano; por lo tanto, la tecnología por sí sola no puede ser una solución para tal problema.

La seguridad de la información se basa en la construcción de un conjunto de salvaguardas, que deben incluir cambios organizacionales, seguridad física, protección legal, problemas de recursos humanos y tecnología, con el objetivo de proteger lo más valioso: su información.

Por lo tanto, cualquier iniciativa para aumentar la capacidad de resistencia frente a un posible ciberataque es insuficiente si no se genera un cambio cultural organizacional.

Desarrollar una cultura corporativa orientada a la seguridad parte de comprender que los mecanismos de seguridad informática son solo técnicas o herramientas que se utilizan para fortalecer la confidencialidad, la integridad y la disponibilidad de un sistema informático, pero son los usuarios quienes con sus acciones determinan la utilidad y suficiencia de esos esfuerzos por proteger los activos de información.

Alinear la organización con los requerimientos de la norma ISO/IEC 27001:2013 permitirá que la empresa gestione y aplique de forma adecuada todas las medidas de seguridad necesarias para controlar el estado y la utilización de la información, pudiendo de esta forma gestionar adecuadamente la confidencialidad, integridad y disponibilidad de los activos de información.

4.1. ASPECTOS DE IMPLEMENTACIÓN

RECOMENDACIONES:

Compromiso de la dirección. Para que la iniciativa entregue los resultados esperados es un requisito necesario el apoyo e involucramiento de la dirección, sin su apoyo formal real es casi imposible desarrollar y mantener operativos los proyectos descriptos en el plan estratégico. Aquellos proyectos que provienen de los sectores operativos o tácticos y no cuentan con el respaldo de la alta dirección tienen mayor posibilidad de fracaso.

Concientización: hacer foco para que todos los empleados del grupo sean conscientes de los riesgos y amenazas frente a la protección de la información, así como de reportar todas aquellas desviaciones o fallas de seguridad de la información que se presenten.

Cumplimiento: es importante garantizar que el personal del grupo cumpla con las políticas, procedimientos y prácticas de seguridad de la información. Para ésto es indispensable el entendimiento práctico de los comportamientos esperados por la organización respecto de la protección de la información.

POSIBLES PROBLEMAS A ENFRENTAR

Será necesario hacer foco en la cultura organizacional de seguridad de la información: las empresas que conforman grupo CESIJO presentan una cultura informal, donde no existen procedimientos normalizados.

La mayoría de los directivos son personas entre 55 y 60 años, con una antigüedad laboral promedio de 12 años. Cabe destacar que durante dicho período no se habrían realizado acciones de concientización respeto al uso de la tecnología ni de los riesgos asociados al uso de la misma.

4.2. FUTURAS LÍNEAS

Una vez implementado el plan estratégico, sugerirá tomar las siguientes iniciativas:

- Alinear el resto de los procesos de la empresa Forestal, así como las empresas restantes que conforman el grupo CESIJO a los requerimientos de la norma ISO/IEC 27000:2013.
- Desarrollar las acciones necesarias para alcanzar el nivel 4 del Modelo de Madurez de Capacidad, donde se tendrán indicadores numéricos y estadísticos para reflejar la evolución de los procesos.
- Desarrollar un Plan de Continuidad de Negocio, con el objetivo de mantener la funcionalidad de la organización a un nivel mínimo aceptable durante una contingencia.

5. BIBLIOGRAFÍA

- CASSIDY, A. A Practical Guide to Information Systems Strategic Planning. 2ª ed. Auerbach Publications, 2005. 394 p. ISBN: 9780849350733
- HERNÁNDEZ SAMPIERI, R; FERNÁNDEZ COLLADO, C; BAPTISTA LUCIO, P. Metodología de la investigación. Cuarta Edición, Mc Graw-Hill, México, 2008.
- DEJAN, K. Secure & Simple: A Small-Business Guide to Implementing ISO 27001 On Your Own. 1ª ed. Advisera Expert Solutions Ltd. 2016. 341 p. ISBN: 9789535745273

