PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD TÉCNICA

2019

INTRODUCCIÓN

Con la transformación digital que se está dando en todas las actividades humanas, la información se convierte en uno de los activos más importantes que puede tener una empresa.
Por lo anterior dentro del proceso de desarrollo de una Arquitectura TI es fundamental la estructuración de un plan de tratamiento de riesgos de seguridad y privacidad de la información que ayude a la protección de la información cumpliendo los principios fundamentales de confidencialidad, integridad y disponibilidad.
Para lograr el cumplimiento de este plan es fundamental contar con el apoyo de la alta dirección la cual debe garantizar su articulación con el plan de desarrollo de la entidad.
Este plan deberá ser revisado y ajustado continuamente con el fin de mantenerlo actualizado con los cambios tecnológicos que vaya teniendo la entidad.
Para la formulación de este plan se seguirán todas las recomendaciones que en la materia ha expedido el MINTIC en Colombia.

OBJETIVOS

- Elaborar un documento que le permita a la entidad garantizar la confidencialidad, integridad y disponibilidad de toda la información que maneja.
- Identificar todos los riesgos que de una u otra manera puedan afectar la información de la entidad.
- Establecer acciones estratégicas que ayuden a fortalecer la seguridad y privacidad de la información de TELEMEDELLÍN.
- Fomentar una cultura al interior de la organización de preservación y cuidado de la información que maneja cada uno de sus funcionarios.

ALCANCE

Con este plan se pretende darle alcance a todos los riesgos que puedan afectar cualquier tipo de información que maneje la entidad ya sea archivos multimedia, bases de datos, archivos de usuario, aplicativos web, etc.
Este plan es aplicable a todos los procesos y proyectos de la Entidad y
a todas las acciones ejecutadas por los servidores que de una u otra forma generen, manejen o manipulen información.
Este plan está proyectado para una vigencia de 4 años (2019 – 2023) pero estará sujeto a las revisiones periódicas que se requieran ajustándose a los cambios de la entidad y sus procesos.

DEFINICIONES

Algunos términos que se manejaran en este plan son:

- **Amenaza:** Es la causa potencial de una situación de incidente y no deseada por la organización

- **Causa:** Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

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

- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.

- **Evento**: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

- **Integridad:** supone que la información se mantenga inalterada ante accidentes o intentos maliciosos.

- **Mapa de riesgos:** Un mapa de riesgos es un perfil que se diseña para identificar y cuantificar la probabilidad de eventos y medir el impacto o daño asociado a la ocurrencia.

- **MIPG**: Modelo Integrado de Planeación y Gestión.

- **Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

- **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Valoración del Riesgo**: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

CONTEXTO DE LA ENTIDAD

Telemedellín es un canal de televisión local que opera en la ciudad de Medellín y de naturaleza pública. Al ser un canal de televisión hace que la cantidad de información que se genera, procesa y almacena sea muy grande, lo cual junto con la información corporativa es lo que se pretende mantener protegido con este plan de tratamiento de riesgos.
La formulación de este plan para la entidad no es nuevo pues a través de los años se han venido desarrollando diferentes planes y documentos para el manejo de los riesgos enmarcados en los distintos procesos de aseguramiento de la calidad como el MECI o la norma NTC GP 1000.
Lo que se pretende con este plan es hacer un análisis más profundo y detallado de los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información de la entidad, pero conservando los lineamientos generales del documento "*Políticas de Riesgos de Telemedellín*".

METODOLOGÍA DE IMPLEMENTACIÓN

Para la implementación del presente plan se seguirán todos los lineamientos dados por la norma ISO27001-2013 y todos los documentos del Modelo de Seguridad y Privacidad de TI del Ministerio de Tecnologías de la Información y las Comunicaciones y específicamente la guía #8 *"Seguridad Y privacidad de la información"*

FASES DE IMPLEMENTACIÓN

Para la elaboración de este plan se siguieron las fases recomendadas en el documento *"Modelo de Seguridad y Privacidad de la Información"* del Mintic las cuales son:

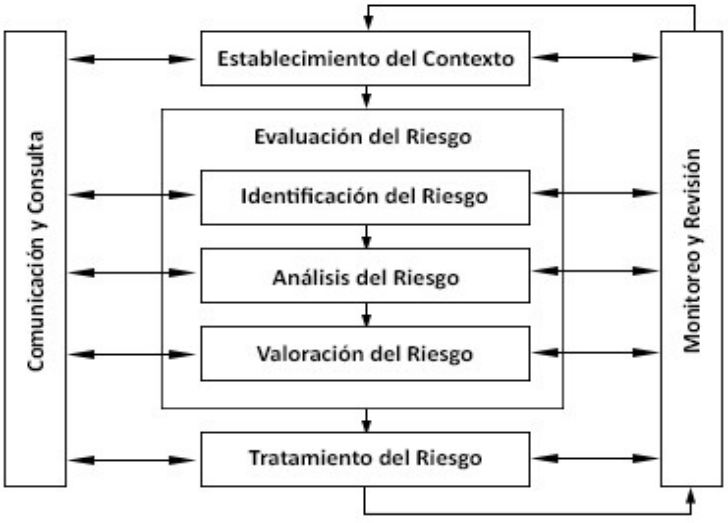
- **Diagnostico o identificación:**
  En esta fase se hace una identificación de todos los posibles riesgos que puedan poner en peligro la información de la entidad.

- **Planificación**
  Con los resultados de la fase de diagnóstico, se procede a la elaboración del mapa de riesgos, definiendo las acciones a implementar.

- **Implementación**
  Se implementan todas las acciones planteadas en el mapa de riegos.

- **Evaluación**
  A través de distintos procesos de evaluación se medirá la eficacia de los controles definidos en el mapa de riesgos.

- **Mejora continua**
  En esta fase se define el plan de mejoramiento continuo donde se toman acciones para mitigar las debilidades encontradas, de acuerdo a los resultados obtenidos en la fase de evaluación.



Tomado de la NTC-ISO/IEC 27005

DIAGNOSTICO O IDENTIFICACIÓN DE LOS RIESGOS

Dentro del proceso de identificar los riesgos se evaluarán los controles del Anexo A del estándar ISO/IEC 27001:2013 y sus dominios con el fin de definir evaluar su aplicabilidad y estado.

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Preguntas
A5	**Políticas de seguridad de la información**		
A5.1	**Directrices de gestión de la seguridad de la información**		
A5.1.1	Políticas para la seguridad de la información	Definido	¿Existe una clara evidencia de un marco / estructura / jerarquía global razonablemente diseñada y administrada? ¿Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes? ¿Cómo se autorizan, comunican, comprenden y aceptan las políticas? ¿Están formalmente obligados a cumplir todos los trabajadores y, en su caso, sus empleadores? ¿Hay acuerdos adecuados de cumplimiento y refuerzo? ¿Hay referencias cruzadas a buenas prácticas (como ISO27k, NIST SP800, CSC20 y otras normas y directrices relevantes)? ¿Están las políticas bien escritas, legible, razonable y viable? ¿Incorporan controles adecuados y suficientes? ¿Cubren todos los activos de información esenciales, sistemas, servicios, etc.? ¿Cuán madura es la organización en esta área?
A5.1.2	Revisión de las políticas para la seguridad de la información	Optimizado	¿Todas las políticas tienen un formato y estilo consistentes? ¿Están todos al día, habiendo completado todas las revisiones debidas? ¿Se han vuelto a autorizar y se han distribuido?
A6	**Organización de la seguridad de la información**		
A6.1	**Organización interna**		

A6.1.1	Roles y responsabilidades en seguridad de la información	Administrado	¿Se le da suficiente énfasis a la seguridad y al riesgo de la información? ¿Hay apoyo de la administración? ¿Existe un foro de alta gerencia para analizar el riesgo de la información y las políticas, los riesgos y los problemas de seguridad? ¿Los roles y las responsabilidades están claramente definidos y asignados a personas adecuadamente capacitadas? ¿Tiene cada rol responsabilidad específica con respecto al riesgo y la seguridad de la información? ¿Hay suficiente presupuesto para las actividades de seguridad y riesgo de la información? ¿Hay coordinación dentro de la organización entre las unidades de negocio? ¿funciona efectivamente en la práctica? ¿Existe una conciencia y un apoyo adecuados para la estructura de riesgo y seguridad de la información?
A6.1.2	Segregación de tareas	No aplicable	¿Son los deberes / funciones segregados entre roles o individuos cuando sea relevante para reducir la posibilidad de incompetencia, negligencia y actividades inapropiadas? ¿Se utiliza una matriz tipo RACI para mantener la identificación para cada tarea? Responsable | Accountable | Consulted | Informed ¿Existe una política que cubra la segregación de deberes? ¿Cómo llegan las decisiones con respecto a tal segregación? ¿Quién tiene la autoridad para tomar tales decisiones? ¿Se realiza un seguimiento regular de las actividades y los registros de auditoría?
A6.1.3	Contacto con las autoridades	Definido	¿Hay disponible una lista de detalles de contacto para las autoridades reguladoras u otras autoridades y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias? ¿Quién es el responsable de contactar a las autoridades y en qué punto de un incidente / evento se realiza este contacto y cómo? ¿La lista es actual y correcta? ¿Hay un proceso de mantenimiento?
A6.1.4	Contacto con grupos de interés especial	No aplicable	¿Hay un contacto regular, con grupos especiales de interés, foros y listas de correo profesionales en riesgo de la información y la seguridad, tales como los capítulos locales de ISACA, ISC 2, ISSA, ISO27k? ¿Se comparte información sobre amenazas emergentes, nuevas tecnologías de seguridad, buenas prácticas de seguridad, advertencias tempranas de alertas y advertencias,

