DIAGNÓSTICO DEL NIVEL DE CUMPLIMIENTO ISO 27002
AREVALO S.A
MARZO DE 2013

CONTENIDO

Control Documental

Versión	Autor	Fecha	Descripción
0.1	Gustavo Arévalo	Marzo 2013	Creación de documento.

Revisión del Documento

Nombre	Cargo	Versión	Fecha	Comentarios

Aprobación del Documento

Versión	Aprobación	Fecha	Descripción

1. Diagnóstico de Cumplimiento ISO 27001

El presente documento reúne el estudio de la etapa de análisis de cumplimiento del modelo de seguridad de la información actualmente implementado en AREVALO S.A., frente a los controles propuestos en el anexo A del estándar ISO 27002.

Este documento no pretende ser el plan estratégico de seguridad, pero sí aportar para ayudar a mejorar la seguridad de la información y alinear el modelo actual a la norma ISO 27002. Cada una de las recomendaciones debe ser analizadas y soportadas por los resultados del análisis de riesgos.

1.1. Objetivos

La etapa de diagnóstico del cumplimiento en AREVALO S.A.**,** está basado en el estándar ISO 27002, y tiene como objetivo determinar el estado actual del modelo de seguridad de la organización, y con base en el análisis, generar algunas recomendaciones para que sean implantadas con el fin de mejorar el modelo y establecer el punto de partida donde se medirá el desarrollo de las mejoras en seguridad aplicadas en el futuro.

1.2. Alcance

En base a los tiempos y el plan de trabajo establecido en el cronograma del proyecto, las actividades desarrolladas fueron las siguientes:

- Entrevistas con diferentes áreas de AREVALO S.A. que soportan los procesos de negocio como lo son: recursos humanos, área jurídica y legal, tecnología y riesgos; para realizar la búsqueda y establecer el plan a seguir para el levantamiento de las políticas y procedimientos implementados frente al modelo de seguridad de la información.
- Revisión de la documentación y planes con los cuales cuenta AREVALO S.A. en la actualidad, para el desarrollo de su operación y administración de seguridad de la Información.
- Hallazgos y oportunidades de mejora para cada dominio de la norma.
- Calificación general de seguridad.

1.3. Revisión de Cumplimiento del Estándar ISO 27002

Para la revisión del modelo de seguridad y para la medición del estado actual de su administración, se toma como parámetro el estándar ISO 27002, el cual está basado en las mejores prácticas de seguridad de la información. El estándar se encuentra divido en 11 dominios, los cuales a su vez tienen secciones para así sumar 133 controles que cubren todos los aspectos más relevantes relacionados con la seguridad de la información.

El estándar ISO 27002, es un estándar internacionalmente aceptado, el cual especifica los requisitos y la manera de adoptar un proceso que permita establecer, revisar, mantener y mejorar

el “Sistema de Administración de la Seguridad de la Información – SGSI” para que sea efectivo, teniendo como base los objetivos y las necesidades propias del negocio y de la organización.

Adicionalmente, tiene como principio que la información debe tratarse como un activo importante para la organización y como tal debe ser protegida de manera adecuada especialmente en cuanto a tres características fundamentales: Integridad, Confidencialidad y Disponibilidad.

Como parte de este modelo, se debe enfatizar en AREVALO S.A y en los usuarios la importancia de:

- Entender los requerimientos de seguridad de la información que tiene AREVALO S.A., y la necesidad de establecer políticas y objetivos para cumplir dichos requerimientos;
- Implementar y operar controles dentro del contexto de los riesgos del negocio.
- Monitorear y revisar la efectividad y el desempeño del sistema implementado.
- Mejorar continuamente el modelo con base en una medición de objetivos y resultados.

1.4. Revisión Documentación

En esta sección se hace un resumen de la documentación entregada por AREVALO S.A para la revisión y análisis del cumplimiento, respecto a los controles propuestos por la norma ISO 27002. Dichos documentos fueron analizados y son la evidencia en el porcentaje del cumplimiento frente al estándar.

Documento	Descripción
	Contratos con Terceros
P-TEC-01-V1	Ejecución de mantenimiento correctivo de software
P-TEC-02-V1	Ejecución de mantenimiento correctivo de hardware
P-TEC-03-V1	Ejecución de mantenimiento preventivo de la infraestructura tecnológica.
P-TEC-04-V1	Respaldo y Contingencia
	Topologías de Red
	Flujogramas del Proceso
	Procedimiento Outsourcing Control de Calidad y Transportes

Tabla 1. Documentación procedimientos y políticas - Sistema de Gestión Seguridad de la Información

2. Cumplimiento según el Estándar ISO 27001

El modelo de administración definido en el estándar establece la necesidad de identificar los requerimientos de seguridad de la información en AREVALO S.A., y establece una serie de controles que deben ser adoptados para que se logre garantizar que el nivel de riesgo de la información sea llevado a niveles aceptables.

Los controles definidos en la Norma ISO 27002 y que se identifican en el Anexo A del estándar ISO 27002 y del presente documento, están establecidos de manera general, de tal forma que cada organización debe analizarlos y adaptarlos a su entorno específico.

2.1. Diagnóstico y Calificación General

Luego del análisis y revisión de seguridad realizada para los procesos de negocio de AREVALO S.A., se puede establecer que el nivel de cumplimiento frente a la norma es del 48%. En términos generales, esto nos presenta un estado de cumplimiento para cada dominio resumido a continuación:

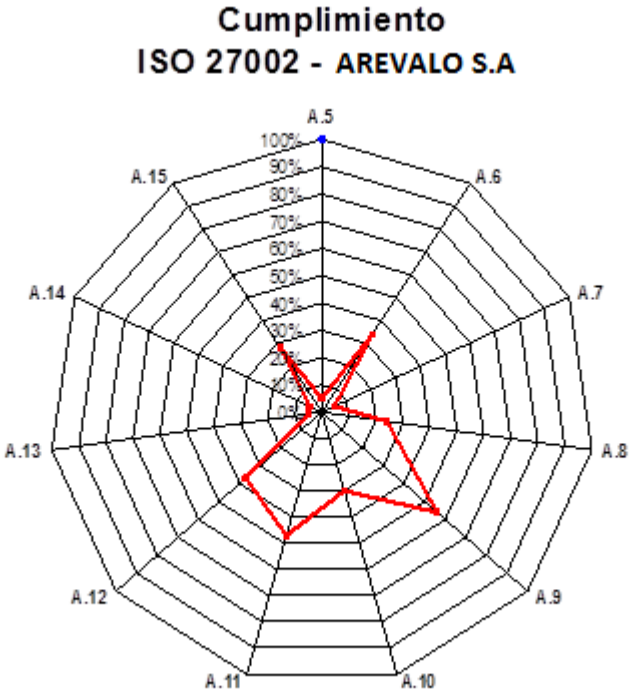


Ilustración 1. Nivel de Cumplimiento actual de AREVALO S.A frente a la Norma ISO 27002.

Los principales hallazgos identificados se relacionan a continuación:

- ***Políticas de Seguridad*****:** No existe un manual de políticas de seguridad de la información que permita alinear los objetivos estratégicos del negocio con el sistema de gestión de seguridad de la información (SGSI). Igualmente, no existen procesos, procedimientos y estándares de seguridad, que permitan identificar y gestionar los riesgos en seguridad de la información de forma adecuada.

- ***Seguridad Organizacional*****:** El gobierno de seguridad no se encuentra definido, y el rol de seguridad es asumido en la actualidad únicamente por el custodio (Tecnología), quien aplica controles solamente en la infraestructura tecnológica, sin establecer procedimientos formales y continuos. Esto permite, que la seguridad no sea un componente transversal de la organización implementando controles que no gestionan integralmente los riesgos asociados al no cumplimiento de los objetivos estratégicos de AREVALO S.A.

- ***Gestión de Activos:*** No existe un inventario de activos de información, ni se encuentran identificados los tipos de información, el dueño de la información y el activo de información que procesa, gestiona o resguarda esta información. Igualmente no existe una adecuada clasificación de la información aumentando el riesgo y la exposición de fuga, robo y/o pérdida de información sensible para AREVALO S.A.

- ***Seguridad del Recurso Humano:*** En la actualidad, no se encuentra incluido dentro del plan de capacitación del área de recursos humanos de AREVALO S.A., un capítulo de entrenamiento y concientización en el uso y seguridad de la información. Adicionalmente, no existen cláusulas de confidencialidad en los contratos con los empleados; y la no existencia de un manual de políticas de seguridad no permite generar un registro de entendimiento y aplicación los controles de seguridad por parte de los empleados, terceros y contratistas.

- ***Gestión de incidentes*****:** Aunque existe una herramienta para documentar y registrar algunos incidentes de seguridad, se debe incluir en la mesa de ayuda procedimientos para tramitar y escalar de forma inmediata y efectiva los incidentes que afectan la seguridad de la información. Se deben desarrollar procedimientos y metodologías claras, únicas y ordenadas que garanticen una gestión efectiva de dichos eventos. La gestión de incidentes debe ser el único punto de partida para la utilización de los planes de continuidad, el soporte operativo y la investigación.

- ***Seguridad con terceros*****:** Se deben definir lineamientos claros en la gestión de seguridad con proveedores que accedan a la información de la organización. En la revisión realizada a los procesos, operados en modalidad de Outsourcing, se evidencian riesgos en el uso, resguardo y transformación de la información de AREVALO S.A. Dentro del contrato o niveles de servicio deben quedar incluidos los controles mínimos definidos para garantizar que la información que accedan los terceros quede protegida.

- ***Control metodológico de cambios*****:** Los cambios de plataforma, procesos, personas deben gestionarse en un único modelo con el fin de minimizar los riesgos y el impacto en la modificación y actualización de las cuentas de usuario, los planes de continuidad y los activos de información.

- ***Gestión de Continuidad del Negocio:*** No existe definido e implementado un Plan de Continuidad del Negocio. Existen algunos controles que protegen la información como

Backups; sin embargo, no existe una estrategia clara de recuperación de los procesos de negocio.