- DEJAN, K. 9 Steps to Cybersecurity. 1ª ed. EPPS Services Ltd. 2012. 109 p. ISBN: 9789535745228
- GUIDO LAVALLE, G. y GADZE, J. Fundamentos de la Dirección de Proyectos; Buenos Aires: Temas – UADE; 2006.
- ISO/IEC 27000. 2005. Information technology - Security techniques - Information security management systems - Overview and vocabulary. Ginebra, Suiza, 2005. 27p.
- ISO/IEC 27001. 2013 - Information technology. Security techniques. Information security management systems. Requirements. Ginebra, Suiza, 2013. 23p.
- ISO/IEC 27002. 2013, Information technology - Security Techniques - Code of practice for information security controls. Ginebra, Suiza, 2013. 80p.
- SERVICIO NACIONAL DE SANIDAD Y CALIDAD AGROALIMENTARIA VIRTUAL [en línea]. [consulta 8 feb. 2019]. <http://www.senasa.gob.ar/senasa-comunica/noticias/bosques-argentinos-actividad-forestal-y-economias-regionales>

6. ANEXOS

6.1. ANEXO 1: ENTREVISTA DIRECTOR FORESTAL

Entrevista	**EF01**
Nombre y Apellido	**K, Ricardo**
Cargo / Función	**Director Forestal**
¿Cuál es la presencia de Pomera en la industria Forestal Argentina?	
Pomera cuenta con 37.000 hectáreas forestadas en la provincia de Misiones y Corrientes. Esto representa el 5,09% del total de las 725.661 hectáreas forestadas en Misiones y Corrientes.	

6.2. ANEXO 2: ENTREVISTA GERENTE FORESTAL

Entrevista	**EF02**
Nombre y Apellido	**I, Gumercindo**
Cargo / Función	**Gerente Forestal**
¿Cuáles son los principales actividades del sector Forestal?	
El ciclo forestal es el conjunto de actividades que incluyen todas las etapas de la actividad, desde el desarrollo en laboratorios y viveros de las plantas que serán trasladadas al bosque, hasta la comercialización de los productos de la madera. Podemos identificar cuatro principales etapas del ciclo forestal: Producción de plantas, Silvicultura, Cosecha y Transporte. La primera etapa del proceso forestal consiste en la producción de los plantines de cada especie, ésto se lleva a cabo en los llamados viveros, donde se trabaja para mejorar la calidad de las plantas. La Silvicultura, comienza con la preparación de los suelos e incluye principalmente la realización de podas y raleos. La poda se realiza con el objetivo de generar madera libre de nudos al tiempo que facilita al acceso al área. El raleo es una intervención que reduce el número de árboles por hectárea y cumple el objetivo de liberar de competencia y permitir el mejor crecimiento de los árboles que quedan en la plantación. En la Cosecha, en los momentos definidos según cada especie, se procede al corte final de los árboles, posterior a ésto, se traslada hacia la zona seleccionada para su carga en camiones. Por último, en el transporte se incluyen los requerimientos de mano de obra vinculados al traslado de la madera desde los predios hasta su lugar de procesamiento industrial o hasta los puntos de salida al exterior en el caso de exportación de madera en bruto.	

