TICSOCIAL S.A.S

# DECLARACIÓN DE APLICABILIDAD

| | |
|---|---|
| Versión: | 003 |
| Fecha de versión: | 10 de enero de 2019 |
| Creado por: | Diana Rodríguez |
| Aprobado por: | |
| Nivel de confidencialidad: | |

## El historial de cambios

| Fecha | Versión | Creado por | Descripción del cambio |
|---|---|---|---|
| 2018-12-17 | 0.1 | Diana Rodríguez | Esquema básico del documento. |
| 2019-01-07 | 0.2 | Diana Rodríguez | Modificación controles y riesgos residuales. |
| 2019-01-10 | 0.3 | Diana Rodríguez | Modificación controles y riesgos residuales. |

## Tabla de contenido

1. PROPÓSITO, ALCANCE Y USUARIOS. ..... 86
2. DOCUMENTOS DE REFERENCIA ..... 86
3. APLICABILIDAD DE LOS CONTROLES ..... 86
4. ACEPTACIÓN DE RIESGOS RESIDUALES. ..... 100
5. VALIDEZ Y GESTIÓN DOCUMENTAL. ..... 101

## 1. Propósito, alcance y usuarios.

El propósito de este documento es definir cuáles son los controles apropiados para ser implementados en TICSOCIAL S.A.S, los objetivos de dichos controles y como sería su implementación al momento de enfrentar las amenazas y riesgos.

Se abordarán todos los controles enumerados en el Anexo A de la norma ISO/IEC 27001:2013, estos controles se aplican a todo ámbito del SGSI.

Los usuarios involucrados en este seguimiento son Diana Rodríguez a cargo de la construcción del alcance y Robinson Salazar quien supervisara que lo indicado tenga la finalidad adecuada y sea posible.

## 2. Documentos de referencia

- Norma ISO / IEC 27001, cláusula 6.1.3 d)
- Política de seguridad de la información
- Evaluación de riesgos y metodología de tratamiento de riesgos.
- Evaluación de riesgos e informe de tratamiento de riesgos

## 3. Aplicabilidad de los controles

Son aplicables los siguientes controles del Anexo A de ISO 27001:

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.5 | Políticas de seguridad de la información | | | | | |
| A.5.1 | Directrices de gestión de la seguridad de la información | | | | | |
| A.5.1.1 | Políticas para la seguridad de la información | NO | | | | |
| A.5.1.2 | Revisión de las políticas para la seguridad de la información | NO | | | | |
| A.6 | Organización de la seguridad de la información | | | | | |
| A.6.1 | Organización interna | | | | | |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.6.1.1 | Roles y responsabilidades en seguridad de la información | SI | No existe una definición de roles y/o responsabilidades frente a la seguridad de la información (S.I.) | Creación de roles y responsabilidades. | Dichos roles y responsabilidades se irán nombrando y delegando en la construcción del plan de implementación | Inexistente |
| A.6.1.2 | Segregación de tareas | NO | | | | |
| A.6.1.3 | Contacto con las autoridades | NO | | | | |
| A.6.1.4 | Contactos con grupos de interés especial | NO | | | | |
| A.6.1.5 | Seguridad de la información en la gestión de proyectos | NO | | | | |
| A.6.2 | Los dispositivos móviles y el teletrabajo | | | | | |
| A.6.2.1 | Política de dispositivos móviles | NO | | | | |
| A.6.2.2 | Teletrabajo | NO | | | | |
| A.7 | Seguridad relativa a los recursos humanos | | | | | |
| A.7.1 | Seguridad de recursos humanos | | | | | |
| A.7.1.1 | Proyección | NO | | | | |
| A.7.1.2 | Términos y condiciones de empleo | SI | Dejar claridad de las responsabilidades, términos y condiciones de cada uno de los cargos. | Especificar que las funcionalidades de cada cargo | Contratación definida y clara | Definido |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.7.2 | Durante el empleo | | | | | |
| A.7.2.1 | Responsabilidades de gestión | SI | Cada empleado debe aplicar la S.I. siguiendo las políticas establecidas | Garantizar que toda la información tenga la seguridad adecuada para el tratamiento de la misma según sea el caso de cada empleado | Participación y compromiso de todos los empleados de la organización | Inexistente |
| A.7.2.2 | Sensibilización sobre la seguridad de la información, educación y capacitación | SI | No existe claridad sobre cómo y porque aplicar la S.I. pertinentes a las labores de cada empleado | Concientización sobre la S.I. | Socialización de políticas y formación para la aplicación en cada uno de los cargos | Inexistente |
| A.7.2.3 | Proceso disciplinario | NO | | | | |
| A.7.3 | Terminación y cambio de empleo | | | | | |
| A.7.3.1 | Terminación o cambio de responsabilidades laborales | SI | Cambios de personal en los diferentes cargos que hay en la organización | Continuidad y confidencialidad en el proceso de la S.I. de acuerdo al cargo y no al empleado | Incluir en los acuerdos contractuales dichas responsabilidad y explicación sobre las políticas y la forma de implementación | Inexistente |
| A.8 | Gestión de activos | | | | | |
| A.8.1 | Responsabilidad de los activos | | | | | |
| A.8.1.1 | Inventario de activos | NO | | | | |
| A.8.1.2 | Propiedad de los activos | NO | | | | |
| A.8.1.3 | Uso aceptable de los activos | NO | | | | |
| A.8.1.4 | Retorno de activos | NO | | | | |
| A.8.2 | Clasificación de la información | | | | | |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.8.2.1 | Clasificación de la información | NO | | | | |
| A.8.2.2 | Etiquetado de la información | NO | | | | |
| A.8.2.3 | Manejo de activos | NO | | | | |
| A.8.3 | Manejo de medios | | | | | |
| A.8.3.1 | Gestión de medios extraíbles | NO | | | | |
| A.8.3.2 | Eliminación de medios | NO | | | | |
| A.8.3.3 | Transferencia de medios físicos | NO | Si la salida de equipos institucionales es necesaria | Tener control sobre los equipos que salen y las medidas de seguridad adecuadas | Registro de los equipos que salen y entran de las instalaciones | Inexistente |
| A.9 | Control de acceso | | | | | |
| A.9.1 | Requisitos de negocio de control de acceso. | | | | | |
| A.9.1.1 | Política de control de acceso | SI | Limitar el acceso a la información manejada de acuerdo a la competencia de cada empleado y/o cargo | Documentar y revisar una política de control de acceso, de acuerdo a los requisitos del negocio y la S.I. | Establecer los accesos especialmente lógicos mediante privilegios. | Inexistente |
| A.9.1.2 | Acceso a redes y servicios de red | NO | | | | |
| A.9.2 | Gestión de acceso de usuarios | | | | | |
| A.9.2.1 | Registro de usuario y anulación de registro | NO | | | | |
| A.9.2.2 | Aprovisionamiento de acceso de usuario | SI | Es necesario definir los privilegios de cada uno de los usuarios | Que no existan ambigua des o irregularidades en cuanto a los accesos que protegen la información | Capacitación y concientización de los accesos a los que cada empleado tiene derecho | Inexistente |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.9.2.3 | Gestión de derechos de acceso privilegiados | SI | Aclaración de los derechos de acceso a la información | Restringir y controlar los accesos a los empleados a los sistemas y servicios | Identificar para cada empleado a que información tiene acceso y si es necesario la duración de dicho acceso | Inexistente |
| A.9.2.4 | Gestión de la información de autenticación secreta de los usuarios | NO | | | | |
| A.9.2.5 | Revisión de los derechos de acceso de los usuarios | SI | No existe claridad en cuanto a los derechos de acceso | Comprobar que cada uno de los usuarios tenga los accesos que le competen de acuerdo a sus responsabilidades | Identificar para cada empleado a que información tiene acceso y si es necesario la duración de dicho acceso | Inexistente |
| A.9.2.6 | Eliminación o ajuste de derechos de acceso | NO | | | | |
| A.9.3 | Responsabilidades del usuario | | | | | |
| A.9.3.1 | Uso de información de autenticación secreta | NO | | | | |