- ***Gestión de la plataforma***: Se debe contar con una gestión continua de la plataforma, identificando, valorando y mitigando los riesgos, vulnerabilidades o amenazas que puedan afectar la plataforma tecnológica.

A través de la aplicación de las recomendaciones y tomando como patrón de medición el presente documento, AREVALO S.A. estará en condiciones de optimizar su seguridad de la información hasta alcanzar los niveles adecuados definidos por la norma.

A continuación se detalla cada uno de los requerimientos definidos por la norma, los hallazgos identificados y el plan de acción a seguir.

3. Análisis de Cumplimiento ISO 27001

El estudio de análisis de cumplimiento se basa en el desarrollo de una guía de validación de la implementación de controles desarrollada por Gustavo Arévalo Arenas, para identificar el estado actual en el que se encuentra AREVALO S.A. frente al análisis, estudio, desarrollo e implantación de controles que minimizan el riesgo en el procesamiento de la información.

El análisis verifica la implantación y definición de cada uno de los objetivos de control desarrollados por AREVALO S.A., otorgando una valoración que mide el estado actual de cada dominio de control.

La siguiente tabla muestra la valoración a utilizar y su significado.

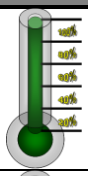
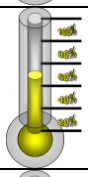
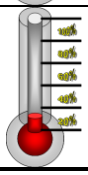
Estado	Significado
	Se han establecido los parámetros necesarios para cumplir con los requisitos impuestos por el dominio de control definidos por la norma.
	Se establece la necesidad ó lineamiento, pero no ha sido implementado. Hace falta mejorar las políticas o procedimientos debido a que no cubre todo el universo.
	No existen lineamientos. No se ha definido la política.

Tabla 2. Valoración de cumplimiento de controles.

Para facilitar el entendimiento de las preguntas, estas se han organizado de la misma forma en que se presentan los controles de la norma ISO-27002, siguiendo incluso su esquema de numeración para asociar muy fácilmente el proceso del análisis GAP con el estándar.

Para mayor facilidad se dará una calificación por dominio, y una calificación general del cumplimiento actual del sistema de gestión de seguridad de la información. **Es necesario aclarar que la calificación debe ser asociada con el cumplimiento y no es una valoración de la efectividad del control.**

Para la calificación se obtiene un promedio de cumplimiento, donde cada control tiene el mismo peso sobre la calificación global.

A.5 Política de Seguridad

Para cumplir con este dominio de la norma ISO 27002, se requiere que los responsables del nivel gerencial aprueben y publiquen un documento que contenga la política de seguridad y comunicarlo a todos los empleados, según corresponda. El nivel gerencial debe poner de manifiesto su compromiso y establecer el enfoque de la organización con respecto a la administración de la seguridad de la información. La política debe ser comunicada a todos los usuarios de la organización de manera pertinente, accesible y comprensible.

5.1 Política de Seguridad de la Información

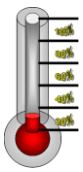
Objetivo: Proveer una dirección y soporte a la seguridad de la información alineada con los requerimientos del negocio y las regulaciones y leyes relevantes.

La gerencia debe definir una dirección clara alineada con los objetivos de negocios y demostrando soporte y compromiso a la seguridad de la información a través del mantenimiento de una política de seguridad de la información implementada en toda la organización.

Análisis

Riesgo Actual	Hallazgos	Recomendaciones
Sin una política de seguridad, el riesgo se incrementa debido a una ausencia de seguimiento en los controles administrativos y/o no son implementados consistentemente a través de la organización. Sin un propietario, una revisión periódica y comparación de las políticas contra las prácticas actuales del negocio y los incidentes de seguridad, el riesgo se incrementa debido a que la política puede estar desactualizada, poco práctica o sea difícil de implementar.	En la actualidad no existe un documento de políticas de seguridad de la información que establezca criterios adecuados para gestionar los riesgos en seguridad existentes en AREVALO S.A. No existe un Comité de Gobierno de seguridad, que se responsabilice por la gestión y revisión en el cumplimiento de las políticas de seguridad y/o nuevos riesgos asociados a la operación de la compañía.	Se debe definir un manual de políticas de seguridad, alineado con el nivel de riesgo e involucrando los diferentes roles y responsabilidades en seguridad de la información. La definición e implementación de los controles deben ser aceptadas y formalizadas por el Comité de Seguridad.

El cumplimiento actual de la organización frente al objetivo de control de política de seguridad de la información es:



Bajo

A.6 SEGURIDAD ORGANIZACIONAL

Para cumplir con este dominio de la norma ISO 27002, la organización debe establecer foros de administración liderados por niveles gerenciales, a fin de aprobar la política de seguridad de la información, asignar funciones de seguridad y coordinar la implementación de la seguridad en toda la organización.

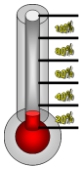
6.1 Organización Interna

Objetivo: Gestionar la seguridad de la información dentro de la organización.

Análisis

Riesgo Actual	Hallazgos	Recomendación
Una seguridad efectiva requiere una trazabilidad en las responsabilidades y asignaciones como dueños de activos, custodios, proveedores y usuarios de información. Sin los contactos apropiados con autoridades externas, se puede incrementar el riesgo de que las acciones apropiadas sean realizadas durante un incidente de seguridad. El riesgo se incrementa si las prácticas de seguridad de la organización son poco efectivas o no reflejan la política de seguridad.	En la actualidad la alta dirección es conciente de la necesidad del tema de seguridad de la información. En la actualidad no existe un comité multidisciplinario de continuidad del negocio. No existe una clara definición de roles y responsabilidades y no se ha definido un líder frente al tema de seguridad. (Oficial de Seguridad). No se han definido acuerdos de confidencialidad con los empleados y con todos los terceros. Los procesos de manejo de crisis no incluyen a autoridades externas para responder de forma efectiva a los eventos. En la actualidad no cuentan con asesoría de terceros expertos en el tema de seguridad de la información. Al no existir políticas de seguridad, los usuarios no se encuentran sensibilizados frente a su existencia y a su necesidad de aplicación.	Definir el gobierno de seguridad de la información en el cual se incluyan modelos de decisión, políticas completas de seguridad, procesos y estructura organizacional. El área de seguridad debe definir claramente los contactos externos y garantizar su actualización para responder de forma efectiva frente a eventos que afectan la integridad, confidencialidad y disponibilidad de la información. Se debe realizar un seguimiento frente al cumplimiento, efectividad y aplicabilidad de las políticas de seguridad. Involucrar en el proceso de capacitación realizado por recursos humanos, entrenamiento y sensibilización en las políticas y lineamientos en seguridad de la información

El cumplimiento actual de la organización frente al objetivo de control de organización interna es:



Bajo

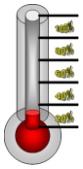
6.2 Terceros

Objetivo: Mantener la seguridad de la información de la organización y de las instalaciones de procesamiento que son accedidas, procesadas, comunicadas o gestionadas por terceros.

Análisis:

Riesgo Actual	Hallazgos	Cumplimiento Actual
Existe un riesgo si el acceso de servicios de terceros no esta alineado con la política de seguridad de la compañía y si la información confidencial y los programas no están asegurados adecuadamente para dicho acceso. Existe el riesgo de que los accesos de clientes y/o contratistas no estén de acuerdo a la política de seguridad de la información de la organización y que la confidencialidad de la información y de los programas no sea asegurada adecuadamente para dicho acceso. Si no se especifican todos los requerimientos de seguridad en los acuerdos con terceros se incrementa el riesgo de no cumplimiento con la política de seguridad y estándares debido al no entendimiento entre la organización y los terceros.	No se ha analizado el riesgo frente al acceso de terceros a la información de AREVALO S.A., por lo tanto no se han definido controles o lineamientos que mitiguen riesgos frente a la pérdida de confidencialidad, integridad y disponibilidad. En la actualidad, el proceso de Outsourcing Control de Calidad y Transportes, se encuentra tercerizado con xxxxxxxS.A. Durante la revisión realizada a este tercero, se evidenciaron altos riesgos en el uso de la información, acceso a la información, protección de la información (la plataforma tecnológica no es administrada y gestionada por AREVALO S.A, es responsabilidad de XXXXXXXX.S.A), disponibilidad de la información (generación de backups irregulares). No se realiza por parte de AREVALO S.A seguimiento al cumplimiento de los niveles de servicio (SLA), establecidos y definidos contractualmente. Los usuarios de xxxxxxx.S.A no conocen las políticas de seguridad de AREVALO S.A, aumentando el riesgo de fraude y/o fuga o robo de información. No existe un procedimiento claramente definido para que los terceros accedan a las instalaciones o a los sistemas de información de AREVALO S.A.	Incluir dentro del análisis de riesgo a proveedores y definir los requerimientos mínimos de seguridad para los proveedores de acuerdo con la clasificación de la información a la cual van a acceder. Definir un procedimiento claro para garantizar que los proveedores conozcan los lineamientos de seguridad y cumplan con los controles y políticas definidas. Revisar los niveles de servicio establecidos con terceros y proveedores, auditando el cumplimiento de los controles de seguridad definidos por el dueño de la información de AREVALO S.A. Realizar auditoría de seguridad a otros terceros y/o proveedores en AREVALO S.A

El cumplimiento actual de la organización frente al objetivo de control de terceros es:



Bajo

A7 Gestión de Activos

Para cumplir con este dominio de la norma ISO 27002, se deben identificar propietarios para todos los activos importantes y se debe asignar la responsabilidad por el mantenimiento de los controles apropiados. La rendición de cuentas por los activos ayuda a garantizar que se mantenga una adecuada protección. La responsabilidad por la implementación de los controles puede ser delegada. En último término, el propietario designado del activo debe rendir cuentas por el mismo.

7.1 Responsabilidad de los Activos

Objetivo: Garantizar y mantener una protección apropiada de los activos de la organización.

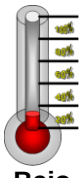
Todos los activos deben ser identificados y se debe definir un dueño quien será su directo responsable.