6.3. ANEXO 3: ENTREVISTA GERENTE FORESTAL

Entrevista	**EF03**
Nombre y Apellido	**I, Gumercindo**
Cargo / Función	**Gerente Forestal**
¿Cómo se realiza el proceso de cosecha?	
Durante el último año se ha mejorado el proceso de cosecha, actualmente el mismo inicia con una solicitud de ventas, donde se definen los datos del cliente, tipo de árbol, importe por tonelada que serán vendidos, entre otros datos. Luego por medio de un acta de intervención, se declara los datos de los contratistas que van a realizar el proceso de cosecha, donde se especifica el lote en el que se realizarán las tareas, el importe que se pagará por tonelada o el valor del metro si la venta corresponde a postes. Cuando finaliza el proceso manual de cosecha, el camión con los rollos o postes se dirige a una báscula. Donde se realiza el registro en el "Software de básculas": aquí se hace el pesaje de los rollos (descontando el peso del camión), si fuesen postes, adicionalmente se especifica la cantidad de los mismos, el precio del flete, los datos del contratista que realizó el proceso de cosecha y del cliente. Con esta información se genera el Remito. Los remitos generados en el sistema de básculas son registrados en el sistema ERP automáticamente, por medio de una interface. Los días viernes, en el sistema ERP se realiza un proceso donde se asocia el acta de intervención con los remitos correspondientes a la misma. Este procedimiento, genera la facturación relacionada a la Solicitud de Venta y permite determinar el importe a pagar a los contratistas creando un certificado de elaboración. Ésto es posible, por los datos brindados tanto en el acta de intervención como en el remito. El certificado de elaboración es entregado a los contratistas para que realicen la factura por los servicios prestados.	

6.4. ANEXO 4: ENTREVISTA SUPERVISOR DE COSECHA

Entrevista	**EF04**
Nombre y Apellido	**C, Pablo**
Cargo / Función	**Supervisor de Cosecha**
¿Cuáles son las etapas del proceso de cosecha?	
Las etapas del proceso de cosecha comienzan con el apeo, donde se cortan los árboles utilizando distintos mecanismos, cada uno de ellos dependerá de las características del lote. Se busca dirigir la caída de los árboles en un mismo sentido, a fin de permitir una rápida extracción y reducir el posterior tránsito de maquinaria sobre el lote. La altura del tocón deberá ser la menor posible, de acuerdo a las características del terreno, las máquinas y el árbol. Continúa con el desrame donde se busca quitar las ramas de los árboles que fueron cortados, buscando dejar el tronco lo más limpio posible. Posteriormente se procede con la extracción a borde de camino o a un punto específico que se determina según las particularidades del lote. La extracción se realiza con maquinaria y requiere de ciertos cuidados para no dañar la masa forestal remanente y conseguir la mayor productividad posible en el proceso. Luego se realiza la medición y clasificación de los troncos, esta tarea es muy importante dado que se definen las clases de productos que saldrán del bosque, por tanto, es necesario procurar la máxima utilización del fuste y respectar las clases indicadas por el Supervisor. Por último, la carga en el camión para el traslado.	

6.5. ANEXO 5: ENTREVISTA GERENTE DE TECNOLOGÍA

Entrevista	**SIS01**
Nombre y Apellido	**P, Martín**
Cargo / Función	**Gerente de Tecnología**
¿La dirección invierte en tecnología y en seguridad?	
Analizando los últimos 4 años, podemos identificar que cada vez se dedican más recursos financieros al área de sistemas. En lo que respecta a Infraestructura y Seguridad, las inversiones están únicamente asociada a la adquisición de equipamiento y software, no se aprobaron recursos para gestionar la seguridad de la información.	

A partir del corriente año, tras el cambio de CEO del grupo, se dedicó una partida presupuestaria para comenzar a alinear los procesos del negocio con la norma internacional ISO 27001. Espero que éste sea el punto de partida para comenzar a gestionar adecuadamente los activos de la información.

6.6. ANEXO 6: CUMPLIMIENTO DE CONTROLES DE SEGURIDAD

Con el fin de identificar el estado actual de la seguridad de la información se analizan los 114 controles establecidos por la norma ISO/IEC 27002:2013. Dependiendo del estado de cada uno, se los clasifica según el modelo de capacidad de madurez para cuantificar el cumplimiento de los mismos.

