Empresa de Digital Signage LRD XXX

Diana Marcela Pulecio Lara

Diana Marcela Pulecio Lara
Master Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Director: Antonio José Segovia Henares
Universitat Oberta de Catalunya
Diciembre 2018

Contenido Presentación Dirección

1. Introducción
2. Contexto de la empresa
3. Estructura Jerárquica
4. Alcance del Proyecto
5. Enfoque del Proyecto
6. Requisitos de Seguridad
7. Gap Análisis Inicial
8. Conclusiones
9. Sistema de Gestion Documental
10. Conclusiones Gestión documental
11. Análisis de Riesgo
12. Conclusiones Análisis de Riesgo
13. Propuesta de Proyectos
14. Conclusiones
15. Auditoria de Cumplimiento
16. Conclusiones Auditoria Cumplimiento
17. Conclusiones del proyecto

Introducción

Este documento presenta el resumen ejecutivo de la implementación de un plan de director de seguridad ISO 27001:2013 para la empresa Digital Signage LRDXXX

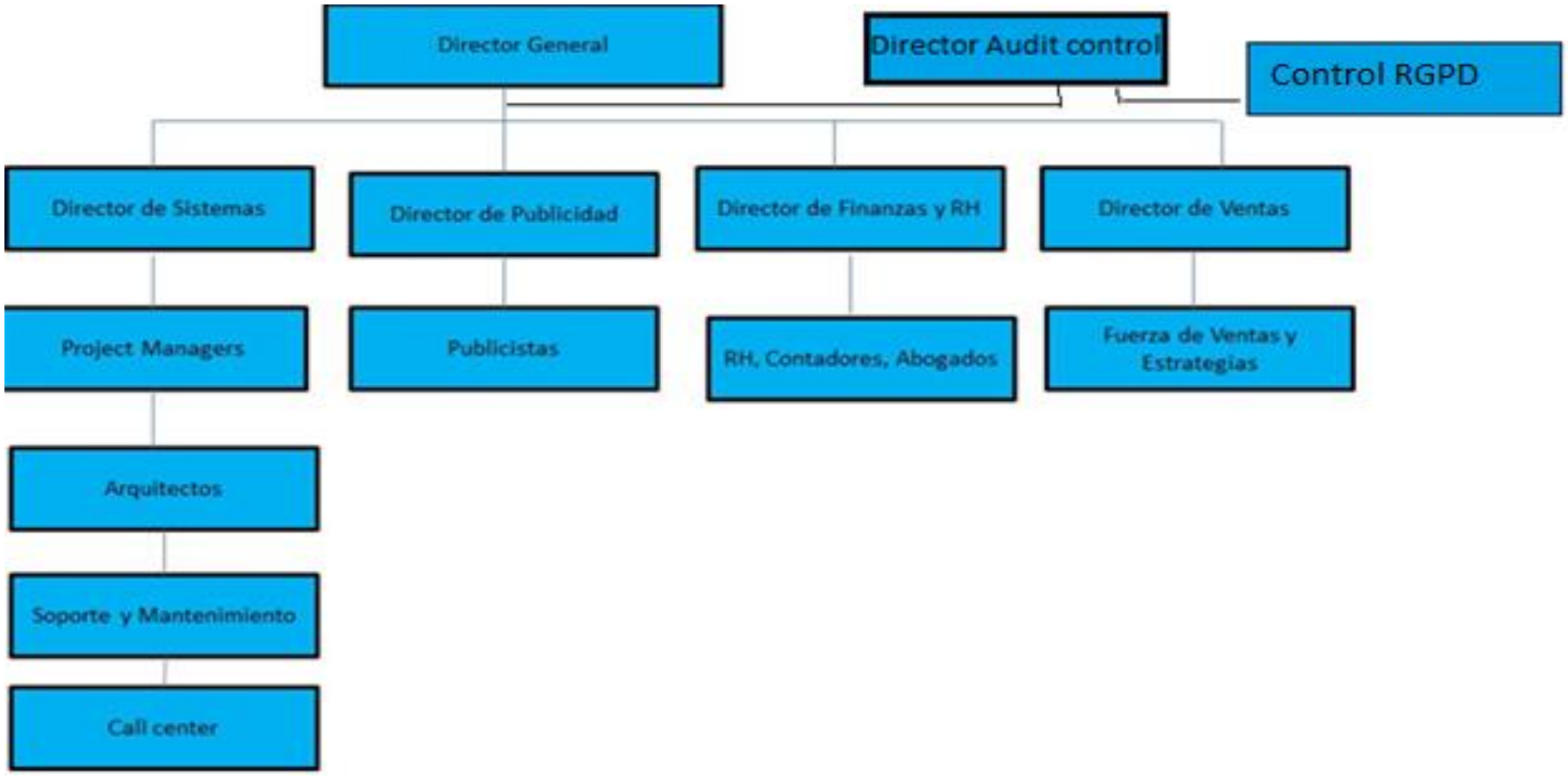
A continuación se describe el estado actual, motivación del Proyecto y propuesta planteada.

Contexto de la empresa

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 ha estado pagando multas por el no cumplimiento de normas legales. Surgiendo la motivación de implementar el plan director de seguridad la cual se pretende optimizar procesos, minimizar riesgos a implementaciones y evitar inversiones innecesarias.
- En este Proyecto es importante proteger la información valiosa y aquellos activos que están asociado a nuestros clientes,nuestras ventas,nuestro personal y operaciones .
- Obteniendo una certificación la compañía pueden tener mayor confianza en su capacidad para gestionar la seguridad de la información, y por ende ayudará a asegurar a sus socios, clientes, y accionistas con quien hacen negocios.