Los dueños deben ser identificados para todos los activos y la responsabilidad por el mantenimiento de los controles apropiados debe designarse. La implementación de controles específicos puede ser delegada por el dueño de la información, pero este continúa siendo responsable por la protección apropiada del activo.

Análisis

Riesgo Actual	Hallazgos	Recomendaciones
Si no se cuenta con un inventario de los activos se incrementa la dificultad de la gestión de riesgos y la protección de activos. Sin un inventario actual de los activos, una organización puede no identificar los riesgos debido a que el activo de información en riesgo no se conoce. Sin un dueño designado, la información asociada con el activo como su ubicación, clasificación y valor puede ser incorrecto o puede estar desactualizado.	No se cuenta con un inventario de activos de información claramente definido. No se ha responsabilizado a empleados de AREVALO S.A. de la información y de sus activos que crean, gestionan o resguardan. Se realiza una capacitación del uso de las herramientas y de los servicios a los usuarios.	Realizar un inventario de activos el cual sea complementado con la base de datos de configuración (Hoja de Vida de los servidores y/o BD) Definir responsables frente a la información y los activos de información.

El cumplimiento actual de la organización frente al objetivo de control de responsabilidad de activos es:



Bajo

7.2 Clasificación de Información

Objetivo: Asegurar que la información posea el nivel apropiado de protección.

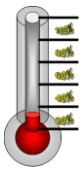
La información debe ser clasificada para indicar las necesidades, prioridades y grado de protección esperado cuando la información es manipulada.

La información cuenta con varios grados de sensibilidad y criticidad. Algunos datos requieren un nivel adicional de protección o tratamiento especial. Un esquema de clasificación de la información, debe usarse para definir un conjunto apropiado de niveles de protección y comunicar las medidas especiales de tratamiento.

Análisis

Riesgo Actual	Hallazgos	Cumplimiento Actual
La ausencia de un esquema de clasificación de la información puede dificultar la identificación de cuales medidas de seguridad son necesarias para proteger la información crítica. La organización puede correr el riesgo de gastar dinero en seguridad para información de bajo riesgo mientras que los datos críticos pueden ser protegidos inadecuadamente. Sin procedimientos adecuados de tratamiento y etiquetado de la información de la organización, se incrementa el riesgo de pérdida de activos, compromiso, o no disponibilidad. El tener tercerizado el proceso Outsourcing Control de Calidad y Transportes,, exige obtener de manera rápida la clasificación de la información (Sistemas de Información de AREVALO S.A).	No se ha definido un esquema de clasificación de información para los activos de información. El proceso de Outsourcing Control de Calidad y Transportes, cuenta con algunos lineamientos y actividades propias de la digitalización de la información, como son guias de transporte, facturas entre otras. No se ha definido un estándar de seguridad adecuado para gestionar la información de AREVALO S.A.	Definir un esquema de clasificación de información y de sistemas de información. Desarrollar procedimientos para etiquetado y tratamiento de información.

El cumplimiento actual de la organización frente al objetivo de control de responsabilidad de activos es:



Bajo

A8 Seguridad del Recurso Humano

Para cumplir con este dominio de la norma ISO 27002, las responsabilidades en materia de seguridad deben estar incluidas en los contratos laborales cuando se realiza la selección del personal y monitoreadas durante el desempeño del individuo como empleado. Los candidatos a ocupar los puestos de trabajo deben ser adecuadamente seleccionados, especialmente si se trata de tareas críticas. Todos los empleados, terceros y/o contratistas de las instalaciones de procesamiento de información deben firmar un acuerdo de confidencialidad (no-revelación).

8.1 Previo a la Contratación

Objetivo: Asegurar que los empleados, contratistas y proveedores comprendan sus responsabilidades y cumplan con los requisitos para llevar a cabo los roles definidos con el fin de minimizar el riesgo de robo, fraude o uso inadecuado de las instalaciones.

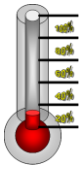
Las responsabilidades de seguridad deben ser definidas antes del ingreso de un empleado en la descripción del empleo y en los términos y condiciones del contrato.

Todos los candidatos para un empleo, contratistas o proveedores deben ser investigados adecuadamente, especialmente para trabajos sensibles.

Los empleados, contratistas y proveedores que tienen contacto con las instalaciones de procesamiento de información deben firmar un acuerdo donde aceptan sus roles y responsabilidades frente a la seguridad.

Riesgo Actual	Hallazgos	Recomendación
Si no se tiene claramente definidos los roles de seguridad y las responsabilidades se incrementan el riesgo de error humano, robo, fraude o mal uso de las instalaciones de procesamiento de información. Si no se incluye las responsabilidades legales y la seguridad de la información dentro de los términos y condiciones de un empleo, la organización es expuesta a un riesgo y no provee un recurso legal en el evento en que la información sensible sea comprometida o utilizada de una forma no apropiada por los empleados.	No se incluyen roles y responsabilidades de seguridad dentro de los contratos de trabajo o en el reglamento interno de trabajo. Se lleva a cabo una validación de antecedentes que incluye el análisis de hoja de vida, pruebas técnicas y psicológicas (no se realiza visita domiciliaría), y validación de referencias y hoja de vida. Dentro de los contratos no se incluyen temas de confidencialidad y no revelación de información.	Definir los roles y responsabilidades de seguridad. Incluir los roles y responsabilidades de seguridad dentro de los contratos de trabajo. Verificar la inclusión de acuerdos de confidencialidad en los contratos con empleados, terceros y contratistas.

El cumplimiento actual de la organización frente al objetivo de control previo a la contratación es:



Bajo

8.2 Durante la Contratación

Objetivo: Asegurar que los empleados, contratistas y proveedores sean sensibilizados acerca de las amenazas de la seguridad de la información y entiendan sus responsabilidades y estén alineados para soportar la política de seguridad de la organización en el curso normal de sus actividades y para reducir el riesgo de error humano.

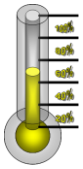
Las responsabilidades de la gerencia deben ser definidas para garantizar que la seguridad es aplicada a través de toda la organización.

Un nivel adecuado de sensibilización, educación y entrenamiento en procedimientos de seguridad y el uso correcto de las instalaciones de procesamiento debe ser proveído a todos los empleados, contratistas y terceros para minimizar los posibles riesgos de seguridad. Un proceso disciplinario formal para tratar las violaciones de seguridad debe estar implementado.

Análisis

Riesgo Actual	Hallazgos	Recomendaciones
Sin requerimientos para aplicar seguridad basada en la política de seguridad de la información, aumenta el riesgo de error humano, robo, fraude o mal uso de las instalaciones de procesamiento de información aumentan. Los usuarios son más afines a seguir con un procedimiento de seguridad si son concientizados sobre este y sobre el beneficio resultante para la organización.	La alta dirección no ha aprobado las políticas de seguridad de la información. Dentro de la inducción no se incluyen lineamientos frente al tema de seguridad. Los responsables de ciertos temas (tecnología) cuentan con entrenamiento o capacitación específica en los de seguridad de la información. No existe un proceso disciplinario definido para el tratamiento en incidentes de violación de políticas de seguridad.	El compromiso de la alta dirección se debe reflejar en la aprobación de políticas, en la ayuda para cumplir con los objetivos de seguridad propuestos. Definir un esquema de entrenamiento y sensibilización en seguridad que garantice que los usuarios, empleados y terceros conozcan y comprendan las políticas de seguridad. Debe existir un registro del nivel de sensibilización frente a la seguridad de todos los empleados. Definir que tipo de sanciones disciplinarias acarreará la violación de políticas de seguridad.

El cumplimiento actual de la organización frente al objetivo de control durante el empleo es:



Medi0

8.3 Terminación o Cambio en el Empleo

Objetivo: Garantizar que los empleados, contratistas y proveedores que salgan de la organización o cambien de puesto, lo hagan de una manera ordenada.

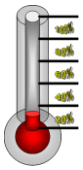
Las responsabilidades deben ser definidas para garantizar que los empleados, contratistas o proveedores que salgan de la organización sean de forma gestionada, y que los equipos y los derechos de acceso sean entregados y removidos completamente.

Los cambios de las responsabilidades y de los contratos dentro de la organización deben ser gestionados como una terminación de las respectivas responsabilidades o del empleo, y el nuevo empleo debe ser gestionado basado en la sección 8.1.

Análisis

Riesgo Actual	Hallazgos	Recomendaciones
Si las responsabilidades para ejecutar la terminación de un contrato o cambio no esta definido, existe un incremento en el riesgo que no sea comunicado adecuadamente.	Se tiene definido un procedimiento para la terminación de un contrato. Dentro de este no esta incluido en su totalidad el cambio de puesto dentro de la organización. No existe un procedimiento alterno para la salida de personal de forma no amistosa. Los activos físicos están asociados a los empleados, para dar el paz y salvo de salida deben entregar todos los que están a su cargo. Los activos no incluyen información, documentos, etc. Existe un proceso de gestión de cuentas que esta incluido en el proceso de terminación de contrato. Sin embargo, Recursos Humanos no comunica la terminación del contrato tecnología generando cuentas de usuario inexistentes aumentando el riesgo de fraude.	Diseñar y reforzar el procedimiento de retiro de empleados a las áreas tecnológicas. (Eliminación de privilegios de acceso).

El cumplimiento actual de la organización frente a los controles de terminación o cambio de empleo es:



Bajo

A9 Seguridad Física y de Medio Ambiente

Para cumplir con este dominio de la norma ISO 27002, las instalaciones de procesamiento de información crítica o sensible de la empresa deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con vallas de seguridad y controles de acceso apropiados. Deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones. La protección provista debe ser proporcional a los riesgos identificados.

9.1 Áreas Seguras

Objetivo: Prevenir el acceso físico no autorizado, el daño o la interferencia a la información o las instalaciones.

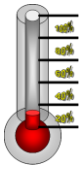
Las instalaciones de procesamiento críticas o sensibles deben ser confinadas en áreas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad apropiadas y controles de acceso. Estos deben estar protegidos físicamente de acceso no autorizado, daño e interferencia.

La protección proveída debe ser acorde con los riesgos identificados.

