Municipalidad Distrital de
SAN BARTOLO

SGSI
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SGSI-DOC-03

Declaración de Aplicabilidad

APROBACIÓN A CARGO DE LOS MIEMBROS DEL COMITÉ DE GOBIERNO Y TRANSFORMACIÓN DIGITAL

ROL	CARGO EN EL COMITÉ	NOMBRES Y APELLIDOS
Elaborador	Secretario Técnico del Comité	**Jorge Alberto Tello Cuya** Subgerente de Tecnologías de la Información Oficial de Seguridad y Confianza Digital
Revisores	Miembros del Comité de Gobierno y Transformación Digital	**August Enrique Frederick Arthur Carbajal Schumacher** Titular de la entidad
		Daniel Ernesto Farfán Soto Secretario General (e)
		Daniel Ernesto Farfán Soto Gerente de Asesoría Jurídica
		Rocío Inés Ardiles Aguirre Gerente de Presupuesto y Planeamiento (e)
		Edilberto Genaro Mendoza Orellana Subgerente de Gestión del Talento Humano (e)
Aprobador	Líder de Gobierno y Transformación Digital	**Maritza Olinda Caycho Tumay** Gerente Municipal (e)

El Comité de Gobierno y Transformación Digital aprueba el presente documento:

MUNICIPALIDAD DE SAN BARTOLO
AUGUST CARBAJAL SCHUMACHER
ALCALDE

Alcalde de la Municipalidad de San Bartolo
Titular de la entidad

MUNICIPALIDAD DISTRITAL DE SAN BARTOLO
CPC. MARITZA LINDA CACHO TUMAY
(JEFE DEL MUNICIPAL (e))

Gerente Municipal
Líder de Gobierno y Transformación Digital

MUNICIPALIDAD DE SAN BARTOLO
Subgerencia de Tecnologías de la Información
JORGE ALBERTO TELLO CUYA
SUBGERENTE

Subgerente de Tecnologías de la Información
Oficial de Seguridad y Confianza Digital
Secretario Técnico del Comité

MUNICIPALIDAD DISTRITAL DE SAN BARTOLO
SECRETARÍA GENERAL
Abog. Daniel Ernesto Farfán Soto
Secretario General (e)

Secretario General (e)
Atención al ciudadano

MUNICIPALIDAD DE SAN BARTOLO
DANIEL FARFAN SOTO
GERENTE DE ASESORÍA JURÍDICA

Gerente de Asesoría Jurídica
Área Legal

MUNICIPALIDAD DISTRITAL DE SAN BARTOLO
GERENCIA DE PRESUPUESTO, PLANEAMIENTO Y RACIONALIZACIÓN
Econ. Rocío Inés Ardiles Aguirre
Gerente (e)

Gerente de Presupuesto, Planeamiento y Racionalización (e)
Área de Presupuesto

MUNICIPALIDAD DISTRITAL DE SAN BARTOLO
SUBGERENCIA DE GESTIÓN DEL TALENTO HUMANO
Lic. Edilberto Genaro Mendoza Orellana
Subgerente (e)

Subgerente de Gestión del Talento Humano (e)
Área de Recursos Humanos

CONTROL DE CAMBIOS

Autor	Descripción del cambio	Fecha de Aprobación	Versión
Jorge Alberto Tello Cuya	Elaboración inicial del documento	25/11/2024	1.0

Contenido

1. OBJETIVO

Definir los controles de seguridad de la información del Anexo A de la NTP ISO/IEC 27001:2022 aplicables al alcance del SGSI de la MDSB, y la justificación de las exclusiones en caso existan.

