



Municipalidad Distrital de Sayán
Gerencia Municipal

DIRECTIVA N° 003-2025-GM/MDS

“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”



	<u>DIRECTIVA N° 003-2025-GM/MDS</u> “DISPOSICIONES DE SEGURIDAD DE LA INFORMACIÓN PARA EL DESARROLLO E IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE SAYÁN”



Municipalidad Distrital de Sayán
Gerencia Municipal

DIRECTIVA N° 003-2025-GM/MDS

"Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán"

DIRECTIVA N° 003-2025-GM/MDS

"DISPOSICIONES DE SEGURIDAD DE LA INFORMACIÓN PARA EL DESARROLLO E IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE SAYÁN"

INDICE

1. ANTECEDENTES
2. OBJETIVOS
3. FINALIDAD
4. ALCANCE
5. BASE LEGAL
6. GLOSARIO DE TERMINOS
7. RESPONSABILIDADES
8. DISPOSICIONES GENERALES
9. DISPOSICIONES ESPECÍFICAS

- 9.1. De la Política de Seguridad de la Información
- 9.2. De la Organización de la Seguridad de la Información.
- 9.3. De la Administración de Dispositivos Móviles.
- 9.4. De la Gestión de la Información y Activos de Información Asociados.
- 9.5. De la Seguridad de los Recursos Humanos.
- 9.6. De los Controles de Accesos.
- 9.7. De la Seguridad de Ambientes Físicos.
- 9.8. De los Equipos Informáticos.
- 9.9. De los Controles Criptográficos.
- 9.10. De la Seguridad de las Operaciones.
- 9.11. De la Seguridad de la Comunicaciones.
- 9.12. De la Adquisición, Desarrollo y Mantenimiento de Sistemas.
- 9.13. De la Relación con los Proveedores.
- 9.14. De la Gestión de Incidentes de Seguridad de la Información.
- 9.15. De la Continuidad de Servicios de TI.
- 9.16. Sobre el Cumplimiento de Requisitos Legales y Contractuales.
- 9.17. Del Cumplimiento y Revisión de los Presentes Lineamientos de Seguridad de la Información.



"Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán"

1. ANTECEDENTES

Para la MUNICIPALIDAD DISTRITAL DE SAYAN, la información es un activo valioso, por ese motivo a través de su Oficina de Tecnología de la Información y Gobierno Digital ha desarrollado los lineamientos con la finalidad de brindar la adecuada protección, salvaguardar la confidencialidad, integridad y la disponibilidad de manera oportuna de la información, permitiendo realizar procesos de gestión de manera eficiente y transparente.

Por lo expuesto y en cumplimiento de lo dispuesto por la Secretaría de Gobierno Digital de la Presidencia de Consejo de Ministros a través de la Resolución Ministerial N° 004- 2016-PCM, aprobar el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2a Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

La MUNICIPALIDAD DISTRITAL DE SAYÁN, a través del presente documento normativo traza los lineamientos a seguir para la implementación del Sistema de Seguridad de la Información, cuyo desarrollo se encontrará alineado a Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2a Edición".

2. OBJETIVOS

Establecer los lineamientos que ayuden a regular la gestión de la seguridad de la información, resguardar los activos de información, recursos informáticos y/o plataformas tecnológicas donde se procesa y almacena la información de la MUNICIPALIDAD DISTRITAL DE SAYAN frente a las amenazas, internas o externas, deliberadas o accidentales con el fin de mitigar los riesgos.

3. FINALIDAD

Identificar, analizar, evaluar y dar tratamiento a los riesgos de seguridad de la información, con la finalidad de lograr la confidencialidad, integridad y disponibilidad de la información de la MUNICIPALIDAD DISTRITAL DE SAYAN, en cumplimiento con la normativa vigente para garantizar razonablemente el logro de los objetivos estratégicos y operativos de la entidad municipal.

4. ALCANCE

El presente lineamiento es de obligatorio cumplimiento para los/las servidores/as de la MUNICIPALIDAD DISTRITAL DE SAYAN bajo cualquier régimen laboral, de la Sede Central y demás sedes. También alcanza a los proveedores que interactúen o brinden servicios a la MUNICIPALIDAD DISTRITAL DE SAYAN.

5. BASE LEGAL

- ❖ Ley N° 27269: Ley de Firmas y Certificados Digitales y modificatorias.
- ❖ Ley N° 27291: Ley que modifica el código civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica.
- ❖ Ley N° 27658: Ley Marco de Modernización de la Gestión del Estado y modificatorias.
- ❖ Ley N° 27806: Ley de Transparencia y Acceso a la Información Pública y modificatorias.
- ❖ Ley N° 28493: Ley que regula el uso del Correo Electrónico comercial no solicitado (SPAM) y modificatoria.
- ❖ Ley N° 28530: Ley de Promoción de Acceso a Internet para personas con discapacidad y adecuación del espacio físico en cabinas públicas de internet y modificatorias.
- ❖ Ley N° 29733: Ley de Protección de Datos Personales y modificatorias.
- ❖ Ley N° 30096: Ley de Delitos Informáticos y modificatorias.



Municipalidad Distrital de Sayán
Gerencia Municipal

DIRECTIVA N° 003-2025-GM/MDS

"Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán"

- ❖ Decreto Legislativo N° 822: Ley de Derechos de Autor y modificatorias.
- ❖ Decreto Legislativo N° 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses y modificatorias.
- ❖ Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital y modificatorias.
- ❖ Decreto Supremo N° 066-2011-PCM, que aprueba el "Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0".
- ❖ Decreto Supremo N° 003-2013-JUS, que aprueba el reglamento de la Ley N° 29733, Ley de Protección de Datos Personales y modificatorias.
- ❖ Decreto Supremo N° 010-2019-RE, que ratifica el "Convenio sobre la Ciberdelincuencia".
- ❖ Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- ❖ Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática y modificatoria.
- ❖ Resolución Directoral N° 056-2017-INACAL-DN, que aprueba como Norma Técnica Peruana (NTP), entre otras, la NTP-ISO/IEC 27002:2017 "Tecnología de la Información. Técnicas de Seguridad Código de prácticas para controles de seguridad de la información, 1° Edición.
- ❖ Resolución Directoral N° 047-2018-INACAL-DN, que aprueba como Norma Técnica Peruana (NTP), entre otras, la NTP-ISO/IEC 27005:2018 "Tecnología de la Información. Técnicas de Seguridad. Gestión de Riesgos de la Seguridad de la Información. 2° Edición.
- ❖ Resolución Directoral N° 029-2019-INACAL-DN, que aprueba como Norma Técnica Peruana (NTP), entre otras, la NTP-ISO/IEC 27035-1 2019 "Tecnología de la Información Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Parte 1 Principios de la gestión de incidencias", 1° Edición.
- ❖ Resolución Directoral N° 014-2018-INACAL-DN, que aprueba como Norma Técnica Peruana (NTP), entre otras, la NTP ISO 31000:2018 "Gestión de Riesgos Principios y Directrices", 2° Edición.
- ❖ Resolución Ministerial N° 087-2019-PCM, que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
- ❖ Resolución Directoral N° 019-2013-JUS/DGPDP, que aprueba la Directiva de Seguridad de la información administrada por los Bancos de Datos Personales.

6. GLOSARIO DE TERMINOS

Para efectos de la presente directiva, con la finalidad de facilitar la comprensión del presente documento, se definen los siguientes términos:

- » **Activo de información:** Cualquier información que tiene valor para la Entidad y para el Sistema de Gestión de Seguridad de la Información. Se consideran también los recursos humanos, tecnológicos que intervienen en el tratamiento directo o indirecto de la información, así como sus procesos y actividades.
- » **Amenaza:** Cualquier factor que tiene el potencial para explotar una debilidad y dar lugar a algún tipo de daño a la información o a la institución.
- » **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarlas de manera objetiva, para determinar el grado de cumplimiento de criterios preestablecidos.
- » **Clasificación de la Información:** Acción de identificar y clasificar los activos de información en términos de la sensibilidad e importancia para la Entidad.