Análisis

Riesgo Actual	Hallazgos	Recomendaciones
Controles físicos inadecuados pueden arriesgar la seguridad, estabilidad y preservación de los recursos de TI. Fallas a los recursos protegidos físicamente puede resultar en el compromiso, daño o destrucción de los recursos incluyendo hardware, software o datos.	El centro de cómputo principal no permite cumplir con los requerimientos mínimos de seguridad establecidos.	Implementar un Centro de Cómputo, acorde al nivel de riesgo de su plataforma tecnológica y cumpliendo con los requerimientos mínimos de seguridad de la información.

El cumplimiento actual de la organización frente a los controles de área segura es:



Bajo

9.2 Seguridad en el Equipamiento

Objetivo: Prevenir pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

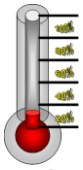
Los equipos deben ser protegidos de las amenazas físicas y ambientales.

La protección de los equipos (incluidos los utilizados fuera de las instalaciones y el retiro de activos) es necesaria para reducir el riesgo de acceso no autorizado a la información y para proteger contra pérdida o daño. También se debe considerar la ubicación del equipo y su eliminación. Controles especiales deben ser requeridos para proteger contra las amenazas físicas y para salvaguardar las instalaciones de soporte como infraestructura de cableado y el suministro de energía.

Análisis

Riesgo/Implicación	Hallazgos	Cumplimiento Actual
Acceso no autorizado al equipamiento puede arriesgar la seguridad, estabilidad y preservación de los recursos de TI. Fallas en la protección de los equipos puede resultar en el compromiso, daño o destrucción de los recursos incluyendo hardware, software y datos. Mantenimiento del equipamiento desatendido puede incrementar el riesgo de fallas en los equipos generando no disponibilidad o pérdida de información. Existe un incremento en el riesgo de pérdida de activos de información debido a que no se retira de forma autorizada. Una disposición descuidada o un reuso de los equipos incrementan los riesgos de comprometer la información confidencial y sensible de la organización.	No existe un centro de cómputo adecuado. Existen equipos que no están raqueados, los cuales pueden ser golpeados y dañados. Las canaletas de datos y energía están protegidas. Existen equipos que se encuentran directamente en el suelo no cumpliendo con requerimientos definidos por fabricante como su ubicación, estática, etc. Se cuenta con procedimientos específicos para retirar o ingresar sistemas al Data Center. No se cuenta con procedimientos para dar de baja sistemas y borrado seguro de información	Cumplir efectivamente con las políticas definidas para centros de computo para garantizar que no se generen eventos catastróficos en el Los equipos que se tengan en el Centro de Cómputo deben estar ubicados en Rack y con los controles mínimos para garantizar que no se golpeen o se accedan de forma no autorizada. Definir un procedimiento de borrado seguro de información y dada de baja de sistemas de información.

El cumplimiento actual de la organización frente a los objetivos de control de seguridad del equipamiento es:



Bajo

A10 Gestión de Operaciones y Comunicaciones

Para cumplir con este dominio de la norma ISO 27002, se deben establecer las responsabilidades y procedimientos para la administración y operación de todas las instalaciones de procesamiento de información.

10.1 Procedimientos y Responsabilidades Operacionales

Objetivo: Garantizar la operación correcta y segura de la instalaciones de procesamiento.

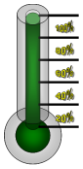
Las responsabilidades y procedimientos para la gestión y operación de todas las instalaciones de procesamiento deben estar establecidas. Esto incluye el desarrollo de los procedimientos operacionales apropiados.

Separación de funciones deben ser implementados, cuando sea posible, para reducir el riesgo de negligencia o uso incorrecto de los sistemas.

Análisis

Riesgo/Implicación	Hallazgos	Cumplimiento Actual
La ausencia de procedimientos de control de cambios incrementa el riesgo de cambios no autorizados que puedan llevarse a cabo en las instalaciones de procesamiento.	El sistema de gestión de calidad garantiza una documentación de los procesos de negocio. .Existe una segregación de tareas. Existe un ambiente de producción y desarrollo.	Definir un procedimiento transversal de control de cambios tanto para la plataforma tecnológica, privilegios de usuarios, planes de continuidad, etc.

El cumplimiento actual de la organización frente a los objetivos de control de seguridad del equipamiento es:



Alto

10.2 Gestión de Entrega de Servicios de Terceros

Objetivo: Implementar y mantener el nivel apropiado de seguridad de información y entrega de servicio alineado con los acuerdos de servicios con terceros.

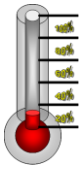
La organización debe revisar la implementación de los acuerdos, monitorear el cumplimiento de los acuerdos y gestionar los cambios para garantizar que los servicios entregados cumplan con todos los requerimientos de los acuerdos de terceros.

Análisis

Riesgo Actual	Hallazgos	Recomendaciones

Riesgo Actual	Hallazgos	Recomendaciones
Al utilizar un servicio de terceros para gestionar las instalaciones de procesamiento se incrementa el riesgo de compromiso, daño o pérdida de información crítica o sensible debido a que los terceros pueden no ser responsables de los controles de seguridad de la organización. Si los terceros no se adhieren a las definiciones de servicio y niveles de entrega se incrementa el riesgo de un servicio inadecuado o incompleto, minimizando la calidad de los procesos de la organización. Sin una adecuada gestión de cambios de los servicios de terceros, se incrementa el riesgo de una entrega de servicio inadecuado introducido en la organización que minimiza la calidad de los procesos de negocio de la organización.	Se definen responsables por los servicios con terceros, quienes deben validar el cumplimiento de objetivos y de niveles de servicio. Los terceros no cuentan con unos lineamientos claros frente a la seguridad de la información. No se cuenta con un procedimiento de gestión de cambios frente a los servicios de terceros.	Analizar los riesgos del acceso de terceros a la información e incluir controles de seguridad y lineamientos claros dentro de los contratos con terceros. Definir un procedimiento de control de cambios e incluir los cambios de los terceros.

El cumplimiento actual de la organización frente al objetivo de control durante el empleo es:



Bajo

10.3 Planeación y Aceptación de Sistemas

Objetivo: Minimizar el riesgo de fallas en sistemas.

Una planeación y preparación avanzada es requerida para garantizar la disponibilidad de una capacidad y recursos adecuados para entregar la ejecución de sistemas requerido.

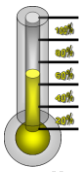
La proyección de requerimientos de capacidad futura debe hacerse para reducir el riesgo de sobrecarga en el sistema.

Los requerimientos operacionales de nuevos sistemas deben ser establecidos, documentados y probados antes de ser aceptados y usados.

Análisis

Riesgo/Implicación	Hallazgos	Cumplimiento Actual
Un plan de capacidad puede minimizar efectivamente el riesgo de fallas en sistema debido a una sobrecarga en el sistema. Adicionalmente reduce el riesgo de cuellos de botella en los sistemas que pueden presentar una amenaza a la seguridad del sistema o a los servicios de usuarios. Si no se define un criterio de aceptación para la implementación o actualización de sistemas de información y si no se lleva a cabo las pruebas de aceptación necesarias antes de su aceptación se incrementa el riesgo que los sistemas no cuenten con la misma ejecución esperada, capacidad y controles de seguridad.	No se cuenta con un monitoreo continuo de los sistemas de información, pero no se refleja de forma estratégica en un plan de capacidad en el cual se analice el crecimiento del mercado y los objetivos de negocio. Se cuenta con un procedimiento claramente definido de desarrollo de software liderado por el área de innovación en el cual se incluye el análisis de requerimientos, validación y asignación de recursos, pruebas, aceptación y puesta en producción.	Definir un plan de capacidad de los sistemas a corto, mediano y largo plazo, el cual es gestionado a través del monitoreo de la capacidad de los sistemas. Incluir dentro de los procedimientos innovación y puesta en producción la gestión de los cambios.

El cumplimiento actual de la organización frente a los objetivos de control de planeación y aceptación de sistemas es:



Medio

10.4 Protección contra Código Malicioso y Código Móvil

Objetivo: Proteger la integridad del software y de la información.

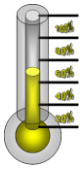
Se requiere estar prevenido para controlar y detectar la introducción del código móvil y el código malicioso no autorizado.

Las instalaciones de procesamiento de información y software son vulnerables a la introducción de código malicioso como virus de computadores, gusanos de red, troyanos y bombas lógicas. Los usuarios deben estar concientizados del daño del código malicioso. Los gerentes deben, cuando sea apropiado, incluir controles para prevenir, detectar y remover código malicioso y controlar el código móvil.

Análisis

Riesgo Actual	Hallazgos	Recomendación
Si no se cuenta con medidas efectivas contra el código móvil se incrementa el riesgo de no disponibilidad de sistemas y/o destrucción de datos.	Se cuenta con herramienta de protección y respuesta frente a virus, spam y malware. No existen controles frente a la protección de código móvil como javascript, ActiveX, etc.	Se debe analizar el código móvil descargado desde Internet y generar conciencia frente a los riesgos de acceder a páginas no autorizadas.

El cumplimiento actual de la organización frente a los objetivos de control de protección de código malicioso es:



Medio

10.5 Back-up

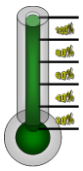
Objetivo: Mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento.

Procedimientos de rutina deben ser establecidos para implementar acuerdos en la política y estrategia de backup (ver también 14.1) para obtener las copias y probar los tiempos de restauración.

Análisis

Riesgo Actual	Hallazgos	Recomendaciones
	Se cuenta con procedimientos de Backup y replicación de los sistemas críticos, y equipos de los empleados claramente definidos.	

El cumplimiento actual de la organización frente a los objetivos de control de backup es:



Alto

10.6 Gestión de Seguridad de Redes

Objetivo: Garantizar la protección de la información en redes y la protección de la infraestructura de soporte.

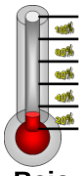
La gestión de seguridad de redes, la cual puede abarcar los límites de la organización, requieren consideraciones cuidadosas de flujo de datos, implicaciones legales, monitoreo y protección.