| A.9.4 | Sistema y control de acceso a aplicaciones. | | | | | |
| A.9.4.1 | Restricción de acceso a la información | SI | Posible acceso a la información de personas no autorizadas | Restringir quienes pueden tener acceso a determinada información | Generación de derechos de acceso a los empleados de la organización | Inexistente |
| A.9.4.2 | Procedimientos de inicio de sesión seguros | NO | | | | |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.9.4.3 | Sistema de gestión de contraseñas | SI | Posible acceso a la información de personas no autorizadas | Gestionar la calidad en las contraseñas de acceso | Otorgar contraseñas seguras a los usuarios autorizados | Inexistente |
| A.9.4.4 | Uso de programas de utilidad privilegiados | NO | | | | |
| A.9.4.5 | Control de acceso al código fuente del programa | SI | Garantizar la seguridad del código fuente | Mantener el código fuente alojado en los repositorios adquiridos | Cuenta para ingreso al repositorio para cada uno de los empleados que lo necesiten | Administrado |
| A.10 | Criptografía | | | | | |
| A.10.1 | Política sobre el uso de controles criptográficos | | | | | |
| A.10.2 | Gestión de claves | NO | | | | |
| A.11 | Seguridad física y ambiental. | | | | | |
| A.11.1 | Perímetro de seguridad física | | | | | |
| A.11.1.1 | Perímetro de seguridad física | NO | | | | |
| A.11.1.2 | Controles de entrada físicos | NO | | | | |
| A.11.1.3 | Asegurando oficinas, salas e instalaciones. | NO | | | | |
| A.11.1.4 | Protección contra amenazas externas y ambientales | NO | | | | |
| A.11.1.5 | Trabajando en áreas seguras | NO | | | | |
| A.11.1.6 | Áreas de entrega y carga. | NO | | | | |
| A.11.2 | Equipo | | | | | |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.11.2.1 | Emplazamiento y protección del equipo. | NO | | | | |
| A.11.2.2 | Utilidades de apoyo | NO | | | | |
| A.11.2.3 | Cableado de seguridad | NO | | | | |
| A.11.2.4 | Mantenimiento de equipos | SI | Realizar un mantenimiento continuo a los equipos para evitar posibles fallos y mantener | Programar mantenimientos continuos a los equipos | Mantener los equipos con actualizaciones al día y arreglo preventivo | Inexistente |
| A.11.2.5 | Eliminación de activos | NO | | | | |
| A.11.2.6 | Seguridad de equipos y activos fuera de las instalaciones | SI | Casos y ocasiones en las que se hace necesario que algunos empelados saquen equipos de las instalaciones | Llevar un control de que equipos salen de la oficina | Verificación de salida de equipos con autorización correspondiente | Inexistente |
| A.11.2.7 | Eliminación segura o reutilización de equipos | NO | | | | |
| A.11.2.8 | Equipo de usuario desatendido | NO | | | | |
| A.11.2.9 | Política de escritorio y pantalla clara | NO | | | | |
| A.12 | Seguridad de operación | | | | | |
| A.12.1 | Procedimientos operacionales y responsabilidades. | | | | | |
| A.12.1.1 | Procedimientos operativos documentados | NO | | | | |
| A.12.1.2 | Gestión del cambio | NO | | | | |
| A.12.1.3 | Gestión de capacidad | NO | | | | |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.12.1.4 | Separación de entornos de desarrollo, pruebas y operacionales | NO | | | | |
| A.12.2 | Protecciones contra malware | | | | | |
| A.12.2.1 | Controles contra malware | SI | Prevención de ingreso de código malicioso | Controlar y/o eliminar el riesgo potencial para los sistemas y equipos | Mantener equipos actualizados de fuentes confiables y software licenciado | Inexistente |
| A.12.3 | Backup | | | | | |
| A.12.3.1 | Copia de seguridad de la información | SI | Poder garantizar copias de seguridad para solventar cualquier inconveniente que se pueda presentar | Tener respaldo de toda la información que maneja la organización | Establecer tiempos en los cuales se realizan las copias de seguridad | Administrado |
| A.12.4 | Registro y seguimiento | | | | | |
| A.12.4.1 | Registro de eventos | NO | | | | |
| A.12.4.2 | Protección de la información de registro | NO | | | | |
| A.12.4.3 | Registros de administrador y operador | NO | | | | |
| A.12.4.4 | sincronización del reloj | NO | | | | |
| A.12.5 | Control de software operativo. | | | | | |
| A.12.5.1 | Instalación de software en sistemas operativos | NO | | | | |
| A.12.6 | Gestión de vulnerabilidad técnica. | | | | | |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.12.6.1 | Gestión de vulnerabilidades técnicas | Si | Falta de monitoreo de los recursos que posee la organización | Tener control sobre las vulnerabilidades y poder mitigarlas para evitar caídas de los sistemas | Vigilancia permanente sobre los recursos | Inicial |
| A.12.6.2 | Restricciones en la instalación del software | SI | No hay restricción en cuanto a instalación de ningún tipo de software en los equipos | Controlar las instalaciones de cualquier software mediante privilegios | Autorización a ciertos empelados para realizar instalaciones que sean necesarias para el correcto funcionamiento de las labores | Inexistente |
| A.12.7 | Consideración de auditoría de sistemas de información. | NO | | | | |
| A.12.7.1 | Controles de auditoría de los sistemas de información. | NO | | | | |
| A.13 | Seguridad de las comunicaciones | | | | | |
| A.13.1 | Gestión de seguridad de red | | | | | |
| A.13.1.1 | Controles de red | SI | No se encuentra en este momento políticas para el control de la red de la organización | Crear políticas para la administración, acceso y monitorizaciones de la res | Implementar las políticas una vez creadas de manera paulatina dentro de la organización | Inicial |
| A.13.1.2 | Seguridad de los servicios de red | SI | Revisión de los niveles de seguridad par ingreso a la red | Aumentar y/o ajustar la seguridad en los servicios de la red tanto para empleados como para visitantes | | Inicial |
| A.13.1.3 | Segregación en redes. | NO | | | | |