Aprobado mediante Resolución de Gerencia Municipal N° 017-2025-GM-MDS

Pág. 4

“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

- » **Ciberseguridad:** Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país.
- » **Confianza digital:** Es el resultado cuando las interacciones digitales entre personas, empresas, entidades públicas o cosas en el entorno digital son veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables, con el propósito de impulsar el desarrollo de la economía digital y la transformación digital. Es un componente de la transformación digital y tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital.
- » **Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o entidades no autorizados.
- » **Control:** Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la entidad que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- » **Control de acceso:** Medios o mecanismo para garantizar que el acceso a los activos de manera autorizada y restringida, basado en los requerimientos de negocios y los requisitos de seguridad.
- » **Comité de Gobierno Digital:** El Comité de Gobierno Digital (CGD) fue establecido con Resolución de Alcaldía N° 095-2020/MDS/A y es responsable de gestionar, mantener y documentar el Modelo de Gestión Documental (MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de la Seguridad de la Información (SGSI) de la MUNICIPALIDAD DISTRITAL DE SAYAN.
- » **Credencial de acceso:** Corresponde al mecanismo mediante el cual se le asigna una identificación única e irrepetible a una persona, para que tenga acceso a las aplicaciones de la Entidad, con el propósito de desempeñar las tareas encomendadas.
- » **Datos personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.
- » **Disponibilidad:** Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada.
- » **Dispositivo móvil:** Aparato de tamaño portable que tiene capacidad de acceso, almacenamiento y/o procesamiento de información, disponiendo además de conexión permanente o intermitente a una red de comunicaciones tales como la Notebook, Tablet o Smartphone.
- » **Equipo informático:** Dispositivo electrónico que permite procesar información y datos con programas diseñados para ello, incluye a las computadoras, impresoras, escáneres y los dispositivos móviles.
- » **Evento:** Un suceso que puede ser interno o externo a la Entidad, que ocurren en un momento determinado y son originados por una causa específica.
- » **Incidente de seguridad de la información:** Evento no deseado que genera amenaza a la seguridad de la información y que tiene una probabilidad significativa de comprometer a la operatividad de la Entidad.
- » **Información:** Cualquier forma de registro de contenidos susceptibles a ser procesados, distribuidos y almacenados, pudiendo estar en formato electrónico, óptico, magnéticos u otro medio de almacenamiento.
- » **Integridad:** Propiedad de precisión y completitud de la información.



"Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán"

- » **Lista de distribución:** Es un servicio para distribuir mensajes de correo electrónico a dos o más personas al mismo tiempo permitiendo difundir comunicados masivos a sus miembros.
- » **Medios removibles:** Dispositivos de almacenamiento de información extraíbles de un equipo informático tales como cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.
- » **Oficial de Seguridad de la Información:** El Oficial de Seguridad de la Información es el responsable del Sistema de Gestión de la Seguridad de la Información (SGSI) y reporta al Comité de Gobierno Digital (CGD). El rol está designado con Resolución de Alcaldía N° 095-2020/MDS/A.
- » **Personal de la MDS:** Comprende a los servidores civiles designados o asignados bajo Contratación Administrativa de Servicios; así como a aquellas personas contratadas en el marco de la Ley N° 29806, Ley que regula la contratación de personal altamente calificado en el Sector Público.
- » **Propietario de activo:** Es el funcionario o servidor asignado de garantizar que el activo asignado bajo su responsabilidad esté protegido con los controles definidos en el SGSI y que le apliquen a dicho activo; es el responsable por la afectación de la confidencialidad, integridad y disponibilidad del mismo, en cualquiera de los procesos que se encuentre involucrado.
- » **Recursos informáticos:** Todos los equipos computacionales, sistemas informáticos, aplicaciones, bases de datos, dispositivos extraíbles, y demás servicios que por su naturaleza registre, procese, almacene o transmita información electrónica o digital.
- » **Redes sociales:** Corresponde a los portales de redes sociales públicos como Facebook, Instagram, Twitter, etc.
- » **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen institucional, etc.) y se pueden aplicar a niveles diferentes (operativo, estratégico, organización).
- » **Seguridad de la información:** Todas las acciones orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los activos asociados a su tratamiento independiente de la forma en la que la información se encuentre.
- » **Sistema de Gestión de Seguridad de la Información:** Es un componente del sistema de gestión de una organización, con base en un enfoque de riesgos, que tiene como función establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. El SGSI está conformado por políticas, procedimientos, directrices, recursos y actividades asociadas, gestionadas por la organización, en la búsqueda de la protección de sus activos de información.
- » **Teletrabajo:** El teletrabajo consiste en la prestación de servicios subordinada, sin presencia física en la MUNICIPALIDAD DISTRITAL DE SAYAN, a través de medios informáticos, de telecomunicaciones y análogos, mediante los cuales, a su vez, se ejerce el control y la supervisión de las labores.
- » **Token:** Dispositivo de almacenamiento criptográfico que contiene el Certificado Digital asignado a la persona titular del mismo, que le permite firmar digitalmente.
- » **Trabajo remoto:** El trabajo remoto consiste en la prestación de servicios subordinada con la presencia física del trabajador en su domicilio o lugar de aislamiento domiciliario, utilizando cualquier medio o mecanismo que posibilite realizar las labores fuera del centro de trabajo, siempre que la naturaleza de las labores lo permita. Este no se limita al teletrabajo, sino que se extiende a cualquier tipo de trabajo que no requiera la presencia física del trabajador en el centro de labores.
- » **Tratamiento del riesgo:** Proceso de selección e implementación de medidas para modificar el riesgo.



Municipalidad Distrital de Sayán
Gerencia Municipal

DIRECTIVA N° 003-2025-GM/MDS

“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

- » **Usuario:** persona que hace uso de un recurso informático o servicio de tecnología de la información para fines laborales.
- » **Video a demanda:** Corresponde a los portales de Video/Audio a demanda y en vivo por internet como Youtube, Vimeo, Spotify, etc. o canales de radio y televisión por internet.
- » **Vulnerabilidad:** Debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad o disponibilidad de dicho activo.

7. RESPONSABILIDADES

- » La Oficina de Tecnologías de la Información y Gobierno Digital será responsable del cumplimiento de las disposiciones de la presente directiva, promover la participación activa del personal en la identificación, análisis, y evaluación de riesgos de seguridad de la información.
- » La Oficina de Tecnologías de la Información y Gobierno Digital será responsable de adoptar las acciones pertinentes para implementar los lineamientos dispuesto en la presente directiva en coordinación con el Comité de Gobierno Digital y la Gerencia Municipal
- » El Comité de Gobierno Digital, será el responsable de gestionar, supervisar y velar su cumplimiento de la presente metodología de gestión de riesgos de seguridad de la información, comprometiendo el apoyo de la Alta Gerencia.
- » El Oficial de Seguridad y Confianza Digital será el responsable de liderar las reuniones a desarrollarse para el tratamiento de los riesgos de seguridad de la información, verificar, supervisar y coordinar el cumplimiento de la presente directiva de Gestión de Seguridad de la Información.

8. DISPOSICIONES GENERALES

La MUNICIPALIDAD DISTRITAL DE SAYAN a través de su Oficina de Tecnología de la Información y Gobierno Digital, gestiona, mantiene, monitorea, documenta y efectúa el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI) en constante coordinación con su Comité de Gobierno Digital (CGD) y promueve el cumplimiento de normas técnicas, estándares internacionales y de las mejores prácticas de seguridad de la información, a fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

Es por ello que se establecen las siguientes disposiciones generales:

- » Todo lo contenido en este documento es de aplicación obligatoria por parte de todo el personal, bajo los distintos regímenes laborales de la MUNICIPALIDAD DISTRITAL DE SAYAN, las personas bajo contratos de locación y los proveedores que prestan servicios a la MUNICIPALIDAD DISTRITAL DE SAYAN.
- » Toda información interna o externa (de propiedad de terceros) contenida en equipos informáticos, en medios físicos o digitales o en sistemas de información de la MUNICIPALIDAD DISTRITAL DE SAYAN, están bajo custodia de la Entidad y por lo tanto deberán ajustarse a la presente Directiva de seguridad de la información.
- » Todos los responsables de las unidades orgánicas con las que cuenta la MUNICIPALIDAD DISTRITAL DE SAYAN deberá asegurarse que el personal a su cargo conozca los niveles de sensibilidad y criticidad de la información que se maneja en su unidad.

Aprobado mediante Resolución de Gerencia Municipal N° 017-2025-GM-MDS

Pág. 7

“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

- » Todo personal deberá utilizar los recursos informáticos y/o sistemas de información puestos a su disposición, de manera legal, profesional y ética, de lo contrario será sometido a un proceso administrativo sancionador.
- » La presente Directiva deberá ser revisada al menos una vez por año para garantizar su vigencia y deberá mantener actualizada toda la documentación necesaria para dar cumplimiento.