Estructura Jerárquica / organigrama



Plan Director de Seguridad

Ilustración 1: Implantando un Plan Director de Seguridad

https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

Alcance

El alcance 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.

Estos son activos importantes que tienen un valor y requiere en consecuencia una protección adecuada. Digital Signage LRD XXX necesita establecer controles necesarios para las amenazas, vulnerabilidades que surgen en el día a día.

- La seguridad de la información se caracteriza aquí como la preservación de:
  - su **confidencialidad**, asegurando que sólo quienes estén autorizados pueden acceder a la información;
  - su **integridad**, asegurando que la información y sus métodos de proceso son exactos y completos.
  - su **disponibilidad**, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

Enfoque del Proyecto:

- El Proyecto está alineado bajo el estandar ISO/IEC 27001+ISO/IEC 27002. Se utiliza la metodología de Análisis y Gestión de Riesgos MAGERIT.
- Actividades principales del plan director:

➢ Análisis diferencial contra la ISO/IEC 27002 para conocer el estado previo.

➢ Identificación de los activos relacionados con los procesos, actividades y servicios relacionados con la información.

➢ Valoración de los activos identificados.

➢ Análisis de amenazas de los activos respecto a las cinco dimensiones de seguridad.

➢ Análisis del nivel de riesgo respecto a los activos, su valoración y sus amenazas.

➢ Proposición de proyectos para la mitigación de los riesgos identificados como críticos.

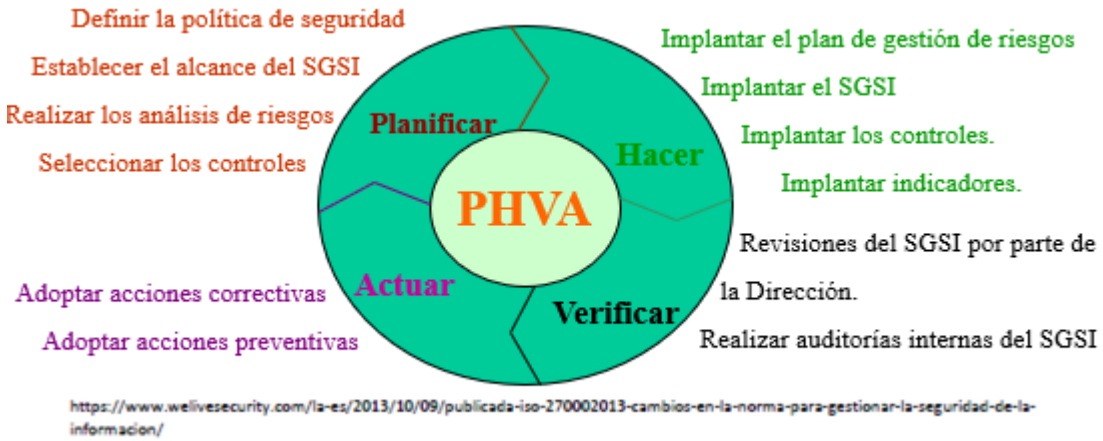
➢ Realización de una auditoría de cumplimiento tras la implementación de los proyectos.

Requisitos de Seguridad

- Se inició con una valoración de los riesgos de cada uno de los activos.
- Se identificarón las amenazas . "**Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización."
- Se evaluaron las vulnerabilidades y la probabilidad de su ocurrencia. "**Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas.". **"Probabilidad:** Medida para estimar la ocurrencia del riesgo. "
- Se estimó su posible impacto. "**Impacto**: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-."
- Se revisó los contratos, SLA (service level agreement) y requisitos legales que deben cumplir.
- Estrategias del negocio que esten alineadas a este plan.

Requisitos de Seguridad

EL SGSI basado en un enfoque de riesgos del negocio, adopta el siguiente modelo



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

GAP ANÁLISIS

FASE 1: Análisis cumplimiento de los requerimientos de la ISO 27001 numerales 4-10 /Controles del Anexo A ISO/IEC 27002

- **Análisis Inicial**

	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

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

Conclusiones

- Se encuentra que algunas políticas y procedimientos no son claras y algunas son obsoletas para la empresa
- No hay procedimientos alternativos para escenarios de desastres, aunque se encuentra un Data Center alterno pero las versiones instaladas están desactualizadas.
- Cambios controlados no existen, certificados deshabilitados.

- Estos son los aspectos mas relevantes para el Desarrollo de proyectos e implementación de la misma, impactando a los dominios :

✓Políticas de Seguridad
✓Organización de la seguridad
✓Gestión de Activos
✓Criptografía
✓Gestión de acceso
✓Adquisición, Desarrollo y mantenimiento de sistemas, gestión de incidentes y cumplimiento.

El plan director esta enfocado alcanzar la meta de cumplimiento del 70%

SISTEMA DE GESTION DOCUMENTAL

Se establece 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.

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.

