**Plan de Implantación ISO/IEC 27001 en SOC**

# Informe Análisis Diferencial

**Tabla del documento**

| | |
|---|---|
| **Tipo de documento** | **Informe** |
| **Autor** | |

**Versión**

| Versión | Fecha | Observaciones |
|---|---|---|
| **1.0** | **16/03/2019** | **Versión inicial del documento** |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| **ISO27001 - PLAN / DO / CHECK / ACT** | | | | |
| | **C. 4.1.** | **4.1 Comprensión de la organización y de su contexto** | La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de seguridad de la información. | **CUMPLE**<br>**Existe un conocimiento expreso del Contexto de la Organización y las Partes interesadas:**<br>**- Existe documentación sobre conocimiento de Mercado, estragegias de la organización y una valoración de riesgos existentes dentro del mercado de la Ciberseguridad.** |
| | **C. 4.2.** | **4.2 Comprensión de las necesidades y expectativas de las partes interesadas** | las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información;<br>los requisitos de estas partes interesadas que son relevantes para la seguridad de la información. | **NO CUMPLE**<br>**Se tiene conocimentos de cuales son las partes interesadas y sus necesidades.**<br>**No están recogidas de manera exhaustiva los requisitos; ni consIderada la valoración de su cumplimiento.** |
| | **C. 4.3.** | **4.3 Determinación del alcance del sistema de gestión de seguridad de la información** | a) las cuestiones externas e internas referidas en el apartado 4.1;<br>b) los requisitos referidos en el apartado 4.2;<br>c) las interfaces y dependencias entre las actividades realizadas por la organización y las que se llevan a cabo por otras organizaciones. | **CUMPLE PARCIALMENTE**<br>**En consideración a los apartados 4.1. (ver)**<br>**En consideración al apartado 4.2. (ver)**<br>**Esta perfectamente delimitado el alcance en base a que se considera el SOC-MADRID y sus actividades y procesos gestionados.** |
| | **C. 4.4.** | **4.4 Sistema de gestión de seguridad de la información** | La organización debe establecer, implementar, mantener y mejorar de manera continúa un sistema de gestión de seguridad de la información, de acuerdo con los requisitos de esta norma internacional. | **NO CUMPLE**<br>**La organización como tal no tiene implantado un sistema de Gestión (tiene algunnos procesos de Gestión parcialmente desarrollados pero no conectados y discontinuados).** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **C. 5.1** | **5.1 Liderazgo y compromiso** | a) asegurando que se establecen la política y los objetivos de seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización;<br>b) asegurando la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización;<br>c) asegurando que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles;<br>d) comunicando la importancia de una gestión de la seguridad de la información eficaz y conforme con los requisitos del sistema de gestión de seguridad de la información;<br>e) asegurando que el sistema de gestión de seguridad de la información consigue los resultados previstos;<br>f) dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de seguridad de la información;<br>g) promoviendo la mejora continua; y<br>h) apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad. | **NO CUMPLE**<br>**No hay establecida como tal una política de Seguridad. Ni objetivos concretos de seguridad de la información.**<br>**Tampoco esta cntemplada esta relación.**<br>**Existe una gestión de recursos en la organizacíon (pero bastante reactiva, sin considerar aspectos de seguridad).**<br>**Existen mecanismos de comunicación discretos y no gestionados sobre aspectos de seguridad.**<br>**No están establecidos mecanismos de seguimiento y medición.**<br>**No se realiza de manera ordenada y procedimentada.**<br>**La mejora contnua no está considerada como un proceso en la organización.**<br>**Actualmente es una preocupación, pero no es un foco en que se esté trabajando.** |
| | **C. 5.2** | **5.2 Política** | La alta dirección debe establecer una política de seguridad de la información que: | **NO CUMPLE**<br>**No hay declarada una Política de Seguridad como tal en la organización.** |
| | **C. 5.3** | **5.3 Roles, responsabilidades y autoridades en la organización** | La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen dentro de la organización. | **NO CUMPLE**<br>**Existe un modelo de organización que es conocido por la Organización. No está establecido, como tal, roles y responsabilidades en Seguridad de la Información.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **C. 6.1.1** | **6.1.1. Acciones para tratar los riesgos y oportunidades. Consideraciones generales** | Al planificar el sistema de gestión de seguridad de la información, la organización debe considerar las cuestiones a las que se hace referencia en el apartado 4.1 y los requisitos incluidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario tratar con el fin de: | **NO CUMPLE**<br>**Hay una identificación de Riesgos asociados al Negocio, al Contexto y laas Partes interesadas**<br>**No hay establecido un proceso, un a metodología de base y por lo tanto no se realiza de manera sistemática un análisis de riesgos en la organización (no están declaradaos los respoinsable , ni el alcance)** |
| | **C. 6.1.2** | **6.1.2 Apreciación de riesgos de seguridad de la información** | La organización debe definir y aplicar un proceso de apreciación de riesgos de seguridad de la información que: | **NO CUMPLE**<br>**No está implementado** |
| | **C. 6.1.3** | **6.1.3 Tratamiento de los riesgos de seguridad de la información** | La organización debe definir y efectuar un proceso de tratamiento de riesgos de seguridad de la información para: | **NO CUMPLE**<br>**No está implementado** |