9. DISPOSICIONES ESPECÍFICAS

9.1. DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

9.1.1 La MUNICIPALIDAD DISTRITAL DE SAYAN sabe que la información obtenida a través de sus procedimientos de gestión es un Activo Vital de suma Importancia, es por ello que se encuentra comprometida en salvaguardar la confidencialidad, integridad y disponibilidad de la información, a través del desarrollo e implementación de un Sistema de Gestión de la Seguridad de la Información

9.1.1. La MUNICIPALIDAD DISTRITAL DE SAYAN asume el compromiso de asegurar el aprovisionamiento de los recursos requeridos para desarrollar, implementar, mantener y mejorar continuamente el sistema de Gestión de Seguridad de la Información; así también, se promoverá la sensibilización y capacitación de los servidores respecto al uso de la información y prácticas de seguridad a través de los mecanismos adecuados de comunicación, a fin de fortalecer los valores y principios.

9.2. DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

La MUNICIPALIDAD DISTRITAL DE SAYAN busca establecer lineamientos que serán tomados como referencia para la implementación, gestión y operación de la Seguridad de la Información dentro de la Entidad.

9.2.1. El Comité de Gobierno Digital en coordinación con la Oficina de Tecnología de la Información y Gobierno Digital determinarán el alcance del Sistema de Gestión de Seguridad de la Información (en adelante SGSI), siendo responsabilidad de esta unidad orgánica, brindar las facilidades para el desarrollo, progreso, mantenimiento y actualizaciones del SGSI.

9.2.2. Las Unidades Orgánicas de la MUNICIPALIDAD DISTRITAL DE SAYAN, deben de asignar roles y responsabilidades a los servidores que tengan a su disposición para la protección de los Activos de Información, así mismo se deberán asignar funciones para que cada servidor maneje determinada información en específico y así reducir las posibilidades de modificación o mal uso de la información que custodia la MUNICIPALIDAD DISTRITAL DE SAYAN.

9.2.3. Los lineamientos de seguridad de la información establecidos en la presente directiva deben formar parte en los procesos de gestión de los proyectos a realizar por las diferentes unidades orgánicas de la MUNICIPALIDAD DISTRITAL DE SAYAN, para garantizar que los riesgos de los activos de información que se presente durante el desarrollo de los proyectos sean identificados y tratados oportunamente. Las unidades orgánicas deberán consultar a la Oficina de Tecnología de la Información y Gobierno Digital sobre los mecanismos y controles de seguridad en lo concerniente a los activos de información.

9.2.4. El SGSI contará con lineamientos que permitan la detección, análisis, evaluación y tratamiento de riesgos de los activos de información, de manera oportuna, todos estos procesos se realizarán en concordancia con lo establecido en la presente directiva.

“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

- 9.2.5. La Oficina de Tecnología de la Información y Gobierno Digital será la encargada de aplicar los controles necesarios para la protección de los datos personales, acorde con la Ley N° 29733, Ley de Protección de Datos Personales.
- 9.2.6. El Oficial de Seguridad de la Información, debe realizar el seguimiento y monitoreo del SGSI, procurando que esté acorde a lo dispuesto en los presentes lineamientos, así mismo es de responsabilidad de cada servidor, en su calidad de actor dentro del SGSI, informar sobre el estado de los controles y actividades de seguridad de la información en el marco de sus responsabilidades.
- 9.2.7. El Comité de Gobierno Digital en coordinación con la Oficina de Tecnología de la Información y Gobierno Digital, serán los responsables de difundir a todas las unidades orgánicas de la municipalidad los presentes lineamientos y concientizar el uso ético de la información a la que tienen acceso.
- 9.2.8. El Comité de Gobierno Digital establecerá protocolos para el contacto adecuado con las autoridades locales, provinciales, regionales y nacionales ligados a la seguridad de la información, para asegurar una comunicación efectiva en caso de incidencias de seguridad de la información en cumplimiento con las leyes y normativas aplicables.
- 9.2.9. El Comité de Gobierno Digital establecerá protocolos para el contacto adecuado con Grupos Especiales de Interés relaciones con la seguridad de la información, tales como proveedores, grupos institucionales claves, especialistas, entre otros, con el propósito de controlar los riesgos y eventos de seguridad de la información.
- 9.2.10. El SGSI contará con lineamientos de Gestión de Proyectos, incorporando prácticas de seguridad de la información que involucren datos sensibles en todas las fases del ciclo de vida de los proyectos municipales.
- 9.2.11. La Oficina de Tecnología de la Información y Gobierno Digital, debe establecer e implementar los mecanismos para permitir el acceso remoto mediante el uso de tecnología de acceso seguro como la VPN y mecanismos de autenticación con credenciales de accesos únicos.
- 9.2.12. Se establecerá los procedimientos para la asignación, uso y revocación del derecho de acceso remoto, para poder brindarle acceso a un personal deberá ser solicitado de manera formal por su jefe inmediato.
- 9.2.13. La Oficina de Tecnología de la Información y Gobierno Digital, debe gestionar y controlar otros mecanismos de acceso o conexión remota no autorizados o institucionales, incluyendo el uso de herramientas y software de escritorio o terminal remoto (Anydesk, Teamviewer, etc).

9.3. DE LA ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES.

La MUNICIPALIDAD DISTRITAL DE SAYAN permite el uso de dispositivos móviles dentro y fuera de la infraestructura de comunicaciones de la Entidad, ya sean estos bienes de propiedad de la MUNICIPALIDAD DISTRITAL DE SAYAN o bienes personales autorizados, donde toda información de la entidad que se almacena, transfiere o procesa siguen perteneciendo a la MUNICIPALIDAD DISTRITAL DE SAYAN por lo que la entidad mantiene el derecho a controlar dicha información, aunque no sea propietaria del dispositivo.

“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

- 9.3.1. La Oficina de Tecnología de la Información y Gobierno Digital, deberá establecer un procedimiento que permita un adecuado registro de entrega de dispositivos móviles (smartphone, laptop, Tablet, etc.) a los servidores de la entidad municipal, así como la devolución de los mismos.
- 9.3.2. El usuario de un dispositivo móvil de propiedad privada (personal) debe solicitar autorización a su jefe inmediato para su uso dentro de la infraestructura de comunicaciones de la MUNICIPALIDAD DISTRITAL DE SAYAN.
- 9.3.3. Establecer lineamientos para la no divulgación de la información sensible, a la cual se tenga acceso, almacenada en los dispositivos móviles, las mismas que deben ser contempladas en los contratos o actas de compromiso celebrados con terceros o proveedores de servicios.
- 9.3.4. Establecer los criterios de asignación de los recursos informáticos en base a la real necesidad de cada servidor municipal, que estará determinado por su cargo y funciones que desempeñará dentro de la entidad municipal, evitando así el acceso a la información de equipos ajenos o no autorizados por la Oficina de Tecnología de la Información y Gobierno Digital.
- 9.3.5. Los servidores de la MUNICIPALIDAD DISTRITAL DE SAYAN no debe utilizar los dispositivos móviles para uso distinto a las actividades laborales, así mismo no deben permitir que personas ajenas a la entidad municipal haga uso de los mismo o instalar aplicativos que pongan en peligro la información que se almacena en su dispositivo asignado.

9.4. DE LA GESTIÓN DE LA INFORMACIÓN Y ACTIVOS DE INFORMACIÓN ASOCIADOS.

La gestión de los activos de información está referida a aquella información contenida en cualquier medio de almacenamiento sea físico o digital, la MUNICIPALIDAD DISTRITAL DE SAYAN, para una mejor gestión de la información deberá de manera obligatoria lo siguiente:

- 9.4.1. A través de la Oficina de Tecnología de la Información y Gobierno Digital debe mantener un inventario de activos de sistemas de información actualizados se recomienda que sea de manera semestral.
- 9.4.2. A través de la Oficina de Abastecimiento se debe de contar con un inventario de todo el parque informático se recomienda que sea actualizado de manera semestral.
- 9.4.3. A través de la Oficina de Abastecimiento se debe establecer un marco para la identificación, clasificación y protección de los activos de información, asegurando que todos los activos estén bajo propiedad adecuada y sean gestionados de acuerdo con las políticas de seguridad de la información.
- 9.4.4. Todos los servidores de la MUNICIPALIDAD DISTRITAL DE SAYAN bajo cualquier modalidad y régimen de contratación, deberán hacer un uso adecuado de la información a la cual tengan acceso y de los activos de información asociados, en el marco de sus funciones.
- 9.4.5. Todas las unidades orgánicas de la MUNICIPALIDAD DISTRITAL DE SAYAN están comprometidas con la seguridad de la información, por lo que se debe consignar en los contratos laborales o términos de referencia, a través de cláusulas, compromisos y/o disposiciones referidas a la confidencialidad y no divulgación de la información a la que hayan tenido acceso, esto aplica para todos los servidores bajo cualquier modalidad y régimen de contratación.



