PARTES INTERESADAS PERTINENTES AL MSPI CON EL SGSI EN LA ETITC Y SUS NECESIDADES

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Escuela Tecnológica Instituto Técnico Central, mediante el presente documento, pretende identificar las partes interesadas que son pertinentes al Modelo de Seguridad y Privacidad de la Información de Gobierno Digital y al Sistema de Gestión de Seguridad de la Información y sus necesidades, con el objetivo de comprenderlas, aceptarlas e incluirlas en el alcance, cumpliendo, de esta manera, con lo establecido en el numeral 4.2 Comprensión de las necesidades y expectativas de las partes interesadas, de la norma NTC-ISO-IEC 27001:2013.

Calle 13 No. 16 - 74 | Bogotá, Colombia | PBX: (+57) 601 344 3000 www.etitc.edu.co | atencionalciudadano@itc.edu.co

2. IDENTIFICACIÓN DE LAS PARTES INTERESADAS Y SUS NECESIDADES

2.1. PARTES INTERESADAS EXTERNAS:

Para el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno Digital y el Sistema de Gestión de Seguridad de la Información (SGSI), las partes interesadas externas, pertinentes, están constituidas por los entes de control y la Policía Nacional.

A continuación, se exponen con detalles, las partes interesadas externas del MSPI de Gobierno Digital y el SGSI, con las respectivas necesidades identificadas:

Ministerio de Educación Nacional

Dentro de las necesidades y expectativas, identificadas para el Ministerio de Educación Nacional tenemos:

1. Realizar seguimiento a la implementación del Modelo de Seguridad y Privacidad de la Información de Gobierno Digital, y al Sistema de Gestión de Seguridad de la Información, mediante la Herramienta de Seguimiento de MINTIC.

2. Ofrecer asistencia técnica para garantizar que la implementación del Modelo de Seguridad y Privacidad de la Información de Gobierno Digital, y el Sistema de Gestión de Seguridad de la Información, se encuentren alineados con los intereses del Gobierno.

Ministerio de Tecnologías de la Información y las Comunicaciones

1. Dentro de las necesidades y expectativas, identificadas para el Ministerio de Tecnologías de la Información y las Comunicaciones tenemos:

2. Orientar la Política de Gobierno Digital (habilitador transversal Seguridad de la Información).

3. Dictar nuevos lineamientos de seguridad de la información, acorde a los intereses del Gobierno Nacional.

4. Realizar análisis de vulnerabilidades y pruebas de penetración, a las entidades públicas de orden Nacional.

5. Ofrecer un adecuado tratamiento a los incidentes de seguridad de la información, reportados en CSIRT Gobierno.

6. Coordinar con el departamento de la Policía Nacional (CSIRT-PONAL), eventos de ciberseguridad para las entidades públicas de orden Nacional.

Departamento Nacional de Planeación

Dentro de las necesidades y expectativas, identificadas para el Departamento Nacional de Planeación tenemos:

1. Participar en las actividades de actualización de la Política de Gobierno Digital (habilitador transversal Seguridad de la Información), de manera articulada con MINTIC.

2. Garantizar que la nueva versión del Modelo Integrado de Planeación y Gestión se encuentre articulada con la Política de Gobierno Digital (habilitador transversal Seguridad de la Información).

Función Pública

Dentro de las necesidades y expectativas, identificadas para la Función Pública tenemos:

1. Cumplimiento de lo establecido en la Ley 1712 de 2014 o Ley de Transparencia y Derecho de Acceso a la Información Pública Nacional.

2. Cumplimiento de lo establecido en el Decreto 103 de 2015, por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Superintendencia de Industria y Comercio

Dentro de las necesidades y expectativas, identificadas para la Superintendencia de Industria y Comercio tenemos:

1. Cumplimiento de lo establecido en la Ley 1581 de 2012 o Ley de Protección de Datos Personales.

2. Ingreso de las bases de datos institucionales al Registro Nacional de Bases de Datos.

Procuraduría General de la Nación

Dentro de las necesidades y expectativas, identificadas para la Procuraduría General de la Nación tenemos:

1. Verificación de los antecedentes disciplinarios de los servidores públicos y/o candidatos a ocupar vacantes en la institución.

