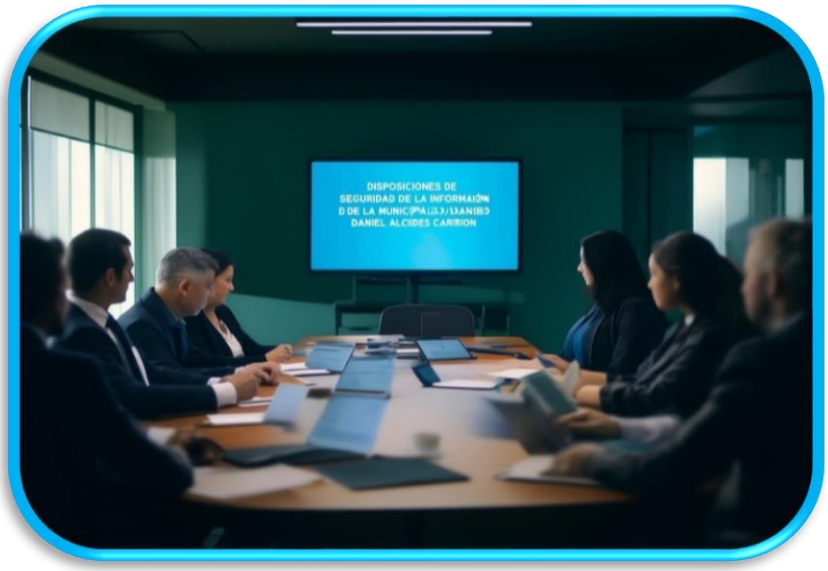
"Año de la Recuperación y Consolidación de la Economía Peruana"



DIRECTIVA

"DISPOSICIONES DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DANIEL ALCIDES CARRIÓN"

"Año de la Recuperación y Consolidación de la Economía Peruana"

DIRECTIVA				
VERSIÓN	**N° DE PAGINAS**	**RESOLUCIÓN DE APROBACIÓN**	**FECHA DE APROBACIÓN**	**N° DE DIRECTIVA**
01	33	000137-2025-MPDAC/A-GM	19-MARZO-2025	002-2025-MPDAC

DISPOSICIONES DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DANIEL ALCIDES CARRIÓN - 2025

RUBRO	NOMBRE	CARGO	FIRMA
REVISADO POR	EVARISTO ROQUE OLIVAS	JEFE DE LA OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN	Firmado digitalmente por ROQUE OLIVAS Evaristo FAU 20154623290 soft Motivo: Soy el autor del documento Fecha: 10.04.2025 08:35:19 -05:00
REVISADO POR	LUIS PRUDENCIO BLAS	GERENTE MUNICIPAL	Firmado digitalmente por PRUDENCIO BLAS Luis FAU 20154623290 soft Motivo: Soy el autor del documento Fecha: 11.04.2025 11:35:30 -05:00
REVISADO POR	AMADEO BERNAL CRISPÍN	JEFE DE LA OFICINA DE GENERAL DE ADMINISTRACIÓN	Firmado digitalmente por BERNAL CRISPIN Amadeo FAU 20154623290 soft Motivo: Soy el autor del documento Fecha: 10.04.2025 11:29:32 -05:00
REVISADO POR	ALEX MORALES GÓMEZ	JEFE DE LA OFICINA DE PLANEAMIENTO Y PRESUPUESTO	Firmado digitalmente por MORALES GOMEZ Alex FAU 20154623290 soft Motivo: Soy el autor del documento Fecha: 11.04.2025 10:13:02 -05:00
REVISADO POR	ROLYS BUSTILLOS BONILLA	GERENCIA DE DESARROLLO SOCIAL	Firmado digitalmente por BUSTILLOS BONILLA Rolys FAU 20154623290 soft Motivo: Soy el autor del documento Fecha: 10.04.2025 11:51:27 -05:00
REVISADO POR	LUIS ALACOTE QUICAÑO	GERENTE DE DESARROLLO URBANO Y RURAL	Firmado digitalmente por ALACOTE QUICAÑO Luis FAU 20154623290 soft Motivo: Soy el autor del documento Fecha: 10.04.2025 11:44:23 -05:00
REVISADO POR	LUIS ALBERTO CRUZ CORTEZ	GERENCIA DE DESARROLLO ECONÓMICO	Firmado digitalmente por CRUZ CORTEZ Luis Alberto FAU 20154623290 soft Motivo: Soy el autor del documento Fecha: 10.04.2025 11:48:07 -05:00
REVISADO POR	NORMA EDITH ESPINOZA LOYOLA	GERENCIA DE SERVICIOS PÚBLICOS Y GESTIÓN AMBIENTAL	Firmado digitalmente por ESPINOZA LOYOLA Norma Edith FAU 20154623290 soft Motivo: Soy el autor del documento Fecha: 11.04.2025 10:05:12 -05:00

1. OBJETIVO

Establecer las disposiciones que regulen la gobernanza de la seguridad de la información y el resguardo de los activos de información, recursos informáticos o plataformas tecnológicas donde se procesa y almacena información en la Municipalidad Provincial Daniel Alcides Carrión, frente a amenazas, internas o externas, deliberadas o accidentales con el fin de mitigar los riesgos.

2. FINALIDAD

Gestionar adecuadamente la seguridad de la información que permita asegurar la confidencialidad, integridad y disponibilidad de la información de la Municipalidad Provincial Daniel Alcides Carrión; así como también:

a) Establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información mediante la implementación de controles que permitan hacer frente a amenazas de ataque o intromisión, error, actos de la naturaleza (inundación, incendio, etc.) o vulnerabilidades inherentes a su uso, en cumplimiento de la Norma Técnica Peruana ISO/IEC 27001:2014 "Tecnología de la Información. Técnicas de Seguridad. Sistemas de Seguridad de la Información".

b) Garantizar el adecuado tratamiento de activos de información que incluya datos personales conforme a lo establecido en la Ley de Protección de Datos Personales, su Reglamento y demás normas relacionadas.

c) Promover y concientizar a los usuarios respecto a las responsabilidades por el uso de la información, así como del cumplimiento de las medidas y controles de Seguridad de la Información.

d) Cumplir con las normas legales y reglamentos estipulados por la ley y los organismos reguladores correspondientes, referidas a la seguridad de la información y protección de datos personales.

3. ALCANCE

Las disposiciones establecidas en la presente directiva son de observancia obligatoria para todo el personal bajo los distintos regímenes laborales de la Municipalidad Provincial Daniel Alcides Carrión.

Asimismo, es aplicable a las personas bajo contratos de locación y proveedores que prestan servicios a la Municipalidad Provincial Daniel Alcides Carrión cuyas obligaciones deberán estar consignadas en los acuerdos de confidencialidad que suscriban.

Comprende toda la información desarrollada, gestionada, transmitida, almacenada y de autoría propia de la Municipalidad Provincial Daniel Alcides Carrión, así como también, a todos los sistemas de información asociados con el almacenamiento, procesamiento y trasmisión de información generada por y a favor de la Municipalidad Provincial Daniel Alcides Carrión.