A continuación las políticas establecidas:

Politicas de Seguridad	Definición y políticas desarrolladas
Roles y responsabilidad	• Definición de Roles • Políticas Uso de Internet • Política Uso apropiado de los recursos • Política Transferencia de Archivos por Internet y Material de Copyright • Política de Comunicaciones Electrónicas (Cifrado de Información Derechos de Privacidad, Privacidad en las Comunicaciones, Monitoreo d los Mensajes, Datos estadísticos, Reenvío de mensajes o Información. • Política de Contraseñas • Política Estándares de desarrollo de aplicaciones • Respaldo • Política Almacenamiento Externo (medios, retención) • Política Uso Aceptable del Computador (software instalado, antivirus propiedad intelectual) • Política Wan network . • Política redes inalámbricas /Wifi security. • Política Gestión de Proveedores. • Política Gestión de Problemas • Política administración de seguridad (Control de acceso).
Procedimiento de Auditorías Internas	En este plan de Auditoria, se establecerá que se auditará el 33% de los controles, e siguiente el 33%, y el tercer y último año, se revisarán el resto de controles.
Gestión de Indicadores	Se crearon estos indicadores de gestión orientados en la medición de efectividad eficiencia y eficacia de los componentes de implementación y gestión definidos e el modelo de operación del marco de seguridad y privacidad de la información. • **Indicador 1.** Activos de Información. • **Indicador** 2. Capacitaciones al año al personal de la organización. • **Indicador** 3. Revisiones de auditoría Interna en el Año • **Indicador** 4. Proceso de Parcheo y actualizaciones del sistema • **Indicador** 5. Configuración y cierre de puertos inseguros del siste • **Indicador** 6. Incidentes resueltos . • **Indicador 7**. Control Acceso • **Indicador 8**. Proceso de envío información encriptada
Procedimiento Revisión por Dirección	El procedimiento inicia con la programación de la fecha de la revisión por l dirección y finaliza con el seguimiento, compromisos establecidos en el Plan d Mejoramiento.
Gestión de Roles y Responsabilidades	Definición de roles y responsabilidades a nivel SGSI
Metodología de Análisis de Riesgo	La metodología MAGERIT se aplicó a este proyecto contemplando: Identificación d activos de información, amenazas, vulnerabilidades, riesgos y control de los nivele aceptables y tratamiento de riesgo.
Declaración de aplicabilidad	

Conclusiones

- 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.

Análisis de Riesgo

Se determina los controles a aplicar, las acciones y tratamientos a realizar de acuerdo a los objetivos establecidos.

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

Se hará uso de la siguiente escala de cada uno de las dimensiones del activo:

Disponiblidad: Propiedad de los activos en que se tiene acceso cuando se requiera.

Integridad: Propiedad de los activos en que el activo de información no ha sido alterada de manera no autorizada.

Confidencialidad: Propiedad de los activos en que la información no ha sido revelada.

Autenticidad: Propiedad en que una entidad dice quien dice ser .

Trazabilidad: Propiedad o característica consitente en que las actuaciones de una entidad pueden ser imputadas exclusiamente a dicha entidad.

Análisis de Riesgo

Impacto= valor X degradación

Riesgo = Impacto X probabilidad o frecuencia

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

Salvaguardas: permiten hacer frente a las amenazas

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

Análisis de Riesgo

Se analizaron las siguientes amenazas vrs Activos : [N] Desastres naturales, [I] De origen industrial, [E] Errores y fallos no intencionados, [A] Ataques intencionados

Amenaza		Activo	recuenci	I	C	D	T	Valo	Impacto = Valor X Frecue	Riesgo= Frecuencia X impacto	Salvaguarda	Proyectos asignados
[E.2] Errores del administrador	[D] datos / información	Autenticación-Ldap y SSO	1	70%	90%	100%	90%	8	8	8	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	TFM_ANEXO13_Proyecto_Software.pdf TFM_ANEXO12_Proyecto_COB.pdf
		Audit Trail o logs de eventos	1	45%	60%	50%	60%	8	8	8		
		Control de Usuarios	1	60%	70%	50%	70%	8	8	8		
		Registro de Incidentes de seguridad CIRT	1	80%	85%	90%	80%	8	8	8		
	[keys] claves criptográficas	Aplicaciones Web	1	70%	80%	100%	80%	7	7	7		
		Aplicaciones Web para el manejo de operación	1	50%	70%	100%	90%	7	7	7		
	[S] servicios	Video Conference	1	40%	40%	80%	80%	7	7	7		
		Gestión de Privilegios	1	90%	60%	80%	80%	7	7	7		
		Servicio de Internet para invitados	1	40%	40%	40%	40%	7	7	7		
	[SW] aplicaciones (software)	Aplicación Robot mesa de ayuda	1	80%	85%	90%	90%	8	8	8		
		Aplicación Monitoreo de	1	40%	40%	40%	40%	8	8	8		
		Control de Acceso	1	70%	80%	100%	80%	8	8	8		
		Aplicaciones Web	1	70%	80%	100%	80%	8	8	8		
		Aplicaciones Web para el manejo de operación	1	70%	80%	100%	80%	8	8	8		
		CRM	1	40%	40%	90%	80%	8	8	8		
	[Media] soportes de información	SAN	1	70%	80%	100%	80%	7	7	7		
		NAS	1	70%	80%	100%	80%	7	7	7		
		Plataforma Backup	1	70%	80%	100%	80%	7	7	7		
	[COM] redes de comunicaciones	Red LAN y ACLs	1	70%	80%	100%	80%	7	7	7		
		RED WAN y ACLs	1	70%	80%	100%	80%	7	7	7		
		RED WIFI corporativa - Manejo con Airwatch	1	60%	70%	70%	80%	7	7	7		
		Cuarto de Comunicación or Tech room	1	80%	90%	100%	80%	7	7	7		
											Protección de los Servicios	