2. Articularse con la Superintendencia de Industria y Comercio, en los procesos de investigación, ante una posible violación al tratamiento de los datos personales de un titular.

Contraloría General de la Nación

Dentro de las necesidades y expectativas, identificadas para la Contraloría General de la Nación tenemos:

1. Verificación de los antecedentes fiscales de los servidores públicos y/o candidatos a ocupar vacantes en la institución.

Policía Nacional de Colombia

Dentro de las necesidades y expectativas, identificadas para la Policía Nacional tenemos:

1. Verificación de los antecedentes judiciales de los servidores públicos y/o candidatos a ocupar vacantes en la institución.

2. Brindar una satisfactoria atención a los incidentes de seguridad de la información, reportados al departamento CSIRT-PONAL.

3. Convocar a las entidades públicas a participar en eventos de ciberseguridad, de manera coordinada con MINTIC.

4. Contribuir al mantenimiento de la convivencia como condición necesaria, para el ejercicio de los derechos y libertades públicas y para aportar a la construcción de paz.

2.2. PARTES INTERESADAS INTERNAS:

Para el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno Digital y el Sistema de Gestión de Seguridad de la Información (SGSI), las partes interesadas internas, pertinentes, están constituidas por los procesos misionales, estratégicos, de apoyo y de evaluación, definidos y aprobados por el Sistema de Aseguramiento de Calidad de la Escuela Tecnológica, de conjunto con las respectivas dependencias y/o áreas que garantizan su operación.

A continuación, se exponen con detalles, las partes interesadas internas del Modelo de Seguridad y Privacidad de la Información de Gobierno Digital y el SGSI de la ETITC, con las respectivas necesidades identificadas:

PROCESOS MISIONALES

Docencia Pes; Extensión y Proyección Social; Docencia IBTI e Investigación

Dentro de las necesidades y expectativas, identificadas para los procesos Docencia PES, Extensión y Proyección Social, Docencia BTO e Investigación tenemos:

1. Participación en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.

2. Participación en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.

3. Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

4. Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.

5. Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de esta.

6. Garantizar que el recurso humano que gestiona el proceso, participe activamente en las charlas de sensibilización que convoca la Oficina de Seguridad de la Información, acorde al documento GSI-PL-01 Plan de Sensibilización y Entrenamiento, controlado por el Sistema de Aseguramiento de Calidad.

7. Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.

8. Se efectúe la respectiva actividad de seguimiento a los planes de mejora, elaborados por el líder del proceso, para de esta manera, la Oficina de Control Interno, pueda dar fe de la eficacia de las acciones tomadas.

9. Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad.

10. Ofrecer una adecuada protección a los equipos de usuarios desatendidos.

11. Garantizar una adecuada implementación de la política de escritorio y pantalla limpia.

12. Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.

13. Establecer la cláusula de confidencialidad, en la relación contractual, con los servidores públicos del proceso.

Calle 13 No. 16 - 74 | Bogotá, Colombia | PBX: (+57) 601 344 3000 www.etitc.edu.co | atencionalciudadano@itc.edu.co

PROCESOS ESTRATÉGICOS

Direccionamiento Institucional

Dentro de las necesidades y expectativas, identificadas para el proceso Direccionamiento Institucional, tenemos:

1. Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.

2. Participación activa en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.

3. Participación activa en la determinación del alcance del MSPI de Gobierno Digital y el SGSI.

4. Asegurarse que la política de seguridad de la información y los objetivos, son compatibles con la dirección estratégica de la organización.