4. BASE NORMATIVA

- 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.
- 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 Nº 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 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 lo Bancos de Datos Personales.
- Resolución de Alcaldía N° 127-2023-MPDAC/A. emitido el 22 de mayo del 2023, que constituye el Comité de Gobierno Digital y Transformación Digital en la Municipalidad Provincial Daniel Alcides Carrión.
- Resolución de Gerencia Municipal N° 0409-2023-MPDAC/GM. emitido el 19 de octubre del 2023, que designa al Oficial de Seguridad de la Información en la Municipalidad Provincial Daniel Alcides Carrión

5. GLOSARIO DE TÉRMINOS

a) **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.

b) **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.

c) **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarlas de manera objetiva, para determinar el grado de cumplimiento de criterios pre-establecidos.

d) **Buzón compartido:** Es un buzón de correo electrónico virtual para permitir la recepción y envío de mensajes de correo desde una o más cuentas de correo de manera compartida, además permite compartir un calendario común. Un buzón compartido también puede servir como una cuenta de correo genérica.

e) **Clasificación de la Información:** Acción de identificar y clasificar los activos de información en términos de la sensibilidad e importancia para la Entidad.

f) **Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o entidades no autorizados.

g) **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.

h) **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.

i) **Comité de Gobierno Digital:** El Comité de Gobierno Digital (CGD) fue establecido con Resolución de Alcaldía N° 127-2023-MPDAC/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 Provincial Daniel Alcides Carrión.

j) **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.

k) **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.

l) **Disponibilidad:** Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada.

m) **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.

n) **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.

o) **Evento:** Un suceso que puede ser interno o externo a la Entidad, que ocurren en un momento determinado y son originados por una causa especifica.

p) **Grupo de colaboración:** Un grupo colaborativo es un espacio de trabajo de colaboración para mensajes de grupo, intercambio de archivos y calendario grupal integrado con los servicios de correo electrónico asignado al personal de la Municipalidad Provincial Daniel Alcides Carrión.

q) **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.

r) **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.

s) **Integridad:** Propiedad de precisión y completitud de la información.

t) **Jefe inmediato:** Para efectos de la presente Directiva se considera como jefe inmediato al responsable de la unidad orgánica conforme a la estructura orgánica establecida en el Reglamento de Organización y Funciones de la Municipalidad Provincial Daniel Alcides Carrión vigente.

u) **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.

v) **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.

w) **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 Gerencia Municipal N° 0409-2023-MPDAC/GM.

x) **Personal de la Municipalidad Provincial Daniel Alcides Carrión:** 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.

y) **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.

z) **Redes sociales:** Corresponde a los portales de redes sociales públicos como Facebook, Instagram, Twitter, etc.).

aa) **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).

bb) **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.

cc) **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.

dd) **Teletrabajo:** El teletrabajo consiste en la prestación de servicios subordinada, sin presencia física en la Municipalidad Provincial Daniel Alcides Carrión, 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.

ee) **Token:** Dispositivo de almacenamiento criptográfico que contiene el Certificado Digital asignado a la persona titular del mismo, que le permite firmar digitalmente.

ff) **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.

gg) **Usuario:** persona que hace uso de un recurso informático o servicio de tecnología de la información para fines laborales.

hh) **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.

ii) **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.

6. SIGLAS

- **CGD:** Comité de Gobierno Digital de la Municipalidad Provincial Daniel Alcides Carrión.
- **MPDAC:** Municipalidad Provincial de Daniel Alcides Carrión

- **NTP:** Norma Técnica Peruana
- **OGA:** Oficina General de Administración
- **OTDYAC:** Oficina de Trámite Documentario y Archivo Central
- **OAJ:** Oficina de Asesoría Jurídica
- **OPP:** Oficina de Planeamiento y Presupuesto
- **OTI:** Oficina de Tecnología de la Información
- **GM:** Gerencia Municipal
- **SGSI:** Sistemas de Gestión de la Seguridad de la Información
- **TI:** Tecnologías de la Información

7. DISPOSICIONES GENERALES

La Municipalidad Provincial Daniel Alcides Carrión gestiona, mantiene, monitorea, documenta y efectúa el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI) mediante 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.

Por ello se establece las siguientes disposiciones generales:

a) Todo lo contenido en este documento es de aplicación obligatoria por parte de todo el personal bajo los distintos regímenes laborales de la Municipalidad Provincial Daniel Alcides Carrión, las personas bajo contratos de locación y los proveedores que prestan servicios a la Municipalidad Provincial Daniel Alcides Carrión.
b) Toda información interna (generada por la de la Municipalidad Provincial Daniel Alcides Carrión, o externa (de propiedad de terceros) contenida en equipos informáticos, en medios físicos o digitales o en sistemas de información de la Municipalidad Provincial Daniel Alcides Carrión, están bajo custodia de la Entidad y por lo tanto deberán ajustarse a la presente Directiva de seguridad de la información.
c) Toda información que se intercambie con otras Instituciones públicas o privadas, deberá ser tratada conforme a los acuerdos de confidencialidad que se encuentren establecidos en la Entidad.
d) Todo responsable de la dirección del órgano o unidad orgánica deberá asegurar que el personal a su cargo conozca los niveles de sensibilidad y criticidad de la información que se maneja en su unidad.
e) Todo personal deberá utilizar los recursos informáticos y/o sistemas de información puestos a su disposición, de manera legal, profesional y ética.
f) Todo personal deberá aplicar las disposiciones de seguridad física, es decir prevenir accesos no autorizados, daños en las instalaciones y resguardar los equipos ubicándolos en áreas protegidas con controles de acceso adecuados.
g) 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.

8. DISPOSICIONES ESPECÍFICAS

8.1. Relativa a la organización de la Seguridad de la Información

La Municipalidad Provincial Daniel Alcides Carrión, busca establecer un marco de referencia para la implementación, gestión y operación de la Seguridad de la Información dentro de la Entidad.

8.1.1. Segregación de funciones

El CGD debe segregar funciones para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de información de la organización, así como para garantizar la protección de los activos de información y la gestión de riesgos de Seguridad de la Información.

8.1.2. Gestión de servicios y proyectos de Tecnologías de la Información (TI)

La OTI debe integrar la seguridad de la información en sus procesos de gestión de servicios y proyectos de TI, para garantizar que los riesgos de seguridad de la información sean identificados y tratados pertinentemente.

8.1.3. Dispositivos móviles

La Municipalidad Provincial Daniel Alcides Carrión, 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 Provincial Daniel Alcides Carrión, o bienes personales autorizados, donde toda información de la entidad que se almacena, transfiere o procesa siguen perteneciendo a la Municipalidad Provincial Daniel Alcides Carrión, por lo que la entidad mantiene el derecho a controlar dicha información, aunque no sea propietaria del dispositivo.

Obligaciones:

a) La OTI debe gestionar el proceso de habilitación de los dispositivos móviles incluyendo su administración, instalación de aplicaciones, configuración de seguridad y asistencia técnica.
b) 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 Provincial Daniel Alcides Carrión.

Prohibiciones:

a) El personal de la Municipalidad Provincial Daniel Alcides Carrión no debe utilizar los dispositivos móviles para uso distinto a las actividades laborales.
b) El personal de la Municipalidad Provincial Daniel Alcides Carrión, no debe permitir el acceso y uso de su dispositivo móvil por parte de otras personas no autorizadas ni debe transferir información de la Municipalidad Provincial Daniel Alcides Carrión, a otros dispositivos personales.

8.1.4. Teletrabajo y trabajo remoto

La de la Municipalidad Provincial Daniel Alcides Carrión, permite el uso del teletrabajo y trabajo remoto para habilitar la ejecución de funciones del personal mediante el uso de equipos informáticos fuera de la Entidad, ya sean estos bienes de propiedad de la Municipalidad Provincial Daniel Alcides Carrión, o bienes personales autorizados, donde toda información que se almacena, transfiere o procesa siguen perteneciendo a la de la Municipalidad Provincial Daniel Alcides Carrión, por lo que la entidad mantiene el derecho a controlar esos datos, aunque no sea propietaria del dispositivo.

Obligaciones:

a) La OGA, mediante la Oficina de Bienes Patrimoniales, debe gestionar la habilitación de los equipos informáticos en el esquema de teletrabajo, de acuerdo a los requerimientos remitidos por las áreas usuarias y la disponibilidad presupuestal de la Entidad.
b) La OTI debe gestionar la administración e instalación de software y aplicaciones, la configuración de seguridad y la asistencia técnica para los equipos informáticos utilizados en el esquema de trabajo remoto.
c) La OTI debe aplicar el mecanismo de conexión remota segura mediante VPN o similar.
d) El usuario debe de asegurar que dispone de un entorno de trabajo adecuado y seguro para proteger el equipo y las credenciales de acceso a los sistemas e información de los que es responsable.