CODIGO	METRIC	CAPITULO	MADURACIÓN	VALOR
5.1.1	5.1.1 - Existencia de políticas de SI	Políticas de seguridad de la información	**0 - Inexistente**	**0%**
5.1.2	5.1.2 - Revisión de las políticas de SI	Políticas de seguridad de la información	**0 - Inexistente**	**0%**
6.1.1	6.1.1 - Roles y responsabilidades de la SI	Organización de la seguridad de la información	**1 - Inicial**	**5%**
6.1.2	6.1.2 - Segregación de funciones	Organización de la seguridad de la información	**1 - Inicial**	**5%**
6.1.3	6.1.3 - Contacto con las autoridades	Organización de la seguridad de la información	**1 - Inicial**	**5%**
6.1.4	6.1.4 - Contacto con grupos de interés especial	Organización de la seguridad de la información	**1 - Inicial**	**5%**
6.1.5	6.1.5 - SI en la gestión de proyectos	Organización de la seguridad de la información	**0 - Inexistente**	**0%**
6.2.1	6.2.1 - Política de uso de dispositivos móviles	Organización de la seguridad de la información	**0 - Inexistente**	**0%**
6.2.2	6.2.2 - Teletrabajo	Organización de la seguridad de la información	**1 - Inicial**	**5%**

CODIGO	METRIC	CAPITULO	MADURACIÓN	VALOR	APLICA
7.1.1	7.1.1 - Investigación de antecedentes	Seguridad relativa a los recursos humanos	2 - Gestionado	15%	1
7.1.2	7.1.2 - Términos y condiciones de empleo	Seguridad relativa a los recursos humanos	2 - Gestionado	15%	1
7.2.1	7.2.1 - Responsabilidades de la dirección	Seguridad relativa a los recursos humanos	0 - Inexistente	0%	1
7.2.2	7.2.2 - Concientización, educación y capacitación en SI	Seguridad relativa a los recursos humanos	0 - Inexistente	0%	1
7.2.3	7.2.3 - Proceso disciplinario	Seguridad relativa a los recursos humanos	0 - Inexistente	0%	1
7.3.1	7.3.1 - Responsabilidades en desvinculación o cambio de puesto	Seguridad relativa a los recursos humanos	0 - Inexistente	0%	1
8.1.1	8.1.1 - Inventario de activos	Gestión de activos	2 - Gestionado	15%	1
8.1.2	8.1.2 - Propiedad de los activos	Gestión de activos	2 - Gestionado	15%	1
8.1.3	8.1.3 - Uso aceptable de los activos	Gestión de activos	0 - Inexistente	0%	1
8.1.4	8.1.4 - Retorno de los activos	Gestión de activos	1 - Inicial	5%	1
8.2.1	8.2.1 - Clasificación de la información	Gestión de activos	1 - Inicial	5%	1
8.2.2	8.2.2 - Rotulado / etiquetado de la información	Gestión de activos	0 - Inexistente	0%	1
8.2.3	8.2.3 - Manipulación de activos	Gestión de activos	0 - Inexistente	0%	1
8.3.1	8.3.1 - Gestión de medios extraíbles	Gestión de activos	0 - Inexistente	0%	1
8.3.2	8.3.2 - Disposición final de medios	Gestión de activos	1 - Inicial	5%	1
8.3.3	8.3.3 - Traslado de medios físicos	Gestión de activos	2 - Gestionado	15%	1
9.1.1	9.1.1 - Política de control de accesos	Control de acceso	1 - Inicial	5%	1
9.1.2	9.1.2 - Acceso a las redes y servicios asociados	Control de acceso	2 - Gestionado	15%	1
9.2.1	9.2.1 - Alta y baja de registros de usuario	Control de acceso	1 - Inicial	5%	1
9.2.2	9.2.2 - Asignación de accesos del usuario	Control de acceso	2 - Gestionado	15%	1