			vulnerabilidades recientemente descubiertas y disponibilidad de parches?
A6.1.5	Seguridad de la información en la gestión de proyectos	Definido	¿Se identifican y abordan los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos, incluidos todos los tipos de proyectos relacionados con la información, los nuevos desarrollos y los cambios / mejoras en los sistemas, aplicaciones y procesos existentes? ¿La etapa del proyecto incluye actividades apropiadas?
A6.2	**Los dispositivos móviles y el teletrabajo**		
A6.2.1	Política de dispositivos móviles	Administrado	¿Existen política y controles seguridad relacionados con los usuarios móviles? ¿Se distinguen los dispositivos personales de los empresariales? ¿Cómo se mantienen y controlan los sistemas portátiles para garantizar que estén actualizados sobre las definiciones de antivirus y los parches de seguridad? ¿Se emplean soluciones de MDM y soluciones MAM para controlar las aplicaciones, el acceso y el cifrado completo de disco?
A6.2.2	Teletrabajo	No aplicable	¿Los controles de seguridad para el teletrabajo son equivalentes a los de los lugares de trabajo de oficina? ¿Existen disposiciones adecuadas para la autenticación del usuario (2FA), la seguridad de la red (Alwayson-VPN), antivirus, copias de seguridad, parches, registro de seguridad y monitoreo, encriptación y continuidad del negocio?
A7	**Seguridad relativa a los recursos humanos**		
A7.1	**Antes del empleo**		

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Preguntas
A7.1.1	Investigación de antecedentes	Definido	¿El proceso de evaluación previa al empleo toma en cuenta las leyes y regulaciones relevantes de privacidad y empleo? ¿Se hace en la empresa o se subcontrata a un tercero? Si se subcontrata a un tercero, ¿Se han revisado sus procesos y se han considerado aceptables? ¿Se hace contacto de referencias y una verificación de antecedentes, según corresponda durante el proceso de selección?

			¿Existen procesos de selección mejorados para los trabajadores en roles críticos? ¿Cómo se logra todo esto? ¿Hay un proceso documentado, consistente y repetible, que sea propiedad y mantenido por RRHH?
A7.1.2	Términos y condiciones del empleo	No aplicable	¿Están claramente definidos los términos y condiciones de empleo? ¿Se hace distinción entre profesionales de la seguridad, los administradores de redes / sistemas de TI, los gerentes, los auditores y los trabajadores en general? ¿Se identifican responsabilidades específicas relacionadas con el riesgo y la seguridad de la información de acuerdo con la naturaleza de los roles? ¿Se mantienen registros para probar que los trabajadores entendieron, reconocieron y aceptaron sus obligaciones de seguridad de la información?
A7.2	**Durante el empleo**		
A7.2.1	Responsabilidades de gestión	Definido	¿Existe un programa de concientización / educación sobre la seguridad de la información dirigido a la gerencia? ¿Se hace de forma regular y está a día? ¿El contenido y la naturaleza / formato / estilo de la información y las actividades de sensibilización son adecuados? ¿Los gerentes reciben el conocimiento y la capacitación apropiados específicamente sobre su riesgo clave de información y roles y responsabilidades relacionados con la seguridad? ¿Se provee información sobre la postura, estrategias y políticas de seguridad de la información de la organización?
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Repetible	¿Están las competencias necesarias y los requisitos de capacitación / concienciación para los profesionales de seguridad de la información y otros con funciones y responsabilidades específicas identificadas explícitamente? ¿Existe un programa estructurado de sensibilización y capacitación sobre seguridad de la información para todos los tipos de trabajadores? ¿Existe una estrategia o plan de comunicación, que incluya folletos, carteles, correos electrónicos, gestión de aprendizaje online, cuestionarios, concursos, videos, redes sociales y otros métodos? ¿Se cubren los requisitos legales, reglamentarios, contractuales, políticos, responsabilidad personal, responsabilidades generales, puntos de contacto y otros recursos?

			¿Se actualiza el contenido para reflejar los riesgos de la información en evolución, como las amenazas emergentes, las vulnerabilidades recientemente identificadas y los incidentes, y los cambios, como las políticas nuevas / revisadas? ¿Hay exámenes y ejercicios periódicos para verificar el nivel de conocimiento? ¿Hay acciones de seguimiento para cualquiera que tenga problemas en dichas pruebas?
A7.2.3	Proceso disciplinario	Administrado	¿Existe un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial por parte de los trabajadores? ¿Cómo se informa a los trabajadores sobre el proceso, incluidas las expectativas de la organización y sus derechos? ¿Está esto cubierto por contratos y acuerdos, capacitación inicial y conocimiento continuo? ¿Se actualiza el proceso de forma regular?
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		
A7.3.1	Responsabilidades ante la finalización o cambio	Administrado	¿Existen políticas de revisión, estándares, procedimientos, directrices y registros relacionados con la seguridad de la información para los trabajadores que se mueven lateral o verticalmente dentro de la organización? ¿Se tienen en cuenta las promociones, degradaciones, cambios de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias, despidos? ¿Se tiene en cuenta la recuperación de los activos de información (documentos, datos, sistemas), las llaves, la eliminación de los derechos de acceso?
A8	**Gestión de activos**		
A8.1	**Responsabilidad sobre los activos**		
A8.1.1	Inventario de activos	Optimizado	¿Hay un inventario de activos de la información? ¿Contiene la siguiente información? • Datos digitales • Información impresa • Software • Infraestructura • Servicios de información y proveedores de servicios • Seguridad física • Relaciones comerciales • Las personas

			¿A quién pertenece el inventario? ¿Cómo se mantiene el inventario en una condición razonablemente completa, precisa y actualizada a pesar de los cambios de equipo / personal, nuevos sistemas, negocios y cambios de TI? ¿Es suficientemente detallado y está estructurado adecuadamente?
A8.1.2	Propiedad de los activos	Optimizado	¿Los activos tienen propietario de riesgo? ¿Los activos tienen responsable técnico? ¿Cómo se asigna la propiedad poco después de crear o adquirir los activos críticos? ¿Cómo se etiquetan los activos? ¿Cómo se informa ante incidentes de seguridad de la información que los afectan?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Preguntas
A8.1.3	Uso aceptable de los activos	Administrado	¿Existe una política sobre el uso aceptable de los recursos tecnológicos, como el correo electrónico, la mensajería instantánea, el FTP, las responsabilidades de los usuarios, etc.? ¿Cubre el comportamiento del usuario en Internet y en las redes sociales? ¿Se permite el uso personal de los activos de la empresa? En caso afirmativo, ¿En qué medida y cómo se controla / asegura esto? ¿Se describe de forma explícita lo qué constituye un uso inapropiado? ¿Se distribuye esta información a toda la empresa? ¿El uso de la criptografía cumple con todas las leyes, acuerdos / contratos y normativas relevantes?
A8.1.4	Devolución de activos	Optimizado	¿Existe un procedimiento para recuperar los activos tras una baja o despido? ¿Es un procedimiento automatizado o manual? Si es manual, ¿Cómo se garantiza que no haya desvíos? ¿Cómo se abordan los casos en los que los activos no han sido devueltos?
A8.2	**Clasificación de la información**		

A8.2.1	Clasificación de la información	Administrado	¿Existen políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados con la clasificación de la información? ¿La clasificación es impulsada por obligaciones legales o contractuales? ¿La clasificación se basa en los requisitos de confidencialidad, integridad y disponibilidad? ¿Se utilizan marcas apropiadas en los activos en función de la clasificación de la información que contienen? ¿El personal conoce los requisitos de seguridad correspondientes para el manejo de materiales clasificados?
A8.2.2	Etiquetado de la información	Administrado	¿Existe un procedimiento de etiquetado para la información tanto en forma física como electrónica? ¿Está sincronizado con la política de clasificación de la información? ¿Cómo se garantiza el correcto etiquetado? ¿Cómo se garantiza que solo aquellos con permisos de acceso aprobados accedan a la información de la clasificación relevante? ¿Cómo se garantiza que no haya acceso no autorizado? ¿Se revisan los niveles de clasificación en intervalos predefinidos?
A8.2.3	Manipulado de la información	No aplicable	Más allá de A.8.2.1 ¿Están los niveles de clasificación adecuadamente asignados a los activos? ¿Se considera los gimiente? Método de etiquetado, transferencia, almacenamiento, manejo de medios extraíbles, eliminación de medios electrónicos y físicos, divulgación, intercambio, intercambio con terceros, etc.
A8.3	**Manipulación de los soportes**		
A8.3.1	Gestión de soportes extraíbles	Administrado	¿Existe un registro de activos completo y actualizado de CD / DVD, almacenamiento USB y otros medios extraíbles? ¿Los medios extraíbles están debidamente etiquetados y clasificados? ¿Los medios se mantienen y almacenan de forma adecuada? ¿Hay controles apropiados para mantener la confidencialidad de los datos almacenados?
A8.3.2	Eliminación de soportes	Definido	Más allá de A.8.3.1 ¿Existen una política específica y documentación de obligaciones contractuales, legales o reglamentarias para la eliminación de los medios? ¿Se documenta la aprobación en cada etapa para la eliminación de los medios? ¿Los datos que aún deben conservarse se copian en otros medios y se verifican antes de su eliminación?