8.2. Seguridad relativa a los recursos humanos

La Municipalidad Provincial Daniel Alcides Carrión debe promover una cultura de seguridad de la información, de tal manera que las acciones del personal de la Municipalidad Provincial Daniel Alcides Carrión, no conduzcan a poner en riesgo a la confidencialidad, integridad y disponibilidad de la información de la entidad.

8.2.1 Previo al vínculo laboral

Obligaciones:

- La OGA debe verificar los antecedentes laborales de la persona seleccionada y las competencias requeridas para el puesto.
- La OGA debe establecer en el Contrato Administrativo de Servicios, las cláusulas de confidencialidad de la información, de derecho de autor y de protección de datos personales, según corresponda.
- La OGA debe informar a la persona seleccionada de las responsabilidades administrativas y judiciales por el no cumplimiento de las disposiciones de la Seguridad de la Información.

8.2.2 Durante el vínculo laboral

Obligaciones:

- La OGA 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 Provincial Daniel Alcides Carrión, así como actualizaciones regulares de corresponder.

- La OGA debe coordinar con el Oficial de Seguridad de la Información, los contenidos de inducción y capacitación sobre seguridad de la información, incluyendo políticas, normas y directivas sobre la materia.
- La OGA debe comunicar al personal sus responsabilidades con respecto a la Seguridad de la Información según las funciones o actividades que realicen.
- La OGA debe comunicar a la OTI, 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.
- La OTI debe ejecutar la "alta" efectiva de los accesos a las aplicaciones, grupos de colaboración y sistemas de información con un (1) día hábil de anticipación a la fecha prevista para el inicio de las labores del personal.
- La OGA comunica a la Secretaría Técnica de los Procedimientos Administrativos Disciplinarios, los actos que suponen el incumplimiento de las disposiciones de seguridad de la información establecidos en el presente instrumento, a fin que se lleve a cabo la precalificación de la supuesta conducta infractora y de ser el caso se disponga el inicio del Procedimiento Administrativo Disciplinario.

8.2.3 Al término del vínculo laboral

Obligaciones:

- La OGA debe comunicar a la OTI, 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.
- La OGTA debe comunicar inmediatamente a la OTI, en los casos en los cuales los órganos y/o unidades orgánicas informen sobre ceses o renuncias autorizadas el mismo día, sin considerarse la comunicación previa de un (01) día de antelación.

- La OTI debe 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.

8.3 Seguridad relativa a los activos de información

8.3.1 Inventario de activos de información

Obligaciones:

- La OTI debe mantener un inventario de activos de sistemas de información actualizado semestralmente.
- La OGA, mediante la Unidad de Bienes Patrimoniales, debe mantener un inventario de equipos informáticos actualizado y revisado semestralmente.

8.3.2 Uso de activos de información

Obligaciones:

- Todo personal debe usar los activos de información para los fines y objetivos de la Municipalidad Provincial Daniel Alcides Carrión, bajo el criterio de buen uso y de acuerdo con las normas, políticas y procedimientos que se definan en la Entidad.

- Todos los órganos y unidades orgánicas de la Municipalidad Provincial Daniel Alcides Carrión, deben cumplir con los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo la presente Directiva.
- Todos los órganos y unidades orgánicas de la Municipalidad Provincial Daniel Alcides Carrión, deben inscribir aquellos activos de información (banco de datos) que estén amparados bajo la Ley de Protección de Datos Personales ante la Dirección General de "Transparencia, Acceso a la Información Pública y Protección de Datos Personales", de acuerdo al reglamento de registro de la mencionada ley; asimismo deberán cumplir y mantener actualizado el inventario de sus activos de información, así como su clasificación y ponderación tomando en cuenta la directiva de Seguridad de la Información administrada por los Bancos de Datos Personales.
- En el marco de las relaciones que la Municipalidad Provincial Daniel Alcides Carrión, establezca con terceros, mediante orden de servicio, convenios y contratos, deben de consignarse cláusulas o disposiciones referidas a la confidencialidad de la información, así como sobre la cesión de derechos, de corresponder.
- Solo podrán desempeñar sus funciones y actividades laborales utilizando los equipos informáticos administrados por la Municipalidad Provincial Daniel Alcides Carrión, ya sean estos asignados por la Unidad de Bienes Patrimoniales, provistos por medio de un servicio contratado y excepcionalmente, con equipos personales previamente autorizados

8.3.3 Retorno de activos de información

Obligaciones:

- La OGA, a través de la Unidad de Bienes Patrimoniales, debe supervisar el retorno de los equipos informáticos de la Entidad, asignados a los servidores que se desvinculan laboralmente de la Municipalidad Provincial Daniel Alcides Carrión.
- La OGA, a través de la Unidad de Bienes Patrimoniales, debe notificar a la OTI respecto a cada equipo de cómputo retornado para las acciones de preparación previa a una nueva asignación.
- La OGA debe de establecer el procedimiento para el retorno de los activos de información correspondiente a expedientes documentales de la Entidad de los servidores que se desvinculan laboralmente de la Municipalidad Provincial Daniel Alcides Carrión.

8.3.4 Clasificación de la información

Obligaciones:

- Todo personal debe considerar que toda información que posea la Municipalidad Provincial Daniel Alcides Carrión, 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.
- El acceso a información PÚBLICA está sujeto a los procedimientos dispuesto por establecidos en el Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública, y su Reglamento.

- Los propietarios de activos de información deben de clasificar la información que generan en cada proceso y/o proyecto, de acuerdo a los criterios establecidos en el Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública.
- Los propietarios de activos de información deben de etiquetar la información únicamente en caso de resultar clasificadas como CONFIDENCIAL o RESERVADA, así mismo, dicha clasificación debe ser notificada al Oficial de Seguridad de la Información para su registro en los inventarios correspondientes.
- No está permitido el traslado, la divulgación y exposición de la información clasificada como CONFIDENCIAL o RESERVADA.
- Toda desclasificación de información se hará cumpliendo lo señalado en la Ley de Transparencia y Acceso a la Información Pública y su Reglamento.
- Todo personal debe velar por la conservación y custodia de toda información.
- Todo personal que tenga acceso a información CONFIDENCIAL o RESERVADA debe ser consciente de la sensibilidad de la información que manejan y comprender a detalle sus responsabilidades relacionadas con la protección de la información.
- Los registros de información, que se encuentren documentados en papel, o medios electrónicos y tecnológicos deben estar almacenados y resguardados en una zona segura con acceso limitado a las personas no autorizadas.

8.3.5 Gestión de medios removibles

Obligaciones:

- La OTI debe establecer el procedimiento para la gestión de medios removibles considerando las labores realizadas por los servidores de acuerdo a la necesidad de uso.
- La OTI debe establecer los controles a las transferencias de información externas por medios físicos, manteniendo lineamientos para los servicios de mensajería y transporte de información en distintos soportes.

8.3.6 Disposición o reutilización segura de equipos y medios

Obligaciones:

- La OTI debe establecer y ejecutar los procedimientos para la disposición de los datos e información almacenados en los equipos informáticos y medios removibles a ser destruidos, donados o transferidos a un nuevo usuario.
- La OTI debe orientar a todo el personal respecto a su responsabilidad de mantener una copia de resguardo de los datos e información almacenados en los equipos de computación previo a su eliminación.

