Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013

Empresa de Digital Signage LRD XXX

Diana Marcela Pulecio Lara

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Área: Sistemas de Gestión de la Seguridad de la Información

Director: Antonio José Segovia Henares

Centro: Universidad Oberta de Catalunya

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013*
Nombre del autor:	*Diana Marcela Pulecio Lara*
Nombre del director TFM:	*Antonio José Segovia*
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Idioma del trabajo:	*Castellano*

Tabla de Contenido

ILUSTRACIONES

TABLAS

Anexos

TFM Anexo1 Políticas de Seguridad

TFM Anexo2 Auditoria Interna

TFM Anexo3 Gestión de Indicadores

TFM Anexo4 Procedimiento Revisión por Dirección

TFM Anexo5 Procedimiento Roles y responsabilidades

TFM Anexo6 Metodología Análisis de Riesgo

TFM Anexo7 Declaración de Aplicabilidad

TFM_Anexo8_InventariodeActivos.pdf

TFM_Anexo9_REsumenTablaValorActivos.excel

TFM_Anexo10_Activos.xls

TFM_ANEXO11_Proyecto_Politica_deSeguridad.pdf

TFM_ANEXO12_COB.pdf

TFM_ANEXO13Software.pdf

Grafico.xls

TFM_Programa Anual de Auditoria.xls

1 INTRODUCCIÓN

En este proyecto se realiza un análisis del estado actual de la seguridad de la información en Digital Signage LRDXXX esta es una empresa dedicada a la publicidad de contenidos y su principal cliente son entidades financieras. La compañía debe asegurar la publicación diaria e información actualizada de indicadores financiero como tasas de interés, comisiones o recargos de servicios, etc. conforme a las normas legales establecidas en la superintendencia.

Con la implementación del plan director de seguridad se pretende optimizar procesos, minimizar riesgos a implementaciones y evitar inversiones innecesarias. Se analizará la información existente y se recolectará información por medio de entrevistas, visitas a las diferentes áreas documentando y evaluando el nivel existente de la compañía teniendo en cuenta documentación de controles, procesos y procedimientos. Se realizará una evaluación de cada uno de los controles y se compartirá la información evaluada con la alta gerencia.

Se identificará los principales stakeholders, tiempos de inicio, planeación, para iniciar el plan de director de SGSI, la alta gerencia aprobará el plan de director con un estimado de 3 años para implementar el mismo adquiriendo la certificación ISO.

Lineamiento.

El Plan Director de Seguridad es uno de los elementos clave con que debe trabajar el Responsable de Seguridad de una organización. Este plan constituye la hoja de ruta que debe seguir la empresa para gestionar de una forma adecuada la seguridad, permitiendo no sólo conocer el estado de la misma, sino en qué líneas se debe actuar para mejorarla. Estamos hablando por tanto de un modelo de mejora continua PDCA (Plan-Do-Check-Act).

El marco legal ha reflejado la importancia de la seguridad de la información (a nivel del estado español, leyes como la 11/2007 artículo 42: “Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad”, lo demuestran). La seguridad no es por tanto un aspecto opcional, sino que debe ser inherente a las actividades de la propia empresa, y constituye un punto de partida ineludible para toda organización en la actualidad.

El planteamiento del proyecto será, por tanto, sentar las bases de un Plan de Director de Seguridad para la empresa. Simplificando, y como iremos viendo, nuestro proceso será el siguiente:

- Analizar y detallar nuestro inventario de activos.
- Estudiar las amenazas a las que están expuestos.
- Estudiar el impacto potencial de dichas amenazas.
- Proponer un plan de acción para luchar contra dichas amenazas.

Evaluar el impacto residual una vez aplicado el plan de acción

2 ISO/IEC 27001 E ISO/IEC 27002

LA ISO27001 es una norma internacional enfocada para la gestión de seguridad de la información que cumple cualquier todo tipo organización. Esta especifica los requisitos para: establecer, implementar, supervisar y mejorar el Sistema de seguridad información.

Se utiliza el modelo PDCA para la gestión de información e identificando riesgos y necesidades de mejora ISO / IEC 27001 se deriva de BS 7799 Parte 2, publicada por primera vez por el British Standards Institute en 1999.

BS 7799 Parte 2 fue revisada en 2002, incorporando explícitamente el ciclo Plan-Do-Check-Act también conocido como circulo Deming.

BS 7799 parte 2 fue adoptada como ISO / IEC 27001 en 2005 con varios cambios para reflejar a sus nuevos custodios.

ISO / IEC 27001: 2005 se revisó exhaustivamente en 2013, lo que concuerda con los otros estándares de sistemas de gestión ISO y eliminó la referencia explícita a PDCA

ISO/IEC270013: Primera revisión de la ISO 27001:2005. Presenta homogeneidad de estructura y mayor libertad y flexibilidad de implementación. Protege la confidencialidad, integridad y disponibilidad de la información evaluando y mitigando cada uno de los riesgos

2.1 DIFERENCIAS

la ISO 27001 es el standard en la cual una compañía obtiene esta certificación. En este estándar la compañía indica los requerimientos que necesita seguir para certificarse. De esta forma estableciendo el marco de trabajo para definir un SGSI, centrándose en la seguridad de información como un proceso continuo en el tiempo.

La ISO 27002 consiste en una guía de buenas prácticas que permiten a las organizaciones mejorar la seguridad de su información. define 133 objetivos de control y gestión que ayudarán a la organización a implantar medidas que reduzcan sus riesgos en cuanto a seguridad de la información. http://www.iso27000.es/faqs.html

2.2 VENTAJAS

Una de la Ventajas de la ISO 27001 son:

Establece un marco de gestión de la seguridad consistente e internacionalmente reconocido.

Garantizan los controles internos, los controles de continuidad de la actividad de negocio.

Cumplimiento de leyes y normativas que se apliquen a la organización.

Promueve la confianza a los clientes y la relación con terceros ofreciendo seguridad en la información.

Reduce los riesgos en la seguridad de la información.

Compromete a la directiva todo el sistema de gestión con la seguridad de la información.

Evita inversiones innecesarias por la ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio, etc.

Fuente: https://advisera.com/27001academy/es/knowledgebase/la-logica-basica-de-iso-27001como-funciona-la-seguridad-de-la-informacion/

Figure 1. ISO 27001 Framework

3 EMPRESA: DIGITAL SIGNAGE LRDXXX

3.1 CONTEXTO:

La empresa **Digital Signage LRDXXX** fundada en 2011, ubicada en Bogotá, Colombia, es reconocida en el uso de contenidos emitidos a través de diferentes pantallas outdoor o indoor. Cumpliendo con lo dispuesto en la ley estatutaria 1581 de 2012 y a su decreto reglamentario 1377 de 2013 del ministerio de Comercio, Industria y Turismo decreto 1074 del 2015, cumplimiento de manejo de datos.

La empresa presta el servicio de diseño de publicidad, alquiler, compra, implementación de la solución, asesoría y soporte de las pantallas como son Marketing Walls e Interactive wall, aplicando un role de atraer a clientes a los diferentes productos que se ofrecen en un establecimiento y de esta forma interactuando con esta tecnología, presentando el producto en un formato interactivo las (24) horas al día (7) días a la semana fomentando al cliente la compra del producto.

El gran reto de la compañía es implementar soluciones a diferentes bancos a través de internet sin que la data sensitiva como un indicador financiero, comisiones e intereses sea alterado durante la transmisión siendo un dispositivo seguro y de esta forma mejorando el servicio y la capacidad operativa.

3.2 MISIÓN

Digital Signage LRDXXX permite ahorrar costos para llegar el mensaje al cliente de una forma diferente y efectiva en la reutilización de publicidad digital, información financiera, indicadores de cambio de moneda como la TRM (tasa representativa del Mercado) en bancos, comisiones, cargos en servicios, portafolio de servicios, Bolsa de valores y establecimientos de casas de cambio de moneda.

3.3 VISIÓN

Proporcionar en tiempo real la publicación de información precisa acerca de eventos, cambios de TRM, emergencia, anuncios, etc. utilizando tecnología a la conservación del medio ambiente, innovando y optimizando los recursos en la implementación de la digital signage.

4 ANÁLISIS DE LA SITUACIÓN ACTUAL

Digital Media es la forma práctica de comunicar, publicar información comercial a nuestros clientes. Esta empresa presta servicios de publicidad a entidades financieras teniendo como norma obligatoria a los bancos la publicación de tasas de interés, rentabilidad, comisiones y otros indicadores que por medio de las pantallas digitales rentadas o compradas cumplen esta norma. Velando por la instalación y transmisión de contenidos sean seguros.

La empresa Digital Signage LRDXXX está conformada por 75 trabajadores y se encuentra ubicado en el Down Town de Bogotá Torre Hill (Colombia).

Su distribución es:

- 15 técnicos en montaje de estructura y cableado
- 15 ingenieros de Sistema encargados de las bases de datos, administración de servidores, monitoreo y Project managers.
- 15 especialistas en mercadeo y publicidad
- 1 Contador
- 2 abogados encargado de validar con la alcaldía para tener la licencia de publicidad y no acarrear con contaminación visual del sector
- 2 financieros
- 8 personas del call center o soporte. 4 persona fuerza de ventas ,4 arquitectos.
- 2 personas encargadas de bodega y control de activos. 2 personas de Recursos humanos
- 5 directores.
    - Un director dedicado a velar por la seguridad de la información e implementación de tecnología e innovación segura.
    - Un director encargado a las políticas RGPD y publicidad.
    - Un director de finanzas encargados de fomentar las políticas y buenas prácticas en la empresa.
    - Un director de Ventas.

4.1 ESTRUCTURA JERÁRQUICA

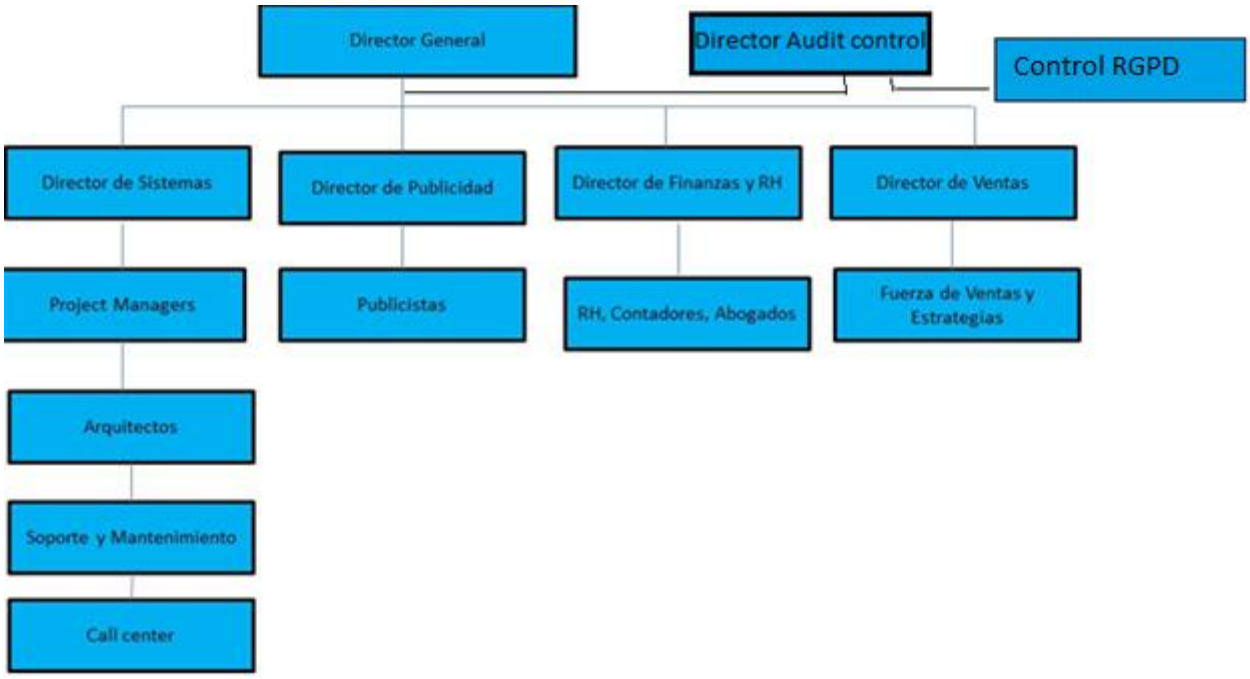

Figure 2..Estructura Jerárquica

La compañía tiene la siguiente solución tecnológica:

- Rack de comunicaciones.
- Players.
- Pantallas.
- Sistema de ventilación.
- Soportes y anclajes para las pantallas
- Energía- UPS cada pantalla consume en promedio 1.08 Amperios o 130 W.
- Sensores de Intrusión
- x1 Prod Server & x40 Prod Client (with no CoB platform)
- x1 UAT Server & x1 UAT Client – Testing Platform
- Licence Server & Client software
- Backend SQL Server databases (Prod & UAT)
- 50 GB storage for each server
- Backup en Disco

4.1.1 POLÍTICAS DE EMPRESA

La empresa no cuenta con ninguna política de divulgación de buenas prácticas de seguridad y de controles de restricción para la fuga de información. Encontrando fuga de información a la competencia e impactando a los clientes. Adicionalmente, se ha encontrado problemas en la implementación de pantallas ocasionando accidentes a nuestros clientes y al personal propio de la empresa.

5 *ALCANCE*

La realización de este proyecto de sistema de gestión de seguridad cubre: Servicios técnicos, software, Hardware y servicios profesionales hacia los clientes internos y externos para procesar la información según los requerimientos.

6 OBJETIVOS

6.1 OBJETIVOS GENERALES

Implementación y certificación de un SGSI conforme al standard ISO27001 y el seguimiento del código de buenas prácticas de la ISO 27002, utilizando la Metodología de Análisis y Gestión de Riesgos MAGERIT para la compañía Digital Signage LRDXXX de los siguientes servicios:

- Desarrollo o edición de video e implementación ilimitada de contenidos como: noticias de ultimas hora, clima e indicadores económicos, restricción vehicular por ciudades, indicadores financieros con actualizaciones diarias, semanales y mensuales de acuerdo con las necesidades del cliente.

6.2 OBJETIVOS ESPECÍFICOS

Aplicando las buenas prácticas de la ISO/ IEC 27002:2013. 14 dominios, 35 Objetivos de control y 114 controles que se tendrán en cuenta en los siguientes objetivos específicos:

- Analizar el estado actual de la compañía en relación al SGSI.
- Definir la metodología de identificación de inventario de activos y su gestión conforme al tratamiento de riesgo con el fin de proteger la inversión.
- Especificar la segregación de roles y responsabilidades contemplado en la metodología de riesgo reduciendo el riesgo empresarial y legal.
- Reconocer al responsable de la seguridad de la información.
- Mantener la Gestión de soporte de almacenamiento (políticas de mantenimiento de información, eliminación y actualización). Para Salvaguardar la confidencialidad e integridad de la información contenida en estos sistemas.
- Definir e identificar las políticas de seguridad de la información que aplican a la organización y procesos de control de riesgo para controles criptográficos, seguridad Física, ambiental, Seguridad en la operativa, Protección de antivirus, retención de backups , licencias y contratos . De esta forma protegiendo el buen nombre de la compañía e incrementando la satisfacción de los clientes.