Análisis de Riesgo

	Identificador	Nombre del Activo	Tipo de Activo	Contenedor	Propietario del Riesgo	Propietario del Activo	Valor	Degradacion	Probabilidad o Frecuencia	IMPACTO= Valor X Degradacion	Riesgo =Probabilidad X Impacto	Nivel de Riesgo
	Equip_Playe	Players	Equipos Informáticos	Players	Manager TI	Sociedad Patrimonial Digital Signage LRD XXX	4	20%	1	0.8	0.8	Muy Bajo- Tolerable
	Equip_wall	Pantallas de Marketing Wall	Equipos Informáticos	Pantallas	Manager TI	Sociedad Patrimonial Digital Signage LRD XXX	10	40%	1	4	4	Medium- Riego Aceptable
Datas/Informacion	Datos_Aut	Autenticación-Ldap y SSO	Datos/Información	Directorio activo	Manager Tecnología	Empleados	9	90%	1	8.1	8.1	Mul Alto - No Tolerable
	Datos_Blo	Datos Biométricos	Datos/Información	Directorio activo	Manager Tecnología	Data PII.	9	100%	1	9	9	Mul Alto - No Tolerable
	Datos_Aud	Audit Trail o logs de eventos	Datos/Información	Logs	Manager Tecnología	Data PII.	5	80%	1	4	4	Medium- Riego Aceptable
	Datos_Usu	Control de Usuarios	Datos/Información	Base de datos	Manager Tecnología	Data PII.	8	80%	1	6.4	6.4	Mul Alto - No Tolerable
	Datos_Reg	Registro de Incidentes de seguridad CIRT	Datos/Información	Base de datos	Manager Tecnología	Sociedad Patrimonial Digital Signage LRD XXX	7	70%	1	4.9	4.9	Medium- Riego Aceptable
	Datos_Man	Manuales de procesos y	Datos/Infor	File Server	Manager	Sociedad Patrimonial	7					

Conclusiones

- 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.
- 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.

Conclusiones

- 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.

Propuesta de Proyectos

Estos proyectos planteados fueron el resultado de agrupar un conjunto de recomendaciones identificadas en la fase de análisis de riesgos para facilitar su ejecución y en la mejora en la gestión de procesos y tecnologías presentes en la organización analizada.

Se presenta estos tres proyectos:

- Proyecto1 Políticas de seguridad de la información.
- Proyecto2 Continuidad del negocio.
- Proyecto3 Control software.

Proyecto1. Políticas de seguridad de la información

<table>
<tr><th colspan="2">Proyecto1. Políticas de seguridad de la información</th></tr>
<tr><td>Análisis de Resultados.</td><td>Aunque la empresa Digital Signage LRDXXX cuenta con una política de Seguridad de la información necesita de una actualización de las políticas de los activos de innovación en tecnología y divulgación de la política a todos los empleados</td></tr>
<tr><td>Fase de Planificación</td><td>
<table>
<tr><th>PLANIFICACION</th><th>Fecha Inicial</th><th>Fecha Final</th><th>RESPONSABLE</th></tr>
<tr><td>Plan de tratamiento de riesgo de seguridad y privacidad de la información</td><td>Nov 13/2018</td><td>Nov 23 2018</td><td>Control Interno</td></tr>
<tr><td>Plan de seguridad y privacidad de la información</td><td>Nov 13/2018</td><td>Nov 23 2018</td><td>Control Interno</td></tr>
</table>
</td></tr>
<tr><td>Implementación</td><td>Se implementará lo especificado en la etapa de planificación para mitigar las siguientes amenazas:
[E.1] Errores de los usuarios.
[E.2] Errores del administrador.
[E.7] Deficiencias en la organización.
[E.18] Destrucción de información.
[E.19] Fugas de información.</td></tr>
<tr><td>Riesgos del proyecto</td><td>No disponibilidad de recursos claves
- Rotación de personal del proyecto
- Múltiples vendors
- Cambios continuos de estrategia y de tecnología
- Resistencia al cambio.</td></tr>
</table>

Proyecto1. Políticas de seguridad de la información

Entregables

ENTREGABLES	Fecha Inicial	Fecha Final	RESPONSABLE
Documento actualizado de control operacional en SGSI y aprobado por la alta gerencia	01/01/2019	30/03/2019	Control Interno, Manager de TI y Tecnología, y alta gerencia
Informe del plan de mitigación o cierre de Riesgos encontrados aprobados por el owner de cada proceso	01/01/2019	30/03/2019	Oficial de Seguridad de la Información, Manager de TI y Tecnología, y alta gerencia, manager de Mercadeo y Finanzas.
Documento de reevaluación de Indicadores actuales	01/01/2019	30/03/2019	Oficial de Seguridad de la Información, Manager de TI y Tecnología, y alta gerencia, manager de Mercadeo y Finanzas.
Documento actualizado de políticas de transmisión de estrategias de mercadeo y data PII aprobado	01/01/2019	30/03/2019	Oficial de Seguridad de la Información, Manager de TI y Tecnología, Alta gerencia

Recursos Financieros

Ítem	Capacidad	Tipo de Soporte	Valor Anual
Oficial de Seguridad	Full time	Especializado	USD 30000
Especialista en Continuidad del negocio	Full time	Especializado	USD 30000
Ethical hacking y retesting	Caja negra/caja gris	Especializado	USD: 20000
Actualización de licencias y soporte de Hardware.	80	Especializado	USD:60000
Actualización de licencias y soporte de Software	80	Especializado	USD: 70000
Herramienta de Monitoreo y alarma	Por procesador	Especializado	USD 25000
Total			USD 205000

umplimiento

DOCUMENTOS	CAPITULO ISO 27001:2013
Registros de capacitación, habilidades, experiencia y calificaciones	7.2
Resultados de supervisión y medición	9.1
Programa de auditoría interna	9.2
Resultados de las auditorías internas	9.2
Resultados de la revisión por partede la dirección	9.3
Resultados de acciones correctivas	8.2 - 8.3
Definición de funciones y responsabilidades de seguridad	10.1
Registros sobre actividades de los usuarios, excepciones y eventos de seguridad	a.12.4.1 - a.12.4.3