- La OTI debe solicitar la autorización a la jefatura de los órganos o unidades orgánicas correspondiente, para la eliminación de datos e información en equipos de cómputo que, por el uso posterior que se les den, requieran de dicha acción.
- Toda información almacenada en soportes externos (CD, DVD, unidades USB, tarjetas de memoria y papel) y en todos los equipos que tienen soporte de almacenamiento interno (equipos de cómputo, teléfonos móviles) deben ser borrados (formateado), o se debe destruir el soporte, antes de ser eliminados o reutilizados.
- La destrucción de información CONFIDENCIAL o RESERVADA debe realizarse por medios o mecanismos que no permitan su regeneración bajo ninguna circunstancia

8.4 Seguridad relativa al control de accesos

8.4.1 Gestión de acceso a recursos de información y estaciones de trabajo

Obligaciones:

- La OTI 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.
- La OTI debe implementar los controles necesarios para garantizar la autenticación y el acceso a los recursos de información relacionados con los servicios de TI y sistemas de información.
- La OTI debe gestionar el acceso a las estaciones de trabajo a fin de evitar accesos no autorizados a recursos o activos de información.
- La OTI debe verificar semestralmente que los usuarios tengan acceso permitido únicamente a aquellos recursos de información para los que fueron autorizados.
- Los responsables de las oficinas y unidades deben solicitar a la OTI 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.
- La OTI debe establecer las pautas para la asignación y cambio de contraseñas.
- La OTI debe generar, a la comunicación del inicio de vínculo laboral de los servidores por parte de la OGA, las credenciales de acceso que identifique única y exclusivamente al servidor para el uso de los siguientes servicios de TI y sistemas de información:
  - Acceso al Dominio
  - Acceso al Intranet de la Entidad
  - Acceso al Correo electrónico institucional y Herramientas colaborativas
- La OTI debe garantizar la aplicación de buenas prácticas de seguridad en cuanto a la elección y uso de contraseñas considerando que todo personal:
- Debe utilizar contraseñas con una secuencia de caracteres con al menos ocho caracteres de longitud, considerando contener como mínimo, un carácter numérico, un carácter alfabético en mayúscula y uno en minúscula.

- Debe cambiar su contraseña si existe un indicio de que haya sido vulnerado o estar en riesgo un activo de información (en ese caso, se debe reportar el incidente de seguridad).
- Debe cambiar las contraseñas por cada periodo de 3 meses o 90 días.
- Debe cambiar las contraseñas generadas por defecto en el primer ingreso a un sistema de información.
- No debe considerar información relacionada directamente con el usuario (nombre, fecha de nacimiento, DNI, etc.)
- No debe revelar las contraseñas a otras personas, incluyendo al personal de asistencia técnica de la OTI y a los administradores de los sistemas de información.
- No debe transferir o distribuir su contraseña por ningún medio (oral, escrito, electrónico, etc.) por ser estrictamente personal y de su responsabilidad.
- No debe llevar un registro de las contraseñas, a menos que se realice en un documento debidamente cifrado o encriptado mediante una contraseña que cumpla los niveles de complejidad descritos en el presente documento.
- No debe considerar el uso de las últimas dos contraseñas pasadas como nueva contraseña
- No debe almacenar contraseñas en un sistema de registro automatizado (por ej., macros o explorador).

8.4.2 Control de acceso a las redes de comunicaciones

Obligaciones:

- El acceso a las redes de comunicaciones y recursos de red internos y externos debe ser gestionado por la OTI de manera que el personal no comprometa la seguridad de los activos de información.
- El control de acceso debe tener en cuenta los siguientes aspectos:
  - Segmentación de las redes (personal de la Municipalidad Provincial Daniel Alcides Carrión o visitantes)
  - Tipo de red de comunicación (red de datos, telefonía fija, telefonía móvil)
  - Ubicación de usuario (acceso local o acceso remoto)
  - Modalidad de conectividad a red de datos (Cableada o inalámbrica).

8.4.3 Control de acceso en los sistemas de información

Obligaciones:

- La OTI debe establecer e implementar las pautas de control de acceso a los sistemas de información que garanticen la restricción efectiva para uso exclusivo del personal debidamente autorizado.
- La OTI debe gestionar el control de acceso, siempre que cuente con los mecanismos para controlar los accesos del sistema de información y mediante los administradores de los sistemas de información, quienes además de llevar un registro de accesos autorizados, deben revisar

semestralmente los accesos concedidos, revocando los derechos de cuya vigencia de autorización haya caducado.

- La OTI debe informar a los usuarios sobre las responsabilidades a la que conlleva los accesos provistos y la obligatoriedad de la confidencialidad y cambio de contraseña de acuerdo a la disposición establecida.
- La OTI debe implementar mecanismos físicos o lógicos para realizar el aislamiento o resguardo de sistemas de información con información sensible.

8.4.4 Gestión de derecho de acceso remoto

Obligaciones:

- La OTI 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.
- La OTI debe establecer los procedimientos para la asignación, uso y revocación del derecho de acceso remoto, el cual debe considerar la autorización del jefe inmediato y justificación de la necesidad.
- La OTI debe notificar cada habilitación de acceso remoto al Oficial de Seguridad de la Información para su correspondiente registro.
- La OTI 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.).

8.4.5 Gestión de derechos de acceso privilegiado

Obligaciones:

- La OTI debe establecer los procedimientos para la asignación, uso y revocación de los derechos de accesos privilegiados, el cual debe considerar la autorización del jefe inmediato y justificación de la necesidad.
- El control de acceso privilegiado debe ser gestionado por la OTI.
- Los derechos de acceso privilegiado sólo deben ser otorgadas al personal de nivel técnico apropiado y únicamente para el cumplimiento de sus funciones.
- Los accesos realizados con credenciales de acceso privilegiados deben ser registrados y controlados periódicamente.
- 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.
- Una credencial de acceso privilegiado no debe ser utilizada en actividades rutinarias para la que exista un perfil de menores privilegios que lo permita.
- 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.
- Se debe asegurar con contar con un mecanismo de recuperación de acceso privilegiado

- El acceso privilegiado debe realizarse desde dispositivos debidamente fortalecidos para tal fin.

8.5 Seguridad relativa a la criptografía

Obligaciones:

- La OTI 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.

8.6 Seguridad relativa a las instalaciones y el entorno físico

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, las mismas que se basan en el convencimiento de que no hay ningún peligro que temer al haberse adoptado las medidas necesarias para evitar todo riesgo.

8.6.1 Áreas físicas

Obligaciones:

- La OTI y la OGA, a través de la Unidad de Bienes Patrimoniales, deben clasificar las áreas físicas para definir el nivel de seguridad de las mismas, las cuales se describen como sigue:

Clasificación	***Etiqueta***	***Definición***
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 trabajadores de la Municipalidad Provincial Daniel Alcides Carrión.
Restringida	**ÁREA RESTRINGIDA**	Aquella zona donde la información que se genera, trata o almacena es crítica para la Municipalidad Provincial Daniel Alcides Carrión. El acceso a este tipo de zonas requiere autorización y/o un control acceso.

- Cada oficina o unidad orgánica, que sea responsable de un área física clasificado como restringida, debe implementar los controles necesarios para garantizar un acceso autorizado a dichos espacios físicos y las medidas de protección contra amenazas externas y ambientales considerando los siguientes, de corresponder:

  - Control de acceso
  - Video vigilancia y seguridad física
  - Control de humedad
  - Detectores de incendio o humo

- Extintores o sistema de extinción de fuego
- Sistema de puesta o pozo a tierra
- Sensores de aniegos
- Sistema de alimentación ininterrumpida (UPS)
- Grupo electrógeno
- Pararrayos

- Cada oficina o unidad orgánica, que sea responsable de un área física clasificado como restringida, deben verificar semestralmente que los usuarios tengan acceso permitido únicamente a aquellas áreas para los que fueron autorizados.
- El acceso a un área física clasificada como restringida está permitido para personas externas a la Municipalidad Provincial Daniel Alcides Carrión, 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 Provincial Daniel Alcides Carrión.
- Las áreas restringidas deben de contar con un circuito cerrado de video, sistema de video vigilancia o equivalente.
- El Centro de Datos es una zona restringida y la OTI debe implementar los controles de acceso para su debida protección.
- La OTI debe proteger el Centro de Datos de fallas por falta de suministro de energía y otras anomalías eléctricas.

8.6.2 Equipos de cómputo

Obligaciones:

- La OGA, a través de la Unidad de Bienes Patrimoniales, debe autorizar las solicitudes de traslados de bienes y/o activos a otra ubicación.
- La OGA, a través de la Unidad de Bienes Patrimoniales y la OTI deben garantizar la protección de los equipos informáticos de fallas por falta de suministro de energía y otras anomalías eléctricas.
- La OTI 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.
- La OTI debe brindar mecanismos necesarios para proteger la confidencialidad, integridad y disponibilidad de los equipos de cómputo dentro y fuera de las instalaciones de la Municipalidad Provincial Daniel Alcides Carrión.
- La OTI 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.