7 GAP ANÁLISIS

En esta fase identificaremos los puntos débiles del sistema con el propósito de diseñar un sistema certificable, de esta forma aprovechando los procedimientos de gestión existente, Se revisa el nivel de madurez de acuerdo al estándar ISO/IEC27001:2013 y a las buenas prácticas de la ISO/ IEC 27002:2013. 14 dominios, 35 Objetivos de control y 114 Controles.

Se recolecta la evidencia por medio de entrevistas, visitas a las diferentes área e inspección de procesos críticos, documentación conforme a estos controles de aplicabilidad:

A.5 Políticas de Seguridad de la información

A.6 Organización de la seguridad

A.7 Seguridad relativa a los recursos humanos

A.8 Gestión de Activos

A.9 Control de acceso

A.10 Criptografía

A.11 Seguridad Física y del entorno

A.12 Seguridad de las operaciones

A.13 Seguridad de las Comunicaciones

A.14 Adquisición, desarrollo y mantenimiento de sistemas de información

A.15 Relación con proveedores

A.16 Gestión de incidentes de seguridad de la información

A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio A.18 Cumplimiento

7.1 CRITERIOS DE EVALUACIÓN

Se determina el grado de cumplimiento la cual podemos medir y reportar a la alta gerencia utilizando un esquema que consiste del Nivel 0 a Nivel 5 donde "0 "es inexistente y "5 "es el nivel optimizado.

Nivel	Descripción	Rango porcentual "ISSN:2011-0065"
Nivel 0	**Inexistente**, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.	(0-10) %
Nivel1	**Inicial**, No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva.	(10-40)%
Nivel2	**Repetible**, se ha elaborado el plan concreto de implementación. No hay formación ni comunicación formal sobre los procedimientos	(40-60) %
	y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.	

Nivel3	**Efectivo**, Se ha comenzado a aplicar, pero de forma parcial, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.	(60-75)%
Nivel4	**Gestionado**, implementado, pero no se han realizado aun pruebas de revisión y mejora	(75-90)%
Nivel5	**Optimizado**, implementado y con procesos de medición, revisión y mejora llevados a cabo con regularidad	(90-100)%

Table 1 Criterios de Evaluación

- Se realiza visitas a las diferentes áreas de alta gerencia y PM (Project Managers) y se plasma la siguiente tabla al cumplimiento ISO 27001.

	Valoración	
4.0 Contexto de la Organización	25%	Inicial
5.0 Liderazgo	9%	Inexistente
6.0 Planificación	15%	Inicial
7.0 Soporte	32%	Inicial
8.0 Operación	45%	Repetible
9.0 Evaluación del desempeño	0%	Inexistente
10. Mejora	0%	Inexistente
PROMEDIO	18%	Inicial

Table 2 Valoración de la compañía

El promedio de madurez de la empresa es el 18% encontrándose en etapa INICIAL

7.1.1.1 Evaluación de Controles

- Se recolecta información de procesos, procedimientos y se compara con las buenas prácticas de implementación al producto y se registra el siguiente análisis.

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**

A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	40	70	**INICIAL**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	35	70	**INICIAL**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	34	70	**INICIAL**
A.8	GESTIÓN DE ACTIVOS	34	70	**INICIAL**
A.9	CONTROL DE ACCESO	33	70	**INICIAL**
A.10	CRIPTOGRAFÍA	30	70	**INICIAL**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	31	70	**INICIAL**
A.12	SEGURIDAD DE LAS OPERACIONES	34	70	**INICIAL**
A.13	SEGURIDAD DE LAS COMUNICACIONES	34	70	**INICIAL**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	33	70	**INICIAL**
A.15	RELACIONES CON LOS PROVEEDORES	30	70	**INICIAL**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	34	70	**INICIAL**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	27	70	**INICIAL**
A.18	CUMPLIMIENTO	32.5	70	**INICIAL**
PROMEDIO EVALUACIÓN DE CONTROLES		**33**	**70**	**INICIAL**

Table 3. Evaluación de Controles

Figure 3. Evaluación de Controles

A continuación, se detalla cada una de estas encontrándose falencias como:

5. **Políticas de seguridad:**
   - Se encuentra que algunas políticas y procedimientos no son claras y algunas son obsoletas para la empresa
   - No están digitalizadas
   - No se encuentran actualizadas y revisas por abogados
   - No son comunicadas y entendidas por los usuarios

6. **Organización de la seguridad**

   - No se tiene claro los roles de seguridad e implementación y cumplimiento de los mismos.
   - No hay políticas claras de medidas de seguridad

- No hay capacitación y no existe cultura de SGSI.

7. Seguridad relativa a los recursos humanos

- Se detecta mal uso de los dispositivos teniendo riesgo de robo de información.
- No hay control interno de las actividades del recurso y contratación acorde a la ética, antecedentes del personal.
- No hay políticas de roles y responsabilidad de la información y cumplimiento.

8. Gestión de Activos

- Se encontró que no existe un control de activos actualizado.
- No hay control de calidad cuando ingresa las pantallas a bodega
- No hay proceso de adquisición y abastecimiento clara y transparente

9. Control de acceso

- Se encuentra usuarios genéricos para la transmisión de contenidos
- No hay control sistematizado como un biométricos para identificar al personal y en la autenticación del sistema central

10. Criptografía

- Se detecta la falta de validación del mensaje que se envía.
- Ausencia de certificados en la transmisión de información

11. Seguridad Física y del entorno

- Falta Aire acondicionado y extintores en algunas zonas donde esta implementada la solución.
- Se detecta fallas en el anclaje del equipo
- El cuarto de control está expuesto al personal no autorizado

Seguridad de las operaciones

- No hay estadísticas de incidencias y estatus de tiempo de solución de las misma.
- Cambios controlados no existen.

12. Seguridad de las Comunicaciones

- Aunque existe una red controlada con ámbito protegido la cual es operada por personal propio. No hay políticas de VTMs o actualización de parches.
- No se están respetando las políticas de almacenamiento y retención de información.
- No hay control de acceso de uso masivo como son las redes sociales. (red no controlada).

13. **Adquisición, desarrollo y mantenimiento de sistemas de información** ➢ La alta gerencia no tiene documentado el TCO.
    - ➢ El ciclo de vida de desarrollo y mantenimiento no está definido.

14. **Relación con proveedores**
    - ➢ Se encuentra acceso no autorizado y manejo de información sensible de la empresa expuesta a proveedores sin cláusula de no divulgación de la misma.
    - ➢ No hay revisión de auditorías del proveedor para revisión del servicio.

15. **Gestión de incidentes de seguridad de la información.**
    - ➢ Se ha detectado afectación en la confidencialidad, integridad y disponibilidad de contenidos al cliente por falta de actualización de parches, antivirus, accesos no autorizados y lineamientos de implementación, etc.

16. **Aspectos de seguridad de la información para la gestión de la continuidad del negocio**
    - ➢ No hay procedimientos alternativos para escenarios de desastres, aunque se encuentra un Data Center alterno pero las versiones instaladas están desactualizadas.
    - ➢ No hay plan de contingencia actualizado y no se encuentra pruebas periódicas para garantizar la continuidad del negocio.

17. **Cumplimiento**
    - ➢ No existe métricas de impacto y análisis de riesgo.
    - ➢ No se evidencias soportes de auditoria interna.

La norma ISO/IEC 27001:2013 nos muestra la siguiente estructura alineada al ciclo de mejora continua.

Capitulo 4. Contexto de la Organización. En esta fase se hace un análisis identificando los problemas externos e internos de la compañía. Con el propósito de incluir las necesidades y acotar el alcance del SGSI.

Capitulo5. Liderazgo: Se define las responsabilidades y compromisos de la alta gerencia con relación al SGSI. Se establece políticas de seguridad de la información aplicadas a la compañía.

Capitulo6. Planeación: Identificación de los objetivos viables de seguridad e identificación de riesgos que afecta la confidencialidad, integridad y disponibilidad.

Capitulo7.Soporte: Se identifica los recursos físicos, lógicos, personas para la implementación del SGSI y asegurar los recursos necesarios para implementación y cumplimiento.

Capítulo 8. **Operación**: Se establece la planificación, implementación, controles y procedimientos para controlar y cumplir los objetivos de las operaciones y requerimientos de seguridad.
Capitulo9 Evaluación del desempeño: Se define indicadores para medir la efectividad, eficacia y el desempeño del SGSI.

Capítulo 10. Mejora: Se establece un plan de mejora a partir de las no-conformidades identificadas las acciones correctivas para que no se repitan.

Figure 4. Ciclo PDCA or PHVA

https://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

8 SISTEMA DE GESTION DOCUMENTAL

En nuestro Sistema de Gestión de seguridad de la información estará establecidos una serie de documentos que dicta la norma ISO/IEC27001 de esta forma garantizando la confidencialidad,

integridad y disponibilidad de la información, protegiendo a los activos y la divulgación de información no autorizada de la información.

8.1 Política de Seguridad:

Estas políticas son internas y se aplican a todos los empleados, directivas y terceros para proteger los activos, reducir riesgos empresariales y legales garantizando integridad y confidencialidad de la información. Digital Signage LRDXXX ha desarrollado la política de seguridad que hace parte del plan de SGSI. Este manual de políticas de seguridad de la información se basa en los controles definidos en el Anexo A de la norma ISO-IEC 27001/2013.

A.5.	Política General de Seguridad de la Información
A.6.	Organización de Seguridad de la Información
A.7.	Seguridad de los Recursos Humanos
A.8.	Gestión de Activos
A.9.	Control de Acceso.
A.10.	Criptografía.
A.11.	Seguridad Física y del Entorno.
A.12.	Seguridad de las Operaciones.
A.13.	Seguridad de las Comunicaciones.
A.14.	Adquisición, Desarrollo y Mantenimiento de Sistemas.
A.15.	Relaciones con los Proveedores.
A.16.	Gestión de Incidentes de Seguridad de la Información.
A.17.	Seguridad de la Información en la Continuidad del Negocio.
A.18.	Cumplimiento de Requisitos Legales y Contractuales.

Table 4. Anexo A de la norma ISO-IEC 27001/2013

Para más detalle, puede ser consultado en el ANEXO1: Anexo1_Politicas de Seguridad.pdf

Para el cumplimiento de estas políticas se ha establecido los siguientes roles y responsabilidades:

8.2 Roles y responsabilidad

Director: El director tiene la responsabilidad de supervisar el desarrollo y la administración de esta política

Director de Sistemas: Bajo la dirección y orientación del director, el director de Sistema tiene la responsabilidad de:

- Desarrollar y mantener políticas y procedimientos escritos para garantizar la implementación y el cumplimiento.
- Proporcionar el apoyo y orientación para ayudar a los empleados cumplir con sus responsabilidades bajo esta directiva.

Directores de Finanzas, ventas, Publicidad, Sistemas, director: Todos los gerentes deben

- Asegurar que todos los empleados comprendan y cumplan con estas políticas. El incumplimiento resultara en una acción disciplinaria de la compañía.

Empleados: Es responsabilidad de cada empleado: Entender y cumplir con la política

9 Procedimiento de Auditorías Internas

Las auditorías internas se realizarán a fin de determinar el grado en el que SGSI está implementado, soportado y si cumple con la norma ISO/IEC 27001: 2013. Las políticas del procedimiento de Auditoria Interna pueden ser consultado en el anexo2: Anexo2_Auditoria_Interna.pdf ver archivo "programa anual de Auditoria.xls".

En este plan de Auditoria, se establecerá que se auditará el 33% de los controles, el siguiente el 33%, y el tercer y último año, se revisarán el resto de controles. Ver anexo: Programa Anual de auditoria.xls

Este documento será aprobado y firmado por la dirección y estará disponible y accesible públicamente.

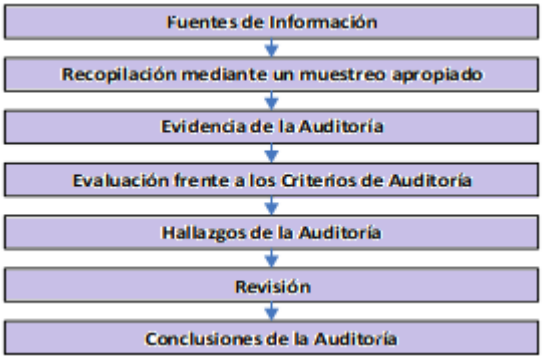

Figure 5. Ciclo Auditoria Interna

10 Gestión de Indicadores

La gestión de indicadores es la forma de medir la eficiencia o efectividad y eficacia de los controles implementados.

Los objetivos son:

- Evaluar la efectividad y eficiencia de la implementación de los controles de seguridad
- Publicar, capacitar en el interior de la entidad los indicadores para gestionar el plan de riesgos y mejoras.

Se ha establecido 7 indicadores para la compañía Digital Signage LRD XXX que pueden ser consultados en: Anexo3_gestiondeindicadores.pdf

11 Procedimiento Revisión por Dirección

Los directivos de la compañía deben revisar el funcionamiento del SGSI según la planificación y necesidades del Sistema de Seguridad de la Información con el objeto de:

- Revisión la política de seguridad de la información
- Revisión de los objetivos de seguridad de la información.
- Documentación y registro de los resultados obtenidos

En caso de detectar problema, este control llevara como resultado acciones correctivas.

El procedimiento se encuentra en el anexo4: ProcedimientoREvisionpor Direccion.pdf

12 Gestión de Roles y Responsabilidades

Es fundamental designar los recursos necesarios para crear, mantener, supervisar y mejorar el sistema. El líder de Seguridad es responsable de velar, dar seguimiento y cumplimiento a cada una de las políticas de seguridad. La definición de la gestión de roles y responsabilidades se encuentra en detalle anexo5: anexo5Procedimientorolesyresponsabilidades.pdf

13 Metodología de Análisis de Riesgo

La empresa Digital Signage LRDXXX debe garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, mitigados y gestionados para prevenir y evitar problemas por perdida, robo, plagio o fraude.
La metodología MAGERIT se estará aplicando para el análisis de riesgo con el fin de garantizar la seguridad de los activos de información y el normal funcionamiento de la compañía.

En esta etapa se estará:

- Identificando los activos
- Identificando amenazas
- Estimando Impactos/probabilidad
- Estimando el coste/criticidad

- Estimando madurez de salvaguardas
- Cálculo de los riesgos

Ver en detalle anexo6: Anexo6: MetodologiaAnalisis de Riesgo.pdf

14 Declaración de aplicabilidad:

Documento que enumera los controles aplicados por el SGSI de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación. Ver en detalle Anexo7: Anexo7Declaraciondeaplicabilidad.pdf

15 Resultados

Se ha elaborado una serie de documentos que establece la estrategia y el control teniendo en cuenta los requisitos de negocio y los requerimientos legales o contractuales relativos a la seguridad de la información. Se ha establecido indicadores que no existían en la compañía para iniciar a medir la eficiencia a los controles implementados con estos resultados se pueden iniciar hacer las correcciones y el plan de mejoramiento.

Se iniciará un plan de entrenamiento a todo el personal para sensibilizar a los empleados de los cambios a todas las políticas de seguridad, se tiene centralizado en un repositorio la información de manuales de capacitación y actas relevantes a la seguridad de la información. Adicionalmente en la compañía se evaluó el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo donde la alta gerencia tiene asignado un equipo para mitigar estos riesgos.

16 Análisis de Riesgo

16.1 Introducción

En esta fase se determinará los controles a aplicar, las acciones y tratamientos a realizar de acuerdo a los objetivos establecidos.