2. BASE LEGAL Y NORMATIVA

- Ley N° 29733, Ley de Protección de Datos Personales y modificatoria, artículo 40, aprobada el 03 de julio del 2011.
- Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales y modificatoria, publicada el 22 de marzo del 2013.
- Resolución Ministerial Nº 119-2018-PCM, que dispone la creación de un Comité de Gobierno y Transformación Digital en cada entidad de la Administración Pública. Publicada el 10 de mayo del 2018.
- Resolución Ministerial Nº 087-2019-PCM, que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno y Transformación Digital. Publicada el 20 de noviembre del 2019.
- Decreto Supremo Nº 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno y Transformación Digital. Publicada el 19 de febrero del 2019.
- Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento. Publicada el 09 de enero del 2020.
- Decreto Supremo Nº 157-2021-PCM, aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital. Publicado el 25 de setiembre del 2021.
- Resolución Directoral N° 022-2022- INACAL/DN, que aprueba la Norma Técnica Peruana NTP ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ª Edición. Publicada el 12 de enero del 2023.
- Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas. Publicada el 08 de setiembre del 2023.
- Resolución de Alcaldía Nº 151-2023-MDSB, que designa al líder de Gobierno y Transformación Digital, designa al Oficial de Seguridad y Confianza Digital y constituye el Comité de Gobierno y Transformación Digital de la Municipalidad Distrital de San Bartolo. Publicada el 01 de junio del 2023.

3. TÉRMINOS Y DEFINICIONES

- **Activo de Información:** Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la Municipalidad.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema o activo de información de la Municipalidad.

- **Confidencialidad:** Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas, las entidades o procesos.
- **Disponibilidad:** Propiedad de ser accesible y utilizable por petición de una entidad autorizada.
- **Integridad:** Propiedad de exactitud e integridad.
- **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.
- **Sistema de información:** Aplicaciones, servicios, activos de tecnología de información, u otros componentes de manejo de la información.
- **Sistema de Gestión de Seguridad de la Información:** Forma parte del Sistema Integrado de Gestión, se basa en un enfoque hacia los riesgos de la entidad, cuyo fin es establecer, implementar, mantener y mejorar la seguridad de la información, basándose en los 3 pilares (Integridad, Disponibilidad y Confidencialidad).
- **Abreviaturas:**
  - **MDSB:** Municipalidad Distrital de San Bartolo.
  - **SAL:** Subgerencia de Abastecimiento y Logística.
  - **SGRD:** Subgerencia de Gestión del Riesgo de Desastres.
  - **SGSI:** Sistema de Gestión de Seguridad de la Información.
  - **SGTH:** Subgerencia de Gestión del Talento Humano.
  - **STI:** Subgerencia de Tecnologías de la Información.
  - **GAF:** Gerencia de Administración y Finanzas.
  - **GM:** Gerencia Municipal.

4. IMPLEMENTACIÓN DE LOS CONTROLES DE LA DECLARACIÓN DE APLICABILIDAD

Debido a la falta de presupuesto para el resto de meses del 2024, se implementarán sólo los controles que no requieren de gasto (Como elaboración de políticas y documentación). El resto de controles serán incluidos en el Plan de Gobierno Digital 2025-2027, mediante el cual se asegurará el presupuesto correspondiente para la contratación de servicios y adquisición de bienes necesarios para la implementación de dichos controles.

5. ANÁLISIS

Clausula	Control	Tipo de Control	Aplicabilidad del Control	Justificación de la inclusión o exclusión	Documentación	Responsable
5	CONTROLES ORGANIZACIONALES					
5.1	Políticas para Seguridad de la información	*#Preventivo*	Sí	Para contar con una política de seguridad de la información y las políticas del tema definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados o cuando ocurran cambios significativos.	Política de Seguridad de la Información	STI y GM
5.2	Roles y responsabilidades en seguridad de la información	*#Preventivo*	Sí	Para definir los roles y responsabilidades de seguridad de la información los cuales deben asignarse de acuerdo con las necesidades de la organización.	Manual de roles y responsabilidad para la seguridad de la información	STI y GM
5.3	Segregación de funciones	*#Preventivo*	Sí	Para segregar los deberes conflictivos y las áreas conflictivas de responsabilidad, respecto a seguridad de la información.	Manual de roles y responsabilidad para la seguridad de la información	STI y GM
5.4	Responsabilidad de la gerencia	*#Preventivo*	Sí	Para que la Gerencia pueda exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.	Manual de roles y responsabilidad para la seguridad de la información	GM
5.5	Contacto con autoridades	*#Preventivo #Correctivo*	Sí	Para que la organización establezca y mantenga contacto con las autoridades pertinentes.	Conocimiento de la Organización y las partes interesadas	STI y GM
5.6	Contacto con grupos especiales de interés	*#Preventivo #Correctivo*	Sí	Para que la organización establezca y mantenga contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.	Conocimiento de la Organización y las partes interesadas	STI y GM
5.7	Inteligencia de amenazas	*#Preventivo #Detectivo #Correctivo*	Sí	Para recopilar y analizar la información relacionada con las amenazas a la seguridad de la información.	Reporte de amenazas de los aplicativos de seguridad	STI