Municipalidad Distrital de Sayán
Gerencia Municipal

DIRECTIVA N° 003-2025-GM/MDS

“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

- 9.4.6. Los Gerentes, Subgerentes y Jefes de las unidades orgánicas de la MUNICIPALIDAD DISTRITAL DE SAYAN, deben gestionar el inventario y la propiedad de los activos de la información, así como supervisar a los responsables del tratamiento y generación de información y los activos asociados, que están bajo su cargo, en cumplimiento de las disposiciones establecidas.
- 9.4.7. La Oficina de Tecnología de la Información y Gobierno Digital en coordinación con la Oficina de Abastecimiento, serán los responsables del procedimiento para la asignación y la devolución de los bienes informáticos y demás asociados a la información de los servidores que ingresan y dejan de laborar en la MUNICIPALIDAD DISTRITAL DE SAYAN.
- 9.4.8. La Oficina de Tecnología de la Información y Gobierno Digital, será el responsable de definir y actualizar las disposiciones específicas para el adecuado uso de los activos informáticos, asociados a la generación, procesamiento y almacenamiento de la información, los cuales están plasmados en la Directiva de Gestión de Recursos Informáticos de la MUNICIPALIDAD DISTRITAL DE SAYAN o el documento que haga sus veces, así mismo la Oficina de Tecnología de la Información y Gobierno Digital será el responsable de la supervisión del cumplimiento de estos lineamientos.
- 9.4.9. Todo personal debe considerar que toda información que posea la MUNICIPALIDAD DISTRITAL DE SAYAN es de acceso PÚBLICO, salvo las excepciones previstas en los artículos 15, 16 y 17 del Texto Único Ordenado de la Ley N°. 27806 - Ley de Transparencia y Acceso a la Información Pública, aprobado por Decreto Supremo N° 021-2019-JUS.
- 9.4.10. La Oficina de Tecnología de la Información y Gobierno Digital debe establecer un sistema de clasificación de la información para garantizar que los activos sean tratados de acuerdo con su valor y nivel de confidencialidad.
- 9.4.11. La Oficina de Tecnología de la Información y Gobierno Digital debe realizar un sistema físico y digital de identificación de los activos de información de acuerdo con su clasificación y criticidad.
- 9.4.12. La Oficina de Tecnología de la Información y Gobierno Digital debe establecer directrices para el manejo adecuado de los activos de información, asegurando que se protejan durante su ciclo de vida.
- 9.4.13. La Oficina de Tecnología de la Información y Gobierno Digital debe establecer el procedimiento para la gestión de medios removibles considerando las labores realizadas por los servidores de acuerdo a la necesidad de uso.
- 9.4.14. La Oficina de Tecnología de la Información y Gobierno deberá crear lineamientos de disposición de medios que garanticen que los medios de almacenamiento que no son necesarios o que estén obsoletos sean desechados de manera segura, asegurando que no se filtren datos sensibles.
- 9.4.15. La Oficina de Tecnología de la Información y Gobierno debe establecer normas claras para la transferencia de medios físicos de información, asegurando que los datos sean protegidos durante su traslado.

Aprobado mediante Resolución de Gerencia Municipal N° 017-2025-GM-MDS

Pág. 11



Municipalidad Distrital de Sayán
Gerencia Municipal

DIRECTIVA N° 003-2025-GM/MDS

"Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán"

9.5. DE LA SEGURIDAD DE LOS RECURSOS HUMANOS.

La Municipalidad Distrital de Sayán a través de la Oficina de Gestión de Recursos Humanos debe promover una cultura de seguridad de la información, de tal manera que las acciones de los servidores no conduzcan a poner en riesgo a la confidencialidad, integridad y disponibilidad de la información de la entidad, de la misma manera se tendrá que aplicar los siguientes lineamientos:

- 9.5.1. La Oficina de Gestión de Recursos Humanos debe verificar los antecedentes laborales de la persona seleccionada y las competencias requeridas para el puesto.
- 9.5.2. Aplicar la normativa vigente y los criterios necesarios para incluir en los acuerdos contractuales o conductuales de empleo, compromisos de confidencialidad de la información y cumplimiento de las normas internas de la MUNICIPALIDAD DISTRITAL DE SAYAN.
- 9.5.3. La Oficina de Gestión de Recursos Humanos debe informar a la persona contratada de las responsabilidades administrativas y judiciales por el no cumplimiento de las disposiciones de la Seguridad de la Información.
- 9.5.4. La Oficina de Gestión de Recursos Humanos debe fortalecer el compromiso del personal con la Seguridad de la Información a través de programas de inducción para el personal que se vincule a la MUNICIPALIDAD DISTRITAL DE SAYAN, así como actualizaciones regulares de corresponder.
- 9.5.5. La Oficina de Gestión de Recursos Humanos debe comunicar a la Oficina de Tecnología de la Información y Gobierno Digital, el inicio o rotación del vínculo laboral del personal para el otorgamiento de los correspondientes accesos a los sistemas de información, con una anticipación no menor a dos (2) días hábiles a la fecha prevista para el inicio de las labores del personal.
- 9.5.6. La Oficina de Gestión de Recursos Humanos debe comunicar a la Oficina de Tecnología de la Información y Gobierno Digital, la finalización del vínculo laboral del personal para la baja de accesos correspondiente, con una anticipación no menor a un (1) día hábil a la fecha prevista para la extinción del vínculo laboral.
- 9.5.7. La Oficina de Tecnología de la Información y Gobierno Digital deberá ejecutar la "baja" efectiva de los accesos a las aplicaciones, grupos de colaboración y sistemas de información el último día del periodo del vínculo laboral del personal.
- 9.5.8. La Oficina de Gestión de Recursos Humanos deberá establecer procedimientos y responsabilidades para gestionar acciones disciplinarias en caso de que los empleados, contratistas o cualquier persona con acceso a la información infrinja políticas y controles establecidos para la seguridad de la información.

9.6 DE LOS CONTROLES DE ACCESOS.

Referido a los accesos a sistemas y demás recursos informáticos, la Oficina de Tecnología de la Información y Gobierno Digital, debe:

Aprobado mediante Resolución de Gerencia Municipal N° 017-2025-GM-MDS

Pág. 12

Calle Plaza de Armas Sur Mza. 17, Lote 1 – Sayán





Municipalidad Distrital de Sayán
Gerencia Municipal

DIRECTIVA N° 003-2025-GM/MDS

"Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán"

- 9.6.1. La Oficina de Tecnología de la Información y Gobierno Digital debe establecer los procedimientos formales para asignar los derechos de acceso a los recursos de información relacionados con los servicios de TI y sistemas de información.
- 9.6.2. Establecer criterios de responsabilidad, basado en la personalización e individualización de los usuarios, a fin de que los mismos, sean responsables del adecuado uso de los accesos concedidos.
- 9.6.3. Definir criterios mínimos de establecimiento de contraseña y cambios periódicos de la misma, de acuerdo a la capacidad operativa y las buenas prácticas.
- 9.6.4. Los Gerentes, Subgerentes y Jefes de las distintas unidades orgánicas de la MUNICIPALIDAD DISTRITAL DE SAYAN, deben solicitar a la Oficina de Tecnología de la Información y Gobierno Digital la alta y baja de accesos a los servicios de TI, sistemas de información para el personal, locadores y proveedores de servicios a su cargo, indicando los niveles de acceso o privilegios.
- 9.6.5. La Oficina de Tecnología de la Información y Gobierno Digital debe generar, a la comunicación del inicio de vínculo laboral de los servidores por parte de la Oficina de Gestión de Recursos Humanos, las credenciales de acceso que identifique única y exclusivamente al servidor para el uso de los siguientes servicios de TI y sistemas de información, y revocar los mismos en el manifiesto de la desvinculación laboral o rotación:
- Dominio.
 - Intranet, sistema de gestión documentaria.
 - Correo electrónico institucional y herramientas colaborativas.
- 9.6.6. El acceso privilegiado debe realizarse desde dispositivos debidamente fortalecidos para tal fin.
- 9.6.7. Revisar periódicamente los accesos concedidos para validar su vigencia o caducidad.
- 9.6.8. Asegurar que los derechos de acceso sean ajustados o removidos de manera adecuada cuando ya no sean necesarios o cuando un usuario cambie de rol, transferido o finalice su vínculo laboral.
- 9.6.9. Garantizar la aplicación de buenas prácticas de seguridad en cuanto a la elección y uso de contraseñas considerando contener como mínimo, un carácter numérico, un carácter alfabético en mayúscula y uno en minúscula.
- 9.6.10. Garantizar que las credenciales de los usuarios (contraseñas, PINs y otros mecanismos de autenticación) sean manejadas de forma segura y cumplan con los estándares de seguridad establecidos.
- 9.6.11. Establecer un sistema de monitoreo para registrar intentos de acceso fallido y políticas de bloqueo o desconexión de sesiones inactivas, que permitan un acceso protegido y evitar accesos no autorizados
- 9.6.12. Implementar una política de bloqueo de pantalla, a fin de evitar el acceso no autorizado y el uso indebido de la información en los equipos PC.