			¿Se tiene en cuenta los periodos de retención? ¿Los datos particularmente confidenciales se eliminan de forma segura (borrado criptográfico, desmagnetización o destrucción física)?
A8.3.3	Soportes físicos en tránsito	Definido	¿Se utiliza un transporte o servicio de mensajería confiable? ¿Se utiliza un mecanismo de cifrado adecuado durante el proceso de transferencia? ¿Se verifica la recepción por el destino?
A9	**Control de acceso**		
A9.1	**Requisitos de negocio para el control de acceso**		
A9.1.1	Política de control de acceso	Administrado	¿Existe una política de control de acceso? ¿Es consistente con la política de clasificación? ¿Hay una segregación de deberes apropiada? ¿Existe un proceso documentado de aprobación de acceso? ¿El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión?
A9.1.2	Acceso a las redes y a los servicios de red	Administrado	¿Se asegura que el acceso VPN e inalámbrico es supervisado, controlados y autorizado? ¿Se utiliza autenticación de múltiples-factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados? ¿Cómo monitoriza la red para detectar acceso no autorizado? ¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)? ¿La organización mide la identificación y los tiempos de respuesta ante incidentes?
A9.2	**Gestión de acceso de usuario**		
A9.2.1	Registro y baja de usuario	Definido	¿Se utiliza un ID de usuario únicos para cada usuario? ¿Se genera en función a una solicitud con aprobaciones y registros apropiados? ¿Se deshabilitan los ID de usuario de forma inmediata tas una baja o despido? ¿Existen una comunicación eficiente ente la Administración de Seguridad y Recursos Humanos? ¿Existe una revisión / auditoría periódica para identificar y deshabilitar los ID de usuario redundantes? ¿Se eliminan los ID deshabilitados después de confirmar que ya no son necesarios? ¿Qué impide que los ID de usuario sean reasignados a otros usuarios?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Preguntas
A9.2.2	Provisión de acceso de usuario	Administrado	¿El acceso a sistemas y servicios de información se basa en las necesidades del negocio? ¿Se garantiza que todo acceso que se concede se ajuste a las políticas de control de acceso y segregación de funciones? ¿Existe un registro documental de la solicitud y aprobación de acceso?
A9.2.3	Gestión de privilegios de acceso	Administrado	Más allá de A.9.2.2 ¿Hay un proceso para realizar revisiones más frecuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios? ¿Se genera un ID de usuario separado para otorgar privilegios elevados? ¿Se ha establecido una caducidad para los ID de usuario con privilegios? ¿Se controlan las actividades de los usuarios privilegiados de forma más detallada?
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Repetible	¿Se implementan controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas en el primer uso, autenticación de múltiples factores, datos biométricos, contraseñas compartidas etc.? ¿Se verifica rutinariamente si hay contraseñas débiles? ¿Se requiere confirmar la identidad de los usuarios antes de proporcionarles contraseñas temporales nuevas? ¿Se transmite dicha información por medios seguros? ¿Se generan contraseñas temporales suficientemente fuertes? ¿Se cambian las contraseñas por defecto de los fabricantes? ¿Se recomienda a los usuarios usar el software adecuado de protección de contraseñas? ¿Se almacenen de forma cifrada las contraseñas en sistemas, dispositivos y aplicaciones?
A9.2.5	Revisión de los derechos de acceso de usuario	Definido	¿Se hace una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones? ¿Participan en dicha revisión los "propietarios" para verificar cambios en las funciones de los usuarios? ¿Se revisan los derechos de acceso para usuarios con privilegios de forma más exhaustiva y frecuente?

A9.2.6	Retirada o reasignación de los derechos de acceso	Administrado	¿Existe un proceso de ajuste de derechos de acceso? ¿Tiene en cuenta empleados, proveedores y contratistas al finalizar o cambiar su empleo, contrato o acuerdo? ¿Incluye el acceso físico a las instalaciones y el acceso lógico a la red? En casos en los que se usan credenciales compartidas, ¿Se cambian las contraseñas cuando ocurren ceses o despidos de empleados que las usan?
A9.3	**Responsabilidades del usuario**		
A9.3.1	Uso de la información secreta de autenticación	Definido	¿Cómo se asegura la confidencialidad de las credenciales de autenticación? ¿Existe un proceso de cambio de contraseñas en caso de ser comprometida? ¿Existen controles de seguridad relativas a las cuentas compartidas?
A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información	Administrado	Más allá de A.9.2.2 ¿Existen controles de acceso adecuados? ¿Se identifican los usuarios de forma individual individuales? ¿Cómo se definen, autorizan, asignan, revisan, gestionan y retiran los derechos de acceso, los permisos y las reglas asociadas?
A9.4.2	Procedimientos seguros de inicio de sesión	Definido	¿Se muestra una pantalla de advertencia en el proceso de inicio de sesión para disuadir el acceso no autorizado? ¿Cómo se autentican las identidades de usuario durante el proceso de inicio de sesión? ¿Se utiliza autenticación multifactor para sistemas / servicios / conexiones remotas críticas a través de VPN s etc.? ¿La información de inicio de sesión solo se valida una vez imputadas las credenciales? ¿Las contraseñas no válidas desencadenan demoras o bloqueos, entradas de registro y alertas / alarmas? ¿Se registran los inicios de sesión exitosos? ¿Se transmiten las contraseñas de modo seguro mediante el uso de cifrado?
A9.4.3	Sistema de gestión de contraseñas	Definido	¿Los sistemas requieran una fortaleza de contraseñas establecidos en las políticas y estándares corporativos? ¿Las reglas tienen en cuenta lo siguiente? • Longitud mínima de la contraseña • Evitan la reutilización de un número específico de contraseñas • Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc.)

			• Requiere el cambio forzado de contraseñas en el primer inicio de sesión • Esconde la contraseña durante la imputación ¿Se almacenan y transmiten de forma segura (cifrado)?
A9.4.4	Uso de utilidades con privilegios del sistema	Administrado	¿Quién controla los servicios privilegiados? ¿Quién puede acceder a ellos, bajo qué condiciones y con qué fines? ¿Se verifica que estas personas necesidad comercial para otorgar el acceso según su roles y responsabilidades? ¿Existe un proceso auditable de aprobación, y cada instancia de su uso está registrado? ¿Se tiene en cuenta la segregación de tareas?
A9.4.5	Control de acceso al código fuente de los programas	Definido	¿El código fuente se almacena en una o más bibliotecas de programas fuente o repositorios? ¿El entorno es seguro, con un acceso adecuado, control de versiones, monitoreo, registro, etc.? ¿Cómo se modifica el código fuente? ¿Cómo se publica y se compila el código? ¿Se almacenan y revisan los registros de acceso y cambios?
A10	**Criptografía**		
A10.1	**Controles criptográficos**		

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Preguntas
A10.1.1	Política de uso de los controles criptográficos	No aplicable	¿Existe una política que cubra el uso de controles criptográficos? ¿Cubre lo siguiente? • Los casos en los que información debe ser protegida a través de la criptografía • Normas que deben aplicarse para la aplicación efectiva • Un proceso basado en el riesgo para determinar y especificar la protección requerida • Uso de cifrado para información almacenada o transferida • Los efectos de cifrado en la inspección de contenidos de software• Cumplimiento de las leyes y normativas aplicables ¿Se cumple con la política y requerimientos de cifrado?