Clausula	Control	Tipo de Control	Aplicabilidad del Control	Justificación de la inclusión o exclusión	Documentación	Responsable
5.8	Seguridad de la información en la gestión de proyectos	*#Preventivo*	Sí	Para integrar la seguridad de la información en la gestión de proyectos	Manual del SGSI	STI
5.9	Inventario de información y otros activos asociados	*#Preventivo*	Sí	Para desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.	Inventario de activos de información	STI
5.10	Uso de la información y otros activos asociados	*#Preventivo*	Sí	Para identificar, documentar e implementar reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.	Política de uso aceptable de activos	STI
5.11	Retorno de activos	*#Preventivo*	Sí	Para gestionar la devolución de los activos que el personal tenga en su poder al cambiar o terminar su empleo, contrato o acuerdo.	Política de uso aceptable de activos	STI
5.12	Clasificación de información	*#Preventivo*	Sí	Para clasificar la información de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.	Política de clasificación de la información. Procedimiento para la clasificación, etiquetado y transferencia de información	STI
5.13	Etiquetado de información	*#Preventivo*	Sí	Para desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización.	Procedimiento para la clasificación, etiquetado y transferencia de información	STI
5.14	Transferencia de información	*#Preventivo*	Sí	Para implementar reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización, además entra la organización y otras partes.	Procedimiento para la clasificación, etiquetado y transferencia de información	STI

Clausula	Control	Tipo de Control	Aplicabilidad del Control	Justificación de la inclusión o exclusión	Documentación	Responsable
5.15	Control de accesos	*#Preventivo*	Sí	Para implementar reglas para controlar el acceso físico y lógico a la información y otros activos asociados, las cuales deben establecerse e implementarse en función de los requisitos comerciales y de seguridad de la información.	Política de creación, control y revocación de accesos. Política de seguridad de información - Acceso físico	STI
5.16	Gestión de identidades	*#Preventivo*	Sí	Para implementar el procedimiento de identificación única de personas y sistemas que acceden a la información de la organización y otros activos asociados y permitir la asignación adecuada de derechos de acceso.	Procedimiento para la gestión de la identidad	STI
5.17	Información de autenticación	*#Preventivo*	Sí	Para implementar un proceso de gestión de la autenticación que controle la asignación y gestión de la información de autenticación, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.	Procedimiento correspondiente	STI
5.18	Derechos de acceso	*#Preventivo*	Sí	Para contar con el procedimiento que regule la gestión de los derechos de acceso a la información y otros activos asociados. Esta gestión debe permitir revisar, modificar y eliminar de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.	Política de creación, control y revocación de accesos.	STI
5.19	Seguridad de la información en las relaciones con los proveedores	*#Preventivo*	Sí	Para definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.	Política de seguridad en la relación con los proveedores	STI, GAF y SAL
5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	*#Preventivo*	Sí	Para establecer y acordar con cada proveedor los requisitos de seguridad de la información pertinentes en función del tipo de relación con el proveedor.	Política de seguridad en la relación con los proveedores	STI, GAF y SAL
5.21	Gestión de seguridad de la información en la cadena de suministro de las TIC	*#Preventivo*	Sí	Para definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.	Política de seguridad en la relación con los proveedores	STI, GAF y SAL
5.22	Seguimiento, revisión y gestión de cambios en los servicios de proveedores	*#Preventivo*	Sí	Para monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.	Política de seguridad en la relación con los proveedores	STI, GAF y SAL