- La OGA, a través de la Unidad de Bienes Patrimoniales y la OTI deben mantener un plan de mantenimiento preventivo de los equipos de acondicionamiento de temperatura, humedad, filtrado de aire, sistemas de energía ininterrumpida (UPS) y detección o extinción de fuego a fin de garantizar su operatividad.
- La OTI y su personal de asistencia técnica son los únicos autorizados para realizar instalaciones y configuraciones de los equipos de cómputo, escaneo e impresión.

8.6.3 Equipos de usuarios desatendido

Obligaciones:

- La OTI debe promover y orientar 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.

8.7 Seguridad relativa a las operaciones

La Municipalidad Provincial Daniel Alcides Carrión, 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 Provincial Daniel Alcides Carrión.

8.7.1 Procedimientos operativos documentados

Obligaciones:

- La OTI 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.

- La OITEC debe mantener actualizada la documentación relacionada con los manuales de configuración, operación y uso de los sistemas de información e la Entidad.

8.7.2 Gestión de cambios

Obligaciones:

- La OTI 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.
- Todo cambio debe ser solicitado a la OTI 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.

8.7.3 Gestión de la capacidad

Obligaciones:

- La OTI 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.

- La OTI debe 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.
- La OITEC debe realizar un monitoreo continuo del uso de sus capacidades para advertir eventos e incidencias relacionadas.

8.7.4 Separación de entornos de desarrollo de software

Obligaciones:

- La OTI debe separar los entornos de desarrollo, control de calidad, aceptación de usuario y producción a fin de garantizar el mejor desempeño requerido por los sistemas de información durante todo su ciclo de vida.
- La OTI debe gestionar los recursos necesarios para la implantación de controles que permitan la separación de entornos.

8.7.5 Protección contra software y código malicioso:

La Municipalidad Provincial Daniel Alcides Carrión proporciona los mecanismos necesarios para garantizar la protección de la información y el equipamiento informático donde se procesa y almacena la información contra el hurto, modificación o daño ocasionados por el contagio de software malicioso.

Obligaciones:

- La OTI debe gestionar los controles para garantizar la prevención, detección y eliminación de software y código malicioso en todo equipo informático de la Municipalidad Provincial Daniel Alcides Carrión.
- La OTI debe asegurar que todas las estaciones de trabajo cuenten con el software antivirus y que estos se encuentren debidamente actualizados a fin de prevenir la ejecución de software malicioso.
- La OTI debe asegurarse que todas las aplicaciones y sistemas operativos se encuentren actualizados a fin de que minimicen los riesgos por vulnerabilidades.
- La OTI debe proveer asistencia técnica y ejecutar medidas de control frente a los reportes de incidentes de usuarios.

8.7.6 Respaldo de información

Obligaciones:

- La OTI 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 Provincial Daniel Alcides Carrión.
- La OTI debe 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.
- La OTI debe registrar las operaciones de respaldo ejecutadas.
- La OTI debe realizar pruebas de restauración en base a las copias de respaldo a fin de garantizar la recuperación de información en el momento de ser necesaria.

- La OTI debe establecer las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información de ser almacenadas externamente.
- La OTI debe evaluar periódicamente la vigencia tecnológica de la infraestructura de hardware y software utilizados para el respaldo y recuperación de la información.
- La OTI debe establecer los procedimientos para el almacenamiento y resguardo de información de las estaciones de trabajo de los usuarios para que se soporten bajo el servicio de almacenamiento en nube de la Municipalidad Provincial Daniel Alcides Carrión.

8.7.7 Registro y Monitoreo

Obligaciones:

- La OTI debe generar los registros de eventos de los sistemas de información tal como la activación de registros de auditoría, registros de uso de recursos y de conexiones.
- La OTI debe realizar un monitoreo de los registros para seguimiento e investigación de incidencias presentadas.
- La OTI debe gestionar los accesos a los repositorios de registros.
- Todos los servicios de TI y sistemas de información deben estar sujetos a un monitoreo por parte de la OTI

8.7.8 Control de software operacional

Obligaciones:

- La OTI debe implementar los mecanismos de restricción para la instalación de software en los equipos de cómputo.
- La OTI debe restringir y limitar el otorgamiento de privilegios para la instalación de software en los equipos de cómputo de la Municipalidad Provincial Daniel Alcides Carrión.
- La OTI debe autorizar todo software previo a su instalación en equipos de cómputo de la Municipalidad Provincial Daniel Alcides Carrión, así mismo es responsable por la validación del licenciamiento de corresponder para evitar el incumplimiento de uso ilegal de software.

8.8 Seguridad relativa a las comunicaciones

La Municipalidad Provincial Daniel Alcides Carrión, 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.

8.8.1 Acceso al dominio de la Municipalidad Provincial Daniel Alcides Carrión.

Obligaciones:

- La OTI debe establecer los procedimientos para la asignación, uso y revocación de las cuentas de dominio.
- La OTI debe asegurar que los equipos de cómputo cuenten con adherencia al dominio de la Municipalidad Provincial Daniel Alcides Carrión, 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 grupo de trabajo de la Municipalidad Provincial

Daniel Alcides Carrión.

- La OTI debe asignar una cuenta de dominio individual al personal de la Municipalidad Provincial Daniel Alcides Carrión, la cual debe permitir el inicio de sesión en un equipo de cómputo.
- 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.
- La OTI 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 Provincial Daniel Alcides Carrión. Una cuenta de dominio para terceros debe ser autorizado por los directores de Oficina y de Unidad quienes se responsabilizan de la custodia y uso del mismo.
- 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 Provincial Daniel Alcides Carrión. El uso de dispositivos móviles personales será posible únicamente bajo autorización previa.
- El acceso remoto, requerido para los esquemas de tele-trabajo o acceso a servicios internos, debe ser efectivo mediante el uso de las cuentas de dominio asignadas.

8.8.2 Acceso a internet

Obligaciones:

- La OTI debe garantizar la protección del servicio de internet contra ataques de intrusiones o denegación de servicio, así como el acceso a páginas no autorizadas.
- La OTI debe promover la concientización a los usuarios respecto a las consideraciones de seguridad que deben adoptar para el adecuado uso del internet.
- La OTI debe realizar el monitoreo de los servicios prestados por los proveedores a fin de asegurarse la adecuada provisión y operatividad de los servicios acordados.
- La OTI debe supervisar las medidas de seguridad implementadas por parte de los proveedores de servicio.

- El acceso a Internet es un servicio de TI que está disponible para todo el personal de la Municipalidad Provincial Daniel Alcides Carrión, para uso estricto de actividades laborales relacionadas con las funciones que desempeñan y no para uso con propósitos de índole personal o comercial.
- La OTI debe habilitar 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 Provincial Daniel Alcides Carrión.
- La OTI puede habilitar accesos a internet con navegación especial previa autorización de los jefes de Oficina y de Unidad 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 auditorias con la finalidad de garantizar el buen uso del servicio.
- Las operaciones o actividades realizadas con el servicio de acceso a internet es de exclusiva responsabilidad del usuario exonerándose a la

Municipalidad Provincial Daniel Alcides Carrión, de toda responsabilidad con respecto al uso del mismo.