| | **C. 6.2** | **6.2 Objetivos de seguridad de la información y planificación para su consecución** | La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes. | **NO CUMPLE**<br>**En la organización quedan establecidos objetivos asociados a Negocio, atención a nuevas necesidades pero no están declarados ni desglosados en Base a Objetivos de Seguridad de la Información.**<br>**Lo cual implica que no hay una planificación específica para su control y seguimiento.** |
| | **C. 7.1** | **7.1 Recursos** | La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información. | **CUMPLE PARCIALMENTE**<br>**Dentro de la Capa Operativa de los servicios del SOC existen recursos establecidos con competencias específicas en SI; pero a nivel de gestión no hay una implementación efectiva; con lo cual existe un modelo incompleto.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **C. 7.2** | **7.2 Competencia** | control, un trabajo que afecta a su<br>desempeño en seguridad de la información; y<br>b) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;<br>c) cuando sea aplicable, poner en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las<br>acciones llevadas a cabo; y<br>d) conservar la información documentada apropiada, como evidencia de la competencia. | **CUMPLE PARCIALMENTE**<br>**Hay una preocupación y prioridad a nivel de la organización por mantener el nivel de formación adecuado a las necesidades para los perfiles técnicos. Sin embargo no se basa en un proceso definido, registrado y controlado** |
| | **C. 7.3** | **7.3 Concienciación** | Las personas que trabajan bajo el control de la organización deben ser conscientes de:<br>a) la política de la seguridad de la información;<br>b) su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los beneficios de una<br>mejora del desempeño en seguridad de la información;<br>c) las implicaciones de no cumplir con los requisitos del sistema de gestión de seguridad de la información. | **CUMPLE PARCIALMENTE**<br>**La conciencación en SI está presente en la Organización.**<br>**Existen iniciativas esporádicas; sin que haya una planificación y seguimiento; y sin que se marquen objetivos y alcance definidos.** |
| | **C. 7.4** | **7.4 Comunicación** | La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de seguridad de la información, que incluyan:<br>a) el contenido de la comunicación;<br>b) cuándo comunicar;<br>c) a quién comunicar;<br>d) quién debe comunicar;<br>e) los procesos por los que debe efectuarse la comunicación. | **NO CUMPLE**<br>**No están desarrolladas. La comunicación y como comunicar se establece en el momento en el que surge la necesidad.** |
| | **C. 7.5** | **7.5 Información documentada** | El sistema de gestión de seguridad de la información de la organización debe incluir:<br>a) la información documentada requerida por esta norma internacional;<br>b) la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de<br>gestión de seguridad de la información. | **CUMPLE PARCIALMENTE**<br>**Está establecido un modelo para la Gestión de la Documentacíon en la Organización; que no está revisado y no se usa de manera normalizada** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **C. 8.1** | **8.1 Planificación y control operacional** | La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el apartado 6.1. La organización debe implementar también planes para alcanzar los objetivos de seguridad de la información determinados en el apartado 6.2. | **NO CUMPLE**<br>**En base al no cumplimiento de los apartados referidos.** |
| | **C. 8.2** | **8.2 Apreciación de los riesgos de seguridad de información** | La organización debe efectuar apreciaciones de riesgos de seguridad de la información a intervalos planificados, y cuando se propongan o se produzcan modificaciones importantes, teniendo en cuenta los criterios establecidos en el punto 6.1.2 a). | **NO CUMPLE**<br>**En base al que no hay formalmente implmentado un proceso de gestión de Riesgos.** |
| | **C. 8.3** | **8.3 Tratamiento de los riesgos de seguridad de información** | La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información. | **NO CUMPLE**<br>**En base al que no hay formalmente implmentado un proceso de gestión de Riesgos.** |
| | **C. 9.1** | **9.1 Seguimiento, medición, análisis y evaluación** | La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de seguridad de la información. | **NO CUMPLE**<br>**En base a que no hay un SGSI implementado.** |
| | **C. 9.2** | **9.2 Auditoría interna** | La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de seguridad de la información: | **CUMPLE**<br>**Este proceso esta desarrollado dado que el SOC está periódicamente sometido a Auditorías técnicas (Pentesting, Análisis de Vulnerabilidades, etc). Contempla la planificación de las auditoríoas, suejcución y el seguimiento de las no conformidades y acciones correctivas.**<br>**Habría que hacerlo más extensivo para cubrir auditorías desde la óptica de un sistema de Gestión.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **C. 9.3** | **9.3 Revisión por la dirección** | La alta dirección debe revisar el sistema de gestión de seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas. | **NO CUMPLE**<br>**En la organización no se están desarrollando y tratando los aspectos que aparecen en la Revisión por la Dirección.**<br>**No está configurado el Comité de Seguridad , ni están implemntados los procesos que generan la información para su explotación y seguimiento.** |
| | **C. 10.1** | **10.1 No conformidad y acciones correctivas** | Cuando ocurra una no conformidad, la organización debe: | **CUMPLE**<br>**(Ver C.9.2.)** |
| | **C. 10.2** | **10.2 Mejora continua** | La organización debe mejorar de manera continúa la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información. | **NO CUMPLE**<br>**Este proceso no está implementado.** |
| **ISO27002 A.5 - Políticas de seguridad de la información** | | | | |