A10.1.2	Gestión de claves	No aplicable	¿La política de criptografía abarca todo el ciclo de vida de la gestión de claves (de principio a fin)? ¿Se protege el equipo utilizado para generar, almacenar y archivar claves criptográficas? ¿Se generan claves diferentes para sistemas y aplicaciones? ¿Se evitan claves débiles? ¿Existen reglas sobre cambio / actualización de claves (ej. autorizar, emitir, comunicar e instalar claves)? ¿Se hacen copias de respaldo de las claves? ¿Se registran las actividades clave de gestión? ¿Cómo se cumplen todos estos requisitos?
A11	**Seguridad física y del entorno**		
A11.1	**Áreas seguras**		
A11.1.1	Perímetro de seguridad física	Optimizado	¿Las instalaciones se encuentran en una zona de riesgo? ¿Se definen los perímetros de seguridad (edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, salas de máquinas, etc.)? ¿El techo exterior, las paredes y el suelo son de construcción sólida? ¿Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado? ¿Las puertas y ventanas son fuertes y con cerradura? ¿Se monitorea los puntos de acceso con cámaras? ¿Existe un sistema de detección de intrusos y se prueba periódicamente?
A11.1.2	Controles físicos de entrada	Optimizado	¿Se utilizan sistemas de control de acceso adecuados (ej. Tarjetas de proximidad, biométrico, cerraduras de seguridad, monitorización CCTV, detección de intrusos)? ¿Hay procedimientos que cubran las siguientes áreas? • Cambio regular código de acceso • Inspecciones de las guardias de seguridad • Visitantes siempre acompañados y registrados en el libro de visitantes • Registro de movimiento de material • Entrada a áreas definidas del edificio según roles y responsabilidades (acceso a CPD, salas de comunicación y otras áreas críticas) ¿Se utiliza autenticación multi-factor de autenticación (ej. Biométrico más el código PIN)?

			¿Se requiere para las áreas críticas? ¿Existe un registro de todas las entradas y salidas?
A11.1.3	Seguridad de oficinas, despachos y recursos	Optimizado	¿Están los accesos (entrada y salida) de las instalaciones físicamente controlas (ej. Detectores de proximidad, CCTV)? ¿Son proporcionados los controles de seguridad utilizados para salvaguardar las oficinas, salas e instalaciones con respecto a los riesgos? ¿Se tiene en cuenta los activos de información almacenados, procesados o utilizados en dichas ubicaciones?
A11.1.4	Protección contra las amenazas externas y ambientales	Administrado	¿Qué tipo de protecciones existen contra el fuego, el humo, inundaciones, rayos, intrusos, vándalos, etc.? ¿Existe un procedimiento de recuperación de desastres? ¿Se contemplan sitios remotos?
A11.1.5	El trabajo en áreas seguras	Administrado	¿Se verifican al final del día las oficinas, las salas de informática y otros lugares de trabajo? ¿Se hace un análisis para evaluar que los controles adecuados están implementados? Controles de acceso físico Alarmas de intrusión Monitoreo de CCTV (verificar la retención y frecuencia de revisión) Se prohíbe el uso de equipos fotográficos, video, audio u otro tipo de grabación Políticas, procedimientos y pautas ¿Cómo se asegura que la información de carácter sensible permanece confidencial a personal autorizado?
A11.1.6	Áreas de carga y descarga	Administrado	¿Las entregas se hacen en un área segura con control de acceso y limitado a personal autorizado? ¿Se verifica que el material recibido coincide con un número de pedido autorizado? ¿Se registran los detalles de la recepción de material según las políticas y procedimientos de adquisición, gestión de activos y seguridad?
A11.2	**Seguridad de los equipos**		

A11.2.1	Emplazamiento y protección de equipos	Optimizado	¿Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas? ¿Las pantallas de los equipos de trabajo, las impresoras y los teclados están ubicados o protegidos para evitar la visualización no autorizada? ¿Existen controles para minimizar los siguientes riesgos de amenazas físicas y medioambientales? • Agua / inundación • Fuego y humo • Temperatura, humedad y suministro eléctrico • Polvo • Rayos, electricidad estática y seguridad del personal ¿Se prueban estos controles periódicamente y después de cambios importantes?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Preguntas
A11.2.2	Instalaciones de suministro	Optimizado	¿El sistema UPS proporciona una potencia adecuada, confiable y de alta calidad? ¿Hay una capacidad de UPS adecuada para abarcar todos los equipos esenciales durante un período de tiempo suficiente? ¿Hay un plan de mantenimiento pare los UPS y generadores en acuerdo con las especificaciones del fabricante? ¿Son probados con regularidad? ¿Hay una red de suministro eléctrico redundante? ¿Se realizan pruebas de cambio? ¿Se ven afectados los sistemas y servicios? ¿Hay sistemas de aire acondicionado para controlar entornos con equipos críticos? ¿Están ubicados apropiadamente? ¿Hay una capacidad adecuada de A / C para soportar la carga de calor? ¿Hay unidades redundantes, de repuesto o portátiles disponibles? ¿Hay detectores de temperatura con alarmas de temperatura?
A11.2.3	Seguridad del cableado	Optimizado	¿Hay protección física adecuada para cables externos, cajas de conexiones? ¿Se separa el cableado de suministro eléctrico del cableado de comunicaciones para evitar interferencias? ¿Se controla el acceso a los paneles de conexión y las salas de cableado?

			¿Existen procedimientos adecuados para todo ello?
A11.2.4	Mantenimiento de los equipos	Optimizado	¿Se asigna personal cualificado para realizar el mantenimiento de los equipos (infraestructura y dispositivos de red, equipos de trabaja, portátiles, equipos de seguridad y servicios tales como detectores de humo, dispositivos de extinción de incendios, HVAC, control de acceso, CCTV, etc.)? ¿Hay programas de mantenimiento y registros / informes actualizados? ¿Se aseguran los equipos?
A11.2.5	Retirada de materiales propiedad de la empresa	Administrado	¿Existen procedimiento relativos al traslado de activos de información? ¿Hay aprobaciones o autorizaciones documentadas en los niveles apropiados? ¿Existe un control para limitar el traslado de activos de información mediante el uso de unidades de almacenamiento externo? ¿Existe un procedimiento para rastrear movimientos de activos de alto valor o alto riesgo?
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Administrado	¿Existe una “política de uso aceptable” que cubra los requisitos de seguridad y “obligaciones” con respecto al uso de dispositivos móviles o portátiles que se utilizan desde casa o en ubicaciones remotas? ¿Contempla el almacenamiento seguro de los dispositivos, uso cifrado y uso de conexiones seguras? ¿Existen controles para asegura todo esto? ¿Cómo se les informa a los trabajadores sobre sus obligaciones? ¿Se les da suficiente apoyo para alcanzar un nivel aceptable de seguridad?
A11.2.7	Reutilización o eliminación segura de equipos	Administrado	¿Cómo evita la organización que se revele la información almacenada en equipos tras su reasignación o eliminación? ¿Se utiliza cifrado fuerte o borrado seguro? ¿Se mantienen registros adecuados de todos los medios que se eliminan? ¿La política y el proceso cubren todos los dispositivos y medios de TIC?
A11.2.8	Equipo de usuario desatendido	Administrado	¿Se suspenden / finalizan las sesiones a aplicaciones para evitar la pérdida de datos o la corrupción? ¿Se define un tiempo de inactividad adecuado los riesgos de acceso físico no autorizado? ¿Se protegen los bloqueos de pantalla con contraseña?

			¿Se aplica a todos los servidores, equipos de trabajo, portátiles, teléfonos y otros dispositivos TIC? ¿Cómo se verifica el cumplimiento?
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Administrado	¿Existen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas? ¿Funciona en la práctica? ¿Todos los dispositivos informáticos tienen un salvapantallas o bloqueo con contraseña que los empleados usan cuando se alejan de sus dispositivos? ¿Se activa automáticamente tras de un tiempo inactivo definido? ¿Se mantienen las impresoras, fotocopiadoras, escáneres despejados?
A12	**Seguridad de las operaciones**		
A12.1	**Procedimientos y responsabilidades operacionales**		
A12.1.1	Documentación de procedimientos operacionales	Definido	¿Existen procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.? ¿Existe un conjunto completo de procedimientos de seguridad y cuándo se revisaron por última vez? ¿Los procesos son razonablemente seguros y están bien controlados? ¿Los roles y responsabilidades están bien definidos y se capacita adecuadamente al personal? ¿Se tienen en cuenta los cambios, configuraciones, versiones, capacidad, rendimiento, problemas, incidentes, copias de seguridad, almacenamiento, restauración, registros de auditoría, alarmas / alertas, endurecimiento, evaluaciones de vulnerabilidad, parches, configuración / actualizaciones de antivirus, encriptación, etc.)? ¿Los procedimientos están siendo revisados y mantenidos rutinariamente, autorizados / ordenados, compartidos y usados?
A12.1.2	Gestión de cambios	Administrado	¿Existe una política de gestión de cambios? ¿Existen registros relacionados a la gestión de cambios? ¿Se planifican y gestionan los cambios? ¿Se evalúan los riesgos potenciales asociados con los cambios? ¿Los cambios están debidamente documentados, justificados y autorizados por la administración?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Preguntas
A12.1.3	Gestión de capacidades	No aplicable	¿Existe una política de gestión de capacidad? ¿Existen registros relacionados a la gestión de capacidad? ¿Incluye aspectos tales como las SLA, seguimiento de las métricas relevantes (ej. uso de la CPU, almacenamiento y errores de página, capacidad de la red, demanda de RAM, la capacidad de aire acondicionado, espacio de rack, la utilización, etc.), alarmas / alertas en niveles críticos, la planificación hacia adelante? ¿Se basa la prioridad en asegurar el rendimiento y la disponibilidad de servicios críticos, servidores, infraestructura, aplicaciones, funciones en un análisis de riesgos?
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Administrado	¿Se segregan entornos de TIC de desarrollo, prueba y operacionales? ¿Cómo se logra la separación a un nivel de seguridad adecuado? ¿Existen controles adecuados para aislar cada entorno (ej. redes de producción, redes utilizadas para el desarrollo, redes de pruebas, la gestión)? ¿Se tienen acceso a través de perfiles de usuario debidamente diferenciados para cada uno de estos entornos? ¿Cómo se promueve y se lanza el software? ¿Se aplica la gestión de cambios a la autorización y migración de software, datos, metadatos y configuraciones entre entornos en cualquier dirección? ¿Se tiene en cuenta el riesgo de la información y los aspectos de seguridad que incluye el cumplimiento de privacidad si los datos personales se mueven a entornos menos seguros? ¿Se identifica un responsable de garantizar que el software nuevo / modificado no interrumpa las operaciones de otros sistemas o redes?
A12.2	**Protección contra el software malicioso (malware)**		