| A.13.2 | Transferencia de información | | | | | |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.13.2.1 | Políticas y procedimientos de transferencia de información | SI | No existen una reglamentación clara para la transferencia de la información | Contar con políticas y procedimientos para la protección de la transferencia de la información | Creación de políticas para los procedimientos en los cuales se realiza transferencia de información vital para la organización | Inexistente |
| A.13.2.2 | Acuerdos de transferencia de información | NO | | | | |
| A.13.2.3 | Mensajería electrónica | SI | Poder proteger la información que se envía por mensajería electrónica | Proteger los mensajes enviados con los empleados y los clientes | Controles criptográficos que garanticen la seguridad en la transmisión de la información | Inexistente |
| A.13.2.4 | Confidencialidad o acuerdos de no divulgación | NO | | | | |
| A.14 | Adquisición, desarrollo y mantenimiento de sistemas. | | | | | |
| A.14.1 | Requisitos de seguridad del sistema de información. | | | | | |
| A.14.1.1 | Análisis y especificación de los requisitos de seguridad de la información | SI | No hay una definición claro de requisitos relacionados con la seguridad de la información | Identificar los requisitos para la S.I. | Creación de las políticas de la S.I. de acuerdo a los requerimientos de la organización y/o clientes (proyectos) | Inexistente |
| A.14.1.2 | Asegurando servicios de aplicaciones en redes públicas | NO | | | | |
| A.14.1.3 | Protección de transacciones de servicios de aplicaciones | NO | | | | |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.14.2 | Seguridad en procesos de desarrollo y soporte. | | | | | |
| A.14.2.1 | Política de desarrollo seguro | SI | Inexistencia de política de desarrollo seguro | Poder proteger los desarrollos y cambios sobre el código fuente | Crear e implementar posibles controles para el código fuente | Inicial |
| A.14.2.2 | Procedimientos de control de cambio de sistema | NO | | | | |
| A.14.2.3 | Revisión técnica de aplicaciones después de cambios en la plataforma operativa | NO | | | | |
| A.14.2.4 | Restricciones a los cambios en los paquetes de software | NO | | | | |
| A.14.2.5 | Principios de ingeniería de sistemas seguros | NO | | | | |
| A.14.2.6 | Entorno de desarrollo seguro | SI | Tener un control sobre los entornos de desarrollo de cada uno de los desarrolladores | Establecer políticas y normas para los entornos de desarrollo | Evaluar cada entorno de desarrollo y verificar que políticas se podrían implementar | Inexistente |
| A.14.2.7 | Desarrollo externalizado | NO | | | | |
| A.14.2.8 | Pruebas de seguridad del sistema | SI | Aplicar procedimientos para las pruebas y verificación de funcionamientos | Revisar existencia de acuerdos de licencias, propiedad de código y /o derechos de propiedad | Complementar los procedimientos para las pruebas de seguridad del sistema | Inicial |
| A.14.2.9 | Pruebas de aceptación del sistema | NO | | | | |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.14.3 | Datos de prueba | NO | | | | |
| A.14.3.1 | Protección de datos de prueba | NO | | | | |
| A.15 | Relaciones con proveedores | | | | | |
| A.15.1 | Seguridad de la información en las relaciones con proveedores. | | | | | |
| A.15.1.1 | Política de seguridad de la información para relaciones con proveedores | NO | | | | |
| A.15.1.2 | Abordar la seguridad dentro de los acuerdos con proveedores | SI | Dar a conocer a los proveedores los acuerdos de seguridad que se manejan en la organización | Socializar las políticas de seguridad | Definir de manera adecuada las políticas de seguridad | Inicial |
| A.15.1.3 | Cadena de suministro de tecnologías de la información y la comunicación | NO | | | | |
| A.15.2 | Proveedor de gestión de entrega de servicios. | | | | | |
| A.15.2.1 | Seguimiento y revisión de los servicios del proveedor | NO | | | | |
| A.15.2.2 | Gestión de cambios en los servicios del proveedor | NO | | | | |
| A.16 | Gestión de incidentes de seguridad de la información. | | | | | |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.16.1 | Gestión de incidentes de seguridad de la información y mejoras. | | | | | |
| A.16.1.1 | Responsabilidades y procedimientos | NO | | | | |
| A.16.1.2 | Informe de eventos de seguridad de la información | NO | | | | |
| A.16.1.3 | Informe de debilidades de seguridad de la información | NO | | | | |
| A.16.1.4 | Evaluación y decisión sobre eventos de seguridad de la información | NO | | | | |
| A.16.1.5 | Respuesta a incidentes de seguridad de la información | NO | | | | |
| A.16.1.6 | Aprendiendo de incidentes de seguridad de la información | NO | | | | |
| A.16.1.7 | Recolección de evidencia | NO | | | | |
| A.17 | Aspectos de seguridad de la información en la gestión de la continuidad del negocio. | | | | | |
| A.17.1 | Continuidad de la seguridad de la información. | | | | | |
| A.17.1.1 | Planificación de la continuidad de la seguridad de la información | NO | | | | |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.17.1.2 | Implementando la continuidad de la seguridad de la información | NO | | | | |
| A.17.1.3 | Verificar, revisar y evaluar la continuidad de la seguridad de la información | NO | | | | |
| A.17.2 | Redundancias | | | | | |
| A.17.2.1 | Disponibilidad de instalaciones de procesamiento de información | NO | | | | |
| A.18 | Conformidad | | | | | |
| A.18.1 | Cumplimiento de los requisitos legales y contractuales. | | | | | |
| A.18.1.1 | Identificación de la legislación aplicable y requisitos contractuales | NO | | | | |
| A.18.1.2 | Derechos de propiedad intelectual | NO | | | | |
| A.18.1.3 | Protección de registros | NO | | | | |
| A.18.1.4 | Privacidad y protección de la información de identificación personal | NO | | | | |
| A.18.1.5 | Regulación de los controles criptográficos | NO | | | | |
| A.18.2 | Revisiones de seguridad de la información | | | | | |

