
# POLÍTICAS PARA EL CUMPLIMIENTO DE LAS NORMAS TÉCNICAS SOBRE TECNOLOGÍAS DE INFORMACIÓN

# POLÍTICAS PARA EL CUMPLIMIENTO DE LAS NORMAS TÉCNICAS SOBRE TECNOLOGÍAS DE INFORMACIÓN

**1.4.1.2 MB-CUI-Pol-01-Seguridad de la Información**

**1.4.3.2 MB-CUI-Pol-01-Seguridad Física y Ambiental**

**1.4.4.2 MB-CUI-Pol-01-Transparencia y Confidencialidad de la Información**

**1.4.5.2 MB-CUI-Pol-01-Control de Accesos**

**1.4.6.1 MB-CUI-Pol-01-Mantenimiento de Infraestructura**

**1.7.1 MB-CUI-Pol-01-Cumplimiento Regulatorio de TI**

# 1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

**Versión 2.0 – Julio 2017**

**Control de versiones**

| Versión | Fecha | Descripción | Autor |
|---|---|---|---|
| 1.0 | 22/12/16 | Política de Seguridad de la Información | Deloitte Touche S.A. |
| 2.0 | 18/7/2017 | Ajustes de formato acorde a lo señalado por la Coordinadora de Informática | Deloitte Touche S.A. |

## 1- Presentación

**En esta sección, se presenta una lista de las actividades correspondientes a las políticas de la Municipalidad de Belén.**

## 2- Objetivo o Propósito

**El propósito de esta política es establecer el alcance de la seguridad de la información en la Municipalidad de Belén y asegurar su control y cumplimiento. Es requerido dejar claro sus límites y prioridades, respetando los fines y principios organizacionales.**

## 3- Alcance

**Esta política es aplicable a todo el ámbito de seguridad de la información en la Municipalidad de Belén, que deberá ser provista por la CUI, involucrando a todo el personal que interactúe con la información gestionada o administrada por el oficial de seguridad de la Unidad de Informática.**

## 4- Abreviaturas y Definiciones

**En esta sección se describe la lista de conceptos y sus respectivas definiciones.**

| Concepto | Definición |
|---|---|
| CGI | Comité Gerencial de Informática |
| CUI | Coordinación de la Unidad de Informática |
| GP | Gestión de Proyectos |
| TI | Tecnologías de la Información |

## 5- Referencia a otros Documentos

**Esta sección contiene la lista de documentos asociados al instructivo.**

| Nombre del documento |
|---|
| Normas Técnicas de la contraloría General de la República. San José, Costa Rica |

## 6- Política

**El ámbito de aplicación del presente reglamento comprende todos los aspectos relacionados con el uso de la Tecnologías de Información de la Municipalidad de Belén.**

| Código | Descripción de la Política |
|---|---|
| 1 | Respecto a las políticas que envuelven la seguridad de la información se tiene las siguientes:<br><br>1.1. La seguridad de la información involucra cualquier acción tendiente a la protección, resguardo (Integridad, viabilidad, disponibilidad) y mantenimiento de la información, tomando en consideración las necesidades de los usuarios, ya sea a nivel interno o externo.<br><br>1.2. Los mecanismos del resguardo, monitoreo y vigilancia de la seguridad de la información recaen en CGI pero la gestión, aplicación y ejecución de los controles recae en la CUI.<br><br>1.3. El Departamento de Seguridad Informática es responsable por mantener la comunicación adecuada con los involucrados para su mantenimiento y mejoras, según los intereses y necesidades institucionales. |
| 2 | La seguridad de la información ofrecida por la CUI abarca lo siguiente:<br><br>2.1. Seguridad de la información, gestión y toma de decisiones.<br><br>2.2. Organización de la seguridad de la información, grupos de interés, niveles de autoridad, roles y responsabilidades durante los procesos, dispositivos móviles y teletrabajo.<br><br>2.3. Gestión de activos, responsabilidad, clasificación de la información y manejo de los medios. |