“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

- 9.6.13. Implementar mecanismos y/o procedimientos para el control de acceso de equipos externos (personales, de visitantes o proveedores) estableciendo las restricciones de acceso correspondientes.
- 9.6.14. El acceso a las redes de comunicaciones y recursos de red internos y externos debe ser gestionado por la Oficina de Tecnología de la Información y Gobierno Digital de manera que el personal no comprometa la seguridad de los activos de información.
- 9.6.15. La Oficina de Tecnología de la Información y Gobierno Digital, para el correcto control de acceso de las redes de comunicaciones deberá tener en cuenta la segmentación, tipo, ubicación y modalidad.
- 9.6.16. La Oficina de Tecnología de la Información y Gobierno Digital, deberá implementar las pautas de control de acceso a los sistemas de información que garanticen la restricción efectiva para uso exclusivo del personal debidamente autorizado.
- 9.6.17. Definir los mecanismos de control de acceso al ambiente, tales como sistemas de acceso biométrico o similares, así mismo determinar el respectivo mecanismo para monitorear y registrar los accesos.
- 9.6.18. Todos los servidores de la MUNICIPALIDAD DISTRITAL DE SAYAN deberán proteger (no compartir y/o divulgar) los accesos asignados, puesto que estos son personales e intransferibles, y la responsabilidad de su uso recae sobre el/la titular de las mismas.
- 9.6.19. La Oficina de Tecnología de la Información y Gobierno Digital, deberá gestionar los derechos de accesos privilegiados, y sólo deben ser otorgadas al personal de nivel técnico apropiado y únicamente para el cumplimiento de sus funciones.
- 9.6.20. Una credencial de acceso privilegiado sólo debe ser utilizada en la actividad de administración o configuración del sistema para la cual se requieren dichos privilegios y deben ser registrados y controlados periódicamente.
- 9.6.21. Las credenciales de acceso privilegiadas tales como “administrador”, “root” o similares que son definidas por defecto en los sistemas y componentes, no deben ser utilizadas siempre que sea posible generar cuentas de acceso privilegiados.
- 9.6.22. La Oficina de Tecnología de la Información y Gobierno Digital debe asegurar con contar con un mecanismo de recuperación de acceso privilegiado.
- 9.6.23. La Oficina de Tecnología de la Información y Gobierno Digital debe controlar y limitar el uso de programas utilitarios con privilegios elevados para proteger los sistemas de abusos o accesos no autorizados a funciones críticas.
- 9.6.24. La Oficina de Tecnología de la Información y Gobierno Digital debe garantizar que el acceso al código fuente de los sistemas de información sean estrictamente controlados para evitar modificaciones no autorizadas o vulneraciones de seguridad.



“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

9.7. DE LA SEGURIDAD DE AMBIENTES FÍSICOS.

La seguridad en las instalaciones y el entorno físico se alcanza mediante la adopción de medidas destinadas a prevenir, detectar, neutralizar y/o disminuir los riesgos que la amenazan, la Oficina de Tecnología de la Información y Gobierno Digital la Oficina General de Administración a través de la Oficina Abastecimiento deben clasificar las áreas físicas para definir el nivel de seguridad de las mismas, aplicando los siguientes lineamientos:

- 9.7.1. Identificar adecuadamente los ambientes físicos en cada local o sede, definiendo los niveles de acceso por cada ambiente, considerando la clasificación de la siguiente manera:

CLASIFICACIÓN	ETIQUETA	DESCRIPCIÓN
Pública	ÁREA PÚBLICA	Aquella zona que es de uso público y de recepción de personas externas (visitantes) a la Entidad.
Común	ÁREA COMÚN	Aquella zona de uso común para los servidores de la MUNICIPALIDAD DISTRITAL DE SAYAN.
Restringida	ÁREA RESTRINGIDA	Aquella zona donde la información que se genera, trata o almacena es crítica para la MUNICIPALIDAD DISTRITAL DE SAYAN. El acceso a este tipo de zonas requiere autorización y/o un control acceso.

- 9.7.2. Definir mecanismos de control de acceso a los ambientes de la MUNICIPALIDAD DISTRITAL DE SAYAN, tales como: personal de seguridad, cámaras de video vigilancia, puertas con cerraduras, entre otros que se considere necesario para proteger los activos de información.
- 9.7.3. Identificar y acondicionar las áreas y/o ambientes de acceso restringido, usados para el resguardo de la información física, con los respectivos mecanismos de control, especialmente para los ambientes que resguarden información sensible, clasificada y aquellas protegidas por la Ley de Protección de Datos Personales.
- 9.7.4. Identificar y acondicionar las áreas y/o ambientes de acceso restringido, usados para el resguardo de la información física, con los respectivos mecanismos de control, especialmente para los ambientes que resguarden información sensible, clasificada y aquellas protegidas por la Ley de Protección de Datos Personales.
- 9.7.5. El acceso a un área física clasificada como restringida está permitido para personas externas a la MUNICIPALIDAD DISTRITAL DE SAYAN, siempre que sea para un motivo específico, que se cuente con la autorización respectiva del jefe inmediato responsable del área en cuestión y debe estar siempre acompañado por un personal de la MUNICIPALIDAD DISTRITAL DE SAYAN.
- 9.7.6. Las áreas restringidas deben de contar con un sistema de circuito cerrado de videovigilancia o equivalente.



Municipalidad Distrital de Sayán
Gerencia Municipal

DIRECTIVA N° 003-2025-GM/MDS

“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

- 9.7.7. La Oficina de Tecnología de la Información y Gobierno Digital debe garantizar que el trabajo en áreas restringidas se realice bajo condiciones controladas, minimizando el riesgo de exposición o pérdida de información confidencial.
- 9.7.8. El Centro de Datos es una zona restringida y la Oficina de Tecnología de la Información y Gobierno Digital debe implementar los controles de acceso para su debida protección.
- 9.7.9. En relación al Centro de Datos, contar con un programa de mantenimiento de los equipos de Tecnologías de información y de los sistemas de acondicionamiento de temperatura, humedad y filtrado de aire, sistemas de energía ininterrumpida (UPS) y sistemas de detección y extinción de fuego, a fin de garantizar la protección de los equipos y la continuidad de los servicios.
- 9.7.10. La Oficina de Tecnología de la Información y Gobierno Digital debe proteger el Centro de Datos de fallas por falta de suministro de energía y otras anomalías eléctricas.
- 9.7.11. El Centro de Datos se debe mantener bajo una temperatura apropiada, mediante uso de aire acondicionado, controles de humedad y otros que se consideren pertinentes.
- 9.7.12. Identificar y acondicionar áreas de despacho y carga mediante un sistema de control de acceso para evitar el acceso no autorizado y la posible manipulación, robo de dispositivos o información confidencial.
- 9.7.13. Todos los servidores de la MUNICIPALIDAD DISTRITAL DE SAYAN bajo cualquier modalidad y régimen de contratación, deberán cumplir con las disposiciones establecidas para el acceso a los ambientes físicos, quedando prohibido cualquier intento de evasión o no cumplimiento del mismo, bajo responsabilidad.

9.8. DE LOS EQUIPOS INFORMÁTICOS

La Oficina de Tecnologías de la Información y Gobierno Digital, implementara los siguientes lineamientos:

- 9.8.1. Establecer, aplicar y monitorear los controles de seguridad para los equipos informáticos, se incluyen los equipos portátiles que según su necesidad son utilizados fuera de las sedes de la MUNICIPALIDAD DISTRITAL DE SAYAN.
- 9.8.1. La Oficina de Tecnología de la Información y Gobierno Digital debe garantizar la protección del cableado de la red de datos y los equipos de comunicaciones de fallas por falta de energía o protección física.
- 9.8.2. La Oficina de Tecnología de la Información y Gobierno Digital debe mantener un plan de mantenimiento preventivo de la infraestructura tecnológica incluyendo los equipos de cómputo, escaneo, impresión y servidores del Centro de Datos a fin de para garantizar la continuación de los servicios.
- 9.8.3. La Oficina de Tecnología de la Información y Gobierno Digital y su personal de asistencia técnica son los únicos autorizados para realizar instalaciones y configuraciones de los equipos de cómputo, escaneo e impresión.



"Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán"

- 9.8.4. La Oficina de Tecnología de la Información y Gobierno Digital deberá realizar la orientación necesaria a los usuarios respecto al procedimiento de bloqueo de sesión de sus equipos de cómputo cuando no se encuentren en su lugar de trabajo. Esto con el fin que la sesión del usuario no quede activa para evitar el uso inadecuado de terceros.
- 9.8.5. La Oficina de Tecnología de la Información y Gobierno Digital deberá realizar la orientación necesaria a los usuarios respecto mantener el escritorio del equipo de cómputo libre de información de uso interno propia de la institución, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- 9.8.6. La Oficina de Tecnología de la Información y Gobierno Digital debe garantizar que los equipos obsoletos o puestos a ser reutilizados que mantengan medios de almacenamientos deben ser verificados para asegurar que cualquier dato sensible se haya sobrescrito de manera segura.
- 9.8.7. La Oficina de Tecnología de la Información y Gobierno Digital debe garantizar que la información sensible no sea accesible cuando los empleados no estén en sus estaciones de trabajo, a través de la implementación de políticas de escritorio limpio y pantalla limpia.

9.9. DE LOS CONTROLES CRIPTOGRÁFICOS.

La Oficina de Tecnología de la Información y Gobierno Digital con el uso de controles de encriptación deberá:

- 9.9.1. La Oficina de Tecnología de la Información y Gobierno Digital debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión interna o externa de información, cuente con mecanismos de cifrado de datos, asimismo, deberá solicitar a los proveedores de servicios de comunicación y transmisión de datos que cumplan con lo señalado en este párrafo.
- 9.9.2. Establecer los criterios técnicos para la aplicación del cifrado de la información, en el marco de las necesidades de integridad y confidencialidad de la información.
- 9.9.3. En base a la viabilidad técnica, implementar el uso de herramientas para cifrar la información bajo un criterio de confidencialidad, y de acuerdo al nivel de exposición al riesgo. Dicho cifrado debe ser requerido y aprobado por el/la titular de la unidad de orgánica dueña de la información y evaluado por la Oficina de Tecnologías de la Información y Gobierno Digital.
- 9.9.4. Para los casos de la contratación de servicios informáticos en la nube, establecer o solicitar conexiones encriptadas, conforme a los lineamientos vigentes establecidos por la Secretaría de Gobierno Digital.
- 9.9.5. La Oficina de Tecnología de la Información y Gobierno Digital deberá informar a todos los servidores de la MUNICIPALIDAD DISTRITAL DE SAYAN bajo cualquier modalidad y régimen de contratación, que no debe intentar descifrar o acceder a la información protegida sin la autorización respectiva.



"Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán"

- 9.9.6. La Oficina de Tecnología de la Información y Gobierno Digital debe garantizar que las claves criptográficas sean gestionadas de manera segura durante todo el ciclo de vida de los sistemas, utilizando algoritmos estándar aprobados y adecuados según el propósito específico.

9.10. DE LA SEGURIDAD DE LAS OPERACIONES.

La Oficina de Tecnologías de la Información y Gobierno Digital debe contar con mecanismos para asegurar que sus operaciones e instalaciones de procesamiento de la información sean correctas y seguras, mitigando los riesgos de seguridad como las intrusiones no autorizadas y ejecución de código malicioso dentro de la infraestructura tecnológica de la MUNICIPALIDAD DISTRITAL DE SAYAN.

- 9.10.1. La Oficina de Tecnologías de la Información y Gobierno Digital debe mantener actualizados los procedimientos relacionados con la operación y administración de seguridad de la infraestructura tecnológica que soporta los sistemas de información, estableciendo responsabilidades y los recursos utilizados para su ejecución eficiente, asimismo, estos deben estar a disposición del personal autorizado.

- 9.10.2. La Oficina de Tecnologías de la Información y Gobierno Digital debe mantener actualizada la documentación relacionada con los manuales de configuración, operación y uso de los sistemas de información e la Entidad.

- 9.10.3. La Oficina de Tecnologías de la Información y Gobierno Digital debe mantener un registro de control de cambios de los sistemas de información, los equipos de comunicaciones, el centro de datos y bases de datos a través de la implementación de acciones y procedimientos orientados a asegurar que todo cambio siga un proceso planificado que incluya responsabilidades y canales de comunicación, identificación de los recursos comprometidos, pruebas de estrés, validación de controles de seguridad, reversión en caso de fallas y análisis de impacto.

- 9.10.4. Todo cambio debe ser solicitado a la Oficina de Tecnologías de la Información y Gobierno Digital por el propietario de la información, y se llevara un registro sobre cada solicitud de cambio. En caso se presente un problema con el cambio realizado, se revertirá al estado anterior al cambio.

- 9.10.5. La Oficina de Tecnologías de la Información y Gobierno Digital debe garantizar la capacidad de los recursos a fin de asegurar el óptimo desempeño y la continuidad de los sistemas de información y la infraestructura tecnológica que la soporta, también deberá realizar estudios sobre las proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la infraestructura tecnológica, así mismo se realizaran monitoreos continuos del uso de sus capacidades para advertir eventos e incidencias relacionadas.

- 9.10.6. Aplicar medidas necesarias para la prevención, detección y eliminación de código malicioso (malware) a nivel de equipos servidores de red, computadoras portátiles, estaciones de trabajo, tabletas, Smartphone, etc. Por lo que debe asegurar que los equipos computacionales de la MUNICIPALIDAD DISTRITAL DE SAYAN cuenten con herramientas antimalware capaces de detectar y eliminar amenazas y posibilitar su monitoreo, tanto para equipos estacionales (computadora de escritorio) como para equipos portátiles (Laptops) y equipos servidores. Dicha herramienta de protección de punto final debe disponer al menos del módulo antimalware con análisis en tiempo real y prevención de intrusos.



"Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán"

- 9.10.7. Establecer procedimientos y tareas para la actualización de software utilizados por la MUNICIPALIDAD DISTRITAL DE SAYAN, y monitorear la vigencia de licencias de software a fin de realizar las renovaciones respectivas para prevenir caer en el uso ilegal de software y la inoperatividad del mismo.
- 9.10.8. La Oficina de Tecnologías de la Información y Gobierno Digital debe establecer los procedimientos rutinarios para la generación y restauración de copias de respaldo de los sistemas de información hospedadas en el centro de datos de la MUNICIPALIDAD DISTRITAL DE SAYAN.
- 9.10.9. Se deberá clasificar y etiquetar las copias de respaldo que le permita la fácil identificación de los medios de almacenamiento, la información contenida y la ubicación física para su posterior ubicación y acceso a los medios que contienen la información resguardada del centro de datos.
- 9.10.10. Asegurar que los medios magnéticos utilizados en la realización de copias de respaldo estén resguardados en un ambiente adecuado (que reúna las condiciones óptimas de acondicionamiento, temperatura y humedad), y procurar que estén en un área con acceso restringido.
- 9.10.11. Dimensionar los recursos necesarios para garantizar las copias de respaldo, las mismas que deben ser presentadas a las áreas correspondientes para su adquisición.
- 9.10.12. Asegurar que los equipos y sistemas para la realización de copias de respaldo cuenten con mantenimiento para prevenir fallas e indisponibilidad del recurso. También, revisar periódicamente la vigencia tecnológica de los equipos y software utilizados para la realización de las copias y restauración de la información.
- 9.10.13. Implementar los controles de seguridad a los sistemas que son resultado de proyectos de interoperabilidad tecnológica, alineado a los estándares de Interoperabilidad del estado y considerando además los estándares internacionales, reforzando así la confianza digital.
- 9.10.14. Asegurar que los entornos de desarrollo, pruebas y operaciones estén claramente separados para evitar la contaminación de los sistemas de producción con código o configuraciones no verificadas y para reducir el riesgo de cambios no controlados.
- 9.10.15. Aplicar registro de actividades de operadores y administradores de los sistemas de la Oficina de Tecnología de la Información y Gobierno Digital, así como el registro de fallas de sistemas. Tener la capacidad, además, de generar registros de auditoría de ser requerido, así mismo mantener sincronizado los relojes de los Sistemas de Información con una fuente exacta que establezca la "Hora Oficial de la República del Perú", para garantizar la exactitud temporal de los registros.
- 9.10.16. Garantizar que la información contenida en los registros de sistemas sea protegida contra accesos no autorizados, alteraciones o destrucción, y que se encuentren disponibles para su auditoría en caso de ser necesario.