8.8.3 Correos electrónicos

Obligaciones:

- La OTi debe asignar una cuenta de correo electrónico institucional a cada personal de la Municipalidad Provincial Daniel Alcides Carrión, la cual debe permitir enviar y recibir correos electrónicos internos y externos a la Municipalidad Provincial Daniel Alcides Carrión.
- La OTi puede asignar un buzón compartido cuando se requiera representar a un evento, un servicio o un sistema para enviar y recibir correos electrónicos internos o externos a la Municipalidad Provincial Daniel Alcides Carrión.
- La OTI puede asignar una cuenta de correo genérica únicamente cuando se requiera la generación de una credencial (usuario y contraseña) de acceso independiente para representar a un evento, un servicio o un sistema que requiera enviar y recibir correos electrónicos internos o externos a la Municipalidad Provincial Daniel Alcides Carrión.
- La OTI puede asignar una lista de distribución cuando se requiera el envío masivo de correos electrónicos a cuentas de correo electrónicos institucionales de la Municipalidad Provincial Daniel Alcides Carrión, de manera continua.
- La OTI puede asignar una cuenta de correo electrónico institucional a personas bajo contratos de locación y proveedores, la cual debe estar habilitada para enviar y recibir correos electrónicos internos y restringido para el envío de correos electrónicos externos a la Municipalidad Provincial Daniel Alcides Carrión.
- El uso del servicio de correo electrónico es de exclusiva responsabilidad del usuario titular de la cuenta exonerándose a la Municipalidad Provincial Daniel Alcides Carrión de toda responsabilidad con respecto al uso del mismo.
- El correo electrónico es para fines netamente laborales vinculadas a las funciones del personal y no debe permitir el envío de mensajes masivos a dominios públicos de internet.
- La OTI puede realizar la des-habilitación temporal o permanente de una cuenta de correo electrónico de evidenciarse un uso indebido que transgreda lo establecido en la presente directiva.
- La OTI debe garantizar la protección de las cuentas de correo electrónicos de accesos no autorizados, denegación de servicios o suplantación de identidad.
- La OTI debe promover la concientización a los usuarios respecto a las consideraciones de seguridad que deben adoptar para el adecuado uso y protección de los mensajes de correos electrónicos principalmente con la encriptación de mensajes durante el intercambio de información con destinatarios externos a la Municipalidad Provincial Daniel Alcides Carrión.

8.8.4 Segmentación de las redes

Obligaciones:

- La OTI debe mantener una red de datos segmentada por redes virtuales, grupos de servicios, grupos de usuarios, ubicación física o cualquier otra

tipificación que se considere conveniente en la Municipalidad Provincial Daniel Alcides Carrión, debiendo estar documentada en la arquitectura correspondiente.

- La OTI debe de segmentar la red de datos, sea esta cableada o inalámbrica, para aislar los accesos de visitantes de la red de datos del personal administrativo, de los servicios de TI y de los sistemas de información.
- La OTI debe implementar controles para minimizar los riesgos contra accesos no autorizados a la infraestructura de redes de comunicaciones interna y para salvaguardar la información de las estaciones de trabajo y los sistemas de información.

8.8.5 Transferencia de información

Obligaciones:

- La OTI debe establecer los controles a las transferencias e intercambios de información externas por medios físicos (medios removibles) y electrónicos (correos electrónicos, archivos compartidos o FTP) de tal manera que solo sea emitida y recibida íntegramente por las personas apropiadas y autorizadas en el momento y lugar oportuno.
- La OTI debe promover la concientización a los usuarios respecto a las consideraciones de seguridad que deben adoptar para el adecuado uso y protección de información clasificada como confidencial y sus restricciones para ser transferidas.

8.8.6 Acuerdos de confidencialidad o de no divulgación

Obligaciones:

- La OGA y la OAJ deben establecer los Acuerdos de Confidencialidad y/o de entrega de información con terceras partes, según corresponda.
- La OTI debe establecer los procedimientos y controles necesarios para el intercambio de información y debe promover el uso de mecanismos seguros en tecnologías de la información y redes de telecomunicaciones.

8.9 Seguridad relativa a la adquisición, desarrollo y mantenimiento de sistemas

La Municipalidad Provincial Daniel Alcides Carrión, 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.

8.9.1 Procesos y documentación de los Sistemas de Información

Obligaciones:

- La OTI debe establecer un procedimiento para la adquisición, desarrollo y mantenimiento de los sistemas de información.
- La OTI debe 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.

8.9.2 Requisitos de seguridad de los Sistemas de Información

Obligaciones:

- La OTI debe establecer en su metodología de desarrollo de software, los requerimientos de seguridad y buenas prácticas de desarrollo de software seguro, así como incluir el diseño de controles de seguridad durante las etapas de análisis y diseño de los sistemas de información.
- La OTI debe proporcionar a todo desarrollador de software las consideraciones elementales de seguridad de la información, controles, estándares y metodologías.
- Todo sistema de información desarrollado por el personal de la Municipalidad Provincial Daniel Alcides Carrión, es de propiedad de la Entidad.
- La OTI debe verificar que los acuerdos con locadores o proveedores sobre materia de adquisición o desarrollo de sistemas, incluyan clausulas relativas a la cesión de derechos a favor de la Municipalidad Provincial Daniel Alcides Carrión, y confidencialidad de la información para el resguardo de la propiedad intelectual de la Municipalidad Provincial Daniel Alcides Carrión.
- La OTI debe asegurarse que todo sistema de información, ya sea este adquirido o desarrollado, implemente los requisitos de seguridad establecidos y utilice los componentes de software debidamente licenciados.

8.9.3 Seguridad en los procesos de desarrollo y pase a producción

Obligaciones:

- La OTI debe asegurarse de que el desarrollo de los sistemas de información sea realizado conforme a los procedimientos establecidos en la NTP ISO/IEC 12207 y otros estándares similares.
- La OTI debe implementar controles para la puesta en práctica de procedimientos orientados a controlar el pase de sistemas de información desarrollados al entorno de producción.
- La OTI debe asegurar la disponibilidad y separación del entorno de desarrollo, entorno de control de calidad, entorno de aceptación de usuario y entorno de producción.
- La OTI debe garantizar una efectiva gestión de accesos a los entornos de producción previniendo accesos no autorizados por personal encargado del desarrollo y mantenimiento de sistemas de información.
- Todo nuevo sistema de información o actualización desarrollada debe ser revisado previamente en los entornos de control de calidad y el de aceptación de usuario antes de su pase a producción.
- El pase a producción mediante medios no automatizados debe ser realizado exclusivamente por el personal autorizado por la OTI, quien debe de registrar su actividad en una bitácora.

8.9.4 Gestión de vulnerabilidades de seguridad

Obligaciones:

- La OTI debe realizar semestralmente pruebas de comprobación técnica para verificar que se cuenta con los controles de seguridad debidamente implementados.
- La OTI debe asegurarse de implementar las recomendaciones resultantes posteriormente a la identificación de vulnerabilidades de seguridad y debe

de determinar los riesgos asociados e implementar los controles necesarios para mitigarlos. Los sistemas de información críticos y en alto riesgos deben ser priorizados.

- La OTI debe validar la efectividad de toda actualización propuesta en el entorno de control de calidad y debe cumplir con los controles establecidos para la gestión de cambios.

8.12. Sobre las relaciones con los proveedores

La de la Municipalidad Provincial Daniel Alcides Carrión, debe garantizar la protección de sus activos de información accesibles por los locadores y proveedores.

8.10.1 Seguridad con relación a los proveedores

Obligaciones:

- La OGA, a través de la Oficina de Logística, debe garantizar que todo proveedor de bienes y servicios suscriba un acuerdo de confidencialidad, el mismo que deberá ser parte del contrato.

- La OGA, a través de la Oficina de Logística, debe de requerir al proveedor, los datos completos de las personas que interactuarán directamente con la Municipalidad Provincial Daniel Alcides Carrión, incluyendo las funciones y responsabilidades asociadas a las actividades a realizar, así como las actualizaciones de cambios de dicho personal (alta, baja o cambio de funciones o responsabilidades) que se presenten durante la ejecución contractual.
- La OGA, a través de la Oficina de Logística, y las áreas usuarias, debe velar porque el proveedor y su personal cumpla con las consideraciones de seguridad aplicables de la presente Directiva.
- La Municipalidad Provincial Daniel Alcides Carrión, puede suministrar al proveedor de bienes y servicios información confidencial, relacionada con sus actividades, productos, servicios y/o su estrategia operativa únicamente si cuenta con una autorización previa por parte del propietario de dicha información.