| Código | Descripción de la Política |
|---|---|
| 2 | **2.4. Control de acceso, requisitos del negocio para éste, la gestión del acceso de usuarios, a sistemas y aplicaciones, así como sus responsabilidades.**<br><br>**2.5. Criptografía y modelo de encriptado, sus controles.**<br><br>**2.6. Seguridad física y ambiental, áreas seguras y disponibilidad de los equipos.**<br><br>**2.7. Seguridad de las operaciones, procedimientos y responsabilidades operacionales, protección contra código malicioso (malware), respaldo, registro y mantenimiento, control de software operativo, gestión de vulnerabilidades técnicas y consideraciones de auditoría de sistemas de información.**<br><br>**2.8. Seguridad de las comunicaciones, gestión de seguridad de la red y transferencia de información.**<br><br>**2.9. Adquisición y desarrollo de sistemas de información, requisitos de seguridad de sistemas de información, seguridad en los procesos de desarrollo y soporte y pruebas de datos.**<br><br>**2.10. Seguridad de la información con relación a los proveedores y gestión de la entrega de servicios de éstos.**<br><br>**2.11. Gestión de incidentes y mejoras en la seguridad de la información.**<br><br>**2.12. Seguridad ligada a los recursos humanos, previo, durante y posterior a la finalización o cambio de personal.**<br><br>**2.13. Aspectos de seguridad de la información en la gestión de la continuidad de los servicios y la redundancia.**<br><br>**2.14. Cumplimiento, requisitos legales y contractuales y revisión de seguridad de la información.**<br><br>**2.15. Los activos informáticos de la Institución que se encuentren debidamente registrados por la Unidad de Contabilidad.** |

| Código | Descripción de la Política |
|---|---|
| 3 | **Las prohibiciones generales son las siguientes:**<br><br>**3.1. Queda terminantemente prohibido la conexión a la Red Institucional de cualquier equipo informático que no sea del conocimiento de la CUI.**<br><br>**3.2. Queda prohibido la conexión de equipo personal a la Red Institucional.**<br><br>**3.3. Queda totalmente prohibido compartir las contraseñas personales de acceso.**<br><br>**3.4. Queda prohibido la instalación de software no autorizado. La instalación de aplicaciones será controlada por el la CUI (Soporte e Infraestructura), según los lineamientos establecidos, y en apego al catálogo de aplicaciones.**<br><br>**3.5. Queda prohibida la publicación de información confidencial según lo establecido en el Esquema de Clasificación de la Información y la normativa de Archivo Institucional.** |

## 7. Control de Periodicidad de Revisiones

**Los lineamientos de esta política deben ser actualizados a medida que ocurran cambios en los elementos de la Seguridad de la Información.**

# 2. POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

**Versión 2.0 – Julio 2017**

## 8. Control de versiones

| Versión | Fecha | Descripción | Autor |
|---|---|---|---|
| 1.0 | 22/12/16 | Política de Seguridad de la Información | Deloitte Touche S.A. |
| 2.0 | 18/7/2017 | Ajustes de formato acorde a lo señalado por la Coordinadora de Informática | Deloitte Touche S.A. |

## 9. Presentación

**En esta sección, se presenta una lista de las actividades correspondientes a las políticas de la Municipalidad de Belén.**

## 10. Objetivo o Propósito

**El aseguramiento de las instalaciones restringidas de accesos dentro de la CUI de manera que se cumpla con los requerimientos físicos y de seguridad para la protección de todos los equipos tecnológicos, frente a eventos que pongan en peligro la continuidad y la calidad de los servicios que ofrece la CUI a los funcionarios de la Municipalidad de Belén, así como de los procesos que se efectúan a lo interno de ésta.**

## 11. Alcance

**Esta política aplica en todas las áreas de acceso restringido ubicadas en la Municipalidad de Belén, sea en oficinas centrales o en oficinas externas, actualmente incluye centros de datos y cuartos de telecomunicaciones, aspecto que se podrá ampliar conforme crezcan los intereses y necesidades tecnológicas. Esta política deberá ser acatada por todo el personal Municipal y/o proveedores.**