Clausula	Control	Tipo de Control	Aplicabilidad del Control	Justificación de la inclusión o exclusión	Documentación	Responsable
5.23	Seguridad de la Información en el uso de servicios en la nube	*#Preventivo*	Sí	Para establecer los procesos de adquisición, uso, gestión y salida de los servicios en la nube de acuerdo con los requisitos de seguridad de la información de la organización.	Política de Seguridad de Información en la Nube	STI
5.24	Planificación y preparación para la gestión de incidentes de seguridad de la información	*#Correctivo*	Sí	Para planificar y preparar para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, funciones y responsabilidades de gestión de incidentes de seguridad de la información.	Procedimiento correspondiente	STI
5.25	Evaluación y decisión sobre eventos de seguridad de la información	*#Detectivo*	Sí	Para evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información.	Procedimiento correspondiente	STI
5.26	Respuesta a incidentes de seguridad de la información	*#Correctivo*	Sí	Para responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.	Procedimiento correspondiente	STI
5.27	Aprendizaje de incidentes de seguridad de la información	*#Preventivo*	Sí	Para gestionar el conocimiento obtenido de los incidentes de seguridad de la información y utilizarlo para fortalecer y mejorar los controles de seguridad de la información.	Procedimiento correspondiente	STI
5.28	Recolección de evidencias	*#Correctivo*	Sí	Para establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.	Procedimiento correspondiente	STI
5.29	Seguridad de la información durante la interrupción	*#Preventivo* *#Correctivo*	Sí	Para planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.	Plan de Recuperación de Servicios de T.I.	STI
5.30	Preparación de las TIC para la continuidad del negocio	*#Correctivo*	Sí	Para preparar, planificar, implementar, mantener y probar las TIC en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.	Plan de Recuperación de Servicios de T.I.	STI y SGRD

Clausula	Control	Tipo de Control	Aplicabilidad del Control	Justificación de la inclusión o exclusión	Documentación	Responsable
5.31	Requisitos legales, estatutarios, regulatorios y contractuales	*#Preventivo*	Sí	Para identificar, documentar y mantener actualizados los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos.	Procedimiento correspondiente	STI y GAJ
5.32	Derechos de propiedad intelectual	*#Preventivo*	Sí	Para implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.	Procedimiento correspondiente	STI
5.33	Protección de registros	*#Preventivo*	Sí	Para proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.	Política en gestión de logs	STI
5.34	Privacidad y protección de datos de carácter personal	*#Preventivo*	Sí	Para identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de los datos personales de acuerdo con las leyes y reglamento aplicables y los requisitos contractuales.	Política de Protección de Datos	STI
5.35	Revisión independiente de la seguridad de la información	*#Preventivo* *#Correctivo*	Sí	Para revisar de forma independiente a intervalos planificados o cuando se produzcan cambios significativos el enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y tecnologías.	Procedimiento correspondiente	STI
5.36	Cumplimiento con políticas, reglas y normas de seguridad de la información	*#Preventivo*	Sí	Para revisar periódicamente el cumplimiento de la política de seguridad de la información de la organización, las políticas específicas del tema, las reglas y los estándares.	Procedimiento correspondiente	STI
5.37	Procedimientos operativos documentados	*#Preventivo* *#Correctivo*	Sí	Para documentar y poner a disposición del personal que lo necesite, los procedimientos operativos para las instalaciones de procesamiento de información.	Procedimiento correspondiente	STI

Clausula	Control	Tipo de Control	Aplicabilidad del Control	Justificación de la inclusión o exclusión	Documentación	Responsable
6	**CONTROLES DE PERSONAL**					
6.1	Selección	*#Preventivo*	Sí	Para garantizar que se apliquen los controles de verificación de antecedentes de todos los candidatos para convertirse en personal, antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, regulaciones y ética aplicables y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accede y los riesgos percibidos.	Procedimiento correspondiente	SGTH
6.2	Términos y condiciones del empleo	*#Preventivo*	Sí	Para incluir en los acuerdos contractuales de empleo términos y condiciones que establezcan las responsabilidades del personal y de la organización para la seguridad de la información.	Informe para incluir términos y condiciones de seguridad de la información	SGTH
6.3	Toma de conciencia, educación y entrenamiento sobre la seguridad de la información	*#Preventivo*	Sí	Para garantizar que el personal de la organización y las partes interesadas relevantes reciban la concientización, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.	Plan de Capacitación y Concientización en Seguridad de la Información	STI y SGTH
6.4	Proceso disciplinario	*#Preventivo* *#Correctivo*	Sí	Para formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación de la política de seguridad de la información.	Informe para en el proceso disciplinario la seguridad de la información	SGTH