| ID | Controles según ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación de aplicabilidad del control | Objetivos del control | Método de implementación | Estado |
|---|---|---|---|---|---|---|
| | | | | | | |
| A.18.2.1 | Revisión independiente de la seguridad de la información | NO | | | | |
| A.18.2.2 | Cumplimiento de políticas y estándares de seguridad | NO | | | | |
| A.18.2.3 | Revisión de cumplimiento técnico | NO | | | | |

## 4. Aceptación de riesgos residuales.

Dado que no todos los riesgos podrían reducirse en el proceso de gestión de riesgos, todos los riesgos residuales se aceptan en este documento:

1. Todos los riesgos con el valor 0, 1 o 2.
2. Riesgos que no podrían reducirse a los niveles antes mencionados después de la aplicación del control, de acuerdo con la siguiente tabla:

| No. | Nombre del activo | Propietario del activo | Amenaza | Vulnerabilidad | Nuevo Impacto | Nueva Probabilidad | Riesgo Residual |
|---|---|---|---|---|---|---|---|
| R002 | WWW | Líder área de desarrollo | Errores de mantenimiento/ actualización de programas | Falta de capacitación de trabajo | 2 | 1 | 3 |
| R003 | WWW | Líder área de desarrollo | Caída del sistema por agotamiento de recursos | Falta de planes de contingencia | 2 | 1 | 3 |
| R005 | Intercambio electrónico de datos | Líder área de desarrollo | Suplantación de la identidad del usuario | Control de acceso inadecuado | 2 | 1 | 3 |
| R006 | Archivos de configuración | Líder área de desarrollo | Suplantación de la identidad del usuario | Falta de conciencia de seguridad | 2 | 1 | 3 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| R007 | Archivos de configuración | Líder área de desarrollo | Acceso no autorizado | Administración deficiente de contraseña | 2 | 1 | 3 |
| R010 | Datos prueba | Líder área de desarrollo | Difusión de software dañino | Testeo inadecuado/ insuficiente | 2 | 1 | 3 |
| R012 | Backups | Líder área de desarrollo | Errores de mantenimiento/ actualización de programas | Instalación/ desinstalación no controlada | 2 | 1 | 3 |
| R014 | Código fuente | Líder área de desarrollo | Difusión de software dañino | Monitoreo insuficiente de medidas de seguridad | 2 | 1 | 3 |

## 5. Validez y gestión documental.

Este documento será revisado y podrá ser modificado por Diana Rodríguez, Robinson Salazar y Luis Fernando Morales a medida que el desarrollo del plan de implementación se vaya efectuando y si se cree conveniente para lograr la efectividad del documento.