5. Asegurar que los recursos requeridos para la implementación del MSPI de Gobierno Digital y el SGSI, se encuentren disponibles.

6. Dirigir y apoyar al recurso humano, encargado de implementar el MSPI de Gobierno Digital y el SGSI, para contribuir a la eficacia respectiva.

7. Participación activa en la elaboración, aprobación e implementación de la política general de seguridad de la información.

8. Asignar y comunicar los roles y responsabilidades respectivas de la seguridad de la información.

9. Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

10. Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.

11. Participación activa en la elaboración de los objetivos de la seguridad de la información y planes para lograrlos.

12. Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de esta.

13. Establecer la cláusula de confidencialidad, en la relación contractual, con los servidores públicos del proceso.

14. Garantizar que el recurso humano que gestiona el proceso, participe activamente en las charlas de sensibilización que convoca la Oficina de Seguridad de la Información, acorde al documento GSI-PL-01 Plan de Sensibilización y Entrenamiento, controlado por el Sistema de Aseguramiento de Calidad.

15. Participación activa en la elaboración de la estrategia de comunicación interna, para los temas referentes a seguridad de la información.

16. Revisar, a intervalos planificados, el MSPI de Gobierno Digital y el SGSI, para asegurarse de su conveniencia, adecuación y eficacia continua.

17. Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.

18. Se efectúe la respectiva actividad de seguimiento a los planes de mejora, elaborados por el líder del proceso, para de esta manera, la Oficina de Control Interno, pueda dar fe de la eficacia de las acciones tomadas.

19. Participación activa en la elaboración del Manual de Políticas de Seguridad y Privacidad de la Información.

20. Revisión del Manual de Políticas de Seguridad y Privacidad de la Información, a intervalos planificados, para su actualización.

21. Impulsar las actividades de toma de conciencia, educación y formación, en temas relacionados con seguridad de la información.

22. Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad.

23. Ofrecer una adecuada protección a los equipos de usuarios desatendidos.

24. Garantizar una adecuada implementación de la política de escritorio limpio y pantalla limpia.

25. Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.

Gestión de Informática y Telecomunicaciones

Dentro de las necesidades y expectativas, identificadas para el proceso Gestión de Informática y Comunicaciones, tenemos:

1. Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.

2. Participación activa en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.

3. Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

4. Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.

5. Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma.

6. Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.

7. Se efectúe la respectiva actividad de seguimiento a los planes de mejora, elaborados por el líder del proceso, para de esta manera, la Oficina de Control Interno, pueda dar fe de la eficacia de las acciones tomadas.

8. Elaborar un procedimiento que permita establecer las actividades a ejecutar cuando se requiere contactar las autoridades externas pertinentes.

9. Contemplar la actividad de la seguridad de la información en la gestión de proyectos.

10. Elaborar e implementar una política para dispositivos móviles.

11. Participar activamente en la elaboración y actualización del inventario de activos de información tipo software, servicios y hardware.

12. Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad.

13. Elaborar e implementar un conjunto de políticas de control de acceso.

14. Establecer controles de seguridad para asignar los privilegios adecuados a los usuarios, para el acceso a la red institucional y sus servicios.

15. Elaborar e implementar un procedimiento para trabajo en áreas seguras.
16. Garantizar un mantenimiento adecuado de equipos.
17. Garantizar una adecuada protección a los equipos de usuarios desatendidos.
18. Garantizar la implementación de la política de escritorio limpio y pantalla limpia.
19. Garantizar la elaboración e implementación de un procedimiento de gestión de cambios.
20. Garantizar la separación de los ambientes de desarrollo, pruebas y producción.
21. Garantizar la implementación de controles de seguridad contra código malicioso.
22. Garantizar la implementación de soluciones de backup automático, para sistemas de información y usuarios del dominio.
23. Garantizar una adecuada sincronización de relojes para el registro de eventos de seguridad de la información.
24. Garantizar un adecuado control de la instalación de software, en los sistemas operativos.
25. Garantizar una adecuada gestión de las vulnerabilidades técnicas identificadas.
26. Garantizar la adquisición de certificados digitales para los sistemas de información.
27. Garantizar que el recurso humano que gestiona el proceso, participe activamente en las charlas de sensibilización que convoca la Oficina de Seguridad de la Información, acorde al documento GSI-PL-01 Plan de

Sensibilización y Entrenamiento, controlado por el Sistema de Aseguramiento de Calidad.