| | **A.5.1.1** | **A.5.1.1 Políticas para la seguridad de la información** | Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes. | **NO CUMPLE**<br>**(No hay política de Seguridad declarada en la Organización)** |
| | **A.5.1.2** | **A.5.1.2 Revisión de las políticas para la seguridad de la información** | Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia. | **CUMPLE PARCIALMENTE**<br>**Están declaradas Políticas de Seguridad que aplican mayoritariamente a Operativas IT.**<br>**Estas políticas no están revisadas y habría que valorar en la práctica el grado de conocimiento y cumplimiento.** |
| **ISO27002 A.6 - Organización de la seguridad de la información** | | | | |
| | **A.6.1.1** | **A.6.1.1 Roles y responsabilidades en seguridad de la información** | Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas. | **NO CUMPLE**<br>**No están claramente establecidas en la organización los Roles y Responsabilidades asociadas a SI.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.6.1.2** | **A.6.1.2 Segregación de tareas Control** | Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización. | **CUMPLE PARCIALMENTE**<br>**En la operativa técnica están establecidos perfiles concretos que tienen responsabilidades y accesos sobre activos de TI concretos.**<br>**No hay documentado un modelo global y no existen procedimientos que gestionen la Segregación de funciones.** |
| | **A.6.1.3** | **A.6.1.3 Contacto con las autoridades** | Deben mantenerse los contactos apropiados con las autoridades pertinentes. | **NO CUMPLE**<br>**Los contactos con las autoridades se realizan en base a cunado se da la necesidad en el momento concreo.**<br>**No están documentados ni procedimentados.** |
| | **A.6.1.4** | **A.6.1.4 Contacto con grupos de interés especial** | Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad. | **CUMPLE**<br>**Dado el foco de Actividad en Ciberseguridad este punto está plemanente cubierto y forma parte del día a día**<br>**Hay una colaboración y presencia directa en las organizaciones de Ciberseguridad.** |
| | **A.6.1.5** | **A.6.1.5 Seguridad de la información en la gestión de proyectos** | La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto. | **CUMPLE**<br>**Existe una Gestión de Proyectos que se usa tanto para los proyectos de los clientes como para los proyectos internos.**<br>**Hay establecida una metodología de Gestión de proyectos y se cuenta con herramientas.** |
| | **A.6.2.1** | **A.6.2.1 Política de dispositivos móviles** | Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles. | **CUMPLE**<br>**Existe una política de Dispositivos móviles (política BYOD, buenas prácticas).**<br>**Los smartphones de la organización son controlados por MDM por lo tanto están sujetos a la aplicación de una política de Seguridad.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.6.2.2** | **A.6.2.2 Teletrabajo** | Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo. | **CUMPLE**<br>**Está implantada una política de Teletrabajo centrada en los aspectos:**<br>**Conexión Segura a través de VPN (INSTALACION Y MANTENIMIENTO DE CERTIFICADOS).**<br>**Normas de seguridad de los puestos de Trabajo.** |
| **ISO27002 A.7 - Seguridad relativa a los recursos humanos** | | | | |
| | **A.7.1.1** | **A.7.1.1 Investigación de antecedentes** | La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normas y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos. | **CUMPLE PARCIALMENTE**<br>**Existe un Departemento dedicado a la gestión de RR.HH. Dentro de la Organización que centraliza todas las funciones de gestión de RR.HH (Selección, contratación , seguimiento del personal, y Baja).**<br>**Tiene de Base las siguientes carencias:**<br>**- La asunción, control y seguimiento de las necesidades en cuanto a formación (tanto en aspectos competenciales, funcionales y de seguridad).**<br>**- Establecimiento de los mecanismos adecuados de aseguramiento de la Seguridad de los empleados en el momento de su contratación:**<br>**- Acuerdos de Confidencialidad, protección de Datos pesonales, regsitro de entregas de equipamiento, políticas de Seguridad, etc.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.7.1.2** | **A.7.1.2 Términos y condiciones del empleo** | Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización. | **CUMPLE PARCIALMENTE**<br>**Ver A.7.1.1** |
| | **A.7.2.1** | **A.7.2.1 Responsabilidades de gestión** | La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización. | **CUMPLE PARCIALMENTE**<br>**Ver A.7.1.2** |
| | **A.7.2.2** | **A.7.2.2 Concienciación, educación y capacitación en seguridad de la información** | Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo. | **CUMPLE PARCIALMENTE**<br>**Ver A.7.1.3** |
| | **A.7.2.3** | **A.7.2.3 Proceso disciplinario** | Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad. | **CUMPLE PARCIALMENTE**<br>**Ver A.7.1.4** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.7.3.1** | **A.7.3.1 Responsabilidades ante la finalización o cambio** | Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir. | **Ver A.7.1.5** |
| **ISO27002 A.8 - Gestión de activos** | | | | |
| | **A.8.1.1** | **A.8.1.1 Inventario de activos** | Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario. | **CUMPLE PARCIALMENTE**<br>**Existen inventarios de los activos de Soporte IT (no se encuentran actualizados y no existe un mecanimso para su mantenimiento)** |
| | **A.8.1.2** | **A.8.1.2 Propiedad de los activos** | Todos los activos que figuran en el inventario deben tener un propietario. | **NO CUMPLE**<br>**No están declarados los propietarios de los activos de manera generalizada.** |
| | **A.8.1.3** | **A.8.1.3 Uso aceptable de los activos** | Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información. | **NO CUMPLE**<br>**Hay establecidas prácticas de uso sobre ciertos activos de información pero no están documentadas ni difundidas.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.8.1.4** | **A.8.1.4 Devolución de activos** | Todos los empleados y terceras partes deben devolver todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo. | **NO CUMPLE**<br>**Ver A 7.1.1.** |