DOCUMENTOS	CAPITULO ISO 27001:2013
Procedimiento para control de documentos	7.5
Controles para gestión de registros	7.5
Procedimiento para auditoría interna	9.2
Procedimiento para medidas correctivas	10.1

cciones

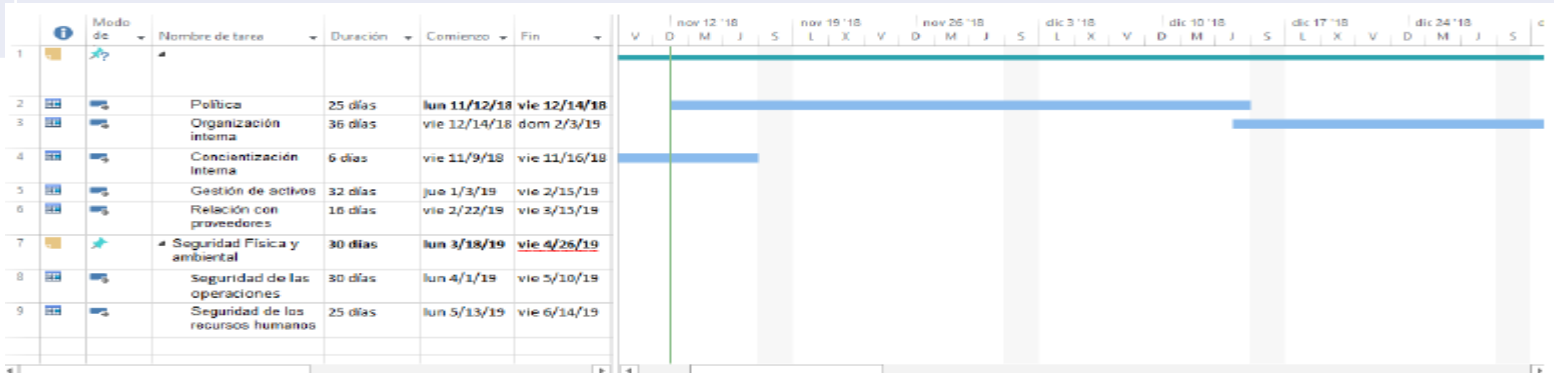
- La asignación de un PC, Laptop debe estar formateado y disco duro encriptado
- El área de Operaciones y gerencia debe tener mecanismos de control, monitoreo y seguridad para envío de mail y correos externos e Internet.
- Se debe hacer una vez al año pruebas de Ethical Hacking.
- Se debe contar con un flujo de autorización de operador y superior para habilitar paginas o accesos.
- El área de TI debe cumplir con las políticas de patches acorde a las vulnerabilidades de red o de software.
- El área de TI debe cumplir con las políticas de EOL a nivel de software y Hardware para el cumplimiento de contratos y garantía.
- Debe existir un proceso de entitlement review o proceso de revisión de roles, privilegios y accesos.
- El inventario de activos debe estar actualizado describiendo la ubicación, responsable y clasificación.
- Capacitación y Cumplimiento de la política de buenas practicas de uso para los activos como laptop, internet, celular, etc.
- Capacitación y Campaña de no compartir password y escritorio limpio.
- Job description, roles y responsabilidades definidos.
- Asegurar Inscripción mínimo 128 bits
- Capacitación de las políticas de seguridad.
- Disgregación de roles y privilegios en las diferentes plataformas
- Activación y configuración de firewall, IDS “sistema de identificación de intrusos”.
- Banner activado cada 10 minutos cuando se presente inactividad.

Proyecto1. Políticas de seguridad de la información

Recursos Fisicos

Planear y Hacer		Verificar y Actuar	
Planificación	Implementación	Evaluación de desempeño	Mejora Continua
Portátiles	Portátiles	Portátiles	Portátiles
Teléfonos	Teléfonos	Teléfonos	Teléfonos
Internet	Internet	Internet	Internet
Impresoras	Impresoras	Impresoras	Impresoras
Plataformas Tecnológicas activas	Plataformas Tecnológicas activas	Plataformas Tecnológicas activas	Plataformas Tecnológicas activas
Acceso al Datacenter y áreas privadas o con limitado acceso	Acceso al Datacenter y áreas privadas o con limitado acceso	Acceso al Datacenter y áreas privadas o con limitado acceso	Acceso al Datacenter y áreas privadas o con limitado acceso
Puesto de trabajo y sala de reuniones	Puesto de trabajo y sala de reuniones	Puesto de trabajo y sala de reuniones	Puesto de trabajo y sala de reuniones
Acceso a cada uno de los servers, base de datos o generar reportes de cada uno de las plataformas activas y licencias de Software o HW.	Acceso a cada uno de los servers, base de datos o generar reportes de cada uno de las plataformas activas y licencias de Software o HW.	Acceso a cada uno de los servers, base de datos o generar reportes de cada uno de las plataformas activas y licencias de Software o HW.	Acceso a cada uno de los servers, base de datos o generar reportes de cada uno de las plataformas activas y licencias de Software o HW.