28. Elaborar e implementar la política de desarrollo seguro.

29. Elaborar e implementar principios para la construcción de sistemas seguros.

30. Seleccionar, proteger y controlar cuidadosamente los datos de prueba.

31. Garantizar una óptima respuesta a los incidentes de seguridad de la información.

32. Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.

33. Garantizar la revisión periódica de los sistemas de información para verificar el cumplimiento de políticas y normas de seguridad técnica.

34. Establecer la cláusula de confidencialidad, en la relación contractual, con los servidores públicos del proceso.

35. Garantizar la elaboración e implementación del plan de contingencia, recuperación y retorno a la normalidad.

Gestión de Bienestar Universitario, Gestión Financiera y Gestión Jurídica

Dentro de las necesidades y expectativas, identificadas para el proceso Bienestar Universitario, Gestión Financiera, Gestión Jurídica tenemos:

1. Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.

2. Participación activa en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.

3. Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

4. Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.

5. Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de esta.

6. Garantizar que el recurso humano que gestiona el proceso, participe activamente en las charlas de sensibilización que convoca la Oficina de Seguridad de la Información, acorde al documento GSI-PL-01 Plan de Sensibilización y Entrenamiento, controlado por el Sistema de Aseguramiento de Calidad.

7. Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.

8. Se efectúe la respectiva actividad de seguimiento a los planes de mejora, elaborados por el líder del proceso, para de esta manera, la Oficina de Control Interno, pueda dar fe de la eficacia de las acciones tomadas.

9. Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad.

10. Ofrecer una adecuada protección a los equipos de usuarios desatendidos.

11. Garantizar una adecuada implementación de la política de escritorio limpio y pantalla limpia.

12. Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.

13. Establecer la cláusula de confidencialidad, en la relación contractual, con los servidores públicos del proceso.

Gestión de Adquisiciones

Dentro de las necesidades y expectativas, identificadas para el proceso Gestión de Adquisiciones, tenemos:

1. Elaboración e implementación de la política de seguridad de la información para las relaciones con proveedores.

2. Establecer todos los requisitos de seguridad de la información, en la relación con los proveedores (cláusulas de confidencialidad y acuerdos de niveles de servicios)

3. Identificar los riesgos de seguridad de la información, relacionados con la cadena de suministro de tecnología de información y comunicación.

4. Evaluar la calidad en la prestación de servicios en los proveedores.

5. Gestionar, de manera óptima, los cambios en el suministro de servicios, por parte de los proveedores.

6. Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.

7. Participación activa en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.

8. Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

9. Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.

10. Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma.

11. Garantizar que el recurso humano que gestiona el proceso, participe activamente en las charlas de sensibilización que convoca la Oficina de Seguridad de la Información, acorde al documento GSI-PL-01 Plan de Sensibilización y Entrenamiento, controlado por el Sistema de Aseguramiento de Calidad.

12. Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.

13. Establecer la cláusula de confidencialidad, en la relación contractual, con los servidores públicos del proceso.

14. Se efectúe la respectiva actividad de seguimiento a los planes de mejora, elaborados por el líder del proceso, para de esta manera, la Oficina de Control Interno, pueda dar fe de la eficacia de las acciones tomadas.

15. Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad.

16. Ofrecer una adecuada protección a los equipos de usuarios desatendidos.

17. Garantizar una adecuada implementación de la política de escritorio limpio y pantalla limpia.

18. Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.