| | **A.8.2.1** | **A.8.2.1 Clasificación de la información** | La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas. | **NO CUMPLE**<br>**No están establecidos crirterios de Clasificación de los activos de informacíon; así como las políticas de seguridad a aplicar en su almacenamiento, tránsito y soporte.** |
| | **A.8.2.2** | **A.8.2.2 Etiquetado de la información** | Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización. | **NO CUMPLE**<br>**Ver A. 8.2.1** |
| | **A.8.2.3** | **A.8.2.3 Manipulado de la información** | Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización. | **NO CUMPLE**<br>**Ver A. 8.2.2** |
| | **A.8.3.1** | **A.8.3.1 Gestión de soportes extraíbles** | Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización. | **CUMPLE**<br>**Existe una política de gestión de soportes extraíbles (integrada en A.6.1.)** |
| | **A.8.3.2** | **A.8.3.2 Eliminación de soportes** | Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales. | **CUMPLE PARCIALMENTE**<br>**Existe un política de eliminación de soportes (habría que revisar dado que da da garantías en cuanto a la trazabilidad y la garantía del borrado de la información).** |
| | **A.8.3.3** | **A.8.3.3 Soportes físicos en tránsito** | Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro. | **CUMPLE PARCIALMENTE**<br>**La operativa está desarrollada pero no documentada** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| **ISO27002 A.9 - Control de acceso** | | | | |
| | **A.9.1.1** | **A.9.1.1 Política de control de acceso** | Se debe establecer, documentar y revisar una política de control de acceso basada en losrequisitos de negocio y de seguridad de la información. | **CUMPLE PARCIALMENTE**<br>**Existe una política de control de acceso (habría que revisar si cumple con la Segregación de funciones ya que puede haber incoherencias).** |
| | **A.9.1.2** | **A.9.1.2 Acceso a las redes y a los servicios de red** | Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados. | **CUMPLE PARCIALMENTE**<br>**Existe una política de control de acceso a los recuros de Red (habría que revisar si cumple con la Segregación de funciones ya que puede haber incoherencias).** |
| | **A.9.2.1** | **A.9.2.1 Registro y baja de usuario** | Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso. | **CUMPLE PARCIALMENTE**<br>**Los accesos están centralizados a través DA.**<br>**Existe un proceimiento de Alta y Baja de Usuarios.**<br>**El procedimeinto de solicitud desde el área de recursos humanos.no se cumple estrictamente.** |
| | **A.9.2.2** | **A.9.2.2 Provisión de acceso de usuario** | Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios. | **CUMPLE PARCIALMENTE**<br>**Las recursos generales son directamente solicitados desde el área de RR.HH.**<br>**Los accesos a recursos, aplicaciones y herramientas específicas son gestionados por los responsables de las distintas áreas técnicas.**<br>**Habría que revisar perfiles, funciones, procedimeintos y uso.** |
| | **A.9.2.3** | **A.9.2.3 Gestión de privilegios de acceso** | La asignación y el uso de privilegios de acceso debe estar restringida y controlada. | **CUMPLE PARCIALMENTE**<br>**Ver A.9.2.2.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.9.2.4** | **A.9.2.4 Gestión de la información secreta de autenticación de los usuarios** | La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión. | **CUMPLE**<br>**Existen Herramientas de Gestión de Credenciales para garantizar la aplicacíon de este control.** |
| | **A.9.2.5** | **A.9.2.5 Revisión de los derechos de acceso de usuario** | Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares. | **NO CUMPLE**<br>**Ver.A. 8.2.1.** |
| | **A.9.2.6** | **A.9.2.6 Retirada o reasignación de los derechos de acceso** | Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio. | **CUMPLE**<br>**Ver A.9.2.2.** |
| | **A.9.3.1** | **A.9.3.1 Uso de la información secreta de autenticación** | Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación. | **CUMPLE**<br>**VER A.9.2.4.** |
| | **A.9.4.1** | **A.9.4.1 Restricción del acceso a la información** | Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida. | **NO CUMPLE**<br>**VER A. 8.2.1., y A.9.2.2.** |
| | **A.9.4.2** | **A.9.4.2 Procedimientos seguros de inicio de sesión** | Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión. | **CUMPLE**<br>**Hay desarroolado y puesto en marcha un procedimiento de control de Acceso.** |
| | **A.9.4.3** | **A.9.4.3 Sistema de gestión de contraseñas** | Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas. | **CUMPLE**<br>**Está implementada una política de Contraseñas que está extendida a todas las Aplicaciones que requieren control de Acceso.** |
| | **A.9.4.4** | **A.9.4.4 Uso de utilidades con privilegios del sistema** | Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación. | **NO CUMPLE**<br>**No existe un inventario de Utililities; por lo tanto no hay un control sobre este tema en cuanto a su uso y los privilegiios de acceso a la informacíon.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.9.4.5** | **A.9.4.5 Control de acceso al código fuente de los programas** | Se debe restringir el acceso al código fuente de los programas. | **NO CUMPLE**<br>**El código desarrollado básicamante es scripting.**<br>**No se están establecidos unos procedimeintos de acceso y uso.** |
| **ISO27002 A.10 - Criptografía** | | | | |
| | **A.10.1.1** | **A.10.1.1 A Política de uso de los controles criptográficos** | Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información. | **NO CUMPLE**<br>**Están implantados y se mantienen Certificados de Servidores, Acceso web seguro (HPPTS/SSL), Aceso VPN/IP SEC, Gestión de credenciales, etc.**<br>**Sin embargo no hay documentada una política de controles Criptográficos.** |