CODIGO	METRIC	CAPITULO	MADURACIÓN	VALOR
9.2.3	9.2.3 - Gestión de los derechos de acceso con privilegios	Control de acceso	**2 - Gestionado**	**15%**
9.2.4	9.2.4 - Gestión de información secreta para autenticación del usuario	Control de acceso	**0 - Inexistente**	**0%**
9.2.5	9.2.5 - Revisión de los derechos de acceso del usuario	Control de acceso	**1 - Inicial**	**5%**
9.2.6	9.2.6 - Remoción o ajuste de los derechos de acceso	Control de acceso	**2 - Gestionado**	**15%**
9.3.1	9.3.1 - Uso de la información secreta de autenticación	Control de acceso	**1 - Inicial**	**5%**
9.4.1	9.4.1 - Restricción del acceso a la información	Control de acceso	**2 - Gestionado**	**15%**
9.4.2	9.4.2 - Procedimientos seguros de inicio de sesión	Control de acceso	**2 - Gestionado**	**15%**
9.4.3	9.4.3 - Sistema de gestión de contraseñas	Control de acceso	**2 - Gestionado**	**15%**
9.4.4	9.4.4 - Uso de herramientas de administración de sistemas	Control de acceso	**1 - Inicial**	**5%**
9.4.5	9.4.5 - Control de acceso al código fuente de los programas	Control de acceso	**2 - Gestionado**	**15%**
10.1.1	10.1.1 - Política de uso de los controles criptográficos	Criptografía	**0 - Inexistente**	**0%**
10.1.2	10.1.2 - Gestión de claves	Criptografía	**0 - Inexistente**	**0%**
11.1.1	11.1.1 - Perímetro de seguridad física	Seguridad Física y del Entorno	**3 - Definido**	**60%**
11.1.2	11.1.2 - Controles de ingreso físico	Seguridad Física y del Entorno	**3 - Definido**	**60%**
11.1.3	11.1.3 - Aseguramiento de oficinas, recintos e instalaciones	Seguridad Física y del Entorno	**3 - Definido**	**60%**
11.1.4	11.1.4 - Protección contra amenazas externas y del entorno	Seguridad Física y del Entorno	**2 - Gestionado**	**15%**
11.1.5	11.1.5 - Trabajo en áreas seguras	Seguridad Física y del Entorno	**2 - Gestionado**	**15%**
11.1.16	11.1.6 - Áreas de carga y descarga	Seguridad Física y del Entorno	**3 - Definido**	**60%**
11.2.1	11.2.1 - Ubicación y protección del equipamiento	Seguridad Física y del Entorno	**3 - Definido**	**60%**

CODIGO	METRIC	CAPITULO	MADURACIÓN	VALOR
11.2.2	11.2.2 - Elementos de soporte	Seguridad Física y del Entorno	**3 - Definido**	**60%**
11.2.3	11.2.3 - Seguridad del cableado	Seguridad Física y del Entorno	**1 - Inicial**	**5%**
11.2.4	11.2.4 - Mantenimiento del equipamiento	Seguridad Física y del Entorno	**3 - Definido**	**60%**
11.2.5	11.2.5 - Retiro de activos	Seguridad Física y del Entorno	**2 - Gestionado**	**15%**
11.2.6	11.2.6 - Seguridad de equipamiento y activos fuera de las instalaciones	Seguridad Física y del Entorno	**1 - Inicial**	**5%**
11.2.7	11.2.7 - Disposición final segura o reúso del equipamiento	Seguridad Física y del Entorno	**2 - Gestionado**	**15%**
11.2.8	11.2.8 - Equipamiento desatendido de usuario	Seguridad Física y del Entorno	**1 - Inicial**	**5%**
11.2.9	11.2.9 - Política de escritorio y de pantalla limpios	Seguridad Física y del Entorno	**0 - Inexistente**	**0%**
12.1.1	12.1.1 - Procedimientos operativos documentados	Seguridad de las Operaciones	**0 - Inexistente**	**0%**
12.1.2	12.1.2 - Gestión del cambio	Seguridad de las Operaciones	**1 - Inicial**	**5%**
12.1.3	12.1.3 - Gestión de la capacidad	Seguridad de las Operaciones	**2 - Gestionado**	**15%**
12.1.4	12.1.4 - Separación de entornos de desarrollo, prueba y producción	Seguridad de las Operaciones	**2 - Gestionado**	**15%**
12.2.1	12.2.1 - Controles contra el código malicioso	Seguridad de las Operaciones	**2 - Gestionado**	**15%**
12.3.1	12.3.1 - Resguardo de la información	Seguridad de las Operaciones	**2 - Gestionado**	**15%**
12.4.1	12.4.1 - Registro de eventos	Seguridad de las Operaciones	**1 - Inicial**	**5%**
12.4.2	12.4.2 - Protección de la información de registros	Seguridad de las Operaciones	**2 - Gestionado**	**15%**
12.4.3	12.4.3 - Registros de administradores y operadores	Seguridad de las Operaciones	**1 - Inicial**	**5%**
12.4.4	12.4.4 - Sincronización de los relojes	Seguridad de las Operaciones	**3 - Definido**	**60%**
12.5.1	12.5.1 - Instalación de software en sistemas de producción	Seguridad de las Operaciones	**2 - Gestionado**	**15%**