Se iniciará con la identificación de los activos disponiendo de un inventario actualizado, se detectará las amenazas y vulnerabilidades para cada activo que apliquen en la compañía.

Se toma como base lo expuesto a la fuente " https://www.pmg-ssi.com/2015/05/iso-27001-analizar-y-gestionar-riesgos-sgsi/"

El submodelo de procesos de MAGERIT dispone cuatro etapas:

Etapa 1 "Planificación de análisis y gestión de riesgos", estableciendo las consideraciones necesarias para poder comenzar con el proyecto de análisis y gestión de riesgos, lo que permite la investigación de la oportunidad definiendo los objetivos que se cumplen y el dominio que engloba.

Etapa 2 "Análisis de riesgos", facilita la identificación y valora las entidades que intervienen en el riesgo, se obtiene la evaluación de dichas áreas de dominio y además, realiza una estimación de los diferentes riesgos.

Etapa 3 "Gestión de riesgos", permite identificar las diferentes funciones que reducen el riesgo detectado, selecciona las medidas necesarias para que sean aceptables las funciones existentes y las restricciones.

Etapa 4 "Selección de salvaguarda", facilita la selección de los diferentes mecanismos que se deben implementar, además elabora una orientación del plan de implantación de los diferentes mecanismos que permitan que se salve la información importante, recoge los diferentes documentos de trabajo del proceso de análisis y gestiona los riesgos.

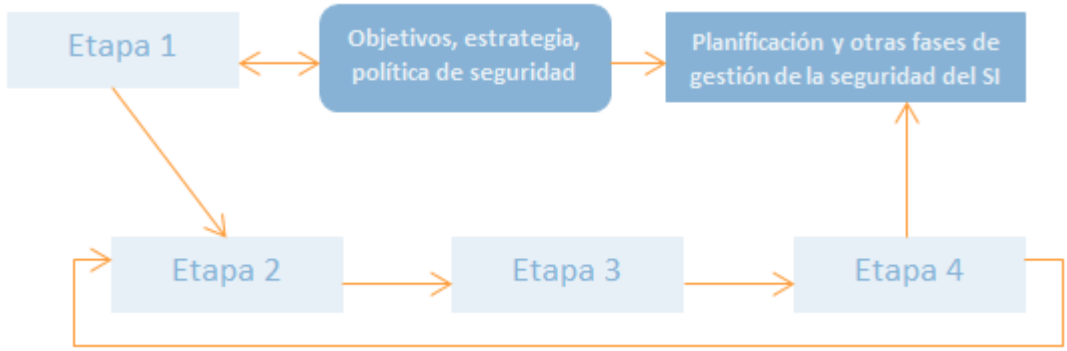

Figure 6. Etapas del proceso Margerit

16.2 Inventario de Activos

El inventario y clasificación de activos es la base para la gestión de riesgo determinando la protección o mitigación que se debe realizar a cada uno de estos.

Se denomina activo a aquello que tiene valor a la compañía. El inventario se actualiza de forma periódica dependiendo de los cambios que ocurren en la empresa o también puede ocurrir después de la auditoria anual. Para mas detalle ver anexo8: TFM_Anexo8_InventariodeActivos.pdf

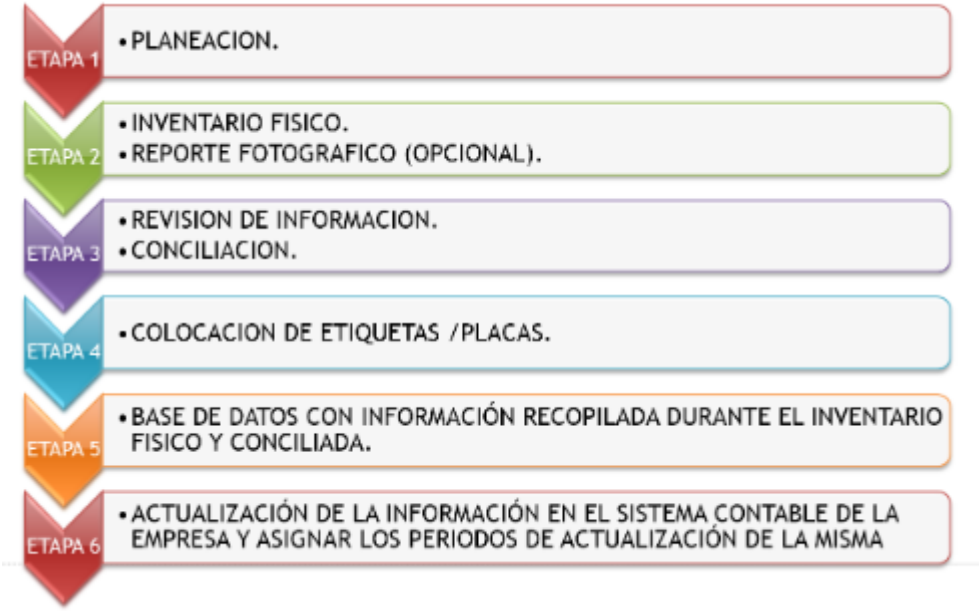

Figure 7. Proceso Control Activos

Fuente: http://asiavaluos.com/servicios/control-de-activos-fijos/

16.3 Valoración de Activos

Los activos se valorarán tomando al impacto en el corto plazo a la perdida de confidencialidad, afectación a la integridad o perdida de disponibilidad

A continuación, se presenta diagrama de dependencia de activos. fuente "https://www.tithink.com/publicacion/MAGERIT.pdf"

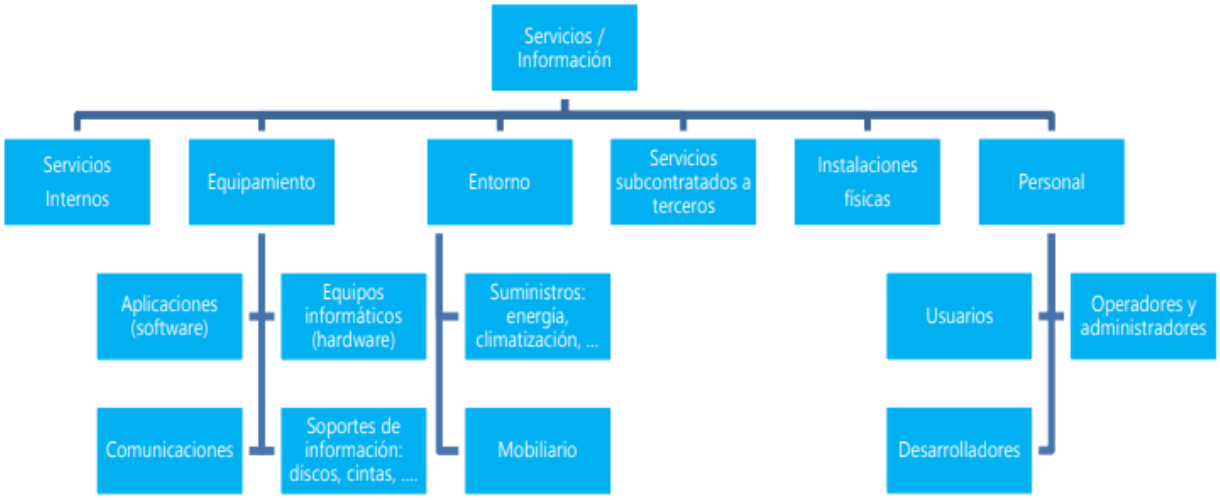

Figure 8. Dependencia de Activos

- Los criterios para la valoración de activos fueron considerados:

- Para evaluaciones de riesgo de seguridad patrimonial solo se evaluará la perdida de confidencialidad.
- Para evaluaciones de riesgo de continuidad de negocio solo se evaluará la perdida de disponibilidad.
- Para Activos identificados como personas se considera el mal uso que este pueda hacer de sus accesos, permisos, autoridades o conocimientos.
- Para activos identificados como maquinaria y equipos se considera el uso no autorizado de los mismos.
- Para activos identificados como información se considera el uso, difusión o acceso no autorizado.
- Para la pedida de integridad se evaluó los errores de procesamiento del sistema.
- Para la perdida de integridad se evaluó cuando el activo funciona incorrectamente o con fallas.
- Para la perdida de integridad se evaluó cuando la persona o recurso humano suministra información errónea.
- Para la perdida de disponibilidad se reviso el no acceso al activo al personal autorizado o la persona líder del proceso no se encuentra.

- Se toma en cuenta el incumplimiento legal a contratos o entes externos para la perdida de disponibilidad o integridad.

En detalle revisar anexo8. Valoraciondeactivos.pdf

A continuación, se dará la siguiente clasificación:

VALOR			CRITERIO
10	MA	MUY ALTO	Daño extremadamente muy Grave
7-9	A	ALTO	Daño Grave
4-6	M	MEDIO	Daño Importante
1-3	MB	BAJO	Daño Menor
0	D	Despreciable	Irrelevante a efectos prácticos

Table 5. valoración de Activos

A continuación, se presenta los activos y Procesos de Digital Signage LRD XXX.

	PROCESOS									
Activos de Informacion	Gestión de **Redes y Comunicaciones**	**Gestion de Prevención y daños**	**Gestion Documental**	**Gestion Contractual**	**Gestion Financiera**	**Gestion Legal**	**Gestión de Tecnologías de Información**	**Gestión de Aplicaciones y Arquitectura**	**Gestion de Implementacion**	**Gestion de Soporte**
SW-Aplicaciones Software	X		X				X	X	X	
Datos de Informacion			X	X	X	X	X	X		
Red de Comunicaciones	X						X		X	X
HW. Equipos Informaticos -Hardware		X					X			X
COM. Redes de Comunicaciones	X						X			X
AUX. Equipamiento Auxiliar	X									X
L. Instalaciones	X									
P. Personal	X	X	X	X	X	X	X	X	X	X
S. Servicios	X								X	X

Table 6. Tabla Activos Vr Procesos

16.4 Exclusiones para evaluación de activos

- No se tendrá en cuenta o no valorar la perdida de integridad para activos clasificados como personas
- Solo se valorará la perdida de disponibilidad de un activo identificado como persona solamente para riesgo de continuidad de negocio

16.5 Dimensiones de Seguridad

Se tendrá cinco (5) dimensiones para la empresa Digital signage LRD XXX definiéndose:

Se consulta la siguiente fuente http://www.aspectosprofesionales.info/2017/10/integrar-la-norma-iso-27001-o-el.html

Confidencialidad, que preserva la información de modo que únicamente sea accesible o conocida por quien tiene autorización para hacerlo.

Integridad, que preserva la información de modo que únicamente sea alterada por quien tiene autorización para hacerlo. Un caso extremo, es la supresión de la información.

Disponibilidad, que garantiza que la información sea accesible durante el período acordado, normalmente mediante un acuerdo de nivel de servicio (SLA/ANS). Habitualmente es una dimensión asociada a los servicios que tratan la información.

Autenticidad, que garantiza que quien realiza un trámite sea realmente quien dice ser o, desde el punto de vista de la información, garantizar que ésta sea auténtica.

Trazabilidad, que asegura que se registren todos los trámites realizados, con indicación de quién los hizo y en qué momento preciso o, desde el punto de vista de la información, posibilitar la comprobación a posteriori de quién la ha accedido, o modificado, y cuando.

Dimensiones de Valoración de Activos
[A] Autenticidad
[C] Confidencialidad de la Información
[I] Integridad de la Información
[D] Disponibilidad
[T] Trazabilidad del uso del servicio

Table 7.Dimensiones de valoración de Activos

VALOR	CRITERIO
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Table 8.Valoración Dimensión

16.6 Tabla resumen de valoración

En el archivo TFM_Anexo9_REsumenTablaValorActivos.excel. Se encuentra las dimensiones y valor de cada uno de los activos de la empresa.

16.7 Análisis de amenazas

Los activos están expuestos a varios tipos de amenazas causando un incidente no deseado el cual puede generar daño al sistema o a la compañía o personas.

- Se lista las siguientes amenazas de acuerdo a la fuente: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

Para más detalle ver archivos activos.xls Hoja de trabajo Amenazas.

Descripción	Descripción	Descripción	Descripción			
Amenazas típicas sobre el activo	**Afectación del tipo de Activo**	**la frecuencia de ocurrencia expresada como tasa anual (incidencias por año)**	**recogen la degradación del activo expresada como porcentaje de su valor**			
	Activo	**Frecuencia**	**I**	**C**	**D**	**T**
N. Desastres naturales						
[N.1] Fuego	•[HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	0,1			70%	
[N.2] Daños por agua	[HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	0,1			70%	

Desastres naturales		Frecuencia	I	C	D	T
N* (03 – CONTAMINACIÓN 04 - SINIESTRO MAYOR 06 - FENÓMENO CLIMÁTICO 07 - FENÓMENO SÍSMICO 08 - FENÓMENO DE ORIGEN VOLCÁNICO 09 - FENÓMENO METEOROLÓGICO 10 - INUNDACIÓN)	[HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	NA			NA	
[I] De origen industrial		Frecuencia	I	C	D	T

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial.
Estas amenazas puede darse de forma accidental o deliberada.