| | **A.10.1.2** | **A.10.1.2 Gestión de claves** | Se debe desarrollar e implementar una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida. | **NO CUMPLE**<br>**A incluir dentro de la Política de Controles Criptográficos (Ver A.10.1.2)** |
| **ISO27002 A.11 - Seguridad física y del entorno** | | | | |
| | **A.11.1.1** | **A.11.1.1 Perímetro de seguridad física** | Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información. | **CUMPLE**<br>**Existen 3 Perímetros de seguridad dentro de las instalaciones:**<br>**- Control de Acceso Físico al Edificio (Nivel 1).**<br>**- Control de Acceso Físico a las Instalaciones de la Compañía (en el edificio) - (Nivel 2).**<br>**- Control de Acceso al SOC (Nivel 3).** |
| | **A.11.1.2** | **A.11.1.2 Controles físicos de entrada** | Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado. | **CUMPLE**<br>**- Nivel 1 (Personal de Seguridad y Tornos de acceso).**<br>**- Nivel 2 (Acceso biométrico).**<br>**- Nivel 3 (Acceso biométrico específico SOC)** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.11.1.3** | **A.11.1.3 Seguridad de oficinas, despachos y recursos** | Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física. | **CUMPLE**<br>**Acceso a salas técnicas restringida (acceso por panel numérico -claves)**<br>**Armarios con llaves distribuidos por las instalaciones custodiados por responsables.**<br>**Cajas fuertes ignifugas (alamcenamiento de backups y custodia forense).** |
| | **A.11.1.4** | **A.11.1.4 Protección contra las amenazas externas y ambientales** | Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes. | **CUMPLE**<br>**Las derivadas de las normas de Seguridad en la construcción y diseño del edificio.**<br>**Planes de Mantenimiento de las instalaciones/planes de Emergencia actualizados y operativos.** |
| | **A.11.1.5** | **A.11.1.5 El trabajo en áreas seguras** | Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras. | **CUMPLE**<br>**El área segura declarado es el espacio del SOC.**<br>**Cuenta con los mecanismos y procedimiento adecuados para mantener la seguridad.** |
| | **A.11.1.6** | **A.11.1.6 Áreas de carga y descarga** | Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados. | **No Aplica** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.11.2.1** | **A.11.2.1 Emplazamiento y protección de equipos** | Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados. | **CUMPLE**<br>**El equipamiento asociado a la Electrónica de Red se encuentra ubicado en las Salas Técnicas (Ver A.11.1.1); cuenta con medida de protección (control de acceso, control de termperatura, control anti-incendios, etc).**<br>**El resto del equipamiento se encuentra ubicado dentro del SOC (puestos clientes y laboratorio (servidores de pruebas).**<br>**La infraestructura de Servidores está alojada en CPDs Homologados de proveedores externos.** |
| | **A.11.2.2** | **A.11.2.2 Instalaciones de suministro** | Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro. | **CUMPLE**<br>**Salas Técnicas-Electrónica de Red (Dotados de SAI local).**<br>**Equipamiento del SOC (infraestructura de edificio - puntos de corriente seguros) y edificio dotado con grupo electrógeno** |
| | **A.11.2.3** | **A.11.2.3 Seguridad del cableado** | El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños. | **CUMPLE**<br>**Cumple con las normativas de instalación y seguridad a nivel de las instalaciones en el edificio y las líneas de comunicaciones contratadas con los proveedores.** |
| | **A.11.2.4** | **A.11.2.4 Mantenimiento de los equipos** | Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas. | **CUMPLE**<br>**Equipamiento de Red y Servidores (Contratos de Soporte y Mantenimiento con los fabricantes).**<br>**Puestos de trabajo, Dispositivos móviles y perféricos (impresoras, faxes, etc) son gestionados directamente por Servicio de Soporte Externo (Firmware, Hardware, Software base)** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.11.2.5** | **A.11.2.5 Retirada de materiales propiedad de la empresa** | Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones. | **CUMPLE PARCIALMENTE**<br>**Existen prácticas de control pero no están documentadas.** |
| | **A.11.2.6** | **A.11.2.6 Seguridad de los equipos fuera de las instalaciones** | Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones. | **CUMPLE**<br>**Para Servidores (Ubicación en CPDs homologados proveedores externos)**<br>**Para el equipamiento móvil (Ver a 6.2.1).** |
| | **A.11.2.7** | **A.11.2.7 Reutilización o eliminación segura de equipos** | Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos. | **CUMPLE PARCIALMENTE**<br>**Ver A.8.3.2.** |
| | **A.11.2.8** | **A.11.2.8 Equipo de usuario desatendido** | Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada. | **No Aplica** |
| | **A.11.2.9** | **A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia** | Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información. | **CUMPLE**<br>**Existe una Política declarada, difundida y en uso dentro de la Organización.** |
| **ISO27002 A.12 - Seguridad de las operaciones** | | | | |
| | **A.12.1.1** | **A.12.1.1 Documentación de procedimientos de los operación** | Deben documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten. | **CUMPLE PARCIALMENTE**<br>**Existe procedimientos de Operación dentro del SOC, que está delegados en su ejecución a los Técnicos de Nivel 1.** |
| | **A.12.1.2** | **A.12.1.2 Gestión de cambios** | Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deben ser controlados. | **CUMPLE PARCIALMENTE**<br>**Existe Herramientas de Service Desk con el proceso de Gestión de Cambios implementado; no se usa de manera habitual para la Gestión de los Cambios del SOC.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.12.1.3** | **A.12.1.3 Gestión de capacidades** | Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema. | **CUMPLE PARCIALMENTE**<br>**Se está realizando una monitorización continua de las infraestructuras del SOC (Rendimiento, consumo. Almacenamiento). Se emite y analiza el reporting de estado y necesidades en base a crecimiento infraestructura.**<br>**La gestión de la Capacidad en Base a:**<br>**- Recursos Humanos.**<br>**- Necesidades de Negocio, etc**<br>**no aparece contemplada.** |