CODIGO	METRIC	CAPITULO	MADURACIÓN	VALOR
12.6.1	12.6.1 - Gestión de vulnerabilidades técnicas	Seguridad de las Operaciones	2 - Gestionado	15%
12.6.2	12.6.2 - Restricciones a la instalación de software	Seguridad de las Operaciones	1 - Inicial	5%
12.7.1	12.7.1 - Controles de auditoría de sistemas	Seguridad de las Operaciones	1 - Inicial	5%
13.1.1	13.1.1 - Controles de red	Seguridad de las Comunicaciones	3 - Definido	60%
13.1.2	13.1.2 - Seguridad de los servicios de red	Seguridad de las Comunicaciones	1 - Inicial	5%
13.1.3	13.1.3 - Segregación en redes	Seguridad de las Comunicaciones	3 - Definido	60%
13.2.1	13.2.1 - Políticas y procedimientos de transferencia de información	Seguridad de las Comunicaciones	0 - Inexistente	0%
13.2.2	13.2.2 - Acuerdos de transferencia de información	Seguridad de las Comunicaciones	1 - Inicial	5%
13.2.3	13.2.3 - Mensajería electrónica	Seguridad de las Comunicaciones	2 - Gestionado	15%
13.2.4	13.2.4 - Acuerdos de confidencialidad	Seguridad de las Comunicaciones	0 - Inexistente	0%
14.1.1	14.1.1 - Análisis y especificación de requisitos de seguridad	Adquisición, Desarrollo y Mantenimiento de Sistemas	2 - Gestionado	15%
14.1.2	14.1.2 - Asegurar servicios de aplicaciones en redes públicas	Adquisición, Desarrollo y Mantenimiento de Sistemas	2 - Gestionado	15%
14.1.3	14.1.3 - Protección de las transacciones en servicios de aplicaciones	Adquisición, Desarrollo y Mantenimiento de Sistemas	3 - Definido	60%
14.2.1	14.2.1 - Política de desarrollo seguro	Adquisición, Desarrollo y Mantenimiento de Sistemas	1 - Inicial	5%
14.2.2	14.2.2 - Procedimientos de control de cambios en sistemas	Adquisición, Desarrollo y Mantenimiento de Sistemas	1 - Inicial	5%
14.2.3	14.2.3 - Revisión técnica de aplicaciones luego de cambios en producción	Adquisición, Desarrollo y Mantenimiento de Sistemas	2 - Gestionado	15%
14.2.4	14.2.4 - Restricciones a cambios en paquetes de software	Adquisición, Desarrollo y Mantenimiento de Sistemas	1 - Inicial	5%
14.2.5	14.2.5 - Principios de seguridad aplicados a ingeniería en sistemas	Adquisición, Desarrollo y Mantenimiento de Sistemas	1 - Inicial	5%
14.2.6	14.2.6 - Entornos seguros de desarrollo	Adquisición, Desarrollo y Mantenimiento de Sistemas	2 - Gestionado	15%