5.2.1. [I.1] Fuego	• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	NA			NA	
5.2.2. [I.2] Daños por agua	• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento	NA			NA	

	auxiliar • [L] instalaciones					
[I.3] Contaminación mecánica	• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	NA			NA	
[I.4] Contaminación electromagnética	• [HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	NA			NA	
[I.5] Avería de origen físico o lógico	• [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	NA			NA	
[I.6] Corte del suministro eléctrico	[HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	NA			NA	
[I.7] Condiciones inadecuadas de temperatura o humedad	[HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	NA			NA	
[I.8] Fallo de servicios de comunicaciones	• [COM] redes de comunicaciones	NA			NA	
[I.9] Interrupción de otros servicios y suministros esenciales	• [AUX] equipamiento auxiliar	NA			NA	
[I.10] Degradación de los soportes de almacenamiento de la información	• [Media] soportes de información	NA			NA	
[I.11] Emanaciones electromagnéticas	• [HW] equipos informáticos (hardware) • [Media] media • [AUX] equipamiento auxiliar • [L] instalaciones	NA		NA		
[E] Errores y fallos no intencionados		Frecuencia	I	C	D	T

[E.1] Errores de los usuarios	• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [Media] soportes de información	10	80%	70%	90%	
[E.2] Errores del administrador	[D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información	100	100%	80%	85%	80%
[E.3] Errores de monitorización (log)	• [D.log] registros de actividad	10	80%		30%	70%
[E.4] Errores de configuración	• [D.conf] datos de configuración	100	100%			100%
[E.7] Deficiencias en la organización	• [P] personal	0,1			50%	
[E.8] Difusión de software dañino	• [SW] aplicaciones (software)	1	90%	70%	100%	
[E.9] Errores de [re-]encaminamiento	• [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	1		60%		
[E.10] Errores de secuencia	• [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	10	80%			
[E.14] Escapes de información	• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	1		90%		
[E.15] Alteración accidental de la información	• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	10	90%			

[E.18] Destrucción de información	• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	1			100%	
[E.19] Fugas de información	• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones • [P] personal (revelación)	1		90%		
[E.20] Vulnerabilidades de los programas (software)	• [SW] aplicaciones (software)	100	100%	100%	100%	
[E.21] Errores de mantenimiento / actualización de programas (software)	• [SW] aplicaciones (software)	10	80%		80%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	• [HW] equipos informáticos (hardware) • [Media] soportes electrónicos • [AUX] equipamiento auxiliar	10			90%	
[E.24] Caída del sistema por agotamiento de recursos	• [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	10			90%	
[E.25] Pérdida de equipos	[HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	10		80%	70%	
[E.28] Indisponibilidad del personal	• [P] personal interno	100			80%	
[A] Ataques intencionados		Frecuencia	C	I	D	T
[A.3] Manipulación de los registros de actividad (log)	• [D.log] registros de actividad	10	60%			70%
[A.4] Manipulación de la configuración	• [D.log] registros de actividad	10	80%	70%	80%	80%

[A.5] Suplantación de la identidad del usuario	• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	1	90%	100%	100%	
[A.6] Abuso de privilegios de acceso	• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	10	100%	100%	100%	
[A.7] Uso no previsto	• [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	1	90%	80%	100%	
[A.8] Difusión de software dañino	• [SW] aplicaciones (software)	1	100%	100%	100%	
[A.9] [Re-]encaminamiento de mensajes	• [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	1		90%		
[A.10] Alteración de secuencia	• [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	1	100%			

[A.11] Acceso no autorizado	[D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	1	80%	100%		
[A.12] Análisis de tráfico	• [COM] redes de comunicaciones	1		90%		
[A.13] Repudio	• [S] servicios • [D.log] registros de actividad	1	80%			
[A.14] Interceptación de información (escucha)	[COM] redes de comunicaciones	1		90%		
[A.15] Modificación deliberada de la información	• [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	1		100%		
[A.18] Destrucción de información	• [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [Media] soportes de información • [L] instalaciones	1			100%	
[A.19] Divulgación de información	• [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	1		90%		
[A.22] Manipulación de programas	• [SW] aplicaciones (software)	10	100%	100%	100%	
[A.23] Manipulación de los equipos	• [HW] equipos • [Media] soportes de información	1		80%	80%	

	• [AUX] equipamiento auxiliar					
[A.24] Denegación de servicio	• [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	10			100%	
[A.25] Robo	• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	1		80%	80%	
[A.26] Ataque destructivo	• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	0,1			100%	
[A.27] Ocupación enemiga	• [L] instalaciones	0,1		100%	100%	
[A.28] Indisponibilidad del personal	• [P] personal interno	1			80%	
[A.29] Extorsión	• [P] personal interno	0,1	100%	90%	80%	
[A.30] Ingeniería social (picaresca)	[P] personal interno	0,1	100%	90%	80%	

Table 9. Analisis de Amenazas Vr Frecuencia Vr Degradacion

PROBABILIDAD o FRECUENCIA DE OCURRENCIA

La frecuencia o probabilidad nos dice cada cuanto se materializa la amenaza.

MA	100	Muy frecuente	A diario
A	10	frecuente	mensualmente
M	1	normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años

Table 10. Valor de la Frecuencia

- **La Degradación**: mide el daño causado por un incidente en el supuesto que ocurriera y nos mostraría cuán perjudicado resultaría el activo.

16.8 Impacto Potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios fuente " https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html"

Impacto= valor X degradación

Riesgo = impacto X probabilidad o frecuencia

Mas detalle ve archivo activos.XLS hoja de trabajo Impacto potencial

En las gráficas se evidencia que el tipo de activo Software y Datos de Información en caso de una amenaza tiene un impacto muy alto a la organización. Lo que significa que es importante diseñar e implementar mecanismos de control a fin de minimizar el riesgo existente.

Figure 9. Impacto Instalaciones

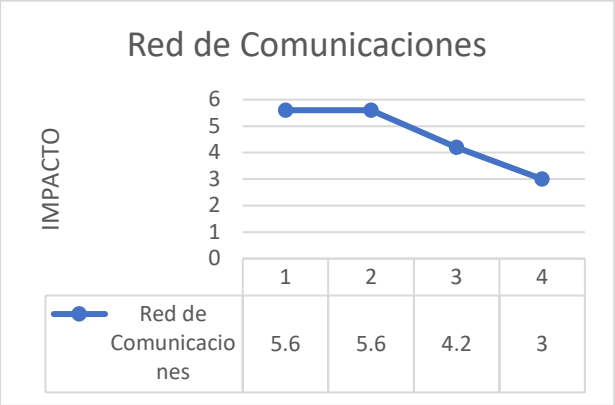

Figure 10. Impacto Comunicaciones

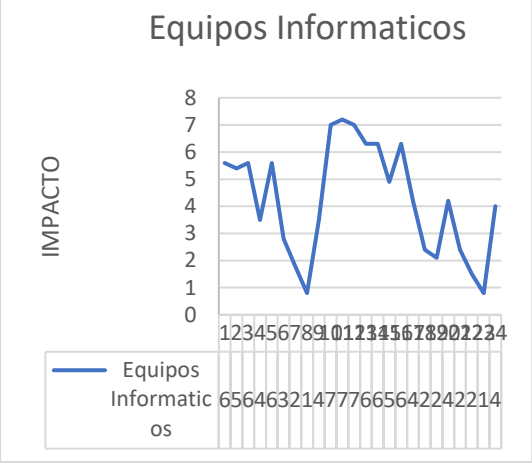

Figure 11 Impacto Equipos Informaticos

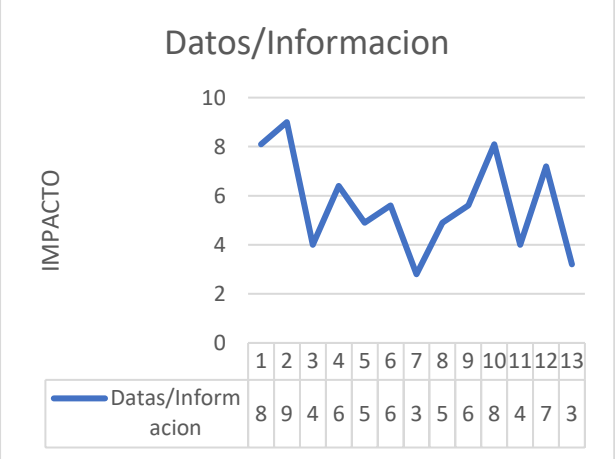

Figure 12. Impacto Datos/Informacion

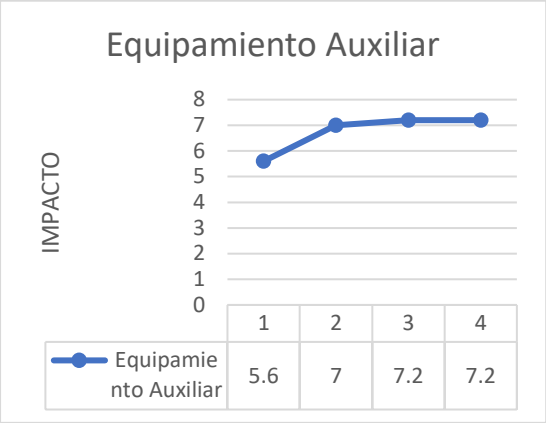

Figure 13. Impacto Equipamiento Auxiliar

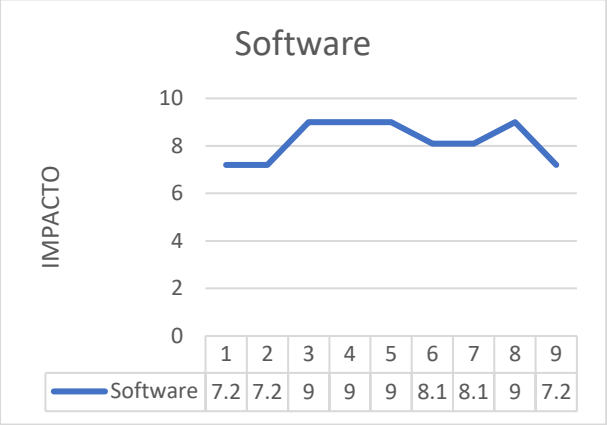

Figure 14. Impacto Software

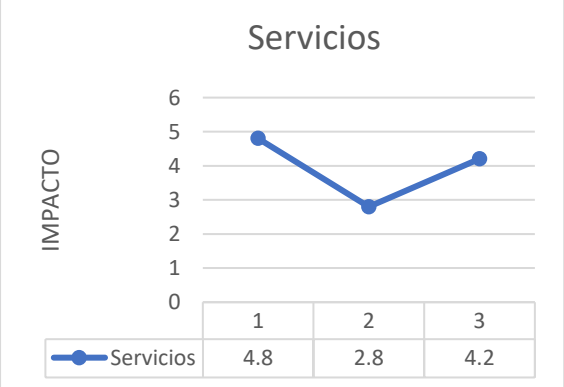

Figure 15 Impacto Servicios

16.9 Nivel de Riesgo Aceptable y Riesgo Residual

De acuerdo Margerit 3.0 el **riesgo aceptable es aceptar la responsabilidad de las insuficiencias**. Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden

establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión, ...).

Riesgo Residual: es el conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que se ha modificado el riesgo, desde un valor potencial a un valor residual.

https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

https://www.tithink.com/publicacion/MAGERIT.pdf

Figure 16. Analisis de Riesgo

Criterios de aceptación del riesgo. Fuente: Manual Administración del Riesgo.

Criterios de Aceptación del Riesgo	
Nivel de Riesgo Residual	**Decision**
Muy Alto	No se asume el riesgo. Se transfiere con pólizas o se establece controles o plan de tratamiento.
Alto	No se asume el riesgo. Se transfiere con pólizas o se establece controles.
Moderado	Se asume el riesgo residual. El plan de tratamiento es opcional, a decisión del líder del proceso. Se recomienda establecer tratamiento a las causas que carezcan de controles, o mejorar los controles existentes de acuerdo a sus calificaciones más bajas.
Bajo	Se asumen el riesgo residual. No requiere plan de tratamiento. Continúa con los controles existentes.

Figure 17. Criterios de Aceptacion de Riesgo

16.10 Las salvaguardas

permiten hacer frente a las amenazas. Para el caso de la compañía Digital signage LRD XXX se sigue las recomendaciones de la fuente " https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html"

Protecciones generales u horizontales

H Protecciones Generales

H.IA Identificación y autenticación

H.AC Control de acceso lógico H.ST Segregación de tareas

H.IR Gestión de incidencias

H.tools Herramientas de seguridad

H.tools.AV Herramienta contra código dañino

H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión

H.tools.CC Herramienta de chequeo de configuración

H.tools.VA Herramienta de análisis de vulnerabilidades

H.tools.TM Herramienta de monitorización de tráfico

H.tools.DLP DLP: Herramienta de monitorización de contenidos

H.tools.LA Herramienta para análisis de logs

H.tools.HP Honey net / honey pot H.tools.SFV Verificación de las funciones de seguridad

H.VM Gestión de vulnerabilidades

H.AU Registro y auditoría

Protección de los datos / información

D Protección de la Información

D.A Copias de seguridad de los datos (backup)

D.I Aseguramiento de la integridad

D.C Cifrado de la información

D.DS Uso de firmas electrónicas

D.TS Uso de servicios de fechado electrónico (time stamping)

Protección de las claves criptográficas

K Gestión de claves criptográficas

K.IC Gestión de claves de cifra de información

K.DS Gestión de claves de firma de información

K.disk Gestión de claves para contenedores criptográficos

K.comms Gestión de claves de comunicaciones

K.509 Gestión de certificados

Protección de los servicios

S Protección de los Servicios

S.A Aseguramiento de la disponibilidad

S.start Aceptación y puesta en operación

S.SC Se aplican perfiles de seguridad

S.op Explotación

S.CM Gestión de cambios (mejoras y sustituciones)

S.end Terminación

S.www Protección de servicios y aplicaciones web

S.email Protección del correo electrónico

S.dir Protección del directorio

S.dns Protección del servidor de nombres de dominio (DNS)

S.TW Teletrabajo

S.voip Voz sobre IP

Protección de las aplicaciones (software)

SW Protección de las Aplicaciones Informáticas

SW.A Copias de seguridad (backup)

SW.start Puesta en producción

SW.SC Se aplican perfiles de seguridad

SW.op Explotación / Producción

SW.CM Cambios (actualizaciones y mantenimiento)

SW.end Terminación

Eficacia	Nivel	Significado
0%	L0	Inexistente
10%	L1	Inicial /ad hoc
50%	L2	Reproducible, pero intuitivo
90%	L3	Proceso definido
95%	L4	Gestionado y Medible
100%	L5	Optimizado

Table 11. Nivel de Madurez para evaluar Salvaguardas - CMM

A continuación, se presenta la siguiente gráfica. Ver archivo anexo: activos.xls

		PROBABILIDAD				
RIESGO		**MB: Muy Raro**	**B: Poco Probable**	**M: Posible**	**A: Probable**	**MA: Practicamente Seguro**
Impacto	**MA: Muy Alto (10)**	A: Importante	MA: CRITICO	MA: CRITICO	MA: CRITICO	MA: CRITICO
	A: Alto (7-9)	M: Apreciable	A: Importante	A: Importante	MA: CRITICO	MA: CRITICO
	M : Medio (4-6)	B: Bajo	M: Apreciable	M: Apreciable	A: Importante	A: Importante
	B: Bajo (1-3)	MB: Despreciable	B: Bajo	B: Bajo	M: Apreciable	M: Apreciable
	MB : Muy Bajo (0-2)	MB: Despreciable	MB: Despreciable	MB: Despreciable	B: Bajo	B: Bajo

Table 12. valor del Riesgo

Activos	Estimación de Impacto	Riesgo	Control	Owner
SW-Aplicaciones Software	MA: Muy Alto	MA: Muy Alto	. Activar la aplicación Biométricos. . Todos los accesos lógicos deben ser por Directorio Activo + Biométrico. . Las aplicaciones deben desarrollarse con el esquema RBAC.	Comite de seguridad (Arquitecto de aplicaciones, Gerente de TI, Gerente de Seguridad, Gerente RGPD, Gerente de Marketing)

Datos de Informacion	MA: Muy Alto	MA: Muy Alto	. Implementar Política de control de Cambios . Implementar Procedimiento de Políticas de Información.	Gerente de Seguridad
Red de Comunicaciones	A: Alto	A: Alto	. Implementar controles y protocolos de Inscripción	Gerente de TI
P. Personal	A: Alto	A. Alto	. Revisión de las hojas de Vida y cumplimiento del Job description. . Aplicar Training o cursos virtuales al personal.	Manager Recursos Humanos
HW. Equipos Informaticos **-Hardware**	A: Alto	A: Alto	. Implementar procesos de alta disponibilidad. . Activar pólizas de robo de equipos	Gerente de TI
AUX. Equipamiento Auxiliar	M: Apreciable	M: Apreciable	. Activar cámara de seguridad	Gerente de Servicios Inmobiliarios
S. servicios	M: Apreciable	M: Apreciable	. Revision de SLA (Service Level Agreement). Revisión de Contratos con el proveedor	Gerente de Servicios Inmobiliarios
COM. Redes de Comunicaciones	B: Bajo	B: Bajo	. Implementar controles y protocolos de Inscripción	Gerente de TI
L. Instalaciones	B: Bajo	B: Bajo	. Cumplimiento TIER III en el centro de datos principal . Debe existir Simulacros de Evacuación	Manager de Servicios Inmobiliarios

Table 13. Riesgo vr Controles Vr Propietario

16.11 RESULTADOS

- La dependencia entre activos expresa la relación funcional entre ellos y de esta forma determina el valor del mismo. En este caso el Activo Personal o Recurso Humano Interactúan con todos los activos identificados teniendo un valor significativo.