| | **A.12.1.4** | **A.12.1.4 Separación de los recursos de desarrollo, prueba y operación** | Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción. | **CUMPLE PARCIALMENTE**<br>**En la Práctica no hay una infraestrcutura paralela que permita la realización de pruebas previas en entornos que no sean de Producción.**<br>**La infraestrcutura de Laboratorio es usado para recrear entornos de Desarrollo y Pruebas pero parcialmente.** |
| | **A.12.2.1** | **A.12.2.1 Controles contra el código malicioso** | Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario. | **CUMPLE**<br>**Dentro del SOC se aplican los procedimientos que están desarrollados para los servicios que se prestan a los clientes.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.12.3.1** | **A.12.3.1 Copias de seguridad de la información** | Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada. | **CUMPLE PARCIALMENTE**<br>**Se realizan copias de Seguridad de los Sistemas Críticos**<br>**Están implementadas políticas de backup pero no están documentadas.**<br>**Sería necesario revisar la permencia y retención de la información de la que se hace backup.**<br>**No se realizan pruebas periódicas de recuperacíon para asgurar la Sanidad de los backups realizados.** |
| | **A.12.4.1** | **A.12.4.1 Registro de eventos** | Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información. | **CUMPLE PARCIALMENTE**<br>**Los eventos de los Servidores y de la electrónica de Red son registrados en Servidores con acceso restringido que sonespecíficos para almacenar logs.**<br>**No están siendo analizados regularmente; salvo que exista una incidencia y/o problema concreto.**<br>**No están alimentando a ninguna herramienta SIEM.** |
| | **A.12.4.2** | **A.12.4.2 Protección de la información de registro** | Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados. | **CUMPLE**<br>**Política de Hardening de Servidores y dispositivos de Red.** |
| | **A.12.4.3** | **A.12.4.3 Registros de administración y operación** | Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema. | **CUMPLE**<br>**Política de Hardening de Servidores y dispositivos de Red (Trazabilidad en la operación y administración).** |
| | **A.12.4.4** | **A.12.4.4 Sincronización del reloj** | Los relojes de todos los sistemas de tratamiento de información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada de tiempo. | **CUMPLE**<br>**Centralización del reloj de tiempo a través de la configuración sobre protocolo NTP contra servidores de tiempo externos.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.12.5.1** | **A.12.5.1 Instalación del software en explotación** | Se deben implementar procedimientos para controlar la instalación del software en explotación. | **CUMPLE**<br>**Existen procedimientos definidos para la instalación del SW en entornos de producción.** |
| | **A.12.6.1** | **A.12.6.1 Gestión de las vulnerabilidades técnicas** | Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado. | **CUMPLE**<br>**Se aplican los mismos procedimientos que los usados con los clientes.** |
| | **A.12.6.2** | **A.12.6.2 Restricción en la instalación de software** | Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios. | **CUMPLE**<br>**Existen procedimientos en el SOC que establecen y limitan la instalación de software** |
| | **A.12.7.1** | **A.12.7.1 Controles de auditoría de sistemas de información** | Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio. | **CUMPLE PARCIALMENTE**<br>**El SOC está sometido a un proeso de monitorizacíon continua.**<br>**Periódcamente se práctican auditorias para detectar vulnerabilidades a los Sistemas..**<br>**No se están practicando con regularidad aauditorias para verificar los mecanismos de acceso a los recursos.** |
| **ISO27002 A.13 - Seguridad de las comunicaciones** | | | | |
| | **A.13.1.1** | **A.13.1.1 Controles de red** | Las redes deben ser gestionadas y controladas para proteger la informaciónen los sistemas y aplicaciones. | **CUMPLE**<br>**La arquitectura y diseño de red contempla la segmentación de acceso y el control de los mecanismos de acceso entre las distintas redes.**<br>**Se usa la segmentación de redes basada en el establecimiento de didtintas VLANs.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.13.1.2** | **A.13.1.2 Seguridad de los servicios de red** | Se deben identificar los mecanismos de seguridad, los niveles de servicio, ylos requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan. | **CUMPLE**<br>**Están gestionados por los priopios equipos técnicos del SOC.**<br>**Para la infraestrctutra de Red que se soporta por los activos que se encunetran iubicados en los CPD's se realiza a través de los mecanismos de soporte de los proveedores externos; con los que están suscritos compromnisos de Disponiblidad y los niveles de Calidad de servicios de red QoS** |
| | **A.13.1.3** | **A.13.1.3 Segregación en redes** | Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas. | **CUMPLE**<br>**Ver A.13.1.1**<br>**La infrestrcutura expuesta en INTERNET está bajo una DMZ.** |
| | **A.13.2.1** | **A.13.2.1 Políticas y procedimientos de intercambio de información** | Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación. | **NO CUMPLE**<br>**Aunque existen prácticas en este sentido no están inventariadas, regsitradas y procedimentadas.** |
| | **A.13.2.2** | **A.13.2.2 Acuerdos de intercambio de información**<br>Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y | | **NO CUMPLE**<br>**Ver A.13.2.1.** |