Municipalidad Distrital de Sayán
Gerencia Municipal

DIRECTIVA N° 003-2025-GM/MDS

“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

- 9.10.17. Garantizar que se realice el registro de todas las actividades relevantes realizadas por administradores y operadores de los Sistemas de TI, que permitan la auditoría y análisis de incidentes.
- 9.10.18. Garantizar que el software instalado en los sistemas operaciones sean seguros y autorizados, que no comprometan la seguridad de los sistemas de información.
- 9.10.19. Definir lineamientos para la identificación, evaluación y mitigación de vulnerabilidades técnicas en los sistemas operacionales y aplicaciones utilizadas por la Municipalidad Distrital de Sayán
- 9.10.20. Definir lineamientos para el control y restricción de instalación de software en los sistemas operacionales utilizados por los usuarios de la Municipalidad Distrital de Sayán, con el fin de prevenir software no autorizados que comprometan la seguridad de los sistemas informáticos.
- 9.10.21. Todos los servidores de la entidad son responsables de la copia de respaldo de su información que es tratada en su equipo PC o laptop asignado.

9.11. DE LA SEGURIDAD DE LA COMUNICACIONES.

La MUNICIPALIDAD DISTRITAL DE SAYAN debe contar con mecanismos para asegurar las redes de comunicaciones y la infraestructura que la soporta, mitigando los riesgos de seguridad como las intrusiones no autorizadas e interceptaciones de información tanto dentro como fuera de la Entidad.

- 9.11.1. La Oficina de Tecnología de la Información y Gobierno Digital debe establecer los procedimientos para la asignación, uso y revocación de las cuentas de dominio.
- 9.11.2. Asegurar que los equipos de cómputo cuenten con adherencia al dominio de la MUNICIPALIDAD DISTRITAL DE SAYAN a fin de garantizar el uso de cuentas de dominio como mecanismo de autenticación y control de acceso. En caso no sea posible la adherencia se debe optar por el uso de un grupo de trabajo.
- 9.11.3. Se asignará una cuenta de dominio individual al personal de la MUNICIPALIDAD DISTRITAL DE SAYAN, la cual debe permitir el inicio de sesión en un equipo de cómputo.
- 9.11.4. La cuenta de dominio asignada es de carácter individual, por consiguiente, ningún otro usuario debe utilizar una cuenta de dominio que no sea la suya.
- 9.11.5. Se debe gestionar la asignación de cuentas de dominio para terceros cuando se requiera el acceso de personal externo a los equipos informáticos y servicios de TI de la MUNICIPALIDAD DISTRITAL DE SAYAN. Una cuenta de dominio para terceros debe ser autorizado por los responsables de cada área quienes se responsabilizan de la custodia y uso del mismo.
- 9.11.6. El uso del dominio y las redes de comunicación interna debe estar restringido para realizarse mediante el uso de equipos de cómputo bajo la gestión de la MUNICIPALIDAD DISTRITAL DE SAYAN. El uso de dispositivos móviles personales será posible únicamente bajo autorización previa.

Aprobado mediante Resolución de Gerencia Municipal N° 017-2025-GM-MDS

Pág. 20



Municipalidad Distrital de Sayán
Gerencia Municipal

DIRECTIVA N° 003-2025-GM/MDS

“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

- 9.11.7. Cuando se requiera acceso remoto, para los esquemas de teletrabajo o acceso a servicios internos, debe ser efectivo mediante el uso de las cuentas de dominio asignadas.
- 9.11.8. Se debe garantizar la protección del servicio de internet contra ataques de intrusiones o denegación de servicio, así como el acceso a páginas no autorizadas.
- 9.11.9. Se debe promover la concientización a los usuarios respecto a las consideraciones de seguridad que deben adoptar para el adecuado uso del internet.
- 9.11.10. Se debe realizar el monitoreo de los servicios prestados por los proveedores a fin de asegurarse la adecuada provisión y operatividad de los servicios acordados.
- 9.11.11. Se debe supervisar las medidas de seguridad implementadas por parte de los proveedores de servicio.
- 9.11.12. El acceso a Internet es un servicio de TI que está disponible para todo el personal de la MUNICIPALIDAD DISTRITAL DE SAYAN para uso estricto de actividades laborales relacionadas con las funciones que desempeñan y no para uso con propósitos de índole personal o comercial.
- 9.11.13. Se habilitará el acceso a internet con navegación básica que permita el acceso a portales web con dominios relacionados a educación, gobierno, cultura, salud, política y economía, así como permitir el acceso al servicio de correo electrónico institucional y a los sistemas de información de la MUNICIPALIDAD DISTRITAL DE SAYAN.
- 9.11.14. Se podrá habilitar accesos a internet con navegación especial previa solicitud de autorización de los responsables de las áreas para que se permita el acceso a portales de redes sociales, video a demanda o a ambos. Los accesos habilitados estarán sujetos a controles y auditorías con la finalidad de garantizar el buen uso del servicio.
- 9.11.15. Las operaciones o actividades realizadas con el servicio de acceso a internet es de exclusiva responsabilidad del usuario exonerándose a la MUNICIPALIDAD DISTRITAL DE SAYAN de toda responsabilidad con respecto al uso del mismo.
- 9.11.16. Establecer criterios formales para envío y recepción masiva de correos, los mismos que deben considerar criterio de necesidad. Del mismo modo, se debe establecer reglas o políticas técnicas para el filtrado de correos no deseados.
- 9.11.17. Establecer criterios de restricción de acceso a la red municipal mediante autenticación con credenciales o autenticación multifactor.
- 9.11.18. Establecer criterios de uso para todos los servicios de red, debiendo alinearse a los estándares de seguridad de la información, minimizando configuraciones predeterminadas y desactivando servicios innecesarios.
- 9.11.19. Establecer y aplicar una adecuada segmentación de redes.
- 9.11.20. Asegurar que la infraestructura de comunicaciones tecnológicas esté adecuadamente identificada y diagramada; los equipos tecnológicos que la componen deben poseer los elementos de seguridad mínimas tales como, claves de acceso, manejo de protocolos de cifrado, monitoreo de operatividad, log de eventos y respaldo de configuraciones.

Aprobado mediante Resolución de Gerencia Municipal N° 017-2025-GM-MDS

Pág. 21



“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

9.11.21. Los servicios prestados por la MUNICIPALIDAD DISTRITAL DE SAYAN a través de Internet (servicios Web) deben contemplar medidas de seguridad del tipo TLS (siglas del inglés Transport Layer Security) o SSL (siglas del inglés Secure Sockets Layer), que son protocolos criptográficos que proporcionan seguridad en las comunicaciones de red a través de internet.

9.11.22. Garantizar que los usuarios participantes en la transferencia de información confidencial deben firmar acuerdos de confidencialidad, en el cual se deben especificar las obligaciones y responsabilidad de las partes en relación con la protección de la información transmitida.

9.12. DE LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

La MUNICIPALIDAD DISTRITAL DE SAYAN debe asegurar que los sistemas de información cumplan con los requisitos de seguridad para evitar pérdidas, modificación o mal uso de la información que se procese en ellas, así como proteger la confidencialidad, autenticidad e integridad de la información.

9.12.1. La Oficina de Tecnología de la Información y Gobierno Digital debe establecer un procedimiento para la adquisición, desarrollo y mantenimiento de los sistemas de información.

9.12.2. Mantener la documentación de los sistemas de información desarrollados con la finalidad de garantizar la ejecución de sus actividades y la realización de mantenimiento posterior.

9.12.3. Definir los criterios de seguridad de la información que deben ser contemplados para la adquisición, desarrollo y mantenimiento de los sistemas, y realizar su seguimiento, aun en caso que estos sean iniciados por otra área de la entidad.

9.12.4. Establecer y actualizar las disposiciones para el desarrollo de sistemas o aplicaciones, basado en la Norma Técnica Peruana vigente, referido a Ingeniería de Software y Sistemas, Procesos del Ciclo de Vida del Software, entre otros estándares aplicables, siendo de uso obligatorio para toda la MUNICIPALIDAD DISTRITAL DE SAYAN.

9.12.5. Incorporar recomendaciones de seguridad para el desarrollo seguro durante todas las etapas del desarrollo de software, con el objetivo de reforzar la confianza digital.

9.12.6. Incluir análisis y evaluaciones de vulnerabilidades a los sistemas desarrollados de manera interna o aquellos desarrollados por terceros, a fin de garantizar la seguridad de las aplicaciones.

9.12.7. Definir los criterios de seguridad de la información a través de redes públicas (internet), las cuales deberán estar protegidas contra accesos no autorizados, ataques cibernéticos y vulnerabilidad que comprometan la seguridad de los datos.

9.12.8. Definir los criterios de seguridad y control para la protección de transacciones realizadas en los servicios de aplicación, asegurando que los datos sensibles estén protegidos durante el proceso de transacción.