- En las gráficas se evidencia que el tipo de activo Software y Datos de Información en caso de una amenaza tiene un impacto muy alto a la organización. Lo que significa que es importante diseñar e implementar mecanismos de control a fin de minimizar el riesgo existente.

- La relación de los tipos de activos de Información y procesos Identificados establece los controles que facilitan la salvaguarda de los tipos de activos identificados.

- Los nuevos niveles de riesgo evaluados con la participación de cada owner o propietario expresan un nivel de riesgo residual. Un nivel Alto de Riesgo significa la detención de los servicios de la compañía ameritando iniciar procesos de implementación de medidas de control en la administración de activos de información.

- El Riesgo Aceptable (calificación 0- 3 “Muy Bajo” , “ Bajo”), significa que su Probabilidad es baja y su Impacto es leve, lo cual permite a la compañía asumirlo, es decir, el riesgo se encuentra en un nivel que puede aceptarlo sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

- El Riesgo Inaceptable (calificación 10, 9 “Muy Alto”, “Alto”), Probabilidad o frecuencia es alta y su Impacto catastrófico, se recomienda eliminar la actividad que genera el riesgo para mitigar el riesgo se debe implementar controles de prevención y protección para evitar la frecuencia del riesgo, de esta forma disminuyendo el Impacto o compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponibles.

- Si el riesgo Moderado (Calificación 4-6) se deben tomar medidas o controles para llevar los Riesgos a la Zona Aceptable.

17 Propuesta de Proyecto

17.1 Introducción

Se realizó un análisis del estado actual de la compañía Digital Signage LRDXXX en relación a la gestión de la seguridad de la información, el cual sirve como entrada para la propuesta de proyecto de un SGSI basado en la norma ISO 27001:2013. La norma sigue un ciclo de HPVA requiriendo un ciclo de revisión y mejora continua donde debe existir recursos a la monitorización, gestión, seguimiento, auditoria y la mejora de los mismos.

17.2 Propuestas

Los proyectos que se proponen son:

- Proyecto Políticas de seguridad de la información: ver anexo TFM_Anexo11Proyecto_Politicas de Seguridad.pdf
- Proyecto Continuidad del negocio ver anexo: TFM_Anexo12COB_Proyecto_continuidad_delnegocio.pdf
- Proyecto Control software ver anexo: TFM_Anexo13Proyecto_control de software.pdf

Para ver la relación entre cada uno de los activos y riesgo se puede encontrar: Anexo: Activos.xls : Hoja de Trabajo Amenazas propia.

Adicionalmente se ver anexo: Programa Anual de auditoria.xls

17.3 Resultados

- El plan de implementación de los 3 proyectos propuesta ha permitido fortalecer la seguridad de la información con la documentación formal y procedimientos estándar alrededor del 30%.
- Con el plan de implementación se encontró información obsoleta y desactualizada lo que requirió una actualización de la misma.
- Con el plan de implementación de proyecto se evidenció la alta rotación del personal lo que se enfatiza capacitación continua para los empleados. enfatizando el plan de mejora continua.
- La capacitación hacer parte de la medidas y control evaluados mejorando y unificados procesos por parte del empleado, beneficiando a los objetivos y alcance de la empresa.

A continuación, se presenta un nuevo análisis diferencial con los controles implementados.

No.	Evaluación de Efectividad de controles				
	DOMINIO	**Calificación Actual**	**Calificacion Proyectada**	**Calificación Ideal**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	70	100	**EFECTIVO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	52	70	100	**EFECTIVO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	54	70	100	**EFECTIVO**
A.8	GESTIÓN DE ACTIVOS	52	80	100	**EFECTIVO**
A.9	CONTROL DE ACCESO	66	80	100	**GESTIONADO**
A.10	CRIPTOGRAFÍA	60	75	100	**EFECTIVO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	52	80	100	**EFECTIVO**
A.12	SEGURIDAD DE LAS OPERACIONES	62	80	100	**GESTIONADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	67	80	100	**GESTIONADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	67	80	100	**GESTIONADO**
A.15	RELACIONES CON LOS PROVEEDORES	50	80	100	**EFECTIVO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	50	80	100	**EFECTIVO**

A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	57	80	100	**EFECTIVO**
A.18	CUMPLIMIENTO	68	80	100	**GESTIONADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**60**	**80**	**80**	**EFECTIVO**

Table 14. Evaluación de Efectividad de Controles

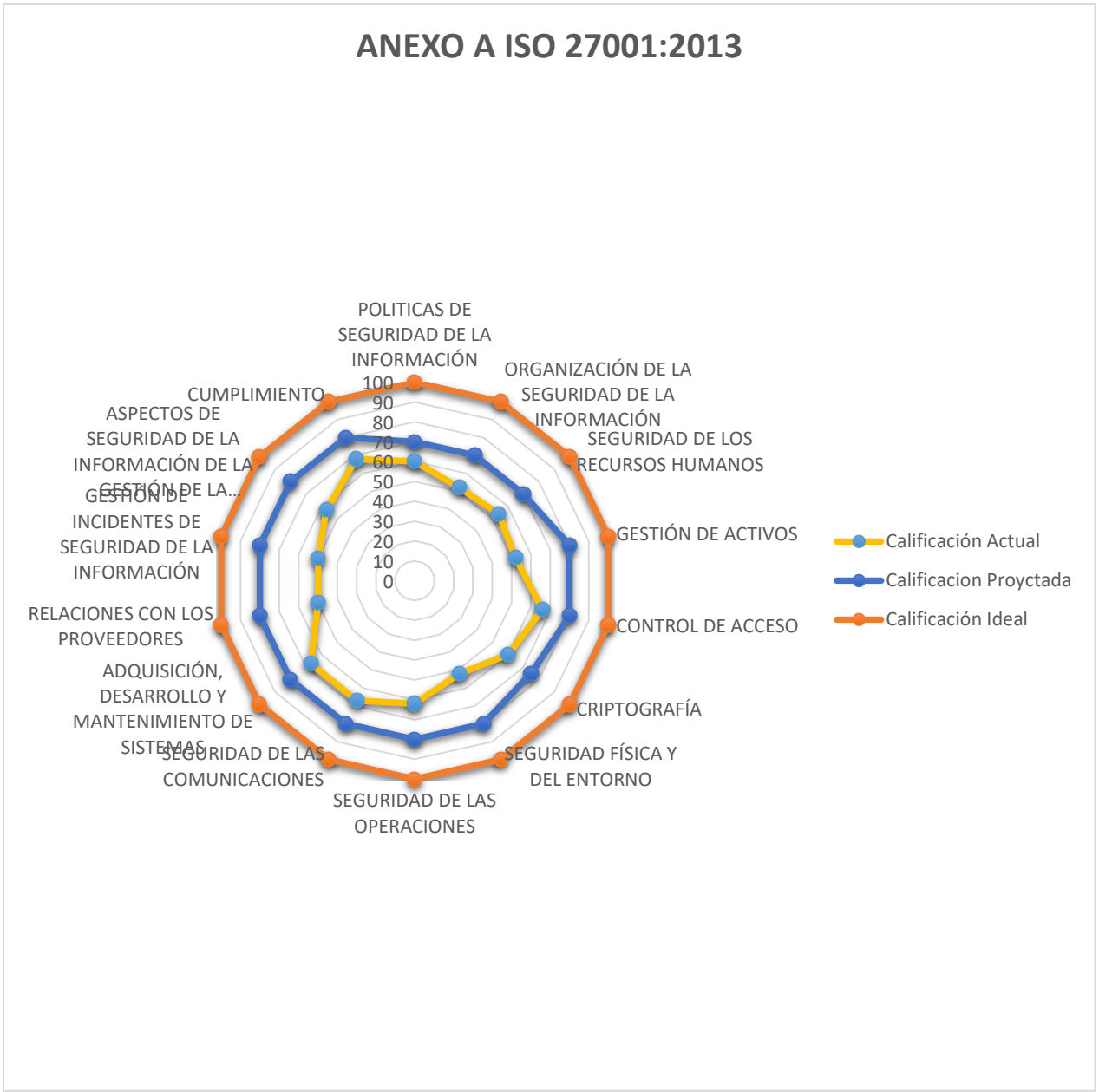

Figure 18. Grafica implementacion de Controles

18 Auditoria de Cumplimiento

18.1 Introducción

Llegados a esta fase, conocemos los activos de la empresa y hemos evaluado las amenazas. Es el momento de hacer un alto en el camino y evaluar hasta qué punto la empresa cumple con las buenas prácticas en materia de seguridad. La ISO/IEC 27002:2013 nos servirá como marco de control del estado de la seguridad.

18.2 Metodología

El estándar ISO/IEC 27002:2013, agrupa un total de 114 controles o salvaguardas sobre buenas prácticas para la Gestión de la Seguridad de la Información organizado en 14 dominios y 35 objetivos de control. Éste estándar es internacionalmente reconocido y es perfectamente válido para la mayoría de organizaciones.

El estudio debe realizar una revisión de los 114 controles planteados por la norma para cumplir con los diferentes objetivos de control – el número de los cuales se indica entre paréntesis para cada uno de los dominios-. Esta estimación la realizaremos según la siguiente tabla, que se basa en el Modelo de Madurez de la Capacidad (CMM):

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	**L0**	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.

50%	**L2**	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	**L4**	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	**L5**	Optimizado	Los procesos están bajo constante mejora.

Table 15. Modelo de Madurez de la Capacidad (CMM)

Para la evaluación de cada uno de los controles se analizará la documentación existente dentro de la compañía, reporte de evidencias, incidentes, informes de auditorías, entrevistas y observaciones en sitio.

18.3 Evaluación de la Madurez

El objetivo de esta fase del proyecto es evaluar la madurez de la seguridad en lo que respecta a los diferentes dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013. Antes de abordar intentaremos profundizar al máximo en el conocimiento de la organización.

De forma resumida, los dominios que deben analizarse son:

- Política de seguridad
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad en los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de Sistemas de Información
- Gestión de incidentes
- Gestión de continuidad de negocio
- Cumplimiento

Después de varios meses de implementación se muestra los resultados.

Dominio	Objetivo/Control	Cumple	Nivel	Efectividad	Observación
	A5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN				
A5. Directrices de la Dirección en seguridad de la Información	Orientar y soportar los requisitos del negocio y con las leyes y reglamentos al cumplimiento de la seguridad de la información		L3	50%	
A.5.1.1. Políticas para la seguridad de la información	Debe Definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes	SI	L3	50%	La empresa Digital Signage LRDXXX cuenta con Manuales Internos de control de Operaciones de seguridad de la Información. Sin embargo, falta más propagación de estas.

	externas pertinentes.				
A5.1.2. Revisión de las políticas para la seguridad de la información	Debe haber una Revisión de Las políticas de la seguridad de la información a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	SI	L3	50%	Existe un procedimiento de Revisión por la Dirección al menos una vez al año que incluye la responsabilidad de validar periódicamente el estado de los sistemas de gestión. Sin embargo, no hay registro de revisiones de las políticas hasta ahora.
	A.6 Aspectos Organizativos de la seguridad de la Información				
A6.1 Organización interna	**Definir y Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización**		L3	50%	
A6.1.1. Roles y responsabilidades para la seguridad de la información	Se debe Definir y asignar las responsabilidades de la seguridad de la información.	Si	L3	50%	Se encuentran conformado un comité de seguridad compuesto por la dirección y primera línea de reporte a los cuales se les deben atribuir funciones relacionadas con el SGSI. Existe un documento de Roles y responsabilidades para cada uno de las posiciones de los empleados.
A6.1.2 Segregacion de tareas	Debe existir Disgregación de los deberes y áreas de responsabilidad en conflicto, se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	si	L3	50%	considerando que hay actividades críticas que deben ser manejadas por diferentes niveles jerárquicos la separación de deberes se hace control fundamental como para mitigar los riesgos. Sin embargo, se encuentra que algunas solicitudes y aprobaciones lo realiza la misma persona o compañero del lado. Y no el manager del proceso.

A6.1.3 Contacto con las autoridades	Debe existir una Actualización y mantenimiento de contactos apropiados con las autoridades pertinentes.	Si	L3	50%	Como proveedor que presta servicios a entidades bancarias tiene contactos con las autoridades y pertenece a la lista de contactos de la superintendencia bancaria de contactos principales.
A.6.1.4 Contacto con grupos de interés especial	Debe existir una Actualización de contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	Si	L3	50%	Se crearon tres listas de contactos con el fin de adquirir conocimiento en buenas prácticas o experiencias que sean de utilidad para minimizar los riesgos de seguridad de la información. Las diferentes vías de contactos son: por email, WhatsApp, y listas telefónicas. Cada una de estas listas participan personal de seguridad, tecnología y empleados.
A6.1.5 Seguridad de la información en la gestión de proyectos.	La seguridad de la información se debe tratar en la gestión de proyectos, independiente mente del tipo de proyecto	si	L3	50%	Se tiene Una PMO manejo de proyectos que administra proyectos críticos. Se evidencia que proyectos de riesgo bajo no están bajo control de la PMO.
A.6.2. Dispositivos móviles y teletrabajo	Garantizar y controlar la seguridad del teletrabajo y el uso de dispositivos móviles		L3	50%	
A6.2.1 Política para dispositivos móviles	Se debe Adoptar política y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	si	L3	50%	Existe un manual de Procedimiento publicado para medidas de seguridad para los dispositivos móviles
A6.2.2 Teletrabajo	Se debe Implementar una política y medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	Si	L3	50%	Existe unas políticas establecidas en el Manual políticas de seguridad. Sección teletrabajo

	A.7 SEGURIDAD DE LOS RECURSOS HUMANOS L4				
A.7.1 Antes de asumir el empleo	Asegurar y verificar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		L3	50%	
A7.1.1 Investigacion de antecedentes	verificación de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos	si	L3	50%	existen procedimientos formales de selección de personal, Responsabilidades de la dirección y recursos humanos. Sin embargo, esta información no es guardada por 10 años si no 5 años.
A7.1.2. Términos y condiciones del empleo	Realizar acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	si	L3	50%	Todos los empleados cuentan con un contrato de trabajo. considerando que la información es vital para todos los cargos se han definido condiciones contractuales con las responsabilidades sobre el uso de la información.
A7.2 Durante la ejecución del empleo	Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan aplicando los procesos establecidos por la compañía.		L3	50%	

A7.2.1 Responsabilidades de la gestión	Aplicación de las políticas de seguridad de la información debe ser obligatoria y exigida a todos los empleados y contratista y procedimientos establecidos por la organización	si	L3	50%	se encuentran que la empresa tiene conformado un comité de seguridad compuesto por la dirección y primera línea de reporte a los cuales se les deben atribuir funciones relacionadas con el SGSI
A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Capacitación a todos los empleados de la organización, y en donde sea pertinente, los contratistas y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	si	L3	50%	Existe un plan de capacitación y actualizado para realizar sensibilizaciones y divulgaciones que permitan la implementación del SGSI
A7.2.3 Proceso disciplinario	Formalizar proceso de comunicación, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	si	L3	50%	Existe un proceso formal y legal de acuerdo al incidente disciplinario.
A.7.3 Terminación y cambio de empleo	Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo o contrato		L3	50%	
A7.3.1. Terminación o cambio de responsabilidades de empleo	Comunicación de responsabilidades y deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir,	si	L3	50%	Procedimiento publicado y aprobado para cambio de responsabilidades o terminación de empleo. - contrato de trabajo se debe actualizar para cambio de posición o terminación de este.