Ingeniero de Sistemas - Líder de Desarrollo y Tecnología
Robinson Salazar Grimaldos

_____




## PLAN TRATAMIENTO DE RIESGO

Para lograr los objetivos del SGSI, se deben realizar las siguientes actividades:

| Descripción de actividades | Descripción del control | Acción de tratamiento | Persona Responsable | Mantenimiento requerido / Comentarios | Estado (no iniciado/en progreso/completado) |
|---|---|---|---|---|---|
| R001 | *A.13.2.1 Políticas y procedimientos de transferencia de información:* Asegurar la transferencia de la información. | Crear las políticas y procedimientos acordes a las necesidades de TICSOCIAL para la transferencia de la información | Diana Rodríguez | Comenzar la implementación por áreas de la organización para poder evaluar la efectividad del control sobre este riesgo | No iniciado |
| R002 | *A.14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas:* Realizar las pruebas necesarias de los desarrollos para comprobar la funcionalidad. | Realizar dichas pruebas durante los desarrollos y que al momento de efectuar | Diana Rodríguez | No realizar los cambios en los ambientes productivos si las pruebas no salen exitosas | En progreso |
| R003 | *A.12.6.1 Gestión de las vulnerabilidades técnicas:* Realizar monitoreos constantes a los recursos del sistema en los ambientes | Designar un empleado a cargo de la monitorización para mitigar o evitar las posibles fallas en el sistema | Diana Rodríguez | Identificar las vulnerabilidades por las cuales se podría dar el agotamiento de los recursos | No iniciado |

| | | | | | |
|---|---|---|---|---|---|
| R004 | *A.13.2.1 Políticas y procedimientos de transferencia de información:* Dar claridad sobre la manera correcta de realizar la transferencia de la información | Crear las políticas y procedimientos para la transferencia de la información tanto al interior de la organización como hacia partes externas, definiendo la sensibilidad que pueda tener la información | Diana Rodríguez | | No iniciado |
| R005 | *A.13.2.3 Mensajería electrónica:* Evitar el acceso no autorizado a los servicios de transferencia de información | Incluir una política para garantizar en envió de información que tenga en cuenta los controles de acceso para este caso específico a mensajería electrónica | Diana Rodríguez | Esta política se deberá aplicar a todas las áreas de la organización | No iniciado |
| R006 | *A.14.2.1 Política de desarrollo seguro de software:* Garantizar la seguridad en los entornos de desarrollo | Crear y capacitar a los desarrolladores sobre las practicas seguras de codificación y desarrollo, enfocadas en la seguridad en las etapas del ciclo vital del desarrollo | Diana Rodríguez | Enfocar dichas políticas y practicas a lenguajes de desarrollo, repositorios, control de versiones, etc. | No iniciado |
| R007 | *A.9.1.1 Política de control de acceso:* Establecer las políticas de control de acceso de naturaleza digital | Definir las políticas necesarias para garantizar que el acceso a los archivos de configuración sea de los empleados autorizados a su uso, restricción de usuarios | Diana Rodríguez | Tener definición clara de los usuarios que tiene privilegio de acceso a dichos archivos | No iniciado |
| R008 | *A.7.2.2 Concientización sobre la seguridad de la información, educación y capacitación:* Educación y capacitación adecuada para los empelados | Los empleados (administradores) deberán recibir capacitaciones y /o actualizaciones de las políticas, normas y procedimientos sobre la seguridad de la información de acuerdo a las funciones que desempeñe cada uno | Diana Rodríguez | Realizar revisiones periódicas de las políticas para que los niveles de seguridad se vayan actualizando | No iniciado |

| | | | | | |
|---|---|---|---|---|---|
| R009 | *A.9.1.1 Política de control de acceso:* Definición de las políticas de acceso | Definición de las políticas de control de acceso para todos los niveles de la organización enfocadas a las responsabilidades de cada empleado | Diana Rodríguez | | No iniciado |
| R010 | *A.14.2.6 Seguridad en entornos de desarrollo:* Protección adecuada de todos los entornos de desarrollo | Manipular de manera adecuada los datos de prueba para evitar y/o mitigar el desarrollo(código) malicioso, el cuál pueda afectar las demás partes del entorno de desarrollo | Diana Rodríguez | Determinar los requisitos, regulaciones y/o políticas para la protección de los entornos de desarrollo | No iniciado |
| R011 | *A.12.3.1 Copia de seguridad de la información:* Asegurar respaldo de la información | Establecer las políticas y periodos para realizar las copias de seguridad de tal manera que se salvaguarde información que garantice la disponibilidad máxima de la misma | Diana Rodríguez | | En progreso |
| R012 | *A.12.6.2 Restricciones en la instalación del software:* Control sobre mantenimientos de programas | Definición de reglas para la instalación y actualización de software necesario para manejar un control y evitar posibles programas de malware | Diana Rodríguez | Es necesario controlar la instalación/actualización para evitar las posibles amenazas y vulnerabilidades que podría traer el software | No iniciado |
| R013 | *A.11.2.4 Mantenimiento de equipos:* Garantizar disponibilidad e integridad de los equipos | Establecer mantenimiento (actualización) rutinario y preventivo de los equipos de acuerdo a su naturaleza, entorno y propósito | Diana Rodríguez | | No iniciado |
| R014 | *A.9.4.5 Control de acceso al código fuente de los programas:* Acceso a los empleados autorizados | Proteger el código fuente de vulnerabilidades | Diana Rodríguez | Definir los accesos correspondientes a los repositorios donde se aloja el código fuente, y controlar dichos | En progreso |