| | **A.13.2.3** | **A.13.2.3 Mensajería electrónica**<br>La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida. | | **NO CUMPLE**<br>**A.8.2.1.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.13.2.4** | **A.13.2.4 Acuerdos de confidencialidad o no revelación**<br>Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación | | **CUMPLE PARCIALMENTE**<br>**Aunque se ha analizado la existencia de acuerdos de confidencialidad tanto para el personal interno como el extrno; así como en los contratos existentes con los proveedores vinculados con la Organización; no se ha realizado una revisión exhaustiva y tampoco hay constancia de la existencia de procedimientos para asegurar el cumplimiento.** |
| **ISO27002 A.14 - Adquisición, desarrollo y mantenimiento de los sistemas de información** | | | | |
| | **A.14.1.1** | **A.14.1.1 Análisis de requisitos y especificaciones de seguridad de la información** | Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes. | **NO CUMPLE**<br>**Se establecen requisitos de Seguruidad ad-hoc en los procesos de contratación de algunos proveedores a través de la emisión de las correspondientes RFPs; sin embargo no están tipificados y documentados los requisitos de seguridad de la organizacíon hacia los proveedores de serviciios.** |
| | **A.14.1.2** | **A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas** | La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas. | **No Aplica en las actividades actuales** |
| | **A.14.1.3** | **A.14.1.3 Protección de las transacciones de servicios de aplicaciones** | La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas. | **No Aplica en las actividades actuales** |
| | **A.14.2.1** | **A.14.2.1 Política de desarrollo seguro** | Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas. | **NO CUMPLE**<br>**No hay establecida una política en la Organización.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.14.2.2** | **A.14.2.2 Procedimiento de control de cambios en sistemas** | La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios. | **Ver A.12.1.2**<br>**Habría que procedimentar el flujo y los mecanismos de revisión y aprobación de cambios.** |
| | **A.14.2.3** | **A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo** | Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización. | **CUMPLE PARCIALMENTE**<br>**Esta práctica se realiza habitualmente; pero no está ni procedimentada ni documentada.** |
| | **A.14.2.4** | **A.14.2.4 Restricciones a los cambios en los paquetes de software** | Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso. | **CUMPLE PARCIALMENTE**<br>**Idem a. 14.2.3.** |
| | **A.14.2.5** | **A.14.2.5 Principios de ingeniería de sistemas seguros** | Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información. | **CUMPLE.**<br>**Dentro de SOC se realizan las tareas de diseño de arquitecturas teniendo una competencia adecuado para ello.** |
| | **A.14.2.6** | **A.14.2.6 Entorno de desarrollo seguro** | Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema. | **CUMPLE**<br>**Se está usando la infraestructura de Laboratorio del SOC para realizar estas actividades.** |
| | **A.14.2.7** | **A.14.2.7 Externalización del desarrollo de software** | El desarrollo de software externalizado debe ser supervisado y controlado por la organización. | **No aplica esta actividad actualmente** |
| | **A.14.2.8** | **A.14.2.8 Pruebas funcionales de seguridad de sistemas** | Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo. | **CUMPLE PARCIALMENTE**<br>**Esta práctica se realiza ; pero no está ni procedimentada ni documentada.** |
| | **A.14.2.9** | **A.14.2.9 Pruebas de aceptación de sistemas** | Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones. | **CUMPLE PARCIALMENTE**<br>**Esta práctica se realiza ; pero no está ni procedimentada ni documentada.** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.14.3.1** | **A.14.3.1 Protección de los datos de prueba** | Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados. | **NO CUMPLE**<br>**No se están considerando los datos de Prueba con el mismo nivel de protección cuando su origen viene desde los entornos de producción.** |
| **ISO27002 A.15 - Relación con proveedores** | | | | |
| | **A.15.1.1** | **A.15.1.1 Política de seguridad de la información en las relaciones con los proveedores** | Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados. | **NO CUMPLE**<br>**Ver A.14.1.1** |
| | **A.15.1.2** | **A.15.1.2 Requisitos de seguridad en contratos con terceros** | Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura IT. | **NO CUMPLE**<br>**Ver A.14.1.1** |
| | **A.15.1.3** | **A.15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones** | Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos. | **CUMPLE PARCIALMENTE**<br>**No están titpificados ni documentados. Se ha verificado la existencia de requisitos de seguridad para los mproveedores más críticos pero no se ha llegado analizado el resto.** |
| | **A.15.2.1** | **A.15.2.1 Control y revisión de la provisión de servicios del proveedor** | Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor | **NO CUMPLE.**<br>**No hay implementado un mecanismo en la organización.** |
| | **A.15.2.2** | **A.15.2.2 Gestión de cambios en la provisión del servicio del proveedor** | Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos. | **NO CUMPLE.**<br>**No hay implementado un mecanismo en la organización.** |
| **ISO27002 A.16 - Gestión de incidentes de seguridad de la información** | | | | |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.16.1.1** | **A.16.1.1 Responsabilidades y procedimientos** | Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información. | **CUMPLE PARCIALMENTE**<br>**La organización tiene implantado un proceso de gestión de Incidentes que aplkica tasnto para la operativa de los Servicios a los Clientes; como para gestionar las incidencias específicas del SOC.**<br>**cuenta con herramientas, tienen establecidos las cetegorizaciones, tratamiento, flujos y mecanismos de escalado.**<br>**No existe una tipificación de los incidentes de seguridad (pero son adaptables dentro del procesos de incidencias ya existente).** |