Clausula	Control	Tipo de Control	Aplicabilidad del Control	Justificación de la inclusión o exclusión	Documentación	Responsable
6.5	Responsabilidades después del cese o cambio de empleo	*#Preventivo*	Sí	Para definir, aplicar y comunicar al personal pertinente y otras partes interesadas las responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la terminación o el cambio de empleo	Procedimiento correspondiente	SGTH
6.6	Acuerdos de confidencialidad o no divulgación	*#Preventivo*	Sí	Para identificar, documentar y revisar regularmente los acuerdos de confidencialidad o no divulgación, firmados por el personal y otras partes interesadas relevantes, que reflejen las necesidades de la organización para la protección de la información.	Política de confidencialidad	SGTH
6.7	Trabajo remoto	*#Preventivo*	Sí	Para implementar medidas de seguridad cuando el personal trabaja de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización.	Política de trabajo remoto	STI
6.8	Reporte de eventos de seguridad de la información	*#Detectivo*	Sí	Para proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna.	Sistema de tickets de soporte informático	STI
7	**CONTROLES FÍSICOS**					
7.1	Perímetros de seguridad física	*#Preventivo*	Sí	Para definir e implementar perímetros de seguridad para proteger las áreas que contienen información y otros activos asociados.	Política de seguridad de información - Ambiente físico	STI
7.2	Ingreso físico	*#Preventivo*	Sí	Para controlar y registrar el acceso a las áreas donde se procesa o almacena información, incluyendo mecanismos de autenticación biométrica o de dos factores.	Política de seguridad de información – Acceso físico	STI

Clausula	Control	Tipo de Control	Aplicabilidad del Control	Justificación de la inclusión o exclusión	Documentación	Responsable
7.3	Asegurar oficinas, salas e instalaciones	*#Preventivo*	Sí	Para diseñar e implementar la seguridad física de las oficinas, salas e instalaciones. (Reubicación del Centro de Datos, sin señales obvias, insonora y no visible desde el exterior)	Política de seguridad de información - Ambiente físico	STI y GDT
7.4	Supervisión de la seguridad física	*#Preventivo #Detectivo*	Sí	Para monitorear las instalaciones continuamente para detectar accesos físicos no autorizados.	Política de seguridad de información – Acceso físico	STI y SSCSV
7.5	Protección contra amenazas físicas y ambientales	*#Preventivo*	Sí	Para diseñar e implementar la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura. En el caso del Palacio Municipal el Centro de Datos debe ser reubicado por riesgo de colapso del local, según el Informe de Gestión de Riesgo de Desastres.	Política de seguridad de información - Ambiente físico	STI, GM y GDT
7.6	Trabajo en áreas seguras	*#Preventivo*	Sí	Para diseñar e implementar medidas de seguridad para trabajar en áreas seguras.	Medidas de seguridad física	STI, SGTH y SGRD
7.7	Escritorio y pantalla limpios	*#Preventivo*	Sí	Para definir y aplicar adecuadamente reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y reglas de pantalla limpia para las instalaciones de procesamiento de información.	Política de Escritorio y Pantalla Limpia	STI
7.8	Ubicación y protección de equipos	*#Preventivo*	Sí	Para ubicar los equipos de forma segura y protegida.	Medidas de seguridad física	STI
7.9	Seguridad de los activos fuera de las instalaciones	*#Preventivo*	Sí	Para proteger los activos fuera del sitio.	Medidas de seguridad para los activos fuera de las instalaciones	STI
7.10	Medios de almacenamiento	*#Preventivo*	Sí	Para gestionar los medios de almacenamiento a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.	Política de medios extraíbles	STI