8.11. Seguridad relativa a la gestión de incidentes de seguridad de la información

La Municipalidad Provincial Daniel Alcides Carrión, debe asegurar que los incidentes de seguridad de la información sean comunicados oportunamente a las instancias correspondiente con finalidad de adoptar acciones preventivas y correctivas que correspondan.

8.11.1 Gestión de incidentes y mejoras de seguridad de la información

Obligaciones:

- La OTI debe realizar el registro de incidentes de la seguridad de la información reportados.
- Los incidentes relativos a la seguridad de la información deben ser reportados a la OTI, conforme al procedimiento que se establezca para tal efecto.
- Se considerará como ataque a la seguridad de la información a cualquier actividad que se realice mediante la exploración y explotación de los recursos informáticos asignados por la Municipalidad Provincial Daniel

Alcides Carrión, siempre que estos se realicen sin la supervisión y/o autorización de la OTI.

- La OTI debe realizar una evaluación permanente de los controles de seguridad existentes en sus sistemas de información para proponer mejoras para prevenir la ocurrencia de futuros incidentes de seguridad de la información.
- La OTI debe garantizar la generación de una base de conocimiento para la asistencia de incidentes de la seguridad de la información.

8.11.2 Respuesta a incidentes de seguridad de la información

Obligaciones:

- La OTI debe disponer de canales de comunicación que permitan que el personal reporte incidentes de seguridad, eventos sospechosos y el mal uso de los recursos informáticos.

- La OTI debe asistir al reporte de un incidente de seguridad como un primer nivel, pudiendo escalar a un nivel superior para la búsqueda de remediación, así como reportarlo al Oficial de Seguridad de la Información para la evaluación de la criticidad del incidente.
- La OTI debe asignar responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.
- La OTI debe considerar la identificación, recolección, preservación y análisis de evidencias, durante el tratamiento de los incidentes.
- La OTI debe reportar los incidentes identificados como masivos o recurrentes al Oficial de Seguridad de la Información y de requerirse podrán ser evaluados por el Comité de Gobierno Digital de la Municipalidad Provincial Daniel Alcides Carrión, a efectos de adoptar acciones correctivas y preventivas.

8.12. Seguridad relativa a la continuidad de servicios de TI

La de la Municipalidad Provincial Daniel Alcides Carrión, 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 el hombre.

8.12.1 Continuidad de la seguridad de la información

Obligaciones:

- La OTI 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.
- La OTI debe validar la efectividad de los controles de continuidad de la seguridad de la información que se han implementado.

8.12.1. Redundancias

Obligaciones:

- La OTI 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.
- La OITEC debe asegurar que los componentes redundantes operan ante la ausencia o caída de los componentes principales.
- La OITEC debe asegurar la disponibilidad de copias de respaldo de información de servidores y la efectividad de su restauración en casos de recuperación de información.

8.13. Sobre el cumplimiento

La de la Municipalidad Provincial Daniel Alcides Carrión, busca prevenir el incumplimiento de las obligaciones legales, reglamentarias o contractuales relativas a la seguridad de la información y así garantizar una gestión de la seguridad de la información en concordancia con la Directiva de Seguridad de la Información de la Municipalidad Provincial Daniel Alcides Carrión.

8.13.1. Cumplimiento de los requisitos legales y contractuales

Obligaciones:

- La de la Municipalidad Provincial Daniel Alcides Carrión, debe establecer los términos, condiciones y finalidades para la protección de datos personales en cumplimiento con la Ley vigente.

- La OTI debe garantizar el uso de software legal que no atente contra los derechos de propiedad intelectual (software pirata, ilegal).
- La OTI debe implementar mecanismos para obtener el consentimiento para el tratamiento de datos personales con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar o transmitir dichos datos personales, en el marco de las actividades de la entidad.
- La Municipalidad Provincial Daniel Alcides Carrión, tiene los derechos de propiedad intelectual sobre todos los sistemas, aplicativos, manuales, y documentos físicos como digitalizados, desarrollados tanto por personal interno (de cualquier régimen laboral) como por personal externo (proveedores de servicios) que se encuentra en el dominio de la entidad.

8.13.2. Revisión independiente de la seguridad de la información

Obligaciones:

- La OTI debe realizar la supervisión del cumplimiento de procedimientos y políticas relacionadas con la Seguridad Informática y de la Seguridad de la Información que se implemente o estén implementados.
- La OTI debe planificar la pertinencia de auditorías periódicas internas y externas de seguridad de la información y con auditores independiente al proceso a auditar.

9. RESPONSABILIDADES

La Directiva de Seguridad de la Información es de cumplimiento obligatorio para todo el personal de la Municipalidad Provincial Daniel Alcides Carrión, incluyendo a personas bajo contratos de locación y proveedores que prestan servicios a la Municipalidad Provincial Daniel Alcides Carrión, ya sean del sector público o privado, cuyas obligaciones deberán estar consignadas en los acuerdos de confidencialidad que suscriban.

El incumplimiento de la presente Directiva dará lugar a la aplicación de medidas administrativas disciplinarias conforme a las disposiciones señaladas en los documentos normativos de la Entidad, sin perjuicio de la responsabilidad civil y/o penal a que hubiere lugar.

A continuación, se señalan los derechos, obligaciones o prohibiciones de los actores:

9.1 Sobre el personal de la Municipalidad Provincial Daniel Alcides Carrión.

9.1.1 Derechos

- Participar en la implementación y cumplimiento de las disposiciones de seguridad de la información, planes de continuidad, acciones de tratamiento de riesgos y acciones correctivas de acuerdo al alcance de sus funciones.
- Solicitar la asistencia técnica a la OTI para la habilitación o configuración de los equipos informáticos y software para su adecuado uso.
- Reportar o notificar a la OITEC cuando se tenga sospecha de que su contraseña es conocida por otra persona o de algún otro indicio de vulnerabilidad.

9.1.2 Obligaciones

- Proteger la información que se encuentre en las diferentes unidades de almacenamiento (físico y digital) y que esté bajo su administración o permiso de uso, aun cuando no se utilice y contenga información CONFIDENCIAL o RESERVADA.
- Utilizar exclusivamente los servicios e infraestructura institucional para todo flujo y trasmisión de información de propiedad de la Municipalidad Provincial Daniel Alcides Carrión.
- Utilizar los activos de información que le sean asignados sólo y exclusivamente para fines de sus funciones y actividades laborales, debiendo cumplir con los procedimientos formales de tratamiento e intercambio de información.
- Mantener la confidencialidad de las credenciales de acceso otorgadas y usarlas diligentemente, asumiendo la responsabilidad por las acciones que terceras personas puedan realizar.
- Realizar el cambio de su contraseña de acuerdo a la periodicidad establecida.
- Utilizar contraseñas seguras de acuerdo a todas las recomendaciones establecidas.
- Utilizar el software antivirus para el escaneo de software malicioso en los diferentes medios de almacenamiento interno o externo del equipo de cómputo.
- Bloquear su equipo de cómputo cuando se ausente de su lugar de trabajo, así como guardar en una ubicación segura sus documentos, medios magnético u óptico.
- Velar para que los archivos descargados provenientes de adjuntos de los

correos electrónicos, páginas web de internet o copiados de cualquier medio de almacenamiento, provengan de fuentes conocidas y seguras para evitar el riesgo de contagio de virus informáticos y/o instalación de software malicioso en el equipo de cómputo.

- Identificar, organizar y clasificar su información crítica para que pueda ser almacenada y respaldada bajo el servicio de almacenamiento en nube de la Municipalidad Provincial Daniel Alcides Carrión.
- Dejar toda información asignada bajo custodia al jefe inmediato o al que éste designe en caso de ausencia por vacaciones o licencias (> a 30 días) conforme a los procedimientos establecidos en las "Normas para la Entrega y recepción de Cargo del personal de la Municipalidad Provincial Daniel Alcides Carrión", que garantizan una adecuada trasferencia de funciones y continuidad de servicios en las distintas oficinas y unidades de la Municipalidad Provincial Daniel Alcides Carrión.
- Comunicar a su jefe inmediato en caso de evidenciar (ser testigo) una acción o evento que transgreda o que contravengan la presente directiva.