Cronograma



	Modo de	Nombre de tarea	Duración	Comienzo	Fin
1					
2		Política	25 días	lun 11/12/18	vie 12/14/18
3		Organización interna	36 días	vie 12/14/18	dom 2/3/19
4		Concientización interna	6 días	vie 11/9/18	vie 11/16/18
5		Gestión de activos	32 días	jue 1/3/19	vie 2/15/19
6		Relación con proveedores	16 días	vie 2/22/19	vie 3/15/19
7		Seguridad Física y ambiental	30 días	lun 3/18/19	vie 4/26/19
8		Seguridad de las operaciones	30 días	lun 4/1/19	vie 5/10/19
9		Seguridad de los recursos humanos	25 días	lun 5/13/19	vie 6/14/19

Proyecto2. Proyecto Continuidad del negocio

Alcance	Implementación del plan SGSI para la continuidad del negocio, utilizando como guía la norma ISO-IEC 27001:2013.
Fase de Planificación	<table><tr><th>PLANIFICACION</th><th>Fecha Inicial</th><th>Fecha Final</th><th>RESPONSABLE</th></tr><tr><td>Plan de Continuidad del negocio especificando las principales aplicaciones activando el sitio alterno.</td><td>Nov 10/2018</td><td>Nov 23 2018</td><td>Control Interno, tecnología</td></tr><tr><td>Plan de comunicación de Continuidad del negocio</td><td>Nov 10/2018</td><td>Nov 23 2018</td><td>Control Interno, Tecnología</td></tr></table>
Implementación	Se implementará lo especificado en la etapa de planificación para mitigar las siguientes amenazas: [I.1] Fuego [I5] avería de origen físico o lógico [I.6] Corte del suministro eléctrico. [I.12] Sobrecarga eléctrica. [I13] fluctuación eléctrica. [N.1] Fuego [N.2] daños por agua. [N.3] inundación [N.4] Siniestro mayor. [N.5] Fenómeno sísmico. [A.18] Destrucción de información. [A.26] Ataque destructivo.
Riesgos del Proyecto	No disponibilidad de recursos claves - Rotación de personal operativo y del proyecto - Múltiples vendores - Cambios continuos de estrategia y de tecnología - Resistencia al cambio.

Proyecto2. Proyecto Continuidad del negocio

Entregables

ENTREGABLES	Fecha Inicial	Fecha Final	RESPONSABLE
Documento actualizado plan de Continuidad de negocio aprobado por la alta gerencia	03/01/2019	31/03/2019	Control Interno, Manager de TI y Tecnología, y alta gerencia
Informe de las aplicaciones para activar el plan de continuidad del negocio aprobados por el owner de cada proceso y lista de contactos	03/01/2019	31/03/2019	Oficial de Seguridad de la Información, Manager de TI y Tecnología, y alta gerencia, manager de Mercadeo y Finanzas.
Plan de Capacitación	03/01/2019	31/03/2019	Oficial de Seguridad de la Información, Manager de TI y Tecnología, Alta gerencia

Recursos Financieros

Ítem	Capacidad	Tipo de Soporte	Valor Anual
Oficial de Seguridad	Full time	Especializado	USD 30000
Especialista en Continuidad del negocio	Full time	Especializado	USD 30000
Ethical hacking y retesting	Caja negra/caja gris	Especializado	USD: 20000
Actualización de licencias y soporte de Hardware.	80	Especializado	USD:60000
Actualización de licencias y soporte de Software	80	Especializado	USD: 70000
Herramienta de Monitoreo y alarma	Por procesador	Especializado	USD 25000
Total			USD 205000

Proyecto2. Proyecto Continuidad del negocio

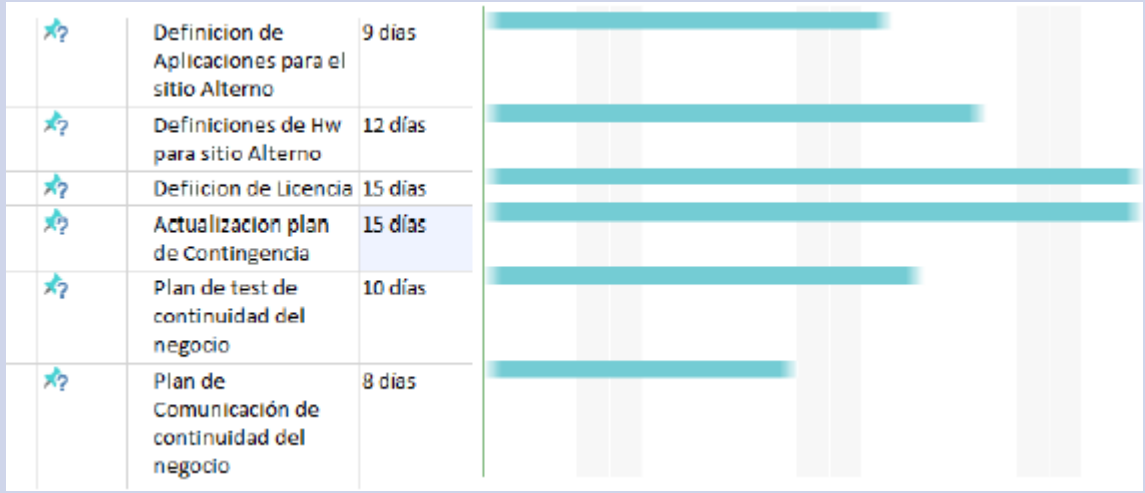
Cumplimiento	
Acciones	Se implementará las siguientes acciones: - Las personas tendrán un PC asignado en el sitio alterno y la persona una vez cada tres meses debe trabajar desde el sitio remoto. - Se tendrá el mismo nivel de parche en los pc y versiones - Se tendrá el mismo nivel de parche en los servers y base de datos en el sitio alterno - Se realizará un full restore el primer día de la semana para asegurar la data en el sitio alterno y un restore incremental en los siguientes días - Se realizará prueba cada 6 meses en el sitio alterno - Se tendrá evidencias técnicas de cada una de las pruebas en el sitio alterno. - Se tendrá evidencia presencial de las personas que ejecutan el proceso - Se tendrá una lista de contactos para llamado de emergencia. - Asegurar la misma configuración en las plataformas del sitio alterno.