19. Establecer la cláusula de confidencialidad, en la relación contractual, con los servidores públicos del proceso.

Gestión de Talento Humano

Dentro de las necesidades y expectativas, identificadas para el proceso Gestión de Talento Humano, tenemos:

1. Verificar de manera satisfactoria los antecedentes disciplinarios, fiscales y penales, de los candidatos a las vacantes ofertadas por la Escuela.

2. Incluir la cláusula de confidencialidad en el Manual de Funciones, para el personal provisional, libre nombramiento y de planta.

3. Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad.

4. Ofrecer una adecuada protección a los equipos de usuarios desatendidos.

5. Garantizar una adecuada implementación de la política de escritorio limpio y pantalla limpia.

6. Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.

7. Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.

8. Participación activa en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.

9. Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

10. Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.

11. Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma.

12. Garantizar que el recurso humano que gestiona el proceso, participe activamente en las charlas de sensibilización que convoca la Oficina de Seguridad de la Información, acorde al documento GSI-PL-01 Plan de Sensibilización y Entrenamiento, controlado por el Sistema de Aseguramiento de Calidad.

13. Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.

14. Se efectúe la respectiva actividad de seguimiento a los planes de mejora, elaborados por el líder del proceso, para de esta manera, la Oficina de Control Interno, pueda dar fe de la eficacia de las acciones tomadas.

Gestión de Recursos Físicos

Dentro de las necesidades y expectativas, identificadas para el proceso Gestión de Recursos Físicos, tenemos:

1. Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad.

2. Ofrecer una seguridad de recintos, oficinas, cajones y archivadores satisfactoria, para de esta manera, preservar la confidencialidad, integridad y disponibilidad de la información almacenada.

3. Garantizar una protección óptima de todos los equipos tecnológicos de la Escuela, contra fallas de energía.

4. Ofrecer una adecuada protección al cableado de energía eléctrica y de datos, para minimizar el riesgo de interceptación, interferencia o daño.

5. Ofrecer una adecuada protección a los equipos de usuarios desatendidos.

6. Garantizar una adecuada implementación de la política de escritorio limpio y pantalla limpia.

7. Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.

8. Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.

9. Participación activa en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.

10. Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

11. Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.

12. Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de esta.

13. Garantizar que el recurso humano que gestiona el proceso, participe activamente en las charlas de sensibilización que convoca la Oficina de Seguridad de la Información, acorde al documento GSI-PL-01 Plan de Sensibilización y Entrenamiento, controlado por el Sistema de Aseguramiento de Calidad.

14. Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.

15. Se efectúe la respectiva actividad de seguimiento a los planes de mejora, elaborados por el líder del proceso, para de esta manera, la Oficina de Control Interno, pueda dar fe de la eficacia de las acciones tomadas.

Gestión Control Disciplinario

Dentro de las necesidades y expectativas, identificadas para el proceso Gestión Control Disciplinario, tenemos:

1. Implementar de manera satisfactoria el procedimiento disciplinario correspondiente, con todo servidor público que viole lo referente a seguridad de la información.

2. Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad.

3. Ofrecer una adecuada protección a los equipos de usuarios desatendidos.

4. Garantizar una adecuada implementación de la política de escritorio limpio y pantalla limpia.

5. Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.

6. Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.

7. Participación activa en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.

8. Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

9. Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.

10. Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma.

11. Garantizar que el recurso humano que gestiona el proceso, participe activamente en las charlas de sensibilización que convoca la Oficina de Seguridad de la Información, acorde al documento GSI-PL-01 Plan de Sensibilización y Entrenamiento, controlado por el Sistema de Aseguramiento de Calidad.

12. Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.

13. Se efectúe la respectiva actividad de seguimiento a los planes de mejora, elaborados por el líder del proceso, para de esta manera, la Oficina de Control Interno, pueda dar fe de la eficacia de las acciones tomadas.