	comunicar al empleado o contratista y se deben hacer cumplir.				
A8 GESTION DE ACTIVOS					
A8.1 Responsabilidad por los activos	Identificar y documentar los activos organizacionales y definir las responsabilidades de protección adecuadas.		L3	50%	
A8.1.1 Inventario de activos	Identificación de los activos asociados con información e instalaciones de procesamiento de información, y elaboración y mantenimiento del inventario de estos activos	si	L3	50%	Existe un procedimiento de inventario de activos, repositorio de almacenamiento y cambio sobre esto.
A8.1.2 Propiedad de los activos	Los activos deben tener un Owner y gestionados por el mismo	si	L3	50%	Se manejan diferentes tipos de activos los cuales son responsabilidad de diferentes áreas lo que implica que cada activo este asignado a un propietario
A8.1.3 Uso aceptable de los activos	Identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información	si	L3	50%	Se ha definido directrices para el manejo de los activos de información con el fin de garantizar su uso adecuado
A8.1.4 Devolución de activos	Al terminar su empleo, contrato, todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo.	si	L3	50%	Hay procedimientos de devolución de activos estipulados en el contrato y esto es un requisito legal para la empresa.
A8.2 Clasificación de la información	Asegurar y clasificar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.		L3	50%	

A8.2.1	Clasificación de la información	si	L3	50%	Existe una política sobre la clasificación de la información, pero hace falta divulgación de la misma.
A8.2.2 Etiquetado de la información	Implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización	si	L3	50%	Existe una política sobre la clasificación de la información, pero hace falta divulgación de la misma.
A8.2.3 Manejo de activos	Desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	si	L3	50%	Se ha definido directrices para el manejo de los activos de información con el fin de garantizar su uso adecuado. Se registra actas de capacitación para el manejo de activos.
A8.3 Manejo de medios	Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios aplicando procedimientos de control		L3	50%	
A8.3.1 Gestión de medio removibles	Implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Si	L3	50%	Se encuentra procedimiento, pero la técnica de ejecución no es confiable ya que se puede recuperar la información
A8.3.2 Disposición de los medios	Disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	si	L3	50%	Existen procedimientos para disponer de los medios cuando ya no se requieran
A8.3.3 Transferencia de medios físicos	Aplicar proceso en manejo de medios para los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte	Si	L3	50%	Existe políticas de Manual político de seguridad. Sección transferencia. Los empleados saben usar laos protocolos de SFTP y winzip con clave e inscripción Sin embargo en muy pocos casos se encuentra la transferencia en texto claro.
A.9 CONTROL DE ACCESO	**Implementar proceso para asegurar el**		L4	50%	

	acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.				
A9.2.1 Registro y cancelación del registro de usuarios	Implementar un proceso formal de registro y de cancelación de registro de usuarios para la asignación de los derechos de acceso	si	L4	50%	Se tiene definidas directrices para registrar y cancelar usuarios cuando corresponda.
A9.2.2 Suministro de acceso de usuarios	Suministro de acceso de usuarios	si	L4	50%	Se tiene registro de los cambios de acceso. Manual control de administración de Usuarios
A9.2.3 Gestión de derechos de acceso privilegiado	Restringir y controlar la asignación y uso de derechos de acceso privilegiado	si	L4	50%	Se tiene definidas directrices para registrar y cancelar usuarios cuando corresponda. Se tiene registro de los cambios de acceso. Manual control de administración de Usuarios
A9.2.4 Gestión de información de autenticación secreta de usuarios	Aplicar métodos de autenticación y la asignación de información por medio de un proceso de gestión formal.	si	L4	50%	Se evidencia que maneja autenticación secreta en varias de sus aplicaciones por lo que ha generado directrices para su gestión
A9.2.5. Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares. Por lo menos cada 3 meses	si	L4	50%	Se tiene definidas directrices para registrar y cancelar usuarios cuando corresponda.
A9.2.6. Retiro o ajuste de los derechos de acceso	Retiro de los accesos a todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios	si	L4	50%	Se tiene definidas directrices para registrar y cancelar usuarios cuando corresponda.
A9.3 Responsabilidades de los usuarios	**Cumplir con las practicas que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.**		L4	50%	
A9.3.1 Uso de información de autenticación secreta	Exigir a los usuarios que cumplan las prácticas de la organización para el uso de	si	L4	50%	Control establecido para manejar autenticación secreta en varias de sus aplicaciones por lo que ha generado directrices para su gestión.

	información de autenticación secreta. Utilización de las herramientas de encripcion.				
A9.4 Control de acceso a sistemas y aplicaciones	Evitar el acceso no autorizado o restringir el acceso a sistemas y aplicaciones.		L4	50%	
A9.4.1 Restricción de acceso a la información	Restringir a los roles acceso a los sistemas de acuerdo con la política de control de acceso.	si	L4	50%	Se evidencia de Creación del procedimiento al control especificado, y está aprobado
A9.4.2. Procedimiento de ingreso seguro	El control de acceso a sistemas y aplicaciones se debe controlar	si	L4	50%	Procedimiento existente pero falta más comunicación a los empleados
A9.4.3 Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas. Implementar un SSO, LDAP.	si	L4	50%	Control establecido para manejar autenticación secreta en varias de sus aplicaciones por lo que ha generado directrices para su gestión.
A9.4.4 Uso de programas utilitarios privilegiados	Restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	si	L4	50%	Control establecido para manejar autenticación secreta en varias de sus aplicaciones por lo que ha generado directrices para su gestión.
A9.4.5. Control de acceso a códigos fuente de programas	Restringir el acceso a los códigos fuente de los programas y debe estar en un repositorio unificado	si	L4	50%	Se ha definido políticas de restricción de acceso a los códigos fuente de los programas
A10 CRIPTOGRAFIA					
A10.1 Controles criptográficos	Implementar políticas para Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información		L3	50%	
A10.1.1 Política sobre el uso de controles criptográficos	Desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	si	L3	50%	recibe y envía información a través de diferentes mecanismos se tiene definido directrices para realizar dichas operaciones

A10.1.2 Gestión de llaves	Desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida	si	L3	50%	recibe y envía información a través de diferentes mecanismos se tiene definido directrices para realizar dichas operaciones
A11 SEGURIDAD FISICA Y DEL ENTORNO					
A11.1 Áreas seguras	Prevenir el acceso físico no autorizado o restringido, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		L3	50%	
A11.1.1 Perímetro de seguridad física	Definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	si	L3	50%	La compañía ha delimitado sus perímetros de seguridad
A11.1.2 Controles de acceso físicos	Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	si	L3	50%	La compañía ha delimitado sus perímetros de seguridad
A11.1.3 Seguridad de oficinas, recintos e instalaciones	diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	si	L3	50%	La compañía ha delimitado sus perímetros de seguridad
A11.1.4 Protección contra amenazas externas y ambientales.	diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	si	L3	50%	cuenta con planes de emergencia, pólizas de seguro y otros controles para garantizar su protección contra amenazas externas, algunas derivadas de la ubicación física de la entidad.
A11.1.5 Trabajo en áreas seguras	diseñar y aplicar procedimientos para trabajo en áreas seguras.	si	L3	50%	las áreas seguras sólo se pueden acceder con autorización y acompañamiento de un funcionario del área
A11.1.6 Áreas de carga, despacho y acceso público	controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las	si	L3	50%	cuenta con áreas de despacho de correspondencia donde pueden entrar personas ajenas al negocio

	instalaciones de procesamiento de información para evitar el acceso no autorizado.				
A11.2 Equipos	Asegurar y Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		L3	50%	
A11.2.1 Ubicación y protección de los equipos	Los equipos o activos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	si	L3	50%	Políticas para definición de manera cuidadosa donde se ubicarán los equipos que se requieren para la operación
A11.2.2 Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. Revisión e UPS y carga eléctrica.	si	L3	50%	Se tiene un sistema de Ups en alta disponibilidad para los equipos del CPD
A11.2.3 Seguridad en el cableado	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	si	L3	50%	El cableado estructurado cumple con la norma
A11.2.4 Mantenimiento de los equipos	Asegurar el mantenimiento de Los equipos y asegurar su disponibilidad e integridad continuas	si	L3	50%	Se evidencia el **Contrato de Garantía de Equipos con fecha de vencimiento cada 3 años.**
A11.2.5 Retiro de activos	Implementar procesos para el retiro de equipos, información o software no se deben retirar de su sitio sin autorización previa	si	L3	50%	Se ha centralizado la autorización de retirar activos físicos o tecnológicos de su sitio. Manual de procesos Equipos
A11.2.6. Seguridad de equipos y activos fuera de las instalaciones	Aplicar medidas de seguridad a los activos que se encuentran fuera de las	si	L3	50%	Existen un manual para la gestión de activos donde se registra actividades que requieren que los funcionarios saquen los equipos y activos de las instalaciones con aprobaciones del superior

	instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones				
A11.2.7 Disposición segura o reutilización de equipos	verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobre escrito en forma segura antes de su disposición o reúso.	si	L3	50%	Existe un manual Custodia de Medios donde se registra que se debe formatear el PC o laptop para reutilización
A11.2.8 Equipos de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada	si	L3	50%	Por las condiciones de trabajo se pueden presentar momentos en que los equipos estén desatendidos. Sin embargo, hay una política de escritorio limpio
A11.2.9 Política de escritorio limpio y pantalla limpia	Adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información	si	L3	50%	Por las condiciones de trabajo se pueden presentar momentos en que los equipos estén desatendidos. Sin embargo, hay una política de escritorio limpio
A12 SEGURIDAD DE LAS OPERACIONES					
A12.1 Procedimientos operacionales y responsabilidades	**Prevenir y Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.**	SI	L4	50%	
A12.1.1 Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan estar en un repositorio centralizado para fácil consulta	SI	L4	50%	Se encuentra evidencia de todos los procedimientos de operación para la seguridad de la información y los ha dispuesto para su consulta en la intra e internet de la entidad
A12.1.2 Gestión de cambios	Controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de	si	L4	50%	Existe un Comité de cambios para aplicaciones criticas

	información que afectan la seguridad de la información				
A12.1.3 Gestión de capacidad	Hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema	si	L4	50%	Existe un procedimiento de cpacity management y Contrato garantía Hw, Procesos actualizados de capacity Management están actualizados y al dia.
A12.1.4 Separación de los ambientes de desarrollo, pruebas y operación	separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	si	L4	50%	Se evidencia que hay servers para cada una de los ambientes de desarrollo, test y producción. pero están en la misma VLAN de red.
A12.2 Protección contra códigos maliciosos	Asegurar y controlar que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos		L4	50%	
A12.2.1 Controles contra códigos maliciosos	implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	si	L4	50%	Se evidencia que los pc y servers cumplen con la política de instalación de antivirus.
A12.3 Copias de respaldo	Proteger contra la perdida de datos		L4	50%	
A12.3.1 Respaldo de la información	hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	si	L4	50%	Existen políticas de backup diaria, semanales, mensuales y anuales, y políticas de retención a 10 años.
A12.4 Registro y seguimiento	Registrar eventos, conservar y generar evidencia		L4	50%	
A12.4.1 Registro de eventos	elaborar, conservar y revisar regularmente los	si	L4	50%	Se revisa la documentación del proceso de activación del Audit Trail para servers , aplicaciones y PCs activados

	registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.				
A12.4.2 Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado	si	L4	50%	Existen procesos de maker and checker or procesos con aprobaciones para modificar la información
A12.4.3 Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad	si	L4	50%	Se revisa la documentación del proceso de activación del Audit Trail para servers , aplicaciones y PCs activados
A12.4.4 Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo. Registrar el protocolo del server NTP como único	si	L4	50%	**Se evidencia Manual de configuración y servicio NTP**
A12.5 Control de software operacional	**Asegurar la integridad de los sistemas operacionales implementando los controles adecuados**	si	L4	55%	
A12.5.1	Instalación de software en sistemas operativos	si	L4	55%	Se ha centralizado la autorización de hacer uso de programas utilitarios y de instalación de software con el fin de garantizar la seguridad de la información
A12.6 Gestión de la vulnerabilidad técnica	Prevenir e instalar los patches a las vulnerabilidades técnicas		L4	55%	
A12.6.1 Gestión de las vulnerabilidades técnicas	obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para	si	L4	50%	Existe procedimiento escrito en el Manual Administración de seguridad e instalación de VTMs

	tratar el riesgo asociado.				
A12.6.2 Restricciones sobre la instalación de software	establecer e implementar las reglas para la instalación de software por parte de los usuarios.	si	L4	50%	Se ha centralizado la autorización de hacer uso de programas utilitarios y de instalación de software con el fin de garantizar la seguridad de la información
A12.7 Consideraciones sobre auditorias de sistemas de información	Verificar y Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos		L4	50%	
A12.7.1 Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	si	L4	50%	Se cumple con los requisitos de auditoria exigidos para las auditorias de gestión y las auditorías internas a sistemas de gestión
A13 SEGURIDAD DE LAS COMUNICACIONES					
A13.1 Gestión de la seguridad de las redes	Asegurar y gestionar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte		L4	50%	
A13.1.1 Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones	Si	L4	50%	Existe Procedimiento de Administración de la Infraestructura de redes y comunicaciones
A13.1.2 Seguridad de los servicios de red	identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	si	L4	50%	Existe Procedimiento de Administración de la Infraestructura de redes y comunicaciones
A13.1.3 separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.Tener	si	L4	50%	Existe Procedimiento de Administración de la Infraestructura de redes y comunicaciones

	asignación de ACL .				
A13.2 Transferencia de información	Mantener y aplicar controles para la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		L4	50%	
A13.2.1 Políticas y procedimientos de transferencia de información	Tener políticas de encripción para la transferencia de datos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones	si	L4	50%	Se encuentra que la empresa cuenta con herramientas de encripcion para la transmisión como SFTP, winzip, etc.
A13.2.2 Acuerdos sobre transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	si	L4	50%	Se encuentra que la empresa cuenta con herramientas de encripcion para la transmisión como SFTP, winzip, etc.
A13.2.3. Mensajería Electronica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	si	L4	50%	Existe proceso y macro para enviar correo automático sin embargo falta divulgación de esta herramienta.
A13.2.4 Acuerdos de confidencialidad o de no divulgación	identificar, revisar periódicamente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	si	L4	50%	Por las características del negocio y considerando que la información es vital para todos los cargos se han definido condiciones contractuales con las responsabilidades sobre el uso de la información**.**
A14 Adquisición, desarrollo y mantenimiento de sistemas					
A14.1 Requisitos de seguridad de los sistemas de información	Asegurar el control a la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.		L3	50%	
A.14.1.1 Análisis y especificación de requisitos de	para nuevos sistemas de información o para mejoras a	Si	L4	50%	Existe Procedimiento de Administración de la Infraestructura de redes y comunicaciones

seguridad de la información	los sistemas de información existente se adicionar las políticas de seguridad establecidas.				
A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Si	L4	50%	Se encuentra proceso manual de red local vrs pública. el algoritmo se está transmitiendo a 256
A.14.1.3 Protección de transacciones de los servicios de las aplicaciones.	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	Si	L4	50%	Se encuentra proceso manual de red local vrs pública. el algoritmo se está transmitiendo a 256
A14.2 Seguridad en los procesos de Desarrollo y de Soporte	Establecer y asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información	si	L4	50%	Se encuentra proceso manual de red local vrs pública. el algoritmo se está transmitiendo a 256
A.14.2.1. Política de Desarrollo Seguro	establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	Si	L4	50%	Se encuentra ambientes por separo desarrollo, test y producción y manual SDLC
A.14.2.2 Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	si	L4	50%	Se encuentra ambientes por separo desarrollo, test y producción y manual SDLC