## 12. Abreviaturas y Definiciones

**En esta sección se describe la lista de conceptos y sus respectivas definiciones.**

| Concepto | Definición |
|---|---|
| **CGI** | **Comité Gerencial de Informática** |
| **CUI** | **Coordinación de la Unidad de Informática** |
| **Área de acceso restringido** | Se refiere a cualquier espacio físico destinado a labores que el uso de la tecnología sea fundamental para su desarrollo y que, por necesidades institucionales, sea considerado de acceso **restringido, incluye Centros de Datos y Centros de** Comunicaciones inicialmente pudiéndose ampliar la lista según **los intereses y necesidades institucionales.** |
| **Bitácora de ingreso** | **Control físico del ingreso de personal y del acontecimiento de eventos en una zona restringida, donde se lleva un registro de la entrada y salida del personal, ya sea éste interno o externo a la Municipalidad de Belén.** |
| **Centro de Datos** | **Localización física donde se encuentran los activos de la CUI que proporcionan el procesamiento y almacenamiento principal, por lo cual, debe cumplir con una serie de condiciones ambientales mínimas, contemplando humedad, temperatura, iluminación, seguridad, aire acondicionado, entre otros. Todo dentro de marco normativo vigente.** |
| **CFIA** | **Colegio Federado de Ingenieros y de Arquitectos** |
| **Cuarto de Telecomunicaciones** | **Localización física que consolida la conectividad de la institución, donde se encuentra almacenados los elementos de terminación del cableado estructurado y los equipos de telecomunicaciones.** |
| **Evento** | **Condición de un sistema, servicio o res, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que es concerniente a la seguridad de la información.** |
| **Generador (Grupo Electrógeno)** | **Máquina o equipo accionada por un motor diésel, gasolina o gas, utilizando para abastecer a consumidores debido a la interrupción en el suministro de energía eléctrica.** |
| **Incidente** | **Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.** |

| Concepto | Definición |
|---|---|
| UPS | Corresponde a las siglas en inglés de Sistemas de Alimentación Ininterrumpida, consiste en una fuente de suministro eléctrico, que provee de energía al dispositivo al cual se encuentra conectado en caso de existir una interrupción eléctrica. |
| Visitantes Internos | Cualquier funcionario de la Municipalidad de Belén que desee ingresar a una de las zonas restringidas de TI, ya sea para actividades propias de su puesto, o bien, para temas de control, atención, entre otros |
| Visitantes Externos | Proveedores de tecnología, auditoría, consultoría o cualquier otro servicio, inspectores, o cualquier otro tercero que no labore en planilla para la Municipalidad de Belén |

1. **Referencia a otros Documentos**

**Esta sección contiene la lista de documentos asociados al instructivo.**

| Nombre del documento |
|---|
| 1.4.4.1 MB-CUI-Pros-01- Gestión de Incidentes de Seguridad |

2. **Política**

**El ámbito de aplicación del presente reglamento comprende todos los aspectos relacionados con el uso de la Tecnologías de Información de la Municipalidad de Belén.**

| Código | Descripción de la Política |
|---|---|
| 1. | Las políticas de acceso y monitoreo del ambiente físico son las siguientes:<br><br>1.1. El personal designado por la CUI es en primera instancia el encargado de monitorear el ambiente físico de las instalaciones restringidas, donde se encuentran los componentes de Tecnología que soportan los servicios de Tecnología de Información y Comunicación, regidos por lo establecido por la CUI.<br><br>1.2. La CUI debe velar porque las regulaciones físicas de construcción, seguridad y salud sean cumplidas en la gestión de las instalaciones restringidas de la CUI. |

| Código | Descripción de la Política |
|---|---|
| | **1.3. El personal designado por la CUI deberá ser capacitado, de modo que cuente con el conocimiento necesario sobre las regulaciones y requerimientos mínimos en el manejo de centro de datos, incluyendo aspectos como: humedad, UPS, aire acondicionado, energía, cableado estructurado, medidas ante desastres, estado de equipo. Además, la CUI, puede buscar apoyo en otras áreas de la Municipalidad de Belén o bien, entidades externas, para un mayor detalle en estos temas.**<br><br>**1.4. La CUI será la encargada de verificar el cumplimiento de los controles de seguridad física por parte del personal de Infraestructura en la gestión del acceso y protección de las instalaciones restringidas de la CUI.**<br><br>**1.5. Los centros de datos, así como los cuartos de telecomunicaciones de la Municipalidad de Belén son de acceso restringido, por lo tanto, la visita a estos lugares deberá realizarse según lo establecido en el procedimiento "Procedimiento Acceso a Instalaciones restringidas de la CUI.**<br><br>**1.6. Todo acceso a las zonas restringidas deberá darse con la escolta de un funcionario de Infraestructura, quien será designado por la CUI.**<br><br>**1.7. El horario para solicitudes de acceso a los centros de datos o cuartos telecomunicaciones, es de lunes a viernes de las 8:00 am a las 4:00 pm. Las gestiones que ingresen fuera de este horario, serán atendidas al siguiente día hábil. La única excepción a este lineamiento será en casos de emergencia, para lo cual, se debe seguir lo establecido en el procedimiento "Procedimiento Acceso a Instalaciones Restringidas de la CUI".**<br>**1.8. Cuando se realice mantenimiento a equipos o dispositivos existentes en las instalaciones restringidas de la CUI por personal externo, el funcionario designado deberá custodiar a los visitantes en su acceso, estadía y salida.**<br><br>**1.9. La CUI deberá de gestionar con la unidad responsable según correspondan sobre el mantenimiento de los aires acondicionados, generadores (grupo electrógeno) y UPS, planta eléctrica, entre otros, ubicados en los centros de datos y cuartos de telecomunicaciones.** |