| | | | | | |
|---|---|---|---|---|---|
| | | | | accesos | |
| R015 | *A.9.4.5 Control de acceso al código fuente de los programas:* Mantenimiento de los programas | Establecer periodos de mantenimiento de los programas, de tal manera que se pueda realizar una programación para que no se vea afectado el software | Diana Rodríguez | | En progreso |
| R016 | *A.7.2.1 Responsabilidades de gestión:* Tener claridad sobre las funciones y responsabilidades de acuerdo al cargo del empleado | Describir de manera clara a cada empleado sus funciones y responsabilidades, concientizar sobre la seguridad de la información que maneja y las repercusiones en el incumplimiento de sus responsabilidades | Diana Rodríguez | Establecer los controles que cada empelado debe seguir para cumplir a cabalidad con sus tareas diarias y/o proyectos asignados | En progreso |
| R017 | *A.9.2.3 Gestión de derechos de acceso privilegiados:* Claridad sobre los accesos | Instituir la administración de los niveles de accesos y control de los mismos sobre los activos y la información | Diana Rodríguez | Definir las reglas de los accesos privilegiados y los usuarios (empleados) que podrían acceder a dichos privilegios | No iniciado |
| R018 | *A.7.3.1 Terminación o cambio de responsabilidades laborales:* Delegación de accesos y responsabilidades | Definición de políticas para la terminación o cambio de responsabilidades laborales, ¿quién queda a cargo?, ¿Qué se hará con las tareas pendientes?, etc. | Diana Rodríguez | Delegar tareas que se crean importantes a empelados con la capacidad de asumirlas mientras llega un nuevo empleado | No iniciado |
| R019 | *A.9.4.1 Restricción de acceso a la información:* Establecer los derechos de acceso | Definir las reglas mediante las cuales se definirá el acceso a la información ya sea para empleados o usuarios, mediante roles, niveles de acceso, etc. | Diana Rodríguez | | No *iniciado* |
| R020 | *A.11.2.4 Mantenimiento de* | Realizar revisiones continuas a los | Diana Rodríguez | | No iniciado |

| | | | | | |
|---|---|---|---|---|---|
| | *equipos:* Garantizar la disponibilidad e integridad de los equipos | equipos para evitar posibles daños y averías y que a su vez esto interfiera en las labores de la organización | | | |
| R021 | *A.9.4.3 Sistema de gestión de contraseñas:* Concientizar para que las contraseñas sean seguras | Garantizar que las contraseñas cumplan con los niveles necesarios, buscar mecanismos para la correcta implementación de contraseñas | Diana Rodríguez | Capacitar a los empleados que necesiten accesos privilegiados sobre los mecanismos que se usaran | No iniciado |
| R022 | *A.6.1.1 Funciones y responsabilidades de seguridad de la información:* Tener claridad sobre las funciones y responsabilidades | Definir y asignar a cada empleado las responsabilidades que conlleva su cargo y como ejercer la seguridad de las mismas de tal manera que la información que maneje tenga la seguridad adecuada | Diana Rodríguez | | No iniciado |
| R023 | *A.12.3.1 Copia de seguridad de la información:* Tener respaldo de acuerdo a las necesidades | Diseñar y definir como serán los respaldos, periodicidad, disponibilidad, etc. de tal manera que se tenga copias de seguridad lo más recientes | Diana Rodríguez | Tener en cuenta las reglas establecidas con anterioridad en cuanto a la periodicidad de las copias de seguridad | En progreso |
| R024 | *A.12.2.1 Controles contra malware* | Establecer los controles para la detección, prevención y recuperación en caso de que la informática personal este protegido de software dañino | Diana Rodríguez | | No iniciado |
| R025 | *A.8.3.3 Transferencia de medios físicos:* Protección de los medios físicos usados en la transferencia de información | Realizar la protección adecuada a los medos físicos para que tenga una defensa en caso de acceso no autorizado, uso indebido o transporte inadecuado que | Diana Rodríguez | De ser posible se establece no llevar estos medios físicos fuera de las instalaciones de la organización | No iniciado |