A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	Si	L4	50%	Se encuentra ambientes por separo desarrollo, test y producción y manual SDLC
A.14.2.4 Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	si	L4	50%	Se encuentra ambientes por separo desarrollo, test y producción y manual SDLC
A.14.2.5. Principio de Construcción de los Sistemas Seguros.	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	si	L4	50%	Se encuentra ambientes por separo desarrollo, test y producción y manual SDLC
A.14.2.6 Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	si	L4	50%	Se encuentra ambientes por separo desarrollo, test y producción y manual SDLC
A.14.2.7 Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	si	L4	50%	Se encuentra ambientes por separo desarrollo, test y producción y manual SDLC
A.14.2.8 Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad	si	L4	50%	Se encuentra ambientes por separo desarrollo, test y producción y manual SDLC

A.14.2.9 Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	si	L4	50%	Se encuentra ambientes por separo desarrollo, test y producción y manual SDLC
A14.3 Datos de prueba	Asegurar la protección de los datos usados para pruebas uso de proceso de Ofuscación.		L3	50%	
A.14.3.1 Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente tener un proceso de Ofuscación.	si	L3	50%	Se encuentra ambientes por separo desarrollo, test y producción y manual SDLC. Se encuentra en el ambiente de desarrollo y test data ofuscada pero algunos puntos están en texto claro
A15 RELACIONES CON LOS PROVEEDORES					
A15.1 Seguridad de la información en las relaciones con los proveedores	Asegurar y proteger los activos de la organización que sean accesibles a los proveedores.		L3	50%	
A15.1.1. Política de seguridad de la información para las relaciones con proveedores	Procedimiento de SLA y confidencialidad de la información para Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	si	L3	50%	Se mantiene relaciones contractuales con proveedores que tienen acceso a los activos de la organización. Pólizas Contratos
A15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	si	L3	50%	Se mantiene relaciones contractuales con proveedores que tienen acceso a los activos de la organización. Pólizas Contratos
A15.1.3 Cadena de suministro de tecnología de	Los acuerdos con proveedores deben incluir	si	L3	50%	Se mantiene relaciones contractuales con proveedores que tienen acceso a los activos de la organización.

información y comunicación	requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación				Pólizas Contratos
A15.2 Gestión de la prestación de servicios de proveedores	Mantener y proteger el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores		L3	50%	
A15.2.1 Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	si	L3	50%	Se mantiene relaciones contractuales con proveedores que tienen acceso a los activos de la organización
A15.2.2 Gestión del cambio en los servicios de los proveedores	gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la reevaluación de los riesgos.	Si	L3	50%	Se mantiene relaciones contractuales con proveedores que tienen acceso a los activos de la organización
A16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION					
A16.1 Gestión de incidentes y mejoras en la seguridad de la información	Asegurar y establecer un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		L3	50%	
A16.1.1 Responsabilidades y procedimientos	Establecer las responsabilidades y procedimientos	si	L3	50%	Existe una herramienta para la gestión de incidentes sin embargo no tienen la prioridad acorde a la criticidad de la aplicación.

	de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.				
A16.1.2 Reporte de eventos de seguridad de la información	los empleados deben reportar cualquier evento de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	si	L3	50%	Existe una herramienta para la gestión de incidentes sin embargo no tienen la prioridad acorde a la criticidad de la aplicación.
A16.1.3 Reporte de debilidades de seguridad de la información	Los empleados deben reportar cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios	si	L3	50%	Existe una herramienta para la gestión de incidentes sin embargo no tienen la prioridad acorde a la criticidad de la aplicación.
A16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información acorde a la criticidad establecida.	si	L3	50%	Existe una herramienta para la gestión de incidentes sin embargo no tienen la prioridad acorde a la criticidad de la aplicación.
A16.1.5 Respuesta a incidentes de seguridad de la información	dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados cumpliendo el tiempo establecido.	si	L3	50%	Existe una herramienta para la gestión de incidentes sin embargo no tienen la prioridad acorde a la criticidad de la aplicación.
A16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	Tener una base de datos de conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	si	L3	50%	Existe una herramienta para la gestión de incidentes sin embargo no tienen la prioridad acorde a la criticidad de la aplicación.
A16.1.7 Recolección de evidencia	definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que	si	L3	50%	Existe una herramienta para la gestión de incidentes sin embargo no tienen la prioridad acorde a la criticidad de la aplicación.

	pueda servir como evidencia.				
A17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO					
A17.1 Continuidad de Seguridad de la información	Garantizar La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		L3	50%	
A17.1.1 Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	si	L3	50%	Se ha definido un plan de continuidad del negocio para reestablecer la operación critica en situación de crisis
A17.1.2 Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa	si	L3	50%	Se ha definido un plan de continuidad del negocio para reestablecer la operación critica en situación de crisis
A17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	verificar intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	si	L3	50%	Se ha definido un plan de continuidad del negocio para reestablecer la operación critica en situación de crisis. Manual del Plan de Continuidad del Negocio
A17.2 Redundancias	Asegurar y garantizar la disponibilidad de instalaciones de procesamiento de información		L3	50%	
A17.2.1 Disponibilidad de instalaciones de procesamiento de información	Control: Procedimiento para redundancia a las instalaciones de procesamientos de información para cumplir los requisitos de disponibilidad.	si	L3	50%	Se ha definido un plan de continuidad del negocio para reestablecer la operación critica en situación de crisis. Manual del Plan de Continuidad del Negocio

A18 CUMPLIMIENTO					
A18.1 Cumplimiento de requisitos legales y contractuales	Implementar procedimientos para evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad		L5	50%	
A18.1.1 Identificación de la legislación aplicable	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	si	L5	50%	Se encuentra Manual de políticas para el tratamiento de datos personales
A18.1.2 Derechos propiedad intelectual (DPI)	implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	si	L5	50%	Se encuentra Manual de políticas para el tratamiento de datos personales
A18.1.3 Protección de registros	Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	si	L5	50%	Se encuentra Manual de políticas para el tratamiento de datos personales
A18.1.4 Privacidad y protección de información de datos personales	asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes,	si	L5	50%	Se encuentra Manual de políticas para el tratamiento de datos personales

	cuando sea aplicable.				
A18.1.5 Reglamentación de controles criptográficos	Utilización de controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	si	L5	50%	Se encuentra manual , es claro el algoritmo criptográfico que están usando256 bits de encripcion
A18.2 Revisiones de seguridad de la información	Revisar y Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.		L5	50%	
A18.2.1 Revisión independiente de la seguridad de la información	revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	si	L5	50%	cuenta con procesos formales de auditoria a la gestión de la entidad
A18.2.2 Cumplimiento con las políticas y normas de seguridad	deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	si	L5	50%	Cuenta con un manual de Administración de Seguridad
A18.2.3 Revisión del cumplimiento técnico	revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	si	L5	50%	Cuenta con un manual de Administración de Seguridad

Table 16. Nivel de Madurez de la Empresa

No.	Aspectos requeridos	Calificación Actual	Calificación Proyectada	Calificación Ideal	Evaluación Efectividad de Control
4	Contexto de la organización	60	70	100%	Efectivo
5	Liderazgo	50	70	100%	Efectivo
6	Planificación	55	70	100%	Efectivo
7	Soporte	51	70	100%	Efectivo
8	Operación	62	70	100%	Efectivo
9	Evaluación del desempeño	60	70	100%	Efectivo
10	Mejora	60	70	100%	Efectivo

Table 17ª. Aspectos requeridos ISO27001

18.4 Presentación de Resultados

Luego de revisar los resultados de madurez se muestra en la siguiente grafica los porcentajes:

- El 10% tiene un porcentaje Optimo correspondiente al dominio A18
- El 31% tiene un porcentaje Gestionado correspondientes a los dominios: A9, A12, A13, A14.
- Y el 59% correspondiente a un proceso definido o Efectivo para los demás dominios.

Nivel Madurez	No. Controles
Inexistente L0	**0**
Inicial / Ad-hoc L1	**0**
Reproducible, pero intuitive L2	**0**
Proceso definido L3	67
Gestionado y medible L4	36
Optimizado L5	11
TOTAL	114

Table 18. Resultados del nivel de madurez

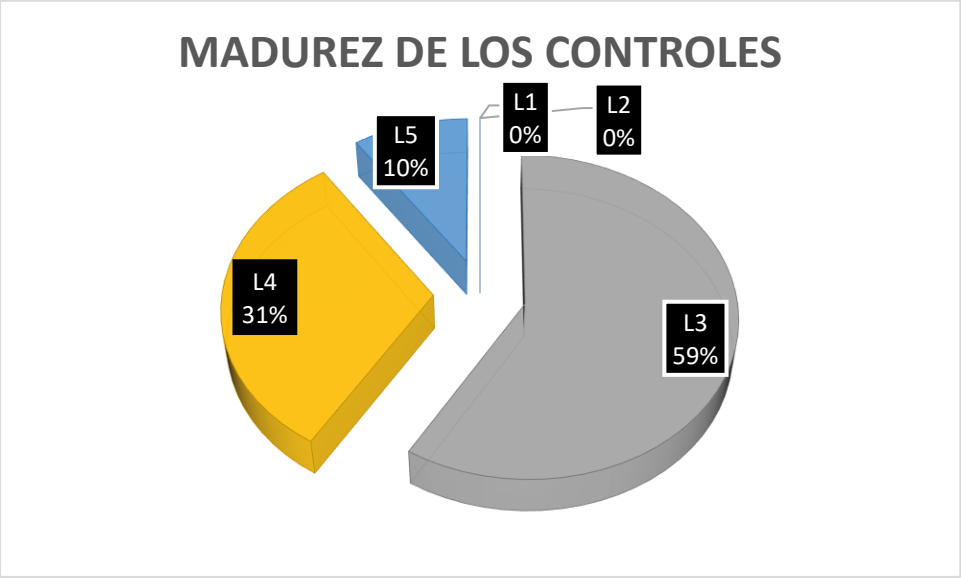

Figure 19. Porcentaje Nivel de Madurez en la empresa

Se ve gran avance en la madurez de todos los controles se presenta la siguiente gráfica.

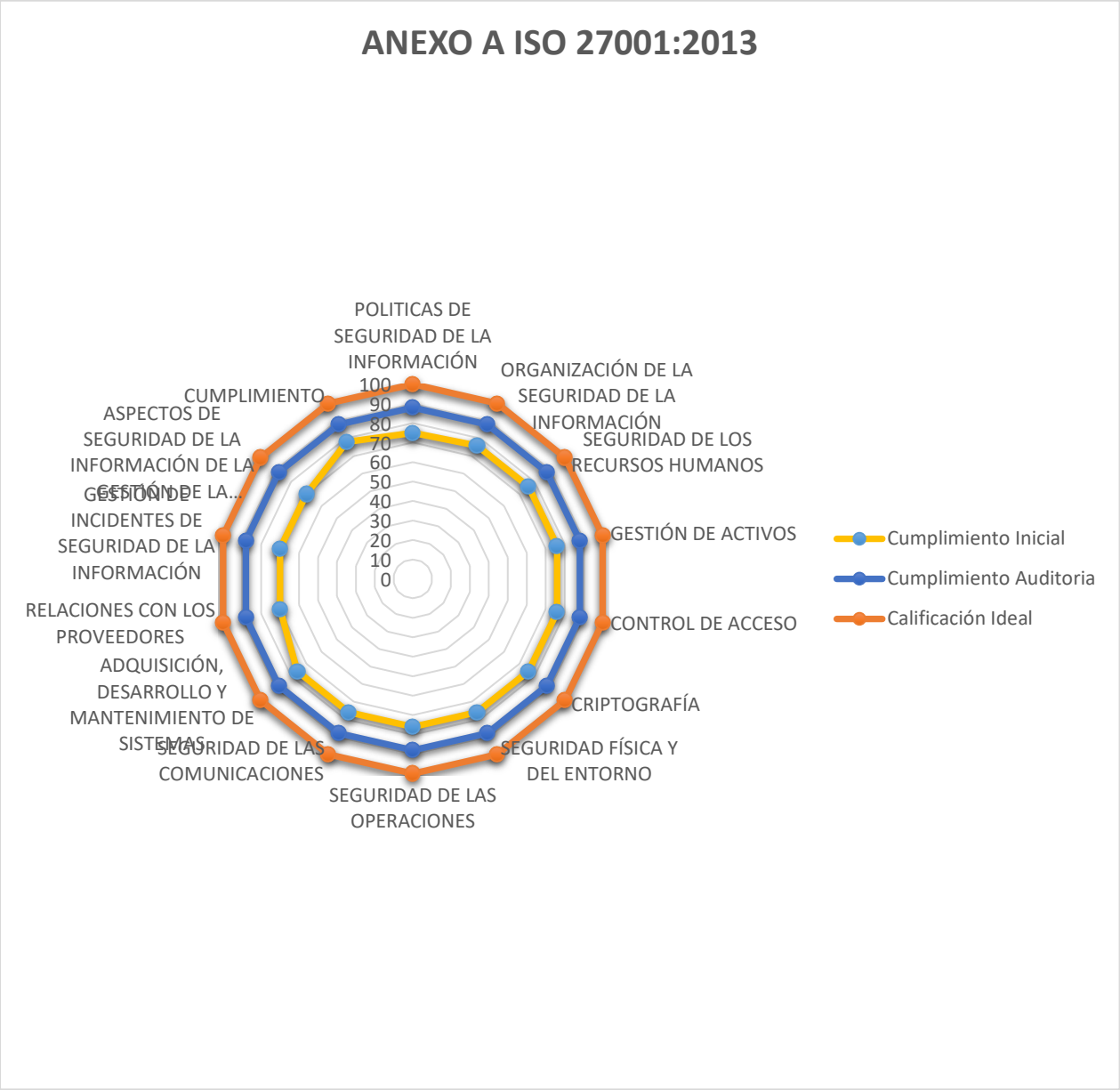

Figure 20. Grafico Radar Nivel de Madurez en la empresa

18.5 Informe de Auditoria

Informe General		
Organización	**Digital Signage LRDXXX**	
Tipo de Auditoria	**Auditoria de Cumplimiento**	
Fecha de Inicio	Nov23 2018	
Auditor	Diana Pulecio	
Objetivo de la Auditoria	Evaluar la madurez de la seguridad de la información planteados por la ISO/IEC:27002:2013 y el cumplimiento a la ejecución de los activos para cada uno de los controles implementados	
Alcance	Se evaluó la disponibilidad, integridad y confidencialidad de la información y recursos para poner en producción el producto del marketing wall.	
Criterios Identificados o de evaluación	▪ Correspondiente a la publicidad de cada cliente antes de que sea pública debe cumplir con las políticas de confidencialidad en el desarrollo del producto. ▪ Todos los contratos y garantías deben estar vigentes. ▪ Capacitaciones deben estar ejecutadas acorde al plan. ▪ Documentación actualizada para cada uno de los procesos. ▪ Políticas de backup y monitoreo reportes actualizados.	
Fases de Auditoria	▪ Recolección de la Información: Se recolecto la información de políticas, procedimientos, reportes, informes y procesos implantados. ▪ Ejecución de Pruebas documentadas: Revisión y verificación de cada una de las pruebas recolectadas ▪ Análisis de la Información: Se determina el nivel de cumplimiento.	