| Código | Descripción de la Política |
|---|---|
| | **1.10. La CUI procurará la adquisición y renovación de pólizas de seguro adecuadas que permitan la continuidad en las gestiones de los equipos tecnológicos, contemplando en todo momento las regulaciones adherentes al ambiente físico, ambiental, laboral y tecnológico.**<br><br>**1.11. Las instalaciones restringidas de la CUI deben tener un perfil bajo, por lo cual, deben evitarse las señalizaciones que indiquen la ubicación del mismo o identificadores que revelen la presencia de equipo crítico.**<br><br>**1.12. El diseño de las zonas restringidas debe basarse en el estándar ANSI/TIA-942-2005 del American National Standards Institute – Telecomunications Industry Associacition, del Uptime Institute, y la Norma Internacional para la Construcción de Centros de Procesamientos de Datos del ICREA.**<br><br>**1.13. Se debe contar con áreas de envío y recepción de equipo separadas del centro de datos, para mayor seguridad del equipo y datos sensibles.**<br><br>**1.14. El perímetro de seguridad de las instalaciones restringidas de la CUI debe contar con mecanismos de control, cámaras de seguridad y de monitoreo, alarmas y sistemas de apertura o cerrojos que protejan estos sitios de acceso no autorizado.**<br><br>**1.15. Los sensores de temperatura, de humedad e incendio o humo deben cumplir con las especificaciones establecidas.**<br><br>**1.16. Dentro de las zonas restringidas de la CUI se debe contar con extintores en caso de incendio del equipo electrónico, o bien tener un sistema automatizado de extinción.**<br><br>**1.17. Los equipos de aire acondicionado deben cumplir con las especificaciones definidas para las zonas restringidas de la CUI.**<br><br>**1.18. Las instalaciones restringidas de la CUI deben contar con generadores eléctricos de emergencia, que permitan mantener la continuidad del suministro de energía eléctrica en caso de interrupción del servicio público.** |

| Código | Descripción de la Política |
|---|---|
| | **Los generadores de emergencia deben iniciar su funcionamiento de forma inmediata y automática al ocurrir el incidente o en su defecto la organización debe contar con equipos institucionales que provean de energía a estos recintos en caso de emergencia.**<br><br>**1.19. Los equipos de las instalaciones restringidas de la CUI, incluyendo aires acondicionados, equipos de red, servidores, iluminación y cualquier otro, deben estar conectados al suministro de energía eléctrica o UPS.**<br><br>**1.20. Trimestralmente, el personal encargado debe comprobar que los generadores eléctricos de emergencia estén en condiciones óptimas para iniciar su funcionamiento cuando se requiera. En el caso de las UPS, se debe realizar cada mes.**<br><br>**1.21.En caso de requerir nuevos equipos para las zonas restringidas de la CUI, se debe comprobar la capacidad de operación de los mismos.**<br><br>**1.22. Es responsabilidad del personal encargado, conocer las políticas y lineamientos establecidos para la gestión y protección de las instalaciones restringidas de la CUI.**<br><br>**1.23. Los riesgos identificados por el personal encargado con respecto a la capacidad de recuperación de recursos y otros relacionados, deben ser reportados a la CUI en primera instancia para que éste se lo comunique a CGI.**<br><br>**1.24. La CUI debe velar porque el personal del área sea capacitado y entrenado para actuar ante situaciones de emergencia, según lo requerido para el resguardo de las zonas restringidas de la CUI.** |
| **2.** | **Para los incidentes de seguridad se cuentan con las siguientes políticas:**<br><br>**2.1. El personal designado por la CUI deberá realizar la gestión de los incidentes de seguridad, los cuales pueden ser originados por una de las siguientes fuentes:**<br>**2.1.1. Mesa de servicio: El caso es presentado por el personal de la Municipalidad de Belén mediante la mesa de servicio.** |