Iso27001:2013	Ítem	Fecha de Inicio	Fecha Final
A17	Continuidad del negocio	06/16/2019	05/30/2019

DOCUMENTOS	CAPITULO ISO 27001:2013
Política de claves	a.9.2.1 / 2 / 4, a.9.3.1, a.9.4.3
Política de eliminación y destrucción	a.8.3.2, a.11.2.7
Política de gestión de cambio	a.12.1.2, a.14.2.4
Política de creación de copias de seguridad	a.12.3.1
Política de transferencia de la información	a.13.2.1 / 2 / 3
Análisis del impacto en el negocio	a.17.1.1
Plan de prueba y verificación	a.17.1.3
Plan de mantenimiento y revisión	a.17.1.3

Proyecto2. Proyecto Continuidad del negocio

Cronograma



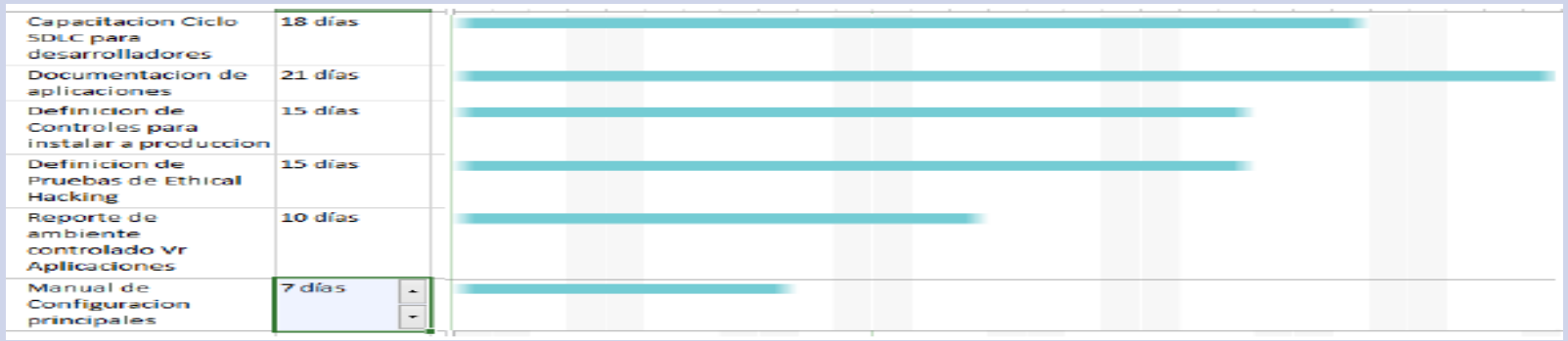
Recursos

Planear y Hacer		Verificar y Actuar	
Planificación	Implementación	Evaluación de desempeño	Mejora Continua
Portátiles	Portátiles	Portátiles	Portátiles
Teléfonos	Teléfonos	Teléfonos	Teléfonos
Internet	Internet	Internet	Internet
Impresoras	Impresoras	Impresoras	Impresoras
Plataformas Tecnológicas activas	Plataformas Tecnológicas activas	Plataformas Tecnológicas activas	Plataformas Tecnológicas activas
Acceso al Datacenter y áreas privadas o con limitado acceso	Acceso al Datacenter y áreas privadas o con limitado acceso	Acceso al Datacenter y áreas privadas o con limitado acceso	Acceso al Datacenter y áreas privadas o con limitado acceso
Puesto de trabajo y sala de reuniones	Puesto de trabajo y sala de reuniones	Puesto de trabajo y sala de reuniones	Puesto de trabajo y sala de reuniones
Acceso a cada uno de los servers, base de datos o generar reportes de cada uno de las plataformas activas y licencias de Software o HW.	Acceso a cada uno de los servers, base de datos o generar reportes de cada uno de las plataformas activas y licencias de Software o HW.	Acceso a cada uno de los servers, base de datos o generar reportes de cada uno de las plataformas activas y licencias de Software o HW.	Acceso a cada uno de los servers, base de datos o generar reportes de cada uno de las plataformas activas y licencias de Software o HW.

Proyecto3. Proyecto Control Software

Análisis de resultadOs	Objetivo: Este plan de proyecto define las estrategias que conducen a la gestión de software para asegurar la integridad y disponibilidad del mismo.
Fase de Planificación	

PLANIFICACION	Fecha Inicial	Fecha Final	RESPONSABLE
Arquitectura recomendada y aprobada para la instalación de las aplicaciones.	Nov 10/2018	Nov 23 2018	Control Interno, tecnología
Revisión y monitoreo en las comunicaciones para evitar intrusión o Sql injection	Nov 10/2018	Nov 23 2018	Control Interno, Tecnología

Implementación	Se implementará lo especificado en la etapa de planificación para mitigar las siguientes amenazas: [A.14] Interceptación de información. [A.18] Destrucción de información [E.8] Difusión de software dañino
Riesgos del proyecto	No disponibilidad de recursos claves - Rotación de personal operativo y del proyecto - Múltiples vendors - Cambios continuos de estrategia y de tecnología - Resistencia al cambio.
Cronograma	