	▪ Elaboración y presentación de resultados: Informe de Auditoria dirigido a la alta gerencia.
Relación de Hallazgo y Recomendaciones	**Puntos Fuertes:** ▪ La Alta dirección tiene el compromiso y está comprometida con el SGSI de la compañía. ▪ Cuenta con un comité de seguridad interno que puede da gestión a los diferentes temas del SGSI. **Oportunidades de Mejora** ▪ Incentivar al personal tener más actitud de pertenencia hacia la empresa para poder retener el talento humano. ▪ Crear jornadas de capacitación y más publicidad en el control de Información y escritorio limpio.
Plan de Mejoramiento	Digital Signage LRD XXX debe ajustar el plan de mejoramiento que se encuentra vigente, con acciones correctivas y preventivas. Así mismo se estará evaluando estas acciones para medir la efectividad de las mismas.
Reviso: Comité interno Seguridad Elaboro: Diana Pulecio	Aprobó: Comité general de Auditoria.

Table 19. Informe de Auditoria Cumplimiento

18.6 Cuadro de No Conformidades - Encontradas

Tipo : Menor

Ref. Fecha: Nov28 2018	Descripción de la No Conformidad	Control	Dominio	Acción Correctiva	Responsable de la acción Correctiva
Nc-01	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	6.1.5 Seguridad de la información en la gestión de proyectos.	A.6 Aspectos Organizativos de la seguridad de la Información	Definir una política en el manejo de proyectos que consolide todos los proyectos en la seguridad de la información.	PMO y alta gerencia

Table 20. Cuadro(1) de No conformidades Menor

Ref. Fecha: Nov28 2018	Descripción de la No Conformidad	Control	Dominio	Acción Correctiva	Responsable de la acción Correctiva
Nc-02	Adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	**A11.2.9** Política de escritorio limpio y pantalla limpia	A.11 Equipos	Aunque la política está establecida no está difundia entre los empleados	Control área y alta gerencia

Table 21. Cuadro(2) de No conformidades Menor

Ref. Fecha: Nov28 2018	Descripción de la No Conformidad	Control	Dominio	Acción Preventiva	Responsable de la acción Correctiva
Nc-03	Hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	Gestion de capacidad	A.12.1 Procedimientos operacionales y responsabilidades	Se recomienda disminuir el umbral de alarmas que está configurado actualmente	Capacity management y alta gerencia

Table 22. Cuadro(3) de No conformidades Menor

Tipo Mayor

Ref. Fecha: Nov28 2018	Descripción de la No Conformidad	Control	Dominio	Acción Correctiva	Responsable de la acción Correctiva
Nc-05	los empleados deben reportar cualquier evento de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. .	Reporte de eventos de seguridad de la información	A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Aunque se cuenta con una herramienta de gestión todos los incidentes tienen prioridad bajar lo cual esta impactando los tiempos de respuesta al SLA	Indicident management, alta genrecia

				establecido(Service level agreement)	

Table 23. Cuadro(4) de No conformidades Mayor

18.7 Resultados

El resultado de la auditoria fue satisfactorio. Mostrando los siguientes resultados a la alta gerencia:

cuatro hallazgos:

- Tres (3) son hallazgos de no conformidad menor con acciones correctiva.
- Un (1) hallazgo preventivo.
- Un (1) hallazgo de tipo mayor con acción correctiva.

Dominios	**Mayor**	**Menor**
A5. Políticas de seguridad		
A6 Aspectos Organizativos de la seguridad de la Información		X
A7 SEGURIDAD DE LOS RECURSOS HUMANOS		
A8 GESTION DE ACTIVOS		
A9 CONTROL DE ACCESO		
A10.CRIPTOGRAFIA		
A11 SEGURIDAD FISICA Y DEL ENTORNO		X
A12 SEGURIDAD DE LAS OPERACIONES		X
A13 SEGURIDAD DE LAS COMUNICACIONES		
A14 Adquisición, desarrollo y mantenimiento de sistemas		
A15 RELACIONES CON LOS PROVEEDORES		
A16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	X	
A17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO		
A18 CUMPLIMIENTO		
Total	**1**	**3**

Table 24. Resultados de No conformidad

18.8 Conclusiones

LA compañía está implementando los controles necesarios para garantizar un manejo seguro del SGSI.

Se cuenta con el apoyo de la alta gerencia la cual apoya el plan de implementación y mejoramiento del SGSI para proteger los activos de la compañía.

El nivel de Madurez de la empresa se encuentra entre un L3 y L4 la cual significa que es un nivel Efectivo o definido y Gestionado. Reflejando el mejoramiento de cada una de las políticas y procesos implantadas debido a los diferentes proyectos ejecutados y de esta forma minimizando las falencias y el riesgo.

Aunque se encontró una (1) no conformidad mayor y tres (3) no conformidad menor, la alta gerencia está comprometida con el plan Director del SGSI, siguiendo el plan de mejora en cada uno de los controles correspondiente a los dominios establecidos para proteger la integridad, confidencialidad y disponibilidad de la información.

19 PRESENTACIÓN DE RESULTADOS Y ENTREGA DE INFORMES

19.1 Conclusiones del Proyecto

Etapa Inicial

- Se encuentraron políticas y procedimientos obsoletas para la empresa**.**
- No hay procedimientos alternativos para escenarios de desastres. Cambios controlados no existen, certificados deshabilitados. Afectando al usuario y generando multas y costos adicionales.

Etapa de Implementación

- Se elaboró una serie de documentos que mitiga el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.
- En el análisis de riesgo se evidenció que el Activo Personal o Recurso Humano Interactúan con todos los activos identificados teniendo un valor significativo. Donde el tipo de activo Software y Datos de Información en caso de una amenaza tiene un impacto muy alto a la organización.
- Se diseñó e implementó tres (3) proyectos que fortalecieron las políticas de seguridad de la información, la continuidad del negocio y control de software que fueron los mecanismos de control a fin de minimizar el riesgo existente.
- plan de Auditoria, se estableció que se auditará el 33% de los controles, el siguiente año el 33%, y el tercer y último año, se revisarán el resto de controles.
- Durante la auditoría de Cumplimiento el resultado fue satisfactorio encontrando a la empresa un L3 y L4. Reflejando el mejoramiento de cada una de las políticas y procesos implantados debido a los diferentes proyectos ejecutados y de esta forma minimizando las falencias y el riesgo.
- La alta gerencia está comprometida con el plan Director del SGSI, siguiendo el plan de mejora en cada uno de los controles correspondiente a los dominios establecidos para proteger la integridad, confidencialidad y disponibilidad de la información.

19.2 INTRODUCCIÓN

Llegados a este punto debéis haber realizado los diferentes pasos necesarios para la puesta en funcionamiento del Plan Implementación de un SGSI. Es el momento de recopilar la información y darle el formato pertinente para su presentación.

19.3 OBJETIVOS DE LA FASE

Resumen ejecutivo: breve descripción en que se incluya la motivación, enfoque del proyecto y principales conclusiones extraídas

19.4 Entregables

- Presentación Resumen Ejecutivo
- Presentación tratamiento de riesgo
- Presentación a la dirección.

20 Glosario

Acción correctiva

(Inglés: Corrective action). Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Acción preventiva

(Inglés: Preventive action). Medida de tipo pro-activo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.

Activo

(Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza

(Inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos

(Inglés: Risk analysis). Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo

Declaración de aplicabilidad

(Inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Impacto

(Inglés: Impact). El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.

Integridad

(Inglés: Integrity). Propiedad de la información relativa a su exactitud y completitud.

ISO/IEC 27001

Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

ISO/IEC 27002

Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.

No conformidad

(Inglés: Nonconformity). Incumplimiento de un requisito.

Riesgo

(Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

PDCA

Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.

Seguridad de la información

(Inglés: Information security). Preservación de la confidencialidad, integridad y disponibilidad de la información.

Selección de controles

(Inglés: Control selection). Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI

(Inglés: ISMS). Véase: Sistema de Gestión de la Seguridad de la Información.

Sistema de Gestión de la Seguridad de la Información

(Inglés: Information Security Management System). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Stakeholder

Véase: Parte interesada.

Vulnerabilidad

(Inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Alcance de la Auditoría: Extensión y límites de una auditoría.
Nota: El alcance de la auditoría incluye generalmente una descripción de las ubicaciones, las unidades de la organización, las actividades y los procesos, así como el período de tiempo cubierto.

Auditado: Organización que es auditada.

Auditor: Persona que lleva a cabo una auditoría.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría.

Nota 1: Las auditorías internas, denominados en algunos casos auditorías de primera parte, se realizan por la organización, o en nombre, para la revisión por la Dirección y para otros propósitos internos. Pueden formar la base para una autodeclaración de conformidad de una organización. En muchos casos, particularmente en organizaciones pequeñas, la independencia puede demostrarse al estar libre el auditor de responsabilidades en la actividad que se audita o al estar libre del sesgo o conflicto de intereses.

Nota 2: Las auditorías externas incluyen auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por partes que tienen un interés en la organización, tal como los clientes, o por otras personas en su nombre. Las auditorías de tercera parte se llevan a cabo por organizaciones auditoras independientes y externas, tales como las autoridades reglamentarias o aquellas que proporcionan la certificación.

Cliente de la Auditoría: Organización o persona que solicita una auditoría.
Nota 1: En el caso de auditoría interna, el cliente de la auditoría también puede ser el auditado o la persona que gestiona el programa de auditoría. Las solicitudes de una auditoría externa pueden provenir de fuentes como autoridades reglamentarias, partes contratantes o clientes potenciales.

Competencia: Capacidad para aplicar conocimientos y habilidades para alcanzar los resultados pretendidos.

Conclusiones de la Auditoría: Resultado de una auditoría, tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría.

Criterios de Auditoría: Conjunto de políticas, procedimientos o requisitos usados como referencia frente a la cual se compara la evidencia de la auditoría.

Equipo Auditor: Uno o más auditores que llevan a cabo una auditoría, con el apoyo si es necesario, de expertos técnicos.
Nota 1: A un auditor del equipo se le designa como líder del mismo.
Nota 2: El equipo auditor puede incluir auditores en formación.

Evidencia de la Auditoría: Registros, declaraciones de hechos o cualquier otra información que son pertinentes para los criterios de auditoría y que son verificables.
Nota: La evidencia de la auditoría puede ser cualitativa o cuantitativa.

Experto Técnico: Persona que aporta conocimientos o experiencia específicos al equipo auditor.
Nota 1: El conocimiento o experiencia específicos son los relacionados con la organización, el proceso o la actividad a auditar, el idioma o la orientación cultural.
Nota 2: Un experto técnico no actúa como un auditor en el equipo auditor.

Hallazgos de la Auditoría: Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría.
Nota 1: Los hallazgos de auditoría indican conformidad o no conformidad.
Nota 2: Los hallazgos de auditoría pueden llevar a la identificación de oportunidades de mejora o al registro de mejores prácticas

No Conformidad: Incumplimiento de un requisito.

Observador: Persona que acompaña al equipo auditor pero que no audita.
Nota 1: Un observador no es parte del equipo auditor y no influye ni interfiere en la realización de la auditoría.
Nota 2: Un observador puede designarse por el auditado, una autoridad reglamentaria u otra parte interesada que testifica la auditoría.

Plan de Auditoría: Descripción de las actividades y de los detalles acordados de una auditoría.

Programa de la Auditoría: Detalles acordados para un conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico.

Acción Correctiva: Acción tomada para eliminar la causa de una No Conformidad y evitar que ésta vuelva a ocurrir.
Nota 1: Puede haber más de una causa para una no conformidad.

Corrección: Acción tomada para eliminar una no conformidad detectada.

Auditoría Extraordinaria: Auditoría realizada fuera del Programa Anual de Auditoría.

Oportunidad de Mejora: Falla aislada o esporádica en el contenido o implementación del sistema de gestión, o cualquier situación en la que pueda mejorarse algún aspecto del sistema.

Reunión: Reunión del equipo auditor en la cual se analizan las evidencias de auditoría, se determinan y clasifican los hallazgos de la Auditoría, teniendo el auditor líder la responsabilidad final sobre estos resultados.

Aceptación de riesgo: Decisión informada de asumir un riesgo concreto.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

Confiabilidad de la Información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: La información debe ser accedida sólo por aquellas personas autorizadas. La revelación no autorizada de la información implica un grave impacto en términos económicos, de su imagen y ante sus clientes.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.
Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros: pérdida de reputación, implicaciones legales, etc.

Inventario de Activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud. La falta de integridad de la información puede exponer a la empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas económicas.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Probabilidad: Medida para estimar la ocurrencia del riesgo.

Propietario del riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Recursos de tratamiento de la información: Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Selección de controles: Proceso de elección de las salvaguardas que aseguren la reducción de los riesgos a un nivel aceptable.

Sistema de Gestión de la Seguridad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.
Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

21 BIBLIOGRAFIA

ISO/IEC 27002:2013, Information Technology. Security Techniques. Code of Practice for Information Security Controls.

GTC-ISO/IEC 27003:2012, Tecnología de la información. técnicas de seguridad. Guía de implementación de un sistema de gestión de la seguridad de la información.

ISO/IEC 27004:2009, Information Technology. Security Techniques. Information Security Management. Measurement.

ISO/IEC 27005:2011, Information Technology. Security Techniques. Information Security Risk Management.

NTC-ISO 31000:2011, Gestión del riesgo. Principios y directrices.

ISO/IEC Directives, Part 1, Consolidated ISO Supplement. Procedures Specific to ISO, 2012

https://advisera.com/27001academy/es/herramienta-gratuita-analisis-de-brecha-para-iso-27001/
https://www.pmg-ssi.com/2015/02/iso-27001-el-modelo-de-madurez-de-la-seguridad-de-la-informacion/ http://www.iso27000.es/herramientas.html

Controles

http://www.iso27000.es/download/ControlesISO27002-2013.pdf

http://www.dintel.org/web/Eventos/CongresosEspana/Observatorio/2010/ponencias/quevedo.pdf
https://protektnet.com/servicios/cumplimiento-normativo/sistema-de-gestion-de-seguridad-de-informacionisoiec-

270012013/?gclid=Cj0KCQjw_7HdBRDPARIsAN_ltcLIsvdGM8hlDxhFB6Fb907skByx4rWSGDkdMeewjeVjPeIlzgtlj6caAgLoEALw_wcB

http://www.novasec.co/en/blog/62-gestion-integral-de-la-seguridad-de-la-informacion
Normas

http://www.sisben.gov.co/Documents/Informaci%C3%B3n/Leyes/LEY%20TRATAMIENTO%20DE%20DATOS%20-%20LEY%201581%20DE%202012.pdf

Seguridad de las comunicaciones y las TIC

https://www.youtube.com/watch?v=Tm5AeM7Kp_w

Controles de Seguridad

https://www.youtube.com/watch?v=ymDHe2ca1Ks

http://www.iso27000.es/glosario.html