CODIGO	METRIC	CAPITULO	MADURACIÓN	VALOR
14.2.7	14.2.7 - Desarrollo de terceras partes	Adquisición, Desarrollo y Mantenimiento de Sistemas	2 - Gestionado	15%
14.2.8	14.2.8 - Pruebas de seguridad de los sistemas	Adquisición, Desarrollo y Mantenimiento de Sistemas	2 - Gestionado	15%
14.2.9	14.2.9 - Pruebas de aceptación de sistemas	Adquisición, Desarrollo y Mantenimiento de Sistemas	1 - Inicial	5%
14.3.1	14.3.1 - Protección de datos de pruebas	Adquisición, Desarrollo y Mantenimiento de Sistemas	2 - Gestionado	15%
15.1.1	15.1.1 - Política de SI para relación con proveedores	Relaciones con los Proveedores	2 - Gestionado	15%
15.1.2	15.1.2 - Tratamiento de la SI en acuerdos con proveedores	Relaciones con los Proveedores	2 - Gestionado	15%
15.1.3	15.1.3 - Cadena de suministro en TI y comunicaciones	Relaciones con los Proveedores	1 - Inicial	5%
15.2.1	15.2.1 - Seguimiento y revisión en servicios de proveedores	Relaciones con los Proveedores	2 - Gestionado	15%
15.2.2	15.2.2 - Gestión de cambios en servicios de proveedores	Relaciones con los Proveedores	0 - Inexistente	0%
16.1.1	16.1.1 - Responsabilidades y procedimientos	Gestión de incidentes de seguridad de la información	0 - Inexistente	0%
16.1.2	16.1.2 - Reporte de eventos de SI	Gestión de incidentes de seguridad de la información	1 - Inicial	5%
16.1.3	16.1.3 - Reporte de debilidades de SI	Gestión de incidentes de seguridad de la información	1 - Inicial	5%
16.1.4	16.1.4 - Evaluación y decisión sobre eventos de SI	Gestión de incidentes de seguridad de la información	1 - Inicial	5%
16.1.5	16.1.5 - Respuesta a incidentes de SI	Gestión de incidentes de seguridad de la información	0 - Inexistente	0%
16.1.6	16.1.6 - Aprendizaje de los incidentes de SI	Gestión de incidentes de seguridad de la información	1 - Inicial	5%
16.1.7	16.1.7 - Recolección de evidencias	Gestión de incidentes de seguridad de la información	1 - Inicial	5%
17.1.1	17.1.1 - Planificación de la continuidad de la SI	Aspectos de SI en la Gestión de Continuidad del Negocio	1 - Inicial	5%
17.1.2	17.1.2 - Implementación de la continuidad de la SI	Aspectos de SI en la Gestión de Continuidad del Negocio	1 - Inicial	5%
17.1.3	17.1.3 - Verificación, revisión y evaluación de la continuidad de la SI	Aspectos de SI en la Gestión de Continuidad del Negocio	0 - Inexistente	0%

CODIGO	METRIC	CAPITULO	MADURACIÓN	VALOR
17.2.1	17.2.1 - Disponibilidad de las instalaciones	Aspectos de SI en la Gestión de Continuidad del Negocio	1 - Inicial	5%
18.1.1	18.1.1 - Identificación de la legislación aplicable	Cumplimiento	1 - Inicial	5%
18.1.2	18.1.2 - Derechos de propiedad intelectual	Cumplimiento	1 - Inicial	5%
18.1.3	18.1.3 - Protección de los registros de información	Cumplimiento	2 - Gestionado	15%
18.1.4	18.1.4 - Privacidad y protección de información personal	Cumplimiento	1 - Inicial	5%
18.1.5	18.1.5 - Regulación de los controles criptográficos	Cumplimiento	0 - Inexistente	0%
18.2.1	18.2.1 - Revisión independiente de la SI	Cumplimiento	0 - Inexistente	0%
18.2.2	18.2.2 - Cumplimiento de políticas y normas de SI	Cumplimiento	0 - Inexistente	0%
18.2.3	18.2.3 - Revisión de cumplimiento técnico	Cumplimiento	0 - Inexistente	0%