A12.2.1	Controles contra el código malicioso	Administrado	¿Existen políticas y procedimientos asociados a controles antimalware? ¿Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado? ¿Cómo se compila, gestiona y mantiene la lista y por quién? ¿Hay controles de antivirus de "escaneado en acceso" y "escaneo programático" en todos los dispositivos relevantes, incluidos servidores, portátiles, ordenadores de sobremesa y dispositivos integrados / IoT? ¿Se actualiza el software antivirus de forma automática? ¿Se general alertas accionables tras una detección? ¿Se toma acción de forma rápida y apropiada para minimizar sus efectos? ¿Cómo se gestionan las vulnerabilidades técnicas? ¿Existe una capacitación y una concienciación apropiada que cubra la detección, el informe y la resolución de malware para usuarios, gerentes y especialistas de soporte?¿Existe un mecanismo de escalación para incidentes graves?
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	Administrado	¿Existen políticas y procedimientos asociados a las copias de seguridad? ¿Existe un mandato basado en el riesgo para un registro preciso y completo de copias de seguridad cuya política de retención y frecuencia reflejen las necesidades del negocio? ¿Las copias de seguridad cubren los datos y metadatos, sistema y programas de aplicación y los parámetros de configuración de copias de seguridad para todos los sistemas, incluyendo servidores, ordenadores de sobremesa, teléfonos / sistemas de red, sistemas de gestión de red, portátiles, sistemas de control, sistemas de seguridad, etc.? ¿Los medios de respaldo están físicamente protegidos / asegurados al menos al mismo nivel que los datos operacionales? ¿Las copias de seguridad se almacenan en ubicaciones adecuadas, protegiendo contra desastres físicos y acceso indebido? ¿Se mantienen copias off-line para evitar una propagación de ransomware catastrófica? ¿Las copias de seguridad se prueban regularmente para garantizar que puedan restaurar? ¿Hay una clara adherencia a principios de confidencialidad, integridad y disponibilidad?

A12.4	Registros y supervisión		
A12.4.1	Registro de eventos	Repetible	¿Existen políticas y procedimientos para el registro de eventos? ¿Se monitorean y registran de manera consistente y segura todos los sistemas clave incluido el registro de eventos en sí? ¿Se registra lo siguiente? • cambios en los ID de usuario • permisos y controles de acceso • actividades privilegiadas del sistema • intentos de acceso exitosos y fallidos • inicio de sesión y cierre de sesión • identidades y ubicaciones de dispositivos • direcciones de red, puertos y protocolos • instalación de software • cambios a las configuraciones del sistema • uso de utilidades y aplicaciones del sistema • archivos accedidos y el tipo de acceso • filtros de acceso web ¿Quién es responsable de revisar y hacer un seguimiento de los eventos informados? ¿Cuál es el periodo de retención de eventos?
A12.4.2	Protección de la información del registro	Repetible	¿Los registros se almacenan / archivan en un formato seguro o mecanismo de control no-editable? ¿El acceso a los registros es adecuadamente controlado, autorizado y monitoreado? ¿Quién tiene o podría obtener acceso a leer / escribir / eliminar registros de eventos? ¿Hay suficiente capacidad de almacenamiento dado el volumen de registros que se generan y los requisitos de retención? ¿Existen copias de seguridad de los registros?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Preguntas
A12.4.3	Registros de administración y operación	No aplicable	¿Hay responsables identificados para la administración de acceso privilegiado al análisis de eventos (SIEM)? ¿Cómo se recogen, almacenan y aseguran, analizan los registros? ¿Existen limitaciones a la capacidad de dichas personas para interferir con los registros o, al menos, no sin generar alarmas de seguridad?

A12.4.4	Sincronización del reloj	Definido	¿Existen políticas, arquitecturas o procedimientos relativos a la sincronización del reloj del sistema su precisión? ¿Hay un tiempo de referencia definido (ej. Reloj atómicos, GPS o NTP)? ¿El método para sincronizar relojes con la referencia cumple con los requisitos comerciales, de seguridad, operacionales, legales, regulatorios y contractuales? ¿Está implementado en todo el entorno TI, incluidos los sistemas de monitoreo tales como CCTV, sistemas de alerta, mecanismos de control de acceso, sistemas de auditoría y registro, etc.? ¿Existe una configuración de respaldo para la referencia de tiempo?
A12.5	**Control del software en explotación**		
A12.5.1	Instalación del software en explotación	Administrado	¿Existe una política acerca de la instalación de software? ¿Se asegura que todo software instalado es probado, aprobado, permitido y mantenido para su uso en producción? ¿Se verifica que ya no se utiliza software sin soporte (firmware, sistemas operativos, middleware, aplicaciones y utilidades)? ¿Se hace esta verificación en ordenadores de sobremesa, portátiles, servidores, bases de datos, etc.? ¿Existen controles para evitar instalaciones de software, excepto por administradores capacitados y autorizados? ¿Existe un monitoreo y alerta para detectar instalaciones de software no aprobadas? ¿Existe un control de cambio y aprobación adecuado para la aprobación de software?
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	Repetible	¿Existe una política la gestión de vulnerabilidades técnicas? ¿Cómo se escanean los sistemas para detectar vulnerabilidades de forma automatizada? ¿Cómo responde la organización ante vulnerabilidades técnicas descubiertas en equipos, servidores, aplicaciones, dispositivos de red y otros componentes? ¿Existen procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes? ¿Se ha realizado una evaluación integral de riesgos de los sistemas TIC? ¿Se han identificado los riesgos y se han tratado apropiadamente, se han priorizado según el riesgo? ¿Se identifican cambios tales como amenazas emergentes,

			vulnerabilidades conocidas o sospechadas, y consecuencias o impactos comerciales en evolución? ¿Los parches son evaluados por su aplicabilidad y riesgos antes de ser implementados? ¿Los procesos para implementar parches urgentes son adecuados? ¿Se emplea una administración automatizada de parches? ¿Existen registros de aprobación o rechazo de implementación de parchas asociado a vulnerabilidades (aceptación de riesgo) en los niveles de administración adecuados?
A12.6.2	Restricción en la instalación de software	Optimizado	¿La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados? ¿Los privilegios de instalación están divididos en categorías y permiten instalar tipos de sistemas específicos? ¿Los controles se aplican a parches, copias de seguridad y descargas de la web, así como a instalaciones de sistemas, servidores, etc.?
A12.7	**Consideraciones sobre la auditoria de sistemas de información**		
A12.7.1	Controles de auditoría de sistemas de información	Inicial	¿Existe una política que requiera auditorias de seguridad de la información? ¿Existe un programa definido y procedimientos para auditoría? ¿Las auditorías se planifican cuidadosamente y se acuerdan para minimizar el riesgo de interrupciones en los procesos comerciales? ¿Se define el alcance de la auditoría en coordinación con la administración? ¿El acceso a las herramientas de auditoría de sistemas están controladas para evitar el uso y acceso no autorizado?
A13	**Seguridad de las comunicaciones**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de red	Administrado	¿Existen políticas de redes físicas e inalámbricas? ¿Existe una separación de la administración de las operaciones de sistemas y la de infraestructuras de red? ¿Existe un mecanismo de registro i monitorización de la red y los dispositivos que se conectan ella? ¿Hay un sistema de autenticación para todos los accesos a la red de la organización? ¿El sistema limita el acceso de personas autorizadas a aplicaciones / servicios legítimos? ¿Los usuarios se autentican adecuadamente al inicio de sesión? ¿Cómo se autentican los dispositivos de red?

			¿Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.? ¿Se controlan los puertos y servicios utilizados para funciones de administración de sistemas?
A13.1.2	Seguridad de los servicios de red	Optimizado	¿Se gestionan, clasifican y protegen los servicios de red de forma adecuada? ¿Existe un monitoreo de servicios de red? ¿Se mantiene un derecho a auditar servicios de red gestionados por terceros (contratos, SLA y requisitos de informes de gestión)? ¿Se emplean mecanismos de autenticación en la red, cifrado de tráfico de red? ¿Se hace una revisión periódica de las configuraciones de cortafuegos, IDS / IPS, WAF, DAM?