| | | | | | |
|---|---|---|---|---|---|
| | | pueda afectar la información que allí está depositada | | | |
| R026 | *A.6.1.1 Funciones y responsabilidades de seguridad de la información:* Tener claridad sobre las funciones y responsabilidades | Definir quienes puede tener acceso a los dispositivos móviles y las funciones a desempeña con dichos dispositivos | Diana Rodríguez | En el momento Ticsocial solo cuenta con un dispositivo móvil institucional que es no tiene un uso periódico | No iniciado |
| R027 | *A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones:* | Aplicar controles a los dispositivos en caso de que estos se encuentren fuera de la organización y los peligros que implica, de igual forma va vinculados definidos dentro de la organización | Diana Rodríguez | El dispositivo móvil no sale de las instalaciones de la organización | No iniciado |
| R028 | *A.11.2.4 Mantenimiento de equipos:* Establecer periodos de mantenimiento | Realizar mantenimientos de manera regular para que los equipos estén disponibles y en buen estado para garantizar la disponibilidad | Diana Rodríguez | | No iniciado |
| R029 | *A.13.1.2 Seguridad de los servicios de red:* Establecer la seguridad en los equipos de red | Tomar todas las medidas de seguridad que los servicios de la red funciones de la manera adecuada | Diana Rodríguez | Realizar mantenimientos de tal manera que no se afecte la red. | No iniciado |
| R030 | *A.13.1.2 Seguridad de los servicios de red:* Establecer la seguridad en los equipos de red | Establecer los accesos a la red de acuerdo a las funciones de cada empleado si así se requiere | Diana Rodríguez | Accesos de acuerdo a los privilegios | No iniciado |
| R031 | *A.13.1.1 Controles de red: Proteger la red local para evitar incidentes* | Verificar y de ser necesario rediseñar la red local, de tal manera que se pueda proteger en mayor proporción la información manejada dentro de | Diana Rodríguez | Verificar que operaciones son indispensables y segregar la red de manera que no afecta las labores normales de la organización | No iniciado |

| | | | | | |
|---|---|---|---|---|---|
| | | la red local | | | |
| R032 | *A.7.3.1 Terminación o cambio de responsabilidades laborales:* Continuidad de la seguridad al cambio o falta de un empleado | Asegurar que la seguridad continúe al efectuarse algún cambio en el personal de la organización | Diana Rodríguez | Estas especificaciones deben ir en una sección de términos y condiciones en los contratos de los empelados | En progreso |
| R033 | *A.9.2.5 Revisión de los derechos de acceso del usuario:* Control de los accesos a la BD | Definir y aclarar los derechos de acceso a los usuarios que posean un rol determinado | Diana Rodríguez | Realizar constantes revisiones de los derechos de accesos de acuerdo a la naturaleza de cada derecho | No iniciado |
| R034 | *A.9.4.1 Restricción de acceso a la información:* Definición de los accesos de acuerdo a las funciones | Realizar lista de consideraciones de las políticas de acceso a la información para aclarar las funciones de cada empelado sobre los accesos privilegiados que posea | Diana Rodríguez | | No iniciado |
| R035 | *A.7.2.2 Concientización sobre la seguridad de la información, educación y capacitación:* Concientizar a los empleados sobre sus labores y la seguridad de las mismas | Educar y capacitar a los empleados para que implementen las políticas y controles de la seguridad, conocimiento de las legislaciones y concientización del ciclo de vida del empleo | Diana Rodríguez | | No iniciado |
| R036 | *A.7.2.2 Concientización sobre la seguridad de la información, educación y capacitación:* Uso de programas con acceso a la información | Capacitar en el uso de los navegadores web y la protección a la seguridad que se debe implementar para evitar accesos no deseas o filtración de información pro transferencia | Diana Rodríguez | | No iniciado |
| R037 | *A.7.2.1 Responsabilidades de gestión:* Definición de responsabilidades | Concientizar a toda la organización en especial al área de desarrollo sobre la seguridad | Diana Rodríguez | Exponer todos los controles que sean relevantes para el área de desarrollo y a medida que los | No iniciado |

| | | | | | |
|---|---|---|---|---|---|
| | | de la información | | riesgos y los controles tengan modificaciones capacitar para que sea de conocimiento dentro de la organización | |
| R038 | *A.9.2.2 Aprovisionamiento de acceso de usuario:* Claridad sobre los accesos | Definir los límites de los accesos a lo que cada empelado tiene derecho según sus funciones y los límites de estos | Diana Rodríguez | Crear una jerarquía de accesos para determinar de acuerdo al cargo una asignación correspondiente a las funciones de cada empelado | No iniciado |
| R039 | *A.15.1.2 Abordar la seguridad dentro de los acuerdos con proveedores:* Relación con los proveedores y el SGSI | Trabajar en una relación de seguridad entre los proveedores y la organización para que exista relación entre los controles de ambas partes y tener la evidencia necesaria | Diana Rodríguez | Realizar actualizaciones continuas de los controles y posibles nuevos riesgos a tratar para que de ser puedan tomar las medidas preventivas que los nuevos riesgos necesites | No iniciado |

Ingeniero de Sistemas - Líder de Desarrollo y Tecnología

Robinson Salazar Grimaldos

_____