Municipalidad Distrital de Sayán
Gerencia Municipal

DIRECTIVA N° 003-2025-GM/MDS

"Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán"

- 9.12.9. Evaluar los aspectos técnicos de seguridad para la recepción de software donado y su viabilidad en el marco de los lineamientos de seguridad de la información establecidos, en el presente documento.
- 9.12.10. Garantizar que todos los cambios realizados en los sistemas informático, tanto de software como hardware, se gestionen de manera controlada y documentada para evitar impactos adversos en la seguridad de la información.
- 9.12.11. Garantizar que todas las aplicaciones que hayan sido modificadas, actualizadas o migradas a nuevas plataformas operativas sean revisadas para identificar posibles problemas de seguridad.
- 9.12.12. Garantizar que los cambios en los paquetes de software se gestionen de forma segura (uso de versiones controladas) y no comprometan la seguridad de la infraestructura de tecnología de información (evaluación de seguridad de paquetes).
- 9.12.13. Incorporar diseños y desarrollo de sistemas de información bajo principios de ingeniería de sistemas seguros para minimizar los riesgos de seguridad en su implementación y puesta en marcha.
- 9.12.14. Implementar ambientes de desarrollo seguro (acceso controlado y aislado) para minimizar los riesgos que comprometan la seguridad de los sistemas y datos sensibles.
- 9.12.15. Garantizar que los sistemas sean sometidos a pruebas de seguridad exhaustivas antes de su implementación o modificación (pruebas de penetración, evaluación de vulnerabilidad y pruebas de seguridad en entornos aislados) para identificar y mitigar posibles vulnerabilidades antes de su puesta en producción.
- 9.12.16. Verificar que los sistemas cumplan con los requisitos funcionales y de seguridad establecidos, cumpliendo con los estándares de la municipalidad antes de su puesta en producción.
- 9.12.17. Incorporar lineamientos de protección de datos de prueba, los mismo que deben ser restringidos, cifrados, monitorizados y destruidos al finalizar la fase de pruebas.
- 9.12.18. Toda unidad de organización, debe contar con la conformidad de la Oficina de Tecnologías de la Información y Gobierno Digital, en la adquisición de una aplicación o sistema de información, así como para contratar personal o empresa desarrolladora de software.
- 9.13. DE LA RELACIÓN CON LOS PROVEEDORES.**
- La MUNICIPALIDAD DISTRITAL DE SAYAN Con respecto a las relaciones con terceros y proveedores, bajo contratos, prestaciones de servicios o cualquier otro tipo de relación, debe garantizar la protección de sus activos de información accesibles, por lo tanto, se debe:
- 9.13.1. La Oficina General de Administración en coordinación con la Oficina de Abastecimiento debe incluir un acuerdo de confidencialidad, el cual formará parte del contrato de prestación de servicios como anexo.

“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

- 9.13.2. La Oficina General de Administración en coordinación con la Oficina de Abastecimiento debe incluir cláusulas específicas de seguridad de la información en sus acuerdos contractuales, en el cual se indiquen responsabilidades de cada parte en la relación a la protección de datos.
- 9.13.3. Todo Proveedor que tenga acceso a la información institucional de la MUNICIPALIDAD DISTRITAL DE SAYÁN está obligado a gestionar y comunicar vulnerabilidades de seguridad de la información relevantes de manera oportuna, a su vez adoptar controles para la prevención de ciberataques.
- 9.13.4. Todo Proveedor que tenga acceso a la información institucional de la MUNICIPALIDAD DISTRITAL DE SAYÁN debe realizar monitoreos periódicos de seguridad en los servicios proporcionados, utilizando auditorías regulares, cumplimiento de requisitos de seguridad acordados, así como la revisión de gestión de vulnerabilidades.

9.13.5. Todo proveedor que tenga acceso a información institucional de la MUNICIPALIDAD DISTRITAL DE SAYÁN, como consecuencia de la ejecución de un contrato u orden de prestación de servicios, debe cumplir con la cláusula de confidencialidad establecida en el contrato correspondiente, aun después de terminada la relación contractual o laboral, a fin de salvaguardar la información a la que tuvo acceso.

9.13.6. La Oficina General de Administración en coordinación con la Oficina de Abastecimiento debe incluir procedimientos formales de gestión de cambios en los servicios de los proveedores, la cual debe seguir un proceso de notificación, evaluación, aprobación e implementación segura del cambio. Finalmente ejecutar una evaluación de impacto de seguridad.

9.13.7. El acceso a los recursos informáticos por parte de proveedores (terceros), debe contar con la opinión previa del Oficial de Seguridad de la Información y autorizado por la Oficina de Tecnología de la Información y Gobierno Digital o de acuerdo a lo establecido en el contrato u orden de servido.

9.14. DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Se adoptarán una serie de acciones para la gestión de incidentes de seguridad de la información con la finalidad de adoptar acciones preventivas y correctivas que correspondan.

9.14.1. Analizar los incidentes que son reportados a efectos de adoptar las medidas correspondientes de atención y proponer y/o delegar acciones preventivas para eventos futuros.

9.14.2. Se realizará el registro de incidentes de la seguridad de la información reportados.

9.14.3. Establecer y mantener actualizado un Plan de Contingencia de Tecnologías de la Información para la atención de Incidentes graves de seguridad en el ámbito informático.

9.14.4. Analizar y atender los incidentes informáticos y aplicar las medidas respectivas o previamente establecidas. Posteriormente analizar las actividades realizadas y estudiar posibles mejoras o cambios, que de considerarlo necesario puedan proponerse al Comité de Gobierno Digital para prevenir la ocurrencia de incidentes de Seguridad de la Información a nivel informático.



Municipalidad Distrital de Sayán
Gerencia Municipal

DIRECTIVA N° 003-2025-GM/MDS

“Disposiciones de Seguridad de la Información para el desarrollo e Implementación del Sistema de Seguridad de la Información de la Municipalidad Distrital de Sayán”

- 9.14.5. Conformar y designar un equipo de respuesta ante incidentes de ciberseguridad. Además, establecer las disposiciones o procedimientos para la atención de dichos incidentes, manteniendo los principios de integridad, disponibilidad, confidencialidad y la protección de los datos personales según corresponda, y en concordancia con las normativas vigentes relacionadas, sin desmedro del equipo de respuesta ante incidentes de ciberseguridad que pueda ser conformado a nivel sectorial.
- 9.14.6. Reportar los incidentes de seguridad, relacionados a los activos informáticos, a la oficina de Tecnologías de la Información y Gobierno Digital, conforme al procedimiento que se establezca para tal fin. Cualquier otra incidencia de seguridad debe ser informada a el Oficial de Seguridad de la Información, para la adopción de las medidas dispuestas, de ser pertinente.
- 9.14.7. Establecer los procedimientos para la identificación de debilidades de seguridad de la información (internos o externos), las cuales deben ser reportadas a la Oficina de Tecnología de la Información y Gobierno Digital encargos de gestionar los incidentes.
- 9.14.8. Establecer los criterios para la clasificación de eventos de seguridad de la información según su gravedad y tipo de incidentes, para su evaluación y priorización de incidentes.
- 9.14.9. Establecer criterios para la identificación, protección y conservación de evidencias relacionadas con los incidentes de seguridad de la información, las cuales deben incluir registros de sistemas, archivos clasificados, correos electrónicos, logs, datos de usuarios involucrados, etc.

9.15. DE LA CONTINUIDAD DE SERVICIOS DE TI.

La MUNICIPALIDAD DISTRITAL DE SAYAN, busca preservar la integridad, confidencialidad y disponibilidad de la información durante un hecho o durante una situación adversa ya sean éstos por desastre natural u ocasionados por error humano.

- 9.15.1. La Oficina de Tecnología de la Información y Gobierno Digital debe incluir la continuidad de la seguridad de la información dentro del proceso de gestión de continuidad operativa para actuar de manera efectiva ante algún posible evento que pudiera afectar la disponibilidad de la información y validar la efectividad de los controles de continuidad de la seguridad de la información que se han implementado.
- 9.15.2. La Oficina de Tecnología de la Información y Gobierno Digital debe desarrollar, implementar y mantener un Plan de Continuidad de la Seguridad de la Información, incluyendo evaluación de riesgos, recuperación y asignación de responsabilidades.
- 9.15.3. La Oficina de Tecnología de la Información y Gobierno Digital debe incluir pruebas periódicas del Plan de Continuidad de Seguridad de la Información, incluyendo simulaciones de incidentes reales, fallos de sistemas críticos, pérdida de datos, ciberataques, etc., debidamente documentada, y los resultados deben ser revisados para identificar oportunidades de mejora en el plan.
- 9.15.4. La Oficina de Tecnología de la Información y Gobierno Digital debe mantener redundancia a nivel de enlace de telecomunicaciones, servidores, base de datos y los otros recursos tecnológicos que asegure la continuidad de los sistemas de información que considere indispensables.