Gestión Documental

Dentro de las necesidades y expectativas, identificadas para el proceso Gestión Documental, tenemos:

1. Garantizar un adecuado transporte de los medios físicos que contengan información.

2. Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad.

3. Ofrecer una adecuada protección a los equipos de usuarios desatendidos.

4. Garantizar una adecuada implementación de la política de escritorio limpio y pantalla limpia.

5. Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.

6. Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.

7. Participación activa en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.

8. Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

9. Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.

10. Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de esta.

11. Garantizar que el recurso humano que gestiona el proceso, participe activamente en las charlas de sensibilización que convoca la Oficina de Seguridad de la Información, acorde al documento GSI-PL-01 Plan de Sensibilización y Entrenamiento, controlado por el Sistema de Aseguramiento de Calidad.

12. Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.

13. Se efectúe la respectiva actividad de seguimiento a los planes de mejora, elaborados por el líder del proceso, para de esta manera, la Oficina de Control Interno, pueda dar fe de la eficacia de las acciones tomadas.

PROCESOS DE EVALUACIÓN

Gestión de Control Interno

Dentro de las necesidades y expectativas, identificadas para el proceso Gestión de Control Interno, tenemos:

1. Realizar auditorías internas a los procesos constituidos por el Sistema de Aseguramiento de Calidad, donde se tengan en cuenta criterios normativos y de Gobierno, en temas de seguridad de la información.

2. Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad.

3. Ofrecer una adecuada protección a los equipos de usuarios desatendidos.

4. Garantizar una adecuada implementación de la política de escritorio limpio y pantalla limpia.

5. Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.

6. Realizar el respectivo seguimiento a los planes de tratamiento de riesgos de seguridad de la información, en todos los procesos internos, verificando la eficacia de las acciones tomadas.

7. Realizar el respectivo seguimiento a los planes de mejora, relacionados con seguridad de la información, en todos los procesos internos, verificando la eficacia de las acciones tomadas.

8. Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.

9. Participación activa en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.

10. Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

11. Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.

12. Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma.

13. Garantizar que el recurso humano que gestiona el proceso, participe activamente en las charlas de sensibilización que convoca la Oficina de Seguridad de la Información, acorde al documento GSI-PL-01 Plan de Sensibilización y Entrenamiento, controlado por el Sistema de Aseguramiento de Calidad.

14. Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.

15. Se efectúe la respectiva actividad de seguimiento a los planes de mejora, elaborados por el líder del proceso, para de esta manera, la Oficina de Control Interno, pueda dar fe de la eficacia de las acciones tomadas.

Sistema de Aseguramiento de Calidad de La Escuela Tecnológica

Dentro de las necesidades y expectativas, identificadas para el proceso Gestión de Calidad, tenemos:

1. Controlar la documentación del Modelo de Seguridad y Privacidad de la Información del Gobierno Digital y el Sistema de Gestión de Seguridad de la Información, que son de interés para el Sistema de Aseguramiento de Calidad.

2. Realizar auditorías internas a los procesos constituidos por el Sistema de Aseguramiento de Calidad, donde se tengan en cuenta criterios normativos y de Gobierno, en temas de seguridad de la información.

3. Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad.

4. Ofrecer una adecuada protección a los equipos de usuarios desatendidos.

5. Garantizar una adecuada implementación de la política de escritorio limpio y pantalla limpia.

6. Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.

7. Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.

8. Participación activa en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.

9. Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

10. Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.

11. Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma.

12. Garantizar que el recurso humano que gestiona el proceso, participe activamente en las charlas de sensibilización que convoca la Oficina de Seguridad de la Información, acorde al documento GSI-PL-01 Plan de Sensibilización y Entrenamiento, controlado por el Sistema de Aseguramiento de Calidad.

13. Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.

14. Se efectúe la respectiva actividad de seguimiento a los planes de mejora, elaborados por el líder del proceso, para de esta manera, la Oficina de Control Interno, pueda dar fe de la eficacia de las acciones tomadas.