Proyecto3. Proyecto Control Software

Entregables

ENTREGABLES	Fecha Inicial	Fecha Final	RESPONSABLE
Documento actualizado plan SDLC aprobado por la alta gerencia	01/01/2019	30/03/2019	Control Interno, Manager de TI y Tecnología, y alta gerencia
Acta de Controles para implementar a producción.	01/01/2019	30/03/2019	Oficial de Seguridad de la Información, Manager de TI y Tecnología, y alta gerencia, manager de Mercadeo y Finanzas.
Control de Ethical hacking aprobado	01/01/2019	30/03/2019	Oficial de Seguridad de la Información, Manager de TI y Tecnología, Alta gerencia

Recursos Financieros

Ítem	Capacidad	Tipo de Soporte	Valor Anual
Oficial de Seguridad	Full time	Especializado	USD 30000
Especialista en Continuidad del negocio	Full time	Especializado	USD 30000
Ethical hacking y retesting	Caja negra/caja gris	Especializado	USD: 20000
Actualización de licencias y soporte de Hardware.	80	Especializado	USD:60000
Actualización de licencias y soporte de Software	80	Especializado	USD: 70000
Herramienta de Monitoreo y alarma	Por procesador	Especializado	USD 25000
Total			USD 205000

Acciones

- Se tendrá control del software por medio de repositorios controlados.
- Debe existir las etapas de desarrollo SDLC.
- Debe existir ambientes controlados para desarrollo, test y producción
- Testeo para cada una de las aplicaciones y corregir los problemas encontrados.
- Entrada a producción controlada

Proyecto3. Control de Software

Cumplimiento

DOCUMENTOS	CAPITULO ISO 27001:2013
Política de claves	a.9.2.1 / 2 / 4, a.9.3.1, a.9.4.3
Política de eliminación y destrucción	a.8.3.2, a.11.2.7
Política de gestión de cambio	a.12.1.2, a.14.2.4
Política de creación de copias de seguridad	a.12.3.1
Política de transferencia de la información	a.13.2.1 / 2 / 3
Análisis del impacto en el negocio	a.17.1.1
Plan de prueba y verificación	a.17.1.3
Plan de mantenimiento y revisión	a.17.1.3

Plan de Monitoreo

	Tratamiento					
Riesgo	**Aceptar**	**Evitar**	**Mitigar**	**Transferir**	**Plan de Monitoreo**	**Responsable**
Difusión de Software dañino			x		Verificación de log y actualización de comunicaciones	Gerente de TI y Tecnología
Errores de Configuración		x			Informe de errores	Arquitectura y tecnología
Errores de Usuarios		x			Informe de errores	Arquitectura y tecnología
Errores de mantenimiento/actualización de equipos (Software)		x			Informe de errores	Arquitectura y tecnología
Fuga de Información		x			Seguimiento al plan de capacitación a la protección de Información	Operaciones y manager de cada área

Conclusión Proposición de Proyectos

- 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

Comparación Gap Analisis

cumplimiento de los requerimientos de la ISO 27001

Análisis Inicial

	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

Análisis Proyecto Fase Implementada

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

Cumplimiento de todos los controles del Anexo A ISO/IEC 27002

Análisis Inicial

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

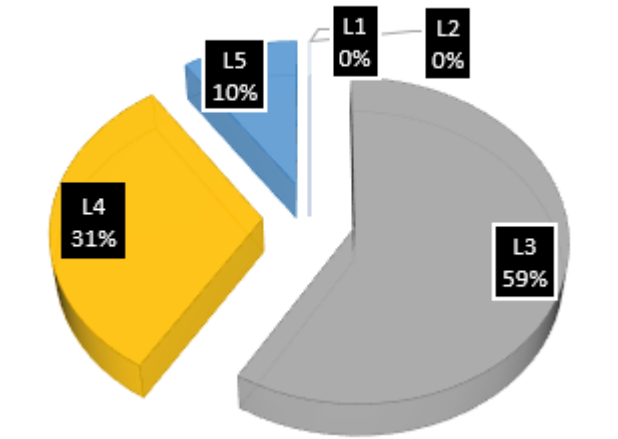
Análisis Proyecto Fase Implementada

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50	70	Reproducible, pero intuitivo
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	50	70	Reproducible, pero intuitivo
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	50	70	Reproducible, pero intuitivo
A.8	GESTIÓN DE ACTIVOS	50	70	Reproducible, pero intuitivo
A.9	CONTROL DE ACCESO	50	70	Reproducible, pero intuitivo
A.10	CRIPTOGRAFÍA	50	70	Reproducible, pero intuitivo L
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	50	70	Reproducible, pero intuitivo L
A.12	SEGURIDAD DE LAS OPERACIONES	50	70	Reproducible, pero intuitivo L
A.13	SEGURIDAD DE LAS COMUNICACIONES	50	70	Reproducible, pero intuitivo
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	50	70	Reproducible, pero intuitivo L
A.15	RELACIONES CON LOS PROVEEDORES	50	70	Reproducible, pero intuitivo
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	50	70	Reproducible, pero intuitivo
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	50	70	Reproducible, pero intuitivo
A.18	CUMPLIMIENTO	50	70	Reproducible, pero intuitivo
PROMEDIO EVALUACIÓN DE CONTROLES		50	70	Reproducible, pero intuitivo

Auditoría de Cumplimiento

Se evalúa 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.

- Luego de revisar los resultados de madurez se muestra en la siguiente gráfica 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.



Auditoría de Cumplimiento

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
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.

Cuadro de No Conformidades

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

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

Cuadro de No Conformidades

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

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

Conclusiones

El resultado de la auditoría 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.

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.

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.

Gracias por su Atención!