| | **A.16.1.2** | **A.16.1.2 Notificación de los eventos de seguridad de la información** | Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible. | **CUMPLE PARCIALMENTE**<br>**Ver A. 16.1.2 y considerar la adaptación del flujo para adecvuar las notificaciones de incidentes de seguridad dentro y fuera de la organización.** |
| | **A.16.1.3** | **A.16.1.3 Notificación de puntos débiles de la seguridad** | Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios. | **CUMPLE PARCIALMENTE**<br>**Estos mecanismos no están procedimentaso y asegurados para todos los contratos con los proveedores.** |
| | **A.16.1.4** | **A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información** | Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información. | **CUMPLE PARCIALMENTE**<br>**A.16.1.1** |
| | **A.16.1.5** | **A.16.1.5 Respuesta a incidentes de seguridad de la información** | Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados. | **CUMPLE PARCIALMENTE**<br>**Ver A.16.1.2** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.16.1.6** | **A.16.1.6 Aprendizaje de los incidentes de seguridad de la información** | El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro. | **CUMPLE PARCIALMENTE**<br>**El conocimiento está extendido de manera natural dentro de los equipos pero no existen herramientas en las que apoyarse; ni se elaboran de manera habitual instrucciones técnicas para tipificar la resolución de los incidentes.** |
| | **A.16.1.7** | **A.16.1.7 Recopilación de evidencias** | La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de información que puede servir de evidencia. | **CUMPLE**<br>**Reutilización de los mecanismos y procedimientos del Análisis Forense que existen en la organización y que se usan habitualmente con los Servicios prestdos a los clientes.** |
| **ISO27002 A.17 - Aspectos de seguridad de la información para la gestión de la continuidad del negocio** | | | | |
| | **A.17.1.1** | **A.17.1.1 Planificación de la continuidad de la seguridad de la información** | La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre. | **NO CUMPLE**<br>**De manera natural la información crítica manejada por el SOC es conocida; pero no se ha realizado de manera formal los BIA's para determinar el alcance y las necesidades.** |
| | **A.17.1.2** | **A.17.1.2 Implementar la continuidad de la seguridad de la información** | La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa. | **NO CUMPLE.**<br>**No están documentados los procesos, procedimientos y controles para el nivel requerido que no ha sido calculado.** |
| | **A.17.1.3** | **A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información** | La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas. | **NO CUMPLE**<br>**No se someten a revisiones y pruebas periódicas** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.17.2.1** | **A.17.2.1 Disponibilidad de los recursos de tratamiento de la información** | Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad. | **CUMPLE PARCIALMENTE**<br>**Existe redundancias en las infraestrcuturas que soportan la información desde el punto de vista del Almacenamiento, tratamiento y transferencia de la información. Sin embargo para ciertas informaciones críticas desde el punto de vista de la operativa del SOC no está garantizada esta redundancia (p.e. Gestión bde credenciales).** |
| **ISO27002 A.18 - Cumplimiento** | | | | |
| | **A.18.1.1** | **A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales** | Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización. | **CUMPLE PARCIALMENTE**<br>**Competencia delegada al área Jurídica. El enfoque está contemplado parcialmente; pero no existe una unificvacíon de los criterios y sobre todo un mecanismos de aplicación y control.** |
| | **A.18.1.2** | **A.18.1.2 Derechos de propiedad intelectual (DPI)** | Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados. | **NO CUMPLE**<br>**No están desarrollados los procedimientos pertinentes.** |
| | **A.18.1.3** | **A.18.1.3 Protección de los registros de la organización** | Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio. | **NO CUMPLE**<br>**Ver A.8.1.2** |

| Análisis Diferencial | | | | |
|---|---|---|---|---|
| **Dominio** | **Control** | **Descripción del Control** | **Explicación/Requisitos** | **Comentarios/Valoración (CUMPLE, CUMPLE PARCIALMENTE, NO CUMPLE)** |
| | **A.18.1.4** | **A.18.1.4 Protección y privacidad de la información de carácter personal** | Deber garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables. | **CUMPLE**<br>**Dentro de la organización existe un Área Jurídica que tiene delegada esta responsablidad.**<br>**Tiene puesta en marcha una adecuación al RGPD teniendo en consideración la Privacidad gestionada desde el SOC (el nivel de sensibilidad de la información personal manejada es bajo).** |
| | **A.18.1.5** | **A.18.1.5 Regulación de los controles criptográficos** | Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes. | **NO CUMPLE**<br>**Ver. A.10.1.1, A.8.2.1 y A.8.2.3** |
| | **A.18.2.1** | **A.18.2.1 Revisión independiente de la seguridad de la información** | El enfoque de la organización para la gestión de seguridad de la información y su implantación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad. | **NO CUMPLE**<br>**No hay un sistema de Gestión de la Seguridad de la Información como tal ya implantado en la organización.** |
| | **A.18.2.2** | **A.18.2.2 Cumplimiento de las políticas y normas de seguridad** | Los directivos deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable | **NO CUMPLE**<br>**Ver A.18.2.1** |
| | **A.18.2.3** | **A.18.2.3 Comprobación del cumplimiento técnico** | Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización. | **NO CUMPLE**<br>**Ver A.18.2.1** |