Clausula	Control	Tipo de Control	Aplicabilidad del Control	Justificación de la inclusión o exclusión	Documentación	Responsable
7.11	Servicios de suministro de apoyo	*#Preventivo #Detectivo*	Sí	Para proteger las instalaciones de procesamiento de información contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.	Adquisición de UPS para los equipos de los procesos misionales	STI
7.12	Seguridad del cableado	*#Preventivo*	Sí	Para proteger contra intercepciones, interferencias o daños los cables que transportan energía, datos o servicios de información de apoyo.	Proyecto de Cableado estructurado	STI
7.13	Mantenimiento de equipo	*#Preventivo*	Sí	Para dar mantenimiento correctamente a los equipos para garantizar la disponibilidad, integridad y confidencialidad de la información.	Plan de mantenimiento preventivo de equipos informáticos	STI
7.14	Eliminación segura o reutilización de equipos	*#Preventivo*	Sí	Para verificar que todos los datos confidenciales y el software con licencia de los equipos se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.	Procedimiento para reutilización de medios de almacenamiento	STI
8	**CONTROLES TECNOLÓGICOS**					
8.1	Dispositivos terminales del usuario	*#Preventivo*	Sí	Para proteger la información almacenada, procesada o accesibles a través de los dispositivos finales de los usuarios.	Procedimiento correspondiente	STI
8.2	Derechos de acceso privilegiado	*#Preventivo*	Sí	Para restringir y gestionar la asignación y el uso de derechos de acceso privilegiado.	Implementación de Directorio Activo	STI
8.3	Restricción de acceso a la información	*#Preventivo*	Sí	Para restringir el acceso a la información y otros activos asociados de acuerdo con la política específica del tema establecida sobre el control de acceso.	Política de creación, control y revocación de accesos	STI
8.4	Acceso al código fuente	*#Preventivo*	Sí	Para administrar adecuadamente el acceso de lectura y escritorio al código fuente, las herramientas de desarrollo y las bibliotecas de software.	Procedimiento correspondiente	STI

Clausula	Control	Tipo de Control	Aplicabilidad del Control	Justificación de la inclusión o exclusión	Documentación	Responsable
8.5	Autenticación segura	*#Preventivo*	Sí	Para implementar las tecnologías y los procedimientos de autenticación segura en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.	Política de creación, control y revocación de accesos	STI
8.6	Gestión de capacidad	*#Preventivo #Detectivo*	Sí	Para monitorear y ajustar el uso de los recursos de acuerdo con los requisitos de capacidad actuales y esperados.	Procedimiento correspondiente	STI
8.7	Protección contra programas maliciosos (malware)	*#Preventivo #Detectivo #Correctivo*	Sí	Para garantizar que la información y otros activos asociados estén protegidos contra el malware.	Antivirus. Concientización	STI
8.8	Gestión de vulnerabilidades técnicas	*#Preventivo*	Sí	Para evaluar la exposición de la organización a la explotación de vulnerabilidades técnicas de los sistemas de información para tomar las medidas apropiadas.	Comunicados del CNSD y otras fuentes	STI
8.9	Gestión de la configuración	*#Preventivo*	Sí	Para garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida, y que la configuración no se vea alterada por cambios no autorizados o incorrectos.	Procedimiento de Gestión de la configuración	STI
8.10	Eliminación de información	*#Preventivo*	Sí	Para eliminar adecuadamente la información innecesaria almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento.	Procedimiento de eliminación de la información	STI
8.11	Enmascaramiento de datos	*#Preventivo*	Sí	Para limitar la exposición de datos confidenciales, incluida la información de identificación personal, y para cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales.	Procedimientos para enmascaramiento o encriptación de datos.	STI
8.12	Prevención de fugas de datos	*#Preventivo #Detectivo*	Sí	Para detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.	Política de medios extraíbles	STI

Clausula	Control	Tipo de Control	Aplicabilidad del Control	Justificación de la inclusión o exclusión	Documentación	Responsable
8.13	Copia de seguridad de la información	*#Correctivo*	Sí	Para permitir la recuperación de la pérdida de datos o sistemas.	Política de copias de seguridad	STI
8.14	Redundancia de las instalaciones de procesamiento de información	*#Preventivo*	Sí	Para asegurar el funcionamiento continuo de las instalaciones de procesamiento de información con suficiente redundancia para cumplir con los requisitos de disponibilidad.	Plan de Implementación de un servidor de respaldo en otra Sede Municipal	STI
8.15	Registro (Inicio de sesión)	*#Detectivo*	Sí	Para registrar eventos, generar evidencia, asegurar la integridad de la información de registro, prevenir contra acceso no autorizado, identificar eventos de seguridad de la información que pueden conducir a una seguridad de la información incidente y para apoyar las investigaciones.	Procedimiento correspondiente	STI
8.16	Actividad de monitoreo	*#Detectivo #Corrección*	Sí	Para evaluar posibles incidentes de seguridad de la información a través del monitoreo de las redes, los sistemas y las aplicaciones para detectar comportamientos anómalos y tomar las medidas apropiadas	Política en gestión de logs	STI
8.17	Sincronización de reloj	*#Detectivo*	Sí	Para permitir la correlación y el análisis de eventos relacionados con la seguridad y otros datos registrados, y para apoyar las investigaciones sobre incidentes de seguridad de la información, los relojes de los sistemas de procesamiento de información deben sincronizarse con las fuentes de tiempo aprobadas.	Procedimiento correspondiente	STI
8.18	Uso de programas de utilidad privilegiados	*#Preventivo*	Sí	Para garantizar que el uso de programas de utilidad no dañe el sistema y los controles de aplicaciones para la información seguridad.	Procedimiento correspondiente	STI
8.19	Instalación de software en sistemas operativos	*#Preventivo*	Sí	Para implementar procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.	Procedimiento correspondiente	STI
8.20	Seguridad de redes	*#Preventivo #Detectivo*	Sí	Para proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo de compromiso a través de la red.	Política de seguridad de la red	STI