Sección	Controles de Seguridad de la Información	Estado	Preguntas
A13.1.3	Segregación en redes	Administrado	¿Existe una política de segmentación de red? ¿Qué tipo de segmentación existe? ¿Es basada en la clasificación, los niveles de confianza, dominios (público, escritorios, servidor, funciones, etc.)? ¿Cómo se monitorea y controla la segregación? ¿Se segmenta la red inalámbrica de la red física? ¿Y la red de invitados? ¿Hay controles adecuados entre ellos? ¿Cómo se controla la segmentación con proveedores y clientes? ¿La seguridad es adecuada dados los riesgos y el apetito de riesgo de la organización?
A13.2	**Intercambio de información**		
A13.2.1	Políticas y procedimientos de intercambio de información	Administrado	¿Existen políticas y procedimientos relacionados con la transmisión segura de información? ¿Contempla mecanismos como correo electrónico, FTP y otras aplicaciones de transferencia de datos y protocolos Web (ej. Los grupos / foros, Dropbox y servicios en la nube similares), WiFi y Bluetooth, CD / DVD, almacenamiento externo USB, mensajería, etc.? ¿Está basado en la clasificación de la información? ¿Existen controles de acceso adecuados para esos mecanismos? ¿Cómo se implementa el uso de criptografía para los mecanismos aceptados (ej. TLS, cifrado de correo electrónico, ZIP codificados)? ¿Se sigue el principio de confidencialidad y privacidad? ¿Existen un programa de concientización, capacitación y cumplimiento?
A13.2.2	Acuerdos de intercambio de información	No aplicable	Más allá de A.13.2.1 ¿Qué tipos de comunicaciones se implementan las firmas digitales? ¿Qué tipo de responsabilidades se asocian a la pérdida, corrupción o divulgación de datos? ¿Existe una identificación y sincronización de los niveles de clasificación de información de todas las partes involucradas? ¿Cómo se mantiene una cadena de custodia para las transferencias de datos?
A13.2.3	Mensajería electrónica	Administrado	¿Existe una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP, etc.?

			¿Hay controles de seguridad adecuados (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)? ¿Existen controles de seguridad para la interacción con sistemas Internet, Intranet relacionados con foros y tableros de anuncios electrónicos?
A13.2.4	Acuerdos de confidencialidad o no revelación	No aplicable	¿Existen acuerdos de confidencialidad? ¿Han sido revisados y aprobados por el Departamento Legal? ¿Cuándo fueron revisados por última vez (periódicos o basados en cambios)? ¿Han sido aprobados y firmados por las personas adecuadas? ¿Existen sanciones adecuadas y acciones esperadas en caso de incumplimiento y / o beneficios por el cumplimiento (ej. una bonificación de rendimiento)?
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		
A14.1	**Requisitos de seguridad en los sistemas de información**		
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Administrado	¿Existen políticas, procedimientos y registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software? ¿Existen procedimientos para analizar riesgos, requisitos funcionales y técnicos, arquitectura de seguridad, las pruebas de seguridad y la certificación de sistemas y desarrollo? ¿Son estos procedimientos obligatorios para todos los nuevos desarrollos y cambios en los sistemas existentes (ej. Actualizaciones de sistema operativo / aplicaciones en las actualizaciones, cambios de criptografía, etc.) ¿Se aplican estos controles para sistemas / software comercial, incluidos los productos “a medida” o personalizados?
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	No aplicable	¿La organización usa o proporciona aplicaciones web de comercio electrónico? ¿Se verifican los aspectos de seguridad como control de acceso y autenticación de usuarios, integridad de datos y la disponibilidad del servicio? ¿Contiene controles tales como validación de datos de entrada, validación de procesamiento, encriptación, autenticación de mensajes e irrenunciabilidad? ¿Se fuerza https? ¿Los sitios web públicos están siendo monitoreados (ej. eventos, vulnerabilidades, etc.)? ¿Se analizan y documentan las amenazas de forma rutinaria? ¿Existe una gestión de incidentes y cambios para tratarlos?

A14.1.3	Protección de las transacciones de servicios de aplicaciones	No aplicable	Más allá de A.14.1.2 ¿Las transacciones se realizan y almacenan en un entorno interno seguro o expuesto a internet? ¿Se protege la información mediante el uso de protocolos seguros, cifrado, firma electrónica, etc.? ¿Cumplen con todos los requisitos legales, regulatorios y de cumplimiento?
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		
A14.2.1	Política de desarrollo seguro	No aplicable	¿Existe una política de desarrollo seguro que abarque la arquitectura de seguridad? ¿Los entornos de desarrollo usan repositorios seguros con control de acceso, seguridad y control de cambios? ¿Los métodos de desarrollo incluyen pautas de programación segura? ¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?
A14.2.2	Procedimiento de control de cambios en sistemas	Definido	¿Existen políticas, procedimientos y registros relacionados de la gestión de cambios? ¿Incluyen planificación y prueba de cambios, evaluaciones de impacto (incluido el riesgo de información y aspectos de seguridad, más los impactos de no cambiar), verificaciones de instalación y procedimientos de retroceso / reversión? ¿Incluye un procedimiento para cambios de emergencia? ¿Se aplica los cambios significativos en equipos informáticos y de telecomunicaciones? ¿Los cambios en el sistema están debidamente documentados, justificados y autorizados por la administración?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Preguntas
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Definido	¿Se requiere una validación / evaluaciones de riesgo y, si es necesario, recertificación de sistemas tras actualizaciones / mantenimiento, parches, cambios sistema operativo, actualizaciones de aplicaciones y cambios de cifrado? ¿Hay registros de estas actividades?
A14.2.4	Restricciones a los cambios en los paquetes de software	Administrado	¿Se hacen cambios a paquetes software adquiridos? ¿Se verifica que los controles originales no han sido comprometidos? ¿Se obtuvo el consentimiento y la participación del proveedor?

			¿El proveedor continúa dando soporte tras los cambios? ¿Se exploró la posibilidad de obtener actualizaciones de programas estándar por parte de los proveedores? ¿Se hace una comprobación de compatibilidad con otro software en uso?
A14.2.5	Principios de ingeniería de sistemas seguros	No aplicable	¿Se siguen principios de SDLC que incluye controles de seguridad? ¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?
A14.2.6	Entorno de desarrollo seguro	Administrado	¿Se aíslan los entornos de desarrollo? ¿Cómo se desarrolla, prueba y lanza el software? ¿Quién es responsable de garantizar que el software nuevo / modificado no interrumpa otras operaciones? ¿Se realizan comprobaciones de antecedentes de los desarrolladores? ¿Tienen que cumplir con un NDA? ¿Cuáles son los reglamentos y los requisitos de cumplimiento que afectan el desarrollo? ¿Cómo se protegen los datos de prueba de la divulgación y dónde están almacenados?
A14.2.7	Externalización del desarrollo de software	Administrado	Más allá de A.14.2.6 ¿Se tienen en cuanta los siguientes aspectos cuando el desarrollo es lleva a cabo por un tercero? • Los acuerdos de licencia, la propiedad del código y los derechos de propiedad intelectual • Requisitos contractuales para prácticas seguras de diseño, desarrollo y prueba • Acceso al código fuente si el código ejecutable necesita ser modificado • Controles de prueba de seguridad de aplicaciones • Evaluación de vulnerabilidad y tratamiento
A14.2.8	Pruebas funcionales de seguridad de sistemas	Administrado	Más allá de A.14.2.7 ¿Existe un procedimiento de pruebas y verificación para sistemas nuevos y actualizados? ¿Tiene en cuenta acuerdos de licencia, propiedad del código y propiedad intelectual?
A14.2.9	Pruebas de aceptación de sistemas	Definido	¿Se efectúan pruebas de seguridad antes de la introducción de nuevos sistemas en la red? ¿Las pruebas replican situaciones y entornos operativos realistas? ¿Los defectos relacionados con la seguridad son tratados antes de que el producto sea certificado / aprobado?

			¿Hay pruebas de aceptación del usuario (UAT) antes del lanzamiento al entorno operativo? ¿Se actualizan los controles de resiliencia y recuperación tras incidentes para reflejar los sistemas nuevos, modificados y retirados?
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos de prueba	Definido	¿Se utilizan mecanismos para proteger datos de prueba como la seudonimización, enmascaramiento, datos falsos, borrado, etc.? ¿Existe un mecanismo de verificación y aprobación para el uso de datos no protegidos para pruebas? ¿Existen registros de estas actividades?
A15	**Relación con proveedores**		
A15.1	**Seguridad en las relaciones con proveedores**		
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	No aplicable	¿Existen políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con proveedores que involucran servicios de TI? ¿Incluyen servicios de nube, logística, servicios públicos, recursos humanos, médicos, financieros, legales y otros servicios subcontratados de alto riesgo? ¿Los contratos y acuerdos abordan lo siguiente? • Arreglos de gestión de relaciones, incluyendo el riesgo de la información y los aspectos de seguridad, la métrica, el rendimiento, problemas, rutas de escalada • Información / propiedad intelectual, y obligaciones / limitaciones derivadas • Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información • Requisitos legales y normativos, como el cumplimiento certificado de ISO 27001 • Identificación de controles físicos y lógicos • Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalado, gestión de respuesta y aspectos de continuidad del negocio • Habilitación de seguridad de los empleados y concienciación• Derecho de auditoría de seguridad por parte de la organización ¿Existe una obligación contractual de cumplimento? ¿Los proveedores de servicios externos son monitoreados rutinariamente y auditados para cumplir con los requisitos de seguridad?