6.7. ANEXO 7: CURRICULUM VITAE

Ing. Martín Pires

Gerente de Tecnología (CTO) en Grupo Insud

EXTRACTO

Ingeniero en Sistemas Informáticos, con vasta experiencia en el área de sistemas, trabajando con diferentes tecnologías y liderando equipos de trabajo. Cuento con sólidos conocimientos de análisis de sistemas y procesos. Mis mayores fortalezas son la gestión de recursos humanos, el análisis de problemas y diagnóstico de situaciones. Poseo alto grado de compromiso con los objetivos a cumplir y estoy fuertemente orientado al trabajo en equipo. Cuento con una actitud positiva y buena predisposición al trabajo, obteniendo así resultados corporativos con alta satisfacción del cliente.

EXPERIENCIA

Grupo Insud - 9 años 7 meses

Gerente de Tecnología (CTO) - junio de 2019 - Presente

Responsable de gestionar el área de IT en 8 sitios distribuidos por Argentina, Uruguay y Paraguay.

Principales funciones: Planificar, diseñar y monitorear la estrategia tecnológica. Planificar, supervisar y evaluar el alineamiento tecnológico con los procesos corporativos. Evaluar y proponer la adecuada infraestructura IT para atender las necesidades de las empresas del grupo. Analizar y proponer mejoras tecnológicas. Definir políticas y normas de seguridad de la información. Mantener las medidas necesarias para la continuidad del negocio.

Gestionar al equipo de IT para garantizar el cumplimiento de los SLA's del área.

Jefe de Infraestructura Corporativo - marzo de 2013 - junio de 2019 (6 años 4 meses)

Principales funciones:

Liderar al equipo humano del área.

Análisis y aprobación de arquitecturas de IT y softwares. Coordinación de proyectos de IT acuerdo a requerimientos, plazos y presupuestos asignados (diseño de nuevo centro de datos en industrias Farmacéuticas, energía renovable, etc) Garantizar que la Infraestructura que soporta los servicios de la compañía se encuentre en óptimas condiciones de funcionamiento. Definir políticas, normas y procedimientos para garantizar el correcto funcionamiento del área. Gestionar el servicio de operaciones de TI, asegurando el cumplimiento de los niveles de servicios. Identificar puntos débiles y posibles conflictos en el funcionamiento del área. Asegurar el correcto funcionamiento de los procesos.

Responsable de Servidores - enero de 2010 - marzo de 2013 (3 años 3 meses)

Garantizar la continuidad y la gestión operativa de los recursos de IT, garantizando un nivel de servicio y calidad a los usuarios. Proporcionar recomendaciones de actualizaciones de sistemas, productos de proveedores y mejoras en el sistema. Crear indicadores de rendimiento y gestionar las acciones correctivas y preventivas. Validar nuevos programas y supervisar su puesta en práctica: programar y llevar a cabo los cambios de versión del software. Monitorear la infraestructura y sistemas para asegurar la disponibilidad a todos los usuarios. Manejo de eventos (diagnóstico, intervención, alertas).

Ministerio de Desarrollo Social de la Nación - 6 años 9 meses

Responsable de Sistemas - enero de 2004 - diciembre de 2009 (6 años)

Liderar al equipo humano del área. Definir políticas, normas y procedimientos para garantizar el correcto funcionamiento del área. Coordinar proyectos de IT. Contacto con los proveedores de software, hardware y servicios. Monitoreo de servicios en búsqueda de vulnerabilidades.

Administrador de Sistemas - abril de 2003 - diciembre de 2004 (1 año 9 meses)

Diseño y Desarrollo de Sistemas. Administración de Bases de Datos. Configuración y Mantenimiento de Servidores.

EDUCACIÓN

UADE Maestría, Dirección estratégica de la información (2018 - 2019)

Universidad Abierta Interamericana Ingeniero en Sistema Informáticos, Tecnología · (2007 - 2015).

LinkedIn https://www.linkedin.com/in/martín-pires-43b71816