9.1.3 Prohibiciones

- Está prohibido el uso de información personal o fácilmente deducible como contraseña.
- Está prohibido que las contraseñas se encuentren en forma legible en cualquier medio impreso, así como dejarlos en lugares visibles o remitirlas por correo electrónico.
- Está prohibido almacenar las contraseñas en aplicativos, programas o sistemas que proporcionen esta facilidad.
- Está prohibida la inhabilitación, eliminación o cambio de la configuración del software de antivirus establecida por la Municipalidad Provincial Daniel Alcides Carrión.
- Está prohibido el envío de cadenas de mensajes (spam) con contenido comercial, político, religioso, discriminatorio y demás contenido que degraden la condición humana y resulte ofensivas.
- Está prohibido el reenvío de correos electrónicos institucionales que contengan información CONFIDENCIAL o RESERVADA hacia otros correos electrónicos que no sean de la Municipalidad Provincial Daniel Alcides Carrión, salvo autorización de su jefe inmediato o quien asuma sus funciones durante su ausencia.
- Está prohibido el uso de servicios de correo electrónico y servidores de almacenamiento no institucionales como los servicios gratuitos de Google, Hotmail, etc. para el intercambio y trasmisión de información de la Municipalidad Provincial Daniel Alcides Carrión.
- Está prohibido abrir correos electrónicos de remitentes desconocidos o con archivos adjuntos con contenido dudoso más aún si estos han sido identificados como correo no deseado o Spam.
- Está prohibido suscribir la cuenta de correo electrónico institucional en grupos, listas de interés o catálogos para recibir ofertas de productos o para recibir publicidad o información que no esté relacionada a las labores institucionales.
- Está prohibido el traslado físico de bienes y/o activos sin la autorización de su jefe inmediato y la Unidad de Bienes Patrimoniales.
- Está prohibido el uso de herramientas informáticas (hardware y software) para vulnerar los controles de seguridad informática, salvo previa autorización, planificación y supervisión de la OTI.

- Está prohibido escribir, generar, copiar, coleccionar, propagar, ejecutar o introducir cualquier tipo de código (programas maliciosos), desarrollados para auto replicar, dañar o afectar el funcionamiento o acceso a los equipos de cómputo, redes o información de la Municipalidad Provincial Daniel Alcides Carrión.

9.2 Sobre los Jefes de Oficina y de Unidad

9.2.1 Derechos

- Difundir las leyes, normas y reglamentos que regulen los temas sobre seguridad de la información, protección de datos personales y otras que salvaguarden los activos de información institucional.
- Designar y autorizar los permisos y privilegios de acceso para todo el personal a cargo, que accederá a los sistemas de información y plataformas informáticas.
- Delegar la gestión de accesos y nombrar administradores de sistemas de información siempre que esta característica esté disponible.
- Reportar las posibles brechas, incidentes y deficiencias en materia de seguridad de la información dentro de su ámbito de gobernanza, funciones y competencias.

9.2.2 Obligaciones

- Cumplir con la presente directiva y coadyuvar en la implementación del Sistema de Seguridad de la Información, garantizando la confidencialidad, disponibilidad e integridad de su información.
- Hacer cumplir las disposiciones de seguridad de la información al interior de cada órgano, unidad orgánica o área a su cargo, en el ámbito funcional, técnico y administrativo, según corresponda.
- Garantizar la confidencialidad de la información bajo su competencia, comprobando que las normas y reglamentos se cumplan.
- Inscribir los bancos de datos (digitales e impresos bajo su responsabilidad) en cumplimiento de la Ley de Protección de Datos Personales.
- Solicitar autorización a la Unidad de Bienes Patrimoniales de la OGA para la movilización o traslado físico de bienes a otra ubicación.
- Gestionar la solicitud de grupos de colaboración, listas de distribución, buzones compartidos, cuentas de acceso para locadores y proveedores de acuerdo a las necesidades de su oficina ante la OTI.
- Asegurar la incorporación de las consideraciones de seguridad de la información (organizativos, jurídicos y técnicos) asociados a la transferencia y/o acceso de información en los requerimientos de bienes y servicios.
- Asegurar que todo proveedor de servicio (directo y subcontratado) que trate información de la Municipalidad Provincial Daniel Alcides Carrión, conozca las políticas y procedimientos de seguridad que le sean aplicables y que suscriba un acuerdo de confidencialidad y de no divulgación.

9.3. Sobre el Oficial de Seguridad de la Información

9.3.1 Obligaciones

- Revisar y evaluar anualmente las políticas, objetivos, planes, normas, directivas, responsabilidades asociadas a la seguridad de la información para su adecuación a la normatividad vigente.
- Proponer al CGD las directivas, políticas, objetivos, planes, roles,

funciones y modificaciones necesarias para gestionar de manera eficiente y efectiva la seguridad de la información, para su aprobación por el titular de la Municipalidad Provincial Daniel Alcides Carrión.

- Coordinar, establecer y aplicar una metodología de gestión de riesgos.
- Auditar y evaluar el cumplimiento de los controles y las prácticas de seguridad de la información; debiendo comunicar al CGD de las faltas e infracciones al cumplimiento del contenido de las disposiciones establecidas.
- Identificar las necesidades de capacitación, difusión y sensibilización en seguridad de la información.
- Informar continuamente al personal de la Municipalidad Provincial Daniel Alcides Carrión, acerca de los objetivos, medidas y reglamentaciones en materia de seguridad de la información que se encuentren en vigencia.
- Evaluar los eventos reportados para actualizar la clasificación de los incidentes de seguridad de la información, evaluando la causa, probabilidad e impacto.
- Gestionar las acciones requeridas para desarrollar el análisis a profundidad de los incidentes reportados pudiendo solicitar la ejecución de técnicas más complejas como la informática forense, mediante un peritaje informático, de corresponder.
- Reportar los incidentes de seguridad de la información al Centro Nacional de Seguridad Digital de la Secretaría de Gobierno Digital, en su calidad de ente rector en gobernanza de datos.
- Reportar el estado de implementación del SGSI a la Secretaría de Gobierno Digital, en su calidad de ente rector en gobernanza de datos.
- Establecer contacto con grupos especializados en seguridad de la información y ciberseguridad a fin de garantizar el aprendizaje y la mejora continua del SGSI.

9.4. Sobre el personal bajo contrato de locación y proveedores

9.4.1. Obligaciones

- Utilizar los activos de información que le sean asignados sólo y exclusivamente para fines de las actividades establecidas según contrato, debiendo cumplir con los procedimientos formales de tratamiento e intercambio de información.
- Mantener la confidencialidad de las credenciales de acceso otorgadas y usarlas diligentemente, asumiendo la responsabilidad por las acciones que terceras personas puedan realizar.
- Atender a lo establecido sobre las relaciones con los proveedores del presente documento.

9.5. Sobre el personal de seguridad física:

9.5.1. Funciones

- Realizar el registro respectivo de cajas, bolsas, paquetes, maletines, carteras y otros que porten los ciudadanos/as en condición de visitante, antes del ingreso y salida de las instalaciones de la Municipalidad Provincial Daniel Alcides Carrión.
- Realizar la supervisión de seguridad correspondiente a fin de mantener asegurado el perímetro de las instalaciones.
- Asegurar que todo personal visitante cuente con la autorización para el ingreso de las instalaciones y áreas restringidas de ser el caso.

- Controlar el ingreso con armas punzo cortantes y/o penetrantes y armas de fuego, en caso de presentarse, debe ser registrado y dejado en custodia en el puesto de seguridad del Edificio. Están exceptuados el propio personal de seguridad de la Municipalidad Provincial Daniel Alcides Carrión.

9.5.2. Obligaciones

- Registrar todas las visitas en el Registro de Visitas, conforme lo dispuesto en la R.M. N° 035-2017 PCM y la normativa vigente.