Controles adicionales se requieren para proteger información sensible que pasa sobre redes públicas.

Análisis

Riesgo Actual	Hallazgos	Recomendaciones
Ausencia de control sobre las características de seguridad de todos los servicios de red incrementa el riesgo de acceso no autorizado y compromiso de datos críticos o sensibles.	Existen solo controles como firewall en la organización con los cuales segmentan y controlan de alguna manera el acceso a los sistemas críticos. No se incluye el derecho a auditar a los terceros.	Se debe realizar auditoria de cumplimiento de políticas de seguridad a terceros que se encuentren gestionando los servicios de red.

El cumplimiento actual de la organización frente a los objetivos de control de protección de código malicioso es:



Bajo

10.7 Tratamiento de Medios

Objetivo: Prevenir la publicación no autorizada, modificación, destrucción retiro de activos e interrupción de actividades de negocio.

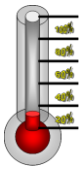
Los medios deben ser controlados y protegidos físicamente.

Los procedimientos operacionales apropiados deben ser establecidos para proteger documentos, medios de cómputo (ej.: cintas, discos), entrada/salida de datos y documentación de sistema de publicación no autorizada, modificación, retiro y destrucción.

Análisis

Riesgo Análisis	Hallazgos	Recomendación
Los intrusos pueden obtener datos sensibles resguardados en medios si no son destruidos apropiadamente. La publicación no autorizada de la documentación del sistema puede resultar en fallas del sistema, corrupción de la configuración y pérdida de la confidencialidad e integridad de la información crítica del negocio.	El manejo de documentos y guias de transporte esta tercerizado y no cumple con estándares frente al tratamiento y transporte en cuanto a seguridad de la información. No cuentan con procedimientos de destrucción de información de forma adecuada. No se cuenta con un tratamiento diferenciado frente a la sensibilidad de la información	Definir un procedimiento de destrucción de información. Llevar a cabo la clasificación de información e implementar controles frente al tratamiento y protección de información de acuerdo a su nivel de clasificación. Incluir auditorías de seguridad a XXXXXX.S.A y terceros.

El cumplimiento actual de la organización frente a los objetivos de control de tratamiento de medios es:



Bajo

10.8 Intercambio de Información

Objetivo: Mantener la seguridad de la información y del intercambio de software entre la organización y entidades externas.

El intercambio de información y de software entre las organizaciones debe basarse en una política formal de intercambio de información, soportado por acuerdo de intercambio y debe cumplir con cualquier legislación relevante (ver cláusula 15).

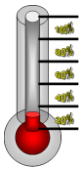
Procedimientos y estándares deben ser establecidos para proteger la información y los medios físicos que contienen información en tránsito.

Análisis

Riesgo Actual	Hallazgos	Recomendación
Sin una política formal de intercambio de información, procedimientos y controles, existe el riesgo que se generen brechas en la confidencialidad o integridad de la información de la organización. Si no se controla el intercambio de	NO se han definido lineamientos como los controles de cifrado, igualmente no existe un procedimiento y lineamiento claro frente a como se debe intercambiar información de acuerdo a su clasificación. No hay controles frente a la entrega de información a través de correo electrónico o mensajería instantánea.	Definir un procedimiento claro de entrega e intercambio de información.

Riesgo Actual	Hallazgos	Recomendación
información se incrementa el riesgo de publicación no autorizada de información sensible. El uso de correo electrónico no cifrado o de mensajes instantáneos incrementa el riesgo de acceso no autorizado o interceptación de mensajes electrónicos, negación de servicio, errores o publicación no autorizada de información crítica transmitida a través de mensajes electrónicos.	.	

El cumplimiento actual de la organización frente a los objetivos de control de intercambio de información es:



Bajo

10.9 Servicios de Comercio Electrónico

Objetivo: Garantizar la seguridad de los servicios de comercio electrónico y el uso seguro de este.

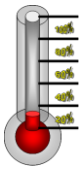
Las implicaciones de seguridad asociadas a los servicios de comercio electrónico, incluyendo transacciones en línea y los requerimientos de control deben ser considerados. La integridad y la disponibilidad de la información publicada a través de sistemas disponibles al público deben ser consideradas.

Análisis

Riesgo Actual	Hallazgos	Recomendaciones
Fallas en la protección de la información implicada en las transacciones en línea puede incrementar el riesgo de actividades fraudulentas, ej.: alteración no autorizada del mensaje, publicación no autorizada, duplicación o reenvío del mensaje no autorizado. Sin la protección adecuada de la	AREVALO S.A. no lleva a cabo comercio electrónico. No existen controles específicos que garanticen la integridad de las operaciones. No existe un procedimiento adecuado para la gestión y publicación de datos que haga parte de información sensible.	Realizar una clasificación de información. Definir controles específicos para garantizar la integridad de las transacciones de los sistemas transaccionales punto a punto. Definir procedimientos de gestión y publicación de datos de información

Riesgo Actual	Hallazgos	Recomendaciones
información electrónica disponible públicamente, la organización puede exponerse a riesgos legales o regulatorios al igual que a riesgos de exposición de información sensible.		sensible.

El cumplimiento actual de la organización frente a los objetivos de control de servicios de comercio electrónico es:



Bajo

10.10 Monitoreo

Objetivo: Detectar actividades de procesamiento de información no autorizadas.

Los sistemas deben ser monitoreados y la información de los eventos de seguridad debe ser registrada. Los registros del operador y de fallas se deben utilizar para garantizar que los problemas de los sistemas de información son identificados.

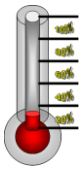
La organización debe cumplir con todos los requerimientos legales aplicables al monitoreo y registro de las actividades.

El monitoreo de sistemas debe ser utilizado para revisar la efectividad de los controles adoptados y para verificar la conformidad del acceso al modelo de política.

Análisis

Riesgo Actual	Hallazgos	Recomendaciones
Fallas en la implementación de las operaciones de monitoreo debe incrementar el riesgo de acceso no autorizado o actividades fraudulentas no notificadas. Computadores no sincronizados en sus relojes reducen la exactitud de los registros de auditoría, obstaculizando la investigación y deteriorando la credibilidad de los registros y de la evidencia en casos disciplinarios o legales.	Se generan registros de auditoría pero no son gestionados de forma permanente. Los equipos no se encuentran sincronizados con un único sistema de tiempo.	Generar un procedimiento de gestión de logs con el fin de generar acciones preventivas frente a problemas o errores en los sistemas. Sincronizar los sistemas de información con la Superintendencia de Industria y Comercio.

El cumplimiento actual de la organización frente a los objetivos de control de monitoreo es:



Bajo

A11. Control de Acceso

Para cumplir con este dominio de la norma ISO 27002, el acceso a la información y los procesos de negocio deben ser controlados sobre la base de los requerimientos la seguridad y de los negocios. Para esto se deben tener en cuenta las políticas de acceso y autorización de la información.

11.1 Requisitos de Negocio para Controlar el Acceso

Objetivo: Controlar el acceso a la información.

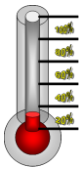
El acceso a la información, instalaciones de procesamiento y procesos de negocio debe ser controlado basado en el negocio y los requerimientos de seguridad.

Las reglas de control de acceso deben tener en cuenta las políticas de diseminación y autorización de información.

Análisis

Riesgo Actual	Hallazgos	Recomendación
La generación de acceso a la información deben ser definidos por el dueño de la información, evitando usos y accesos indebidos que no correspondan al perfil de usuario definido en la Organización	En la actualidad el acceso a la información es otorgada por algunos dueños de la información e implementados por el custodio de la información (tecnología); sin embargo, no existe una política definida por la alta dirección que estandarice el acceso a la información.	No existe una política definida para el acceso a la información. Validar los accesos en la información de acuerdo a los roles asignados al ingresar a la Organización.

El cumplimiento actual de la organización frente a los objetivos de control de requerimientos de acceso de negocio es:



Bajo

11.2 Gestión de Acceso de Usuarios

Objetivo: Garantizar que el acceso de usuarios es autorizado y prevenir el acceso no autorizado a los sistemas de información.

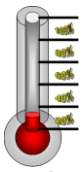
Se deben implementar procedimientos formales para controlar la definición de los derechos de acceso a los sistemas de información y servicios.

Los procedimientos deben cubrir todas las etapas del ciclo de vida del acceso de usuarios, desde el registro inicial de nuevos usuarios hasta el desregistro final de los usuarios que no requieran más su servicio. Se debe prestar especial atención a la necesidad de control de entrega de privilegios de acceso, que proveen la capacidad de sobrescribir controles del sistema.

Análisis

Riesgo Actual	Hallazgos	Recomendación
La ausencia de procesos de revisión formal de acceso de usuarios incrementa el riesgo que usuarios tengan niveles de acceso inapropiados al sistema o a los datos.	No existen procedimientos frente a la gestión de los privilegios y cuentas. Dentro del procedimiento de gestión de accesos no se define auditorías frente a cuentas no utilizadas. Se definen los roles y privilegios para los sistemas críticos.	Llevar a cabo análisis y auditoría sobre las cuentas e incluir dentro del procedimiento de gestión de cuentas la terminación de uso de cuentas.

El cumplimiento actual de la organización frente a los objetivos de control de acceso de usuarios es:



Bajo

11.3 Responsabilidades de Usuario

Objetivo: Prevenir accesos no autorizados para evitar el robo de información o el acceso al procesamiento de la información.

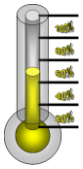
La cooperación de los usuarios autorizados es esencial para la seguridad eficaz.

Los usuarios deben ser conscientes de su responsabilidad para mantener los controles de acceso, particularmente para el uso de contraseñas y la seguridad de los equipos.

Una política de escritorios limpios y de bloqueos de estaciones debe implementarse para reducir el riesgo de accesos no autorizados y el daño a documentos, archivos y sistemas de información.