A15.1.2	Requisitos de seguridad en contratos con terceros	No aplicable	¿Los contratos o acuerdos formales con proveedores cubren lo siguiente? • Gestión de las relaciones, incluyendo riesgos • Cláusulas de confidencialidad vinculantes • Descripción de la información que se maneja y el método de acceder a dicha información • Estructura de la clasificación de la información a usar • La Inmediata notificación de incidentes de seguridad • Aspectos de continuidad del negocio • Subcontratación y restricciones en las relaciones con otros proveedores • Aspectos de personal y RRHH (ej. Rendimiento, antecedentes, "robo de empleados", etc.)
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	No aplicable	Más allá de A.15.1.1 y A.15.1.2 ¿Cómo se validan los requisitos de seguridad de los productos o servicios adquiridos? ¿Cómo se logra una capacidad de recuperación cuando productos o servicios críticos son suministrados por terceros? ¿Se puede rastrear el origen del producto o servicio?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Preguntas
A15.2	**Gestión de la provisión de servicios del proveedor**		
A15.2.1	Control y revisión de la provisión de servicios del proveedor	No aplicable	¿Existe una monitorización de servicios y quien responsable de esta actividad? ¿Se llevan a cabo reuniones de revisión del servicio, con qué frecuencia? ¿Se generan informes y / o métricas relacionadas a las reuniones y las decisiones tomadas? ¿Las reuniones abarcan riesgos, incidentes, políticas, cumplimiento e informes de auditoría? ¿Existen cláusulas de penalización o de bonificación en el contrato relacionadas con el riesgo de la información?
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	No aplicable	¿Cómo se comunican cambios en los servicios relacionados con la información, servicios adicionales o cambios en la forma en que se prestan los servicios contratados? ¿Cómo se comunican cambios en las políticas y requerimientos legales de la organización? ¿Se actualizan los acuerdos relacionados con los cambios?

A16	**Gestión de incidentes de seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
A16.1.1	Responsabilidades y procedimientos	Inicial	¿Existen políticas, procedimientos e ITT´s para la gestión de incidentes? ¿Qué cubre? • I plan de respuesta a incidentes • Puntos de contacto para la notificación de incidentes, seguimiento y evaluación • Monitoreo, detección y reporte de eventos de seguridad • Asignación y escalado de incidentes (N1 > N2) incluyendo las respuestas de emergencia y la continuidad de negocio • Método de recolección de evidencias y pruebas forenses digitales • Revisión post-evento de seguridad y procesos de aprendizaje / mejora ¿Existen evidencias de la notificación de incidentes, registro, clasificación, asignación de resolución, la mitigación y la confirmación de cierre?
A16.1.2	Notificación de los eventos de seguridad de la información	Inicial	¿Cómo se informan los eventos de seguridad de la información? ¿Son conscientes los trabajadores de la necesidad de informar de inmediato y lo hacen? ¿Se crean informes de seguimiento de los incidentes? Desde la detección a la resolución. ¿Qué pasa con esos informes?
A16.1.3	Notificación de puntos débiles de la seguridad	Inicial	Más allá de A.16.1.2 ¿Existe una obligación contractual por parte de los empleados para reportar cualquier tipo de ocurrencia inusual? ¿Las políticas prohíben explícitamente a los trabajadores 'verificar', 'explorar', 'validar' o 'confirmar' vulnerabilidades a menos que estén expresamente autorizados para hacerlo?
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Repetible	¿Qué tipos de eventos se espera que informen los empleados? ¿A quién informan? ¿Cómo se evalúan estos eventos para decidir si califican como incidentes? ¿Hay una escala de clasificación? ¿Hay un proceso de clasificación y / o escalamiento para priorizar los incidentes graves? ¿En qué se basa?
A16.1.5	Respuesta a incidentes de seguridad de la información	Repetible	¿Cómo se recolecta, almacena y evalúa la evidencia? ¿Hay una matriz de escalación para usar según sea necesario? ¿Hay medios para comunicar información de tales incidentes a las organizaciones internas y externas pertinentes?

			¿Se documentan las acciones tomadas para resolver y finalmente cerrar un incidente?
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Repetible	¿Existe un proceso de evaluación / investigación para identificar incidentes de impacto recurrentes? ¿Se aprovecha la información obtenida de la evaluación de incidentes para evitar recurrencias? Además, ¿Se está utilizado para formación y concienciación? ¿La organización cuenta con un proceso de gestión de incidentes relativamente maduro? ¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?
A16.1.7	Recopilación de evidencias	Repetible	¿La recolección de evidencias de hace de forma competente en la empresa o por terceros especializados y capacitados en esta área? ¿Haya personal capacitado, competente y confiable con herramientas adecuadas y procesos definidos para el rol? (cadena de evidencia rigurosamente mantenida, evidencia asegurada en almacenamiento, herramientas y técnicas) ¿Quién decide emprender un análisis forense, y en qué criterio se base? ¿Existen obligaciones relacionadas con la jurisdicción, las diferentes normas forenses y los requisitos legales asociados?
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**		
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	Definido	¿Cómo se determinan los requisitos de continuidad del negocio? ¿Existe un plan de continuidad de negocio? ¿Existen un diseño adecuado de "alta disponibilidad" para sistemas de TI, redes y procesos críticos? ¿Se identifica el impacto potencial de los incidentes? ¿Se evalúan los planes de continuidad del negocio? ¿Se llevan a cabo ensayos de continuidad?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Preguntas
A17.1.2	Implementar la continuidad de la seguridad de la información	Definido	¿Los planes tienen plazos definidos para restaurar servicios tras una interrupción? ¿Los planes tienen en cuenta la identificación y el acuerdo de responsabilidades, la identificación de pérdidas aceptables, la implementación de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares? ¿La planificación de la continuidad es consistente e identifica las prioridades de restauración? ¿Tienen los miembros de los equipos de recuperación / gestión de crisis / incidentes conocimiento de los planes y tienen claro sus roles y responsabilidades? ¿Los controles de seguridad son adecuados en los sitios de recuperación de desastres remotos?
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Repetible	¿Existe un método de pruebas del plan de continuidad? ¿Con qué frecuencia se llevan a cabo dichas pruebas? ¿Hay evidencia de las pruebas reales y sus resultados? ¿Se han identificado deficiencias?, ¿Se han remediado? y ¿Se han vuelto a probar hasta que los resultados sean satisfactorios?
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Definido	¿Cómo se identifican los requisitos de disponibilidad de servicios? ¿Se tienen en cuenta la capacidad de recuperación, la capacidad de rendimiento, el balanceo de carga? ¿Se tienen en cuenta servicios poco fiables, equipos, instalaciones, servidores, aplicaciones, enlaces, funciones, y la organización en sí? ¿Los controles clave de seguridad de la información están implementados y son funcionales en los sitios de recuperación de desastres?
A18	**Cumplimiento**		
A18.1	**Cumplimiento de los requisitos legales y contractuales**		
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Repetible	¿Existe una política acerca del cumplimiento de requisitos legales? LOPD, GDPR, etc. ¿Se mantiene un registro o base de datos de cumplimiento enumerando todas las obligaciones, expectativas legales, reglamentarias y contractuales aplicables?

			¿Hay una persona encargada de mantener, usar y controlar el registro? ¿Cómo se logra y se garantiza el cumplimiento? ¿Existen controles adecuados para cumplir con los requisitos?
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Definido	¿Existen políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento?
A18.1.3	Protección de los registros de la organización	No aplicable	¿Existe una política que contemple lo siguiente? Clasificación, categorización, períodos de retención y medios de almacenamiento permitidos. ¿Se almacenan las firmas digitales de forma segura? ¿Se contempla la posibilidad de destrucción, falsificación y acceso no autorizado? ¿Se verifica periódicamente la integridad de los registros? ¿Se utilizan medios de almacenamiento de larga duración para el almacenamiento a largo plazo?
A18.1.4	Protección y privacidad de la información de carácter personal	Definido	¿Hay un mecanismo para instruir al personal en el manejo de información de carácter personal? ¿Hay un responsable de privacidad en la organización? ¿Es el responsable conocedor de la información de carácter personal que es recopilado, procesado y almacenados por la organización? ¿Cuáles son los controles de acceso a información de carácter personal? ¿Cuál es el nivel de acceso y roles (de personal) que tienen acceso a estos activos?
A18.1.5	Regulación de los controles criptográficos	No aplicable	¿Existe una política que cubra actividades relacionadas con importación / exportación de material criptográfico? ¿Estas actividades cumplen con los requisitos legales y reglamentarios?
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	Repetible	¿Están las prioridades de implementación de controles alineadas con los riesgos a activos de información? ¿Los requisitos de auditoría de sistemas son cuidadosamente planificados, autorizados, implementados y controlados para minimizar los riesgos? ¿Están los objetivos y el alcance de auditoria autorizados por la gerencia? ¿Está adecuadamente controlado el acceso a las herramientas / software de auditoría del sistema de información? ¿Se documentan los hallazgos de auditoría y las actuaciones para solventarlos?