| Código | Descripción de la Política |
|---|---|
| 2. | **2.1.2. Monitoreo: El personal designado por la CUI identifica uno o más incidentes de seguridad mediante los monitoreos de control que realiza periódicamente.**<br><br>**2.1.3. Automático: Un equipo o herramienta automatizada genera una alerta indicando la detección de una intrusión en uno de los sistemas, o cualquier otro tipo de violación a las políticas de seguridad.**<br><br>**2.2. Los incidentes de seguridad serán clasificados según la criticidad e impacto del riesgo que generan para la organización.**<br><br>**2.3. La gestión de los incidentes de seguridad se realizará según lo dictado por Seguridad de la información, utilizando como base el procedimiento "Procedimiento Gestión de Incidentes de Seguridad".**<br><br>**2.4. El control y seguimiento de los incidentes de seguridad debe tomar en cuenta los lineamientos y políticas definidos por Seguridad de la Información, principalmente los definidos en la Política de Seguridad de la Información y en el Reglamento de Seguridad de la Información.**<br>**2.5. Los incidentes de seguridad, así como las actividades realizadas para su atención y solución serán almacenados, para la generación de una base de datos de conocimiento.**<br>**2.6. El personal designado por la CUI deberá compartir un listado de los incidentes de seguridad a la CUI y este al personal de la mesa de servicios, de modo que éstos puedan identificarlos cuando se presenten.** |

## 13. Control de Periodicidad de Revisiones

**Los lineamientos de esta política deben ser actualizados a medida que ocurran cambios en los elementos de la seguridad física y ambiental.**

# 3. POLÍTICA DE TRANSPARENCIA Y CONFIDENCIALIDAD DE LA INFORMACIÓN

**Versión 2.0 – Julio 2017**

## 14. Control de versiones

| Versión | Fecha | Descripción | Autor |
|---|---|---|---|
| 1.0 | 22/12/16 | Política de transparencia y confidencialid | Deloitte Touche S.A. |
| 2.0 | 18/7/17 | Ajustes de formato acorde a lo señalado por la Coordinación de Informática | Deloitte Touche S.A. |

## 15. Presentación

**En esta sección, se presenta una lista de las actividades correspondientes a las políticas de la Municipalidad de Belén.**

## 16. Objetivo o Propósito

**Asegurar la transparencia de la información emitida desde la Municipalidad de Belén, garantizando la integridad, confidencialidad, disponibilidad y protección de los datos. El alcance y las limitaciones de esta información son fundamentales para la gestión organizacional, respetando los fines y principios y en especial, los intereses y expectativas de los usuarios.**

## 17. Alcance

**Esta política se aplica a todos los servicios de entrega de información que se den dentro y desde la Municipalidad de Belén e involucra a todo el personal que solicite o reciba información por medios y canales digitales, según sus intereses y expectativas.**

## 18. Abreviaturas y Definiciones

**En esta sección se describe la lista de conceptos y sus respectivas definiciones.**

| Categoría | Definición |
|---|---|
| CGI | Comité Gerencial de Informática |
| CUI | Coordinación de la Unidad de Informática |
| GP | Gestión de Proyectos |

| | |
|---|---|
| **Respaldo** | **Copia de seguridad de información de alta importancia, por lo cual, es almacenada en un sitio secundario** |
| **Recuperación** | **Proceso de reparar, recuperar o devolver la información al estado anterior, utilizando para ello, un respaldo generado previamente.** |
| **TI** | **Tecnologías de la Información** |

## 19. Referencia a otros Documentos

**Esta sección contiene la lista de documentos asociados al instructivo.**

| Nombre del documento |
|---|
| **Normas Técnicas de la Contraloría General de la República. San José, Costa Rica.** |

## 20. Política

**El ámbito de aplicación del presente reglamento comprende todos los aspectos relacionados con el uso de la Tecnologías de Información de la Municipalidad de Belén.**

| Código | Descripción de la Política |
|---|---|
| **1** | **Las políticas asociadas a la transparencia y confidencialidad de la información son las siguientes:**<br><br>**1.1.** La CUI es responsable por la disponibilidad adecuada de la información a los usuarios, desde cualquier medio o canal digital **e informático de la municipalidad.**<br><br>**1.2.** La información existente en los dispositivos tecnológicos de la Municipalidad, serán de acceso público y privado según lo establece la legislación vigente. |
| **2** | **Los protocolos básicos son los siguientes:**<br>**2.1. El CGI deberá aprobar el conjunto de indicadores de información requeridos por cada una de las instancias organizacionales.**<br><br>**2.2. La transparencia de la información emitida por la CUI estará regida bajo los siguientes lineamientos: Toda solicitud de información específica deberá ser solicitada de manera formal** |