Riesgo/Implicación	Hallazgos	Cumplimiento Actual
Si los usuarios no tienen suficiente conciencia en cuanto a la seguridad de las contraseñas, existe el riesgo de que empleen contraseñas débiles y fácilmente descifrables. La ausencia de protección apropiada sobre los equipos desatendidos puede incrementar la opción de uso no autorizado de dicho equipo. Si no se implementa una política de escritorios limpios o de borrado de pantallas se incrementa el riesgo de acceso no autorizado, pérdida o daño de información.	Hay ausencia de sensibilización frente al uso de contraseñas. Existen documentos con información sensible en los escritorios.	Establecer y sensibilizar a los empleados frente al uso de contraseñas, bloqueo de estaciones y documentos con información sensible sin protección.

El cumplimiento actual de la organización frente a los objetivos de control frente a las responsabilidades de usuario es:



Medio

11.4 Control de Acceso de Red

Objetivo: Prevenir acceso no autorizado a los servicios de red.

Acceso tanto interno como externo a los servicios de red debe ser controlado.

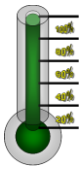
El acceso de los usuarios a las redes o a sus servicios no debe comprometer la seguridad de los servicios de red garantizando:

a) Interfaces apropiadas implementadas entre la red de la organización y las redes de otra organización o redes públicas.
b) Mecanismos de autenticación apropiados son implementados para usuarios y equipos.
c) Controlar el acceso de usuarios a los servicios de información.

Hallazgos

Riesgo Actual	Hallazgos	Recomendación
Muchos equipos de cómputos son instalados con puertos para propósitos de mantenimiento. Estos puertos pueden proveer posibilidades de acceso no autorizado.	Se definen unos lineamientos específicos frente al acceso remoto a los sistemas incluyendo canales dedicados, cifrado, etc. La autenticación remota se realiza con usuario y contraseña y con dirección IP del sistema remoto. Para el acceso remoto se instala software que genera una identificación del sistema remoto. No se han definido estándares de aseguramiento. Las redes se encuentran segregadas.	Desarrollar e implementar estándares de aseguramiento para cada plataforma.

El cumplimiento actual de la organización frente a los objetivos de control de acceso a la red es:



Alto

11.5 Control de Acceso de Sistema Operativo

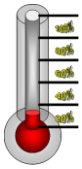
Objetivo: Prevenir el acceso no autorizado al sistema operativo.

Dispositivos de seguridad deben ser usados para restringir el acceso al sistema operativo de usuarios autorizados. Dichos dispositivos deben ser capaces de:

a) Autenticar a los usuarios autorizados, de acuerdo con la política de control de acceso definida.
b) Registras los intentos de autenticación exitosos y fallidos al sistema.
c) Registrar el uso de privilegios especiales del sistema.
d) Generar alarmas cuando las políticas de seguridad no se cumplan.
e) Proveer medios apropiados de autenticación.
f) Cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

Riesgo Actual	Hallazgos	Recomendación
En muchos casos, las contraseñas son la "clave" para acceder a la información. Sin controles adecuados alrededor de la configuración y uso de contraseñas, el sistema se hace vulnerable.	No existe un sistema integrado para la gestión centralizada de contraseñas (Identity Management). No se cuenta con políticas de seguridad con lo cual no se puede garantizar que las contraseñas cumplan con los requerimientos requeridos. Las sesiones no cuentan con controles de bloqueo de sesiones inactivas.	Definir e implementar políticas para garantizar seguridad en las contraseñas de los usuarios.

El cumplimiento actual de la organización frente a los objetivos de control de acceso de sistema operativo es:



Bajo

11.6 Control de Acceso de las Aplicaciones y la Información

Objetivo: Prevenir el acceso no autorizado a la información de los sistemas y las aplicaciones.

Dispositivos de seguridad deben utilizarse para restringir el acceso a las aplicaciones y a los sistemas.

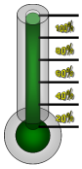
El acceso lógico a las aplicaciones y a la información debe ser restringido a los usuarios autorizados.

Los aplicativos deben:
a) Controlar el acceso de los usuarios a la información y las funciones de la aplicación de acuerdo con la política de control de acceso definida.
b) Proveer protección de acceso no autorizado de cualquier utilidad, software de sistema operativo y software malicioso que sea capaz de sobrescribir o evitar los controles de los sistemas o aplicaciones.
c) No comprometer otros sistemas con los recursos de información que son compartidos.

Análisis

Riesgo Actual	Hallazgos	Recomendación
	Los privilegios son definidos con anterioridad de acuerdo a los requerimientos de negocio y plasmados en la matriz de privilegios de los sistemas. Los sistemas de misión crítica cuenta con más controles de seguridad y se encuentran en redes segregadas.	Realizar auditorías para validar los privilegios de las cuentas creadas en los sistemas.

El cumplimiento actual de la organización frente a los objetivos de control de acceso a las aplicaciones es:



Alto

A12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Para cumplir con este dominio de la norma ISO 27002, se deben tener procesos seguros en el desarrollo, adquisición y mantenimiento de sistemas; esto incluirá infraestructura, aplicaciones comerciales y aplicaciones desarrolladas por el usuario. El diseño e implementación de los procesos comerciales que apoyen la aplicación o servicio pueden ser cruciales para la seguridad. Los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo de los sistemas de información.

Todos los requerimientos de seguridad, incluyendo la necesidad de planes de reanudación, deben ser identificados en la fase de requerimientos de un proyecto y justificados, aprobados y documentados como una parte de la totalidad del caso de negocios de un sistema de información.

12.1 Requerimientos de Seguridad de los Sistemas de Información

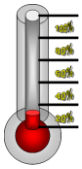
Objetivo: Garantizar que la seguridad sea una parte integral de los sistemas de información.

Todos los requerimientos de seguridad deben ser identificados en la fase de requerimientos del proyecto y justificado, aprobado y documentado como parte del caso de negocio del sistema de información.

Análisis

Riesgo/Implicación	Hallazgos	Cumplimiento Actual
Los controles introducidos en la fase de diseño son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.	En la actualidad existe un proveedor que desarrolla parametrizaciones adicionales en sus sistemas de información. Sin embargo, no existe un procedimiento formal que valide los riesgos en seguridad y aplique antes del desarrollo los controles necesarios para preservar el nivel de seguridad definido por la Organización.	Se debe establecer un procedimiento de gestión de cambios de nuevos desarrollos y versiones. Se debe incluir en la fase de análisis de requerimientos al líder de seguridad de la información.

El cumplimiento actual de la organización frente a los objetivos de control de requerimientos de seguridad es:



Bajo

12.2 Procesamiento Correcto en las Aplicaciones

Objetivo: Prevenir errores, pérdida, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.

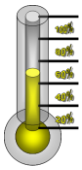
Los controles apropiados deben ser diseñados en las aplicaciones, incluyendo desarrollo de aplicaciones de usuarios para garantizar el procesamiento correcto. Estos controles deben incluir la validación de datos de entrada, procesamiento interno y salida de datos.

Controles adicionales se requieren para los sistemas que procesan o tienen un impacto sobre información crítica o sensible. Dichos controles deben ser determinados basados en los requerimientos de seguridad y un análisis de riesgo.

Análisis

Riesgo/Implicación	Hallazgos	Cumplimiento Actual
Sin autenticación de mensajes, se incrementa el riesgo de que cambios no autorizados o accidentes o corrupción al contenido transmitido por mensajes electrónicos no sea detectado.	Las aplicaciones cuentan con controles de entrada, de procesamiento y de salida de la información procesada. No existen controles para preservar la integridad de mensajes	Se debe realizar una autenticación de las transacciones de los usuarios.

El cumplimiento actual de la organización frente a los objetivos de control de procesamiento correcto de las aplicaciones es:



Medio

12.3 Controles Criptográficos

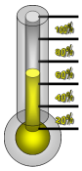
Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información en términos criptográficos.

Se debe desarrollar una política en el uso de controles criptográficos. La gestión de llaves debe implementarse para soportar el uso de técnicas criptográficas.

Análisis

Riesgo Actual	Hallazgos	Recomendación
Fallas en el desarrollo de una política de controles criptográficos puede incrementar el riesgo que información sensible sea protegida de forma inadecuada y que la organización no cumpla con las legislaciones definidas para el uso de cifrado. Una gestión inapropiada de llaves puede comprometer la información cifrada.	No se cuenta con una política de utilización de controles criptográficos.	Establecer procedimientos para la gestión de llaves y equipos criptográficos.

El cumplimiento actual de la organización frente a los objetivos de control criptográficos es:



Medio

12.4 Seguridad en los Sistemas de Archivos

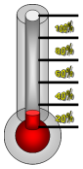
Objetivo: Garantizar la seguridad de los sistemas de archivos.

Acceso a los sistemas de archivos y código fuente de programas debe ser controlado, y los proyectos de IT y actividades de soporte deben ser conducidos de una forma segura. Se debe tener cuidado para evitar la exposición de datos sensibles en los ambientes de pruebas.

Análisis

Riesgo/Implicación	Hallazgos	Cumplimiento Actual
Sin los controles apropiados en la implementación de software, el riesgo de corrupción de sistema operativo se incrementa. Sin los controles apropiados sobre los datos de prueba, el riesgo de publicación no autorizada o obtención de resultados sensibles o información clasificada se incrementa.	No existen controles para garantizar que la instalación de programas sea autorizada y que el software sea el autorizado. Los sistemas de desarrollo y de homologación cuentan con réplicas de datos de producción y no se cuentan con controles efectivos para garantizar su confidencialidad. No existen controles para la protección de código fuente de las aplicaciones.	Gestionar de forma efectiva el software instalado en las máquinas. Garantizar controles sobre la información de producción no pueda ser revelada de forma no autorizada en los sistemas de desarrollo u homologación. Establecer herramientas para la protección de código fuente de las aplicaciones.

El cumplimiento actual de la organización frente a los objetivos de control de los sistemas de archivos:



Bajo

12.5 Seguridad en el Proceso de Desarrollo y Soporte

Objetivo: Mantener la seguridad del software de aplicación del sistema y la información.

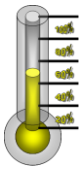
Los ambientes de soporte y proyectos deben ser controlados estrictamente.