Sistema de Gestión Ambiental; Gestión de Autoevaluación; Sistema de Gestión de Seguridad y Salud en el Trabajo

Dentro de las necesidades y expectativas, identificadas para el proceso Gestión Ambiental, tenemos:

1. Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad.

2. Ofrecer una adecuada protección a los equipos de usuarios desatendidos.

3. Garantizar una adecuada implementación de la política de escritorio limpio y pantalla limpia.

4. Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.

5. Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.

6. Participación activa en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.

7. Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

8. Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.

9. Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de esta.

10. Garantizar que el recurso humano que gestiona el proceso, participe activamente en las charlas de sensibilización que convoca la Oficina de Seguridad de la Información, acorde al documento GSI-PL-01 Plan de Sensibilización y Entrenamiento, controlado por el Sistema de Aseguramiento de Calidad.

11. Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.

12. Se efectúe la respectiva actividad de seguimiento a los planes de mejora, elaborados por el líder del proceso, para de esta manera, la Oficina de Control Interno, pueda dar fe de la eficacia de las acciones tomadas.

Sistema de Gestión de Seguridad de la Información

Dentro de las necesidades y expectativas, identificadas para el proceso Gestión de Seguridad de la Información, tenemos:

1. Verificar que la política general de seguridad de la información, los roles y responsabilidades, definidos por la Alta Dirección, se encuentren acorde a los requisitos de la norma NTC-ISO-IEC 27001:2013.

2. Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.

3. Participación activa en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.

4. Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

5. Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.

6. Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma.

7. Garantizar que los objetivos del Modelo de Seguridad y Privacidad de la Información de Gobierno Digital y el Sistema de Gestión de Seguridad de la Información, se encuentren acorde a la norma NTC-ISO-IEC 27001:2013.

8. Garantizar que toda documentación que sea de interés para el Sistema de Aseguramiento de Calidad, se encuentre debidamente ingresada, acorde al procedimiento de control de documentos definido y aprobado.

9. Garantizar que todos los procesos internos, definidos por el Sistema de Aseguramiento de Calidad, tengan incluidos en la respectiva caracterización del proceso, los criterios normativos que le aplican a cada uno ellos.

10. Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.

11. Se efectúe la respectiva actividad de seguimiento a los planes de mejora, elaborados por el líder del proceso, para de esta manera, la Oficina de Control Interno, pueda dar fe de la eficacia de las acciones tomadas.

12. Participación activa en la elaboración del Manual de Políticas de Seguridad y Privacidad de la Información, así como los procedimientos respectivos.

13. Elaborar el Plan de Sensibilización y Entrenamiento, en temas de seguridad de la información, garantizando su implementación al interior de la Escuela.

14. Articularse con las áreas respectivas para garantizar la elaboración y actualización de los inventarios de activos de información de la Escuela.

15. Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad.

16. Ofrecer una adecuada protección a los equipos de usuarios desatendidos.

17. Garantizar una adecuada implementación de la política de escritorio limpio y pantalla limpia.

18. Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.

19. Gestionar de manera adecuada, las vulnerabilidades técnicas identificadas, en la actividad de análisis de vulnerabilidades, con el área respectiva.

20. Cumplir con todo lo establecido por el habilitador transversal seguridad de la información, de Gobierno Digital.

21. Apoyar en la elaboración e implementación del plan de contingencia, recuperación y retorno a la normalidad.

22. Garantizar una adecuada gestión de las vulnerabilidades técnicas identificadas.

23. Garantizar la implementación de controles de seguridad contra código malicioso.

36. Establecer lineamientos acordes al contexto, propósito y directrices de la alta dirección, que permitan la disponibilidad de los servicios y procesos críticos del servicio ante un evento disruptivo.

Elaboró: **Esp. Sandra J. Guerrero G.**
Líder del Sistema de Gestión de Seguridad de la Información
Febrero 2024