A18.2.2	Cumplimiento de las políticas y normas de seguridad	Definido	¿Cómo garantizar que todos los procedimientos de seguridad dentro de un área de responsabilidad se llevan a cabo correctamente? ¿Se hace una verificación periódica?
A18.2.3	Comprobación del cumplimiento técnico	Inicial	¿Se llevan a cabo escaneos de vulnerabilidades de red y pruebas de Pentesting regulares? ¿Las pruebas son realizadas por profesionales debidamente cualificados, competentes y confiables? ¿Cómo informa, analiza y utilizan los resultados de dichas pruebas? ¿La prioridad de tratamiento se basa en un análisis de riesgos? ¿Hay evidencias de medidas tomadas para abordar los problemas identificados?

PLANIFICACIÓN

A continuación, se detallan los criterios que tendrán en cuenta para la elaboración del mapa de riesgos.

Criterios de evaluación del riesgo

Los criterios para la evaluación del riesgo son:

- El valor estratégico del proceso de información para la entidad
- La criticidad de los activos de información involucrados en el proceso
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales
- La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.

Criterios de impacto

Los criterios para la evaluación del impacto son:

- Brechas en la seguridad de la información (ejemplo: pérdidas de confidencialidad, integridad y disponibilidad de la información)
- Fallas en la operación
- Pérdida del negocio
- Daños para la reputación
- Incumplimiento de los requisitos legales

- **Criterios de aceptación del riesgo**

Los criterios para la aceptación del riego son:

- Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas
- Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado y el riesgo estimado
- Los diferentes criterios de aceptación del riesgo pueden aplicar a diferentes clases de riesgos, por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos si esto se especifica como un requisito contractual
- Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

Nivel de aceptación del riesgo

Para la medición del nivel de riesgo se usará la guía para la administración del riesgo de la DAFP:

TABLA DE PROBABILIDAD

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 5 años.
3	Posible	El evento podría ocurrir en algún momento	Al menos de una vez en los últimos 2 años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de una vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año.

TABLA DE IMPACTO

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

IMPLEMENTACIÓN

La implementación y ejecución de este plan inicia desde el momento de su aprobación y dará continuidad al anterior mapa de riesgos que se venía manejando en el Área Técnica.

EVALUACIÓN Y MEJORAMIENTO CONTINUO

La evaluación de este plan se hará de forma periódica revisando y ajustando todas las variables del mapa de riegos y siempre buscando la disminución de los riesgos tecnológicos inherentes de la entidad

MATRIZ DE RIESGOS

El ejercicio de realizar la matriz de riesgos de seguridad y privacidad de la información se realizó entre el área Técnica y Planeación, en el cual participaron el Director de la Unidad Técnica y el Coordinador del Sistema de Calidad.

Entre ambos, identificaron los riesgos que se presentan para la seguridad y privacidad de la información que se genera y se almacena en el canal, para los cuales evidenciaron las causas y las consecuencias que pueden suceder en caso de materializarse estos riesgos. Luego realizaron la evaluación de los riesgos con las tablas antes mencionadas y detectar el nivel de maduración de los riesgos.

El canal cuenta con una serie de controles que restringen a estos riesgos, evitando en su medida que el canal se vea perjudicado en caso de presentarse estas acciones. Los controles van desde capacitaciones al personal hasta software que apoyan al área Técnica en su regulación.

Por último, de nuevo se evalúan los riesgos teniendo en cuenta los controles y se refleja una nueva calificación, la cual en algunos riesgos sigue permaneciendo alta, para lo cual se plantean unas acciones con fecha, a las cuales se les realizará su respectivo seguimiento.

Se adjunta en este documento la matriz levantada para el plan, igualmente se cuenta con ella en formato de Excel para realizar su seguimiento y calificación al realizar las acciones pendientes.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

IDENTIFICACIÓN				CALIFICACIÓN					NUEVA CALIFICACIÓN				CONTROLES		
Código	*RIESGO*	CAUSA (subraye la causa predominante)	EFECTO O CONSECUENCIA	PROBABILIDAD	IMPACTO	CALIFICACIÓN	ZONA DE RIESGO INICIAL	CONTROLES EXISTENTES	PROBABILIDAD	IMPACTO	CALIFICACIÓN	ZONA DE RIESGO FINAL	ACCIONES	FECHA MÁXIMA DE IMPLEMENTACIÓN DE ACCIONES	SEGUIMIENTO A LAS ACCIONES
RG-40-1	***Pérdida de información***	- Ataques informáticos(Virus, malware, ramsonware) - Falla de equipos - Falla humana - Catástrofes (inundación, incendio, terremoto, etc.) - Incumplimientos de Políticas de TI - Falla eléctrica	-Pérdida económica -Sanciones legales -Pérdida de imagen	**Casi seguro**	**Mayor**	**50**	**Zona de riesgo extrema**	- Software de seguridad informática - Mantenimiento de equipos - Capacitación del personal - Sistemas de respaldo de la información. - Sistema eléctrico robusto y con redundancia. - Sistema de protección contraincendios - Perfiles de usuario	**Posible**	**Mayor**	**30**	**Zona de riesgo extrema**	- Implementación del modelo de gobierno digital - Socialización del manual de políticas de TI - Implementación de un directorio activo	31/12/2019	
RG-40-2	***Interrupción de la operación***	- Falla eléctrica - Falla en equipos - Falla software - Falla de conectividad	-Sanciones legales -No prestación del servicio -Pérdida de imagen	**Probable**	**Mayor**	**40**	**Zona de riesgo extrema**	- Sistema eléctrico robusto y con redundancia. - Mantenimiento de equipos - Planes de renovación tecnológica - Sistemas de respaldo para la conectividad - Plan de recuperación de desastres	**Posible**	**Mayor**	**30**	**Zona de riesgo extrema**	- Actualización del plan de recuperación de desastres - Formular proyectos de renovación tecnológica	31/12/2019	
RG-40-3	***Incumplimientos legales***	- Software sin licencia o vencida - Implementación incompleta de Gobierno digital	-Sanciones legales -Pérdida de imagen	**Probable**	**Mayor**	**40**	**Zona de riesgo extrema**	- Control de inventarios de software - Manejo de perfiles de administrador - Implementación de Gobierno Digital	**Posible**	**Mayor**	**30**	**Zona de riesgo extrema**	- Implementación del modelo de gobierno digital - Control de vencimientos de licencias	31/12/2019	
RG-40-4	***Pérdida de activos***	- Falta de mantenimientos preventivos y correctivos - Fallas eléctricas - Catástrofes (inundación, incendio terremoto, etc.) - Riesgo publico (robo,daño,etc) - Mala manipulación	-Detrimento patrimonial -No prestación del servicio	**Probable**	**Moderado**	**20**	**Zona de riesgo alta**	- Sistemas de control de acceso - Mantenimiento de equipos - Capacitación del personal - Control de inventarios - Circuito cerrado de CCTV	**Posible**	**Moderado**	**15**	**Zona de riesgo alta**	- Fortalecer el control de inventarios - Fortalecer el procedimiento de préstamo de equipos - Implementación de RCI en el CER - Actualización de los controles de acceso	31/12/2019	
RG-40-5	***Acceso no autorizado a la información***	-Vulnerabilidades de los sistemas -Fallas humanas -Incumplimientos de Políticas de TI -Sistemas operativos desactualizados -Fallas en la parametrización en los controles	-Demandas -Sanciones legales -Uso indebido de la información	**Probable**	**Moderado**	**20**	**Zona de riesgo alta**	- Mantener actualizados los software - Fortalecimiento de las protecciones perimetrales de la red - Aplicación del Manual de Políticas de TI - Capacitación del personal - Perfiles de usuario	**Posible**	**Moderado**	**15**	**Zona de riesgo alta**	- Implementación del modelo de gobierno digital - Socialización del manual de políticas de TI - Implementación de un directorio activo	31/12/2019	

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

REALIZÓ: CARLOS DUQUE **CARGO:** DIRECTOR TÉCNICO **FECHA:** 03 de octubre de 2019	**REVISÓ:** ANDRÉS JULIÁN PULGARÍN OROZCO **CARGO:** COORDINADOR SIGC **FECHA:** 07 de octubre de 2019	**APROBÓ:** CARLOS DUQUE **CARGO:** DIRECTOR TÉCNICO **FECHA:** 08 de octubre de 2019

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**CAMBIOS REALIZADOS**
V1	08/10/2019	Creación del documento