Los gerentes responsables por los sistemas de aplicación también deben ser responsables por la seguridad del proyecto o el ambiente que lo soporta. Ellos deben garantizar que todos los cambios propuestos al sistema sean revisados y verificados y que no comprometan la seguridad del sistema o del ambiente operacional.

Análisis

Riesgo/Implicación	Hallazgos	Cumplimiento Actual
Sin procedimientos formales de control de cambios, el riesgo de cambios no autorizados, no probados o inapropiados se incrementa, resultando en la corrupción del sistema de información. Revisiones y pruebas insuficientes después de los cambios del sistema operativo (ej.: aplicación de parches de software) puede incrementar el riesgo de fallas en el aplicativo o brechas de seguridad. Modificaciones no controladas, compra o uso de software puede incrementar el riesgo de posibles canales encubiertos y fuga de información.	Se cuenta con procedimientos de cambios. Los cambios cuentan con un proceso de análisis de requerimientos y de impacto sobre la plataforma. La implementación de parches de sistemas no es analizada a través del proceso de desarrollo de innovación. No existen controles frente a la fuga de información.	Implementar controles frente a la fuga de información. Involucrar al proveedor de desarrollo en las etapas de seguridad definidas por la Organización.

El cumplimiento actual de la organización frente a los objetivos de control de desarrollo de sistemas:



Medio

12.6 Gestión de Vulnerabilidades Técnicas

Objetivo: Reducir el riesgo resultante de la explotación de vulnerabilidades técnicas publicadas.

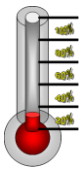
La gestión de vulnerabilidades técnicas debe ser implementada de forma efectiva, sistemática y repetible con mediciones que confirmen su efectividad. Estas consideraciones deben incluir sistemas operativos y otras aplicaciones en uso.

Análisis

Riesgo Actual	Hallazgos	Recomendación
Fallas en la obtención de información en un tiempo prudencial acerca de las vulnerabilidades técnicas incrementa el riesgo de acceso no autorizado, y la ocurrencia de	No existe una gestión adecuada y permanente de identificación y explotación de vulnerabilidades.	Llevar a cabo pruebas de vulnerabilidad efectivas y sistemáticas, que permitan gestionar de forma permanente posibles ausencias de control.

Riesgo Actual	Hallazgos	Recomendación
incidentes de seguridad relacionados con la confidencialidad, integridad y disponibilidad a los sistemas de información de la organización.		

El cumplimiento actual de la organización frente a los objetivos de control de vulnerabilidades técnicas:



Bajo

A13 Gestión de Incidentes de Seguridad

Para cumplir con el dominio de Gestión de Incidentes de la norma ISO 27002, la organización debe contar con un marco de trabajo para garantizar que cada evento de seguridad sea identificado, analizado y tratado de la mejor forma. Cada incidente de seguridad debe proveer al sistema de gestión bases sólidas para su mejora.

13.1 Reporte de Eventos de Seguridad de la Información

Objetivo: Garantizar que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información son comunicados en el tiempo correcto y las acciones correctivas son implementadas.

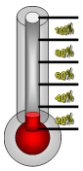
Procedimientos de reporte y de escalamiento de eventos deben ser implementados. Todos los empleados, contratistas y usuarios deben conocer y entender los procedimientos de reporte de los diferentes tipos de eventos y debilidades que pueden generar un impacto en la seguridad de los activos de la organización. Estos se requieren para reportar cualquier evento de seguridad de información y debilidad lo más pronto posible al contacto designado.

Análisis

Riesgo Análisis	Hallazgos	Recomendación
Ausencia de conocimiento de eventos de seguridad de la información incrementa el riesgo que no se lleven a cabo respuestas adecuadas o acciones de mitigación.	No existe una sensibilización adecuada de cuales son incidentes de seguridad dentro de la organización. No se han definido los tipos de incidentes de seguridad al igual que no existe conocimiento de estos por parte del usuario final.	Incluir en la sensibilización la definición de incidentes y el tipo de incidentes. Definir un procedimiento de gestión de incidentes

Riesgo Análisis	Hallazgos	Recomendación
	En la actualidad existe un punto de reporte de eventos (HelpDesk) y puede ser utilizado como el canal para recibir los incidentes de seguridad.	

El cumplimiento actual de la organización frente a los objetivos de control de reporte de eventos de seguridad de la información:



Bajo

13.2 Gestión de incidentes de seguridad de la información y mejora

Objetivo: Garantizar un acercamiento consistente y efectivo implementado para gestionar los incidentes de seguridad de la información.

Las responsabilidades y procedimientos deben ser implementados para tratar eventos de seguridad de información y debilidades efectivamente cuando estos sean reportados. Un proceso de mejora continua debe ser implementado para la respuesta, monitoreo, evaluación y gestión de los incidentes de seguridad.

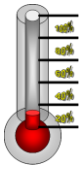
Cuando se requiera evidencia, se debe recolectar con el fin de cumplir con los requerimientos legales.

Análisis

Riesgo Actual	Hallazgos	Recomendación
Fallas en el establecimiento de responsabilidad y procedimientos pueden generar que la respuesta a los incidentes de seguridad no sea efectiva, ordenada y que el tiempo en resolver el evento no sea el adecuado. Fallas en la implementación de mecanismos incrementa el riesgo que no sean notificados incidentes recurrentes o de alto impacto. Fallas en la generación de reglas y estándares para generación y recolección de evidencia puede	En la actualidad no existe un lineamiento frente a la gestión de crisis de eventos que afectan la disponibilidad. No existen metodologías para analizar el costo de los incidentes.	Definir unos lineamientos específicos para responder frente a los incidentes, clasificarlos y medirlos.

Riesgo Actual	Hallazgos	Recomendación
incrementar el riesgo que esta sea inadecuada o inadmisible.		

El cumplimiento actual de la organización frente a los objetivos de control gestión de incidentes de seguridad es:



Bajo

A14 Gestión de Continuidad del Negocio

Para cumplir con este dominio de la norma ISO 27001, se debe implementar un proceso de administración de la continuidad de los negocios para reducir la discontinuidad ocasionada por desastres y fallas de seguridad (que pueden ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas en el equipamiento, y acciones deliberadas) a un nivel aceptable mediante una combinación de controles preventivos y de recuperación.

Se deben analizar las consecuencias de desastres, fallas de seguridad e interrupciones del servicio. Se deben desarrollar e implementar planes de contingencia para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos requeridos. Dichos planes deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y Administración.

La administración de la continuidad de los negocios debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

14.1 Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio

Objetivo: Responder a las interrupciones de las actividades de negocio y para proteger los procesos críticos de negocio de los efectos de fallas mayores de los sistemas de información o desastres y para garantizar su recuperación en el tiempo apropiado.

Una gestión de la continuidad del negocio debe ser implementada para minimizar el impacto en la organización y recuperación de pérdida de los activos de información (resultado de desastres naturales, accidentes, fallas de equipo y acciones deliberadas) a un nivel aceptable mediante combinaciones de controles preventivos y de recuperación. Este proceso debe identificar los procesos críticos del negocio e integrar la gestión de requerimientos de seguridad de información

de la continuidad del negocio con otros requerimientos de continuidad relacionados como son la operación, personal, materiales, transporte e instalaciones.

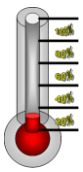
La consecuencia de desastres, fallas de seguridad, pérdida de servicio y disponibilidad del servicio debe soportarse en un análisis de impacto al negocio. Los planes de continuidad deben ser desarrollados e implementados para garantizar una recuperación en el tiempo adecuado de las operaciones esenciales. La seguridad de la información debe integrarse como parte del proceso de continuidad del negocio y otros procesos de gestión dentro de la organización.

La gestión de la continuidad del negocio debe incluir controles para identificar y reducir el riesgo, dentro del proceso de análisis de riesgo, limitando las consecuencias de incidentes de daño y garantizando que la información requerida para el proceso de negocio esta disponible.

Análisis

Riesgo Actual	Hallazgos	Recomendación
Sin un proceso formal para gestionar y asegurar la continuidad del negocio, se incrementa el riesgo que la organización no pueda recuperarse de un desastre significativo. Sin una consideración apropiada de todos los elementos de riesgo, la probabilidad de que la estrategia de continuidad del negocio sea adecuada se reduce. Los planes disminuyen el riesgo y el impacto que un cambio/desastre súbito puede generar la negocio.	No existe un plan definido de continuidad del negocio. No existe un proceso formal para gestionar la continuidad del negocio. No existe un proceso de continuidad del negocio que incluya interfaces con otros procesos como gestión de incidentes, control de cambios gestión de activos y gestión de riesgos. No se han definido escenarios de riesgo específicos. Es necesario contar con una gestión continua analizando si existen nuevos posibles escenarios. Existen planes para garantizar la continuidad de la plataforma tecnológica, pero la operación no se está garantizando. Se llevan a cabo periódicamente pruebas de los planes.	Se debe definir e implementar un plan de continuidad del negocio. El proceso de continuidad del negocio debe estar alineado a la operación y contar con interfaces con otros procesos claves de seguridad. El plan de crisis debe cubrir el peor escenario, por lo tanto el actual no contempla el hecho de que las personas responsables por el plan de crisis están en las instalaciones donde se da el evento. Se debe incluir el centro de operaciones alterno con el fin de garantizar continuidad del negocio.

El cumplimiento actual de la organización frente a los controles de gestión de la continuidad del negocio es:



Bajo

A15 Cumplimiento

Para cumplir con este dominio de la norma ISO 27002, se debe procurar asesoramiento sobre requisitos legales específicos por parte de los asesores jurídicos de la organización, o de abogados convenientemente calificados.

15.1 Cumplimiento con los requerimientos legales

Objetivo: Evitar brechas en las obligaciones legales, estatutarias, regulatorios o contractuales y de cualquier requerimiento de seguridad.

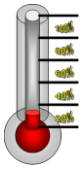
El diseño, operación, uso y gestión de los sistemas de información debe soportarse en los requerimientos de seguridad contractuales, regulatorios y legales.

Advertencias acerca de los requerimientos legales específicos deben ser identificados por los consejeros legales de la organización. Los requerimientos legislativos varían de país a país por lo tanto se debe analizar cuando se transmite información entre diferentes países.