Clausula	Control	Tipo de Control	Aplicabilidad del Control	Justificación de la inclusión o exclusión	Documentación	Responsable
8.21	Seguridad de servicios de red	*#Preventivo*	Sí	Para garantizar la seguridad en el uso de los servicios de red.	Política de seguridad de la red	STI
8.22	Segregación de redes	*#Preventivo*	Sí	Para dividir la red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades de cada área.	Procedimiento correspondiente	STI
8.23	Filtrado de la web	*#Preventivo*	Sí	Para proteger los sistemas contra el malware y evitar el acceso a recursos web no autorizados.	Servicio de Seguridad Perimetral	STI
8.24	Uso de criptografía	*#Preventivo*	Sí	Para garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad o la integridad de la información.	Política de uso de técnicas criptográficas	STI
8.25	Ciclo de vida de desarrollo seguro	*#Preventivo*	Sí	Para establecer y aplicar reglas para el desarrollo seguro de software y sistemas.	Política de Desarrollo Seguro de Software	STI
8.26	Requisitos de seguridad de la aplicación	*#Preventivo*	Sí	Para garantizar que todos los requisitos de seguridad de la información se identifiquen y aborden al desarrollar o adquirir aplicaciones.	Política de Desarrollo Seguro de Software	STI
8.27	Arquitectura de sistemas seguros y principios de ingeniería	*#Preventivo*	Sí	Garantizar que los sistemas de información se diseñen, implementen y operen de forma segura dentro del ciclo de vida del desarrollo.	Política de Desarrollo Seguro de Software	STI
8.28	Codificación Segura	*#Preventivo*	Sí	Garantizar que el software se escriba de forma segura, reduciendo así la cantidad de posibles vulnerabilidades de seguridad de la información en el software.	Política de Desarrollo Seguro de Software	STI

Clausula	Control	Tipo de Control	Aplicabilidad del Control	Justificación de la inclusión o exclusión	Documentación	Responsable
8.29	Pruebas de seguridad en desarrollo y aceptación	*#Preventivo*	Sí	Para validar si se cumplen los requisitos de seguridad de la información cuando las aplicaciones o el código se implementan en el entorno de producción.	Política de Desarrollo Seguro de Software	STI
8.30	Desarrollo subcontratado	*#Preventivo #Detectivo*	Sí	Para garantizar que las medidas de seguridad de la información requeridas por la organización se implementen en el desarrollo de sistemas subcontratados.	Política de Desarrollo Seguro de Software	STI
8.31	Separación de los entornos de desarrollo, prueba y producción	*#Preventivo*	Sí	Para proteger el entorno de producción y los datos contra el compromiso de las actividades de desarrollo y prueba.	Política de Desarrollo Seguro de Software	STI
8.32	Gestión de cambios	*#Preventivo*	Sí	Para contar con procedimientos de gestión de cambios cuando haya cambios en las instalaciones de procesamiento de información y los sistemas de información.	Política de Gestión de Cambios	STI
8.33	Información de prueba	*#Preventivo*	Sí	Para seleccionar, proteger y gestionar adecuadamente la información de las pruebas.	Procedimiento correspondiente	STI
8.34	Protección de los sistemas de información durante las pruebas de auditoría	*#Preventivo*	Sí	Minimizar el impacto de la auditoría y otras actividades de aseguramiento en los sistemas operativos y procesos de la Entidad.	Política de auditoría de sistemas	STI

6. FORMATOS

No aplica.

7. ANEXOS

No aplica.