| Código | Descripción de la Política |
|---|---|
| | **por los responsables y según los mecanismos establecidos por la Unidad de Informática.**<br><br>**2.3. Toda solicitud de información será entregada al personal de la municipalidad máximo a los 10 días hábiles siguientes a la solicitud.**<br><br>**2.4. El manejo y cuido de la información solicitada será responsabilidad total de los funcionarios solicitantes.** |
| **3** | **El área de la municipalidad responsable de disponer la información a los usuarios aprovechará los recursos dispuestos por la Unidad de informática, dentro de los límites dados por el CGI.** |

## 21. Control de Periodicidad de Revisiones

**Los lineamientos de esta política deben ser actualizados a medida que ocurran cambios en los elementos de la transparencia y confidencialidad.**

# 4. POLÍTICA DE CONTROL DE ACCESOS

**Versión 2.0 – Julio 2017**

## 22. Control de versiones

| Versión | Fecha | Descripción | Autor |
|---|---|---|---|
| 1.0 | 23/12/16 | Política de control de Accesos. | Defloitte Touche S.A. |
| 2.0 | 18/7/2017 | Ajustes de formato acorde a lo señalados por la Coordinación de Informática | Defloitte Touche S.A. |

## 23. Presentación

**En esta sección, se presenta una lista de las actividades correspondientes a las políticas de la Municipalidad de Belén.**

## 24. Objetivo o Propósito

**Direccionar la gestión de identidades y cuentas de usuario, con el objetivo de proteger la información de accesos no autorizados, así como mantener la trazabilidad de las actividades ejecutadas del personal de la Municipalidad de Belén en los sistemas de información administrados desde la Unidad de Tecnologías de Información y Comunicación.**

## 25. Alcance

**Esta política contempla la administración de cuentas de usuario para el acceso a los sistemas de información y ámbitos de dominio administrados por la CUI. Involucra el personal de TI (Infraestructura, como el de Seguridad de la Información) y debe ser conocida por los funcionarios de la Municipalidad de Belén, aunado a las políticas de acceso que deben ser también de su conocimiento.**

## 26. Abreviaturas y Definiciones

**En esta sección se describe la lista de conceptos y sus respectivas definiciones.**

| Concepto | Definición |
|---|---|
| CGI | **Comité Gerencial de Informática.** |
| CUI | **Coordinación de la Unidad de Informática.** |
| CDRH | **Coordinación de Recursos Humano** |
| Contraseña | **Cadena alfanumérica con la cual se verifica y prueba la identidad de un usuario, en un sistema de información.** |
| Cuenta | **1. Identificador único del personal Municipal que en combinación con una contraseña permite la autentificación en uno o en varios sistemas de información institucionales.**<br>**2. Nombre atribuido a la identidad digital de un funcionario(a) en un sistema de información institucional.** |
| Dueño del sistema | **Es el responsable de las aplicaciones que soportan los procesos que su área de negocio ejecuta. Por lo general esta responsabilidad recae sobre la persona de mayor rango jerárquico o a quien ésta designe de manera formal.** |
| Perfil | **Combinación de permisos y roles que le permiten a distintos usuarios ejecutar acciones o actividades dentro de un sistema (hardware o software) según su puesto.** |

## 27. Referencia a otros Documentos

**Esta sección contiene la lista de documentos asociados al instructivo.**

| Nombre del Documento |
|---|
| **<Código de Documento> Esquema de Clasificación de la Información** |

## 28. Política

**El ámbito de aplicación del presente reglamento comprende todos los aspectos relacionados con el uso de la Tecnologías de Información de la Municipalidad de Belén.**

| Código | Descripción de la Política |
|---|---|
| 1. | **Los lineamientos de Control de Acceso dictan las siguientes actividades:**<br><br>**1.1. Todos los sistemas de información de la Municipalidad de Belén deben contar como mínimo, con autenticación de usuario y contraseña.**<br><br>**1.2. Los controles de acceso en los sistemas de información deben ser coherentes con la criticidad de la información gestionada en éstos, en alineamiento con el DGTI-EA-011 Esquema de Clasificación de la Información.**<br><br>**1.3. Las solicitudes de creación, modificación, habilitación/inhabilitación y eliminación de cuentas deben ser realizadas por medio de la mesa de