Análisis

Riesgo Actual	Hallazgos	Recomendaciones
Sin una persona responsable frente a las nuevas necesidades regulatorias y de ley, se incrementa el riesgo que la organización no este cumpliendo con los requerimientos legales. Controles apropiados mitigan el riesgo de no cumplir con las restricciones legales sobre los derechos de propiedad intelectual.	En la actualidad existe un responsable directo del cumplimiento regulatorio. El área legal asesora y acompaña pero nadie queda como responsable del cumplimiento. Existe adecuada identificación de la legislación en seguridad aplicable a la Organización. Existen controles para resguardar la pérdida , destrucción o falsificación de los registros clave de la Organización. No existen controles apropiados para garantizar que se cumplan con los derechos de propiedad intelectual. No se persuade y sensibiliza a los usuarios frente al uso de la plataforma en la inducción. No se encuentran alineadas las políticas de seguridad de la información y los aspectos regulatorios de cumplimiento establecidos por la Ley; al igual que no se valida el cumplimiento técnico de estas.	Se debe trabajar en la protección de datos privados. Se debe involucrar los aspectos regulatorios al interior del sistema de gestión de seguridad de la información. Se debe involucrar dentro de la gestión de seguridad, el cumplimiento de aspectos regulatorios. Involucrar en el análisis de riesgo, posibles no cumplimientos regulatorios.

El cumplimiento actual de la organización frente a los objetivos de control de cumplimiento regulatorio es:



Bajo

15.2 Cumplimiento con la Política de Seguridad y Estándares, y Cumplimiento Técnico.

Objetivo: Garantizar el cumplimiento de los sistemas con la política de seguridad y los procedimientos de la organización

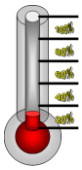
La seguridad de los sistemas de información debe ser revisada regularmente.

Las plataformas técnicas y los sistemas de información deben ser auditados para medir el cumplimiento de la implementación de políticas y estándares de seguridad de la organización.

Análisis

Riesgo Actual	Hallazgos	Recomendación
Sin dichas revisiones, se incrementa el riesgo de problemas de seguridad y no cumplimiento de políticas sin detectar o no correctas. Sin la ejecución de dichas revisiones, el riesgo de incumplimiento en los sistemas frente a la implementación de estándares se incrementa, haciéndolo indetectable o incorregible.	No existe un seguimiento frente al cumplimiento de políticas de seguridad. No se sabe en la actualidad si las políticas son efectivas si gestionan un riesgo latente o si no son aplicables en la organización.	Definir un seguimiento frente al cumplimiento e implementación de políticas de seguridad.

El cumplimiento actual de la organización frente a los objetivos de control de cumplimiento de políticas y estándares es:



Bajo

15.3 Consideraciones de Auditorías de Sistemas de Información

Objetivo: Maximizar la efectividad y minimizar la interferencia del proceso de auditoría de los sistemas de información.

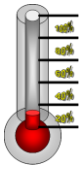
Deben existir controles para salvaguardar los sistemas operacionales y las herramientas de auditoría durante las auditorías de sistemas.

Se requiere una protección adecuada para salvaguardar la integridad y prevenir el uso incorrecto de las herramientas de auditoría.

Análisis

Riesgo Actual	Hallazgos	Recomendación
Utilidades o comandos sensibles pueden ser usados de forma no apropiada para sobrescribir los controles de seguridad y deteriorar la integridad del sistema.	No se generan auditorías de forma gestionada a través de procedimientos en el cual se define el plan de auditoria, el cronograma, etc. No existen controles para garantizar la integridad de los registros de auditoria de los sistemas.	Implementar herramientas y procesos de auditoria en los sistemas de información.

El cumplimiento actual de la organización frente a los objetivos de control de consideraciones de auditoría es:



Bajo

4. Acciones e Implantación de Controles

Basado en el análisis hecho a la situación actual del estándar ISO 27002 que presenta AREVALO S.A., se recomiendan las siguientes acciones para las cuales la organización deberá prestar especial atención e implementar de forma inmediata. Ellas tienen por objetivo preservar la integridad, confidencialidad y disponibilidad de la información las cuales se están viendo comprometidas por la falta de implementación de estas acciones y son los puntos más relevantes del análisis hecho al cumplimiento de la norma.

4.1. ACCIÓN 1 – Clasificación de Información

Implantar el modelo de clasificación de la información de forma inmediata. Se debería comenzar con un esquema simple de clasificación de información.

4.2. ACCIÓN 2 – Organización de Seguridad

Organizar el área de seguridad de la información de la empresa para desarrollar proyectos, generar lineamientos, etc. Definir su gobierno generando modelos de decisión, procesos, políticas, estándares, etc.

4.3. ACCIÓN 3 – Comité de Seguridad

Organizar el Comité de Seguridad, con personal multidisciplinario y acompañamiento de la gerencia, adicionar dicho grupo al organigrama de la empresa otorgándole facultades para definir e implementar todos los temas desarrollados.

4.4. ACCIÓN 4 – Políticas de Seguridad

El Comité de Seguridad deberá generar el documento de políticas de seguridad, donde defina los lineamientos de la Organización frente a la seguridad de la información. Este documento debe ser aceptado por la gerencia, publicado y aceptado por el personal.

4.5. ACCIÓN 5 – Gestión de Vulnerabilidades

Hacer una evaluación del Nivel de Seguridad de los sistemas informáticos que soportan los procesos de negocio, a través de pruebas de vulnerabilidad, diagnósticos de seguridad, etc.

4.6. ACCIÓN 6 – Escritorios Limpios

Implementar políticas de escritorios limpios en toda la organización, dicha política deberá extenderse a documentación entregada por los sistemas de impresión, información escrita en tableros en salas de reuniones, etc.

4.7. ACCIÓN 7 – Estrategia de Sensibilización

Desarrollar una estrategia de sensibilización y entrenamiento en seguridad de la información para todas las personas de AREVALO S.A.

4.8. ACCIÓN 8 – Estándares de Aseguramiento de Plataforma

Se deben definir y desarrollar los controles mínimos necesarios para garantizar una plataforma segura en producción. Todos los sistemas de información que soporten las operaciones de AREVALO S.A. deben tener como mínimo los controles definidos en las plantillas de aseguramiento.

4.9. ACCIÓN 9 – Análisis de Riesgo

Analizar el riesgo y validar el valor de la información que crea, gestiona y se resguarda en los procesos críticos de la organización. Validar los controles necesarios para garantizar la integridad, confidencialidad y disponibilidad de esta.

4.10. ACCIÓN 10 – Gestión de Incidentes de Seguridad

Crear un Equipo de Respuesta ante Emergencias e Incidentes de Seguridad Informática junto con la definición de los procedimientos asociados. Se puede utilizar el HelpDesk actual, pero expandir los procedimientos para administrar y responder frente a los incidentes de seguridad.

4.11. ACCIÓN 11 – Implementación de Recomendaciones

Atender las recomendaciones hechas en cada dominio de la norma para implantar los controles necesarios en AREVALO S.A.

5. Recomendaciones Generales

Estas recomendaciones se hacen para darle a AREVALO S.A. pautas para alinear su Sistema de Seguridad de la Información (SGSI) con la norma ISO 17799:2005 y con el estándar ISO 27001.

Es necesario que se establezcan los lineamientos y alcances del Modelo, y se definan los diferentes activos de Información (Inventario de Activos de Información), sus amenazas y vulnerabilidades, el riesgo o impacto que puedan tener en el negocio (Análisis de Riesgos Informáticos) y los controles necesarios para protegerlos. Esto dentro de un modelo gestionado que permita mantener el ciclo de vida del sistema según lo requiere la norma.

Para esto, AREVALO S.A. deberá desarrollar entre otras las siguientes actividades como parte del proceso de implementación de su Sistema de Administración de Seguridad de la Información:

- Establecer la importancia de la información y de la Seguridad de la Información en sus procesos de negocio.

En este punto se debe establecer claramente:

  - Los objetivos del negocio y los activos de información que soportan el proceso.

  - Mantener y gestionar un proceso completo de Análisis de Riesgos para los activos de Información y establecer los requerimientos de protección para diferentes situaciones de daño.

  - Definir una Política de Seguridad de Información, en la que se consigne la intención y el compromiso de la gerencia con la seguridad de la información, teniendo como base la importancia de la información en el desarrollo del negocio. En resumen, la política debe indicar claramente el convencimiento gerencial que si la información no está segura, el negocio se verá afectado.

- Establecer la organización de Seguridad de la Información en la Organización:

  - Establecer el grupo o comité de Seguridad de la Información, el cual debe estar encabezado por el Director de AREVALO S.A o un delegado suyo y en el cual deben participar representantes de diferentes áreas de la misma.

  - Establecer los diferentes grupos de trabajo para el desarrollo de todas las actividades de Administración necesarias; entre ellos:

    1. Análisis de Riesgos
    2. Planes de concientización
    3. Plan de Contingencia o Recuperación de Desastres
    4. Definición y mantenimiento de políticas
    5. Gestión de Activos de información.

- Implementar el modelo de clasificación de la información, y aplicar los controles necesarios para el manejo de cada una de las categorías.

- Identificar y clasificar los activos de Información y su nivel de acceso, de manera que mantenga coherencia con las políticas definidas y las nuevas políticas que se definan.

- Gestionar y Mantener un proceso de Análisis de Riesgos de los activos de Información y establecer o definir la forma de administrar el riesgo.

- Seleccionar los controles necesarios para lograr los niveles de riesgo aceptados por la organización, con base en los requerimientos identificados por el análisis de riesgos, y por otros aspectos derivados de las normas ISO 17799:2005 e ISO 27001.

- Definir las políticas de seguridad, los procedimientos, estándares y soluciones tecnológicas que se requieran, como parte de los controles seleccionados.

- Implementar las estrategias de mitigación del Riesgo que se hayan definido y monitorear su efectividad. Establecer y mantener un proceso continuo de concientización y educación en seguridad de la Información a todo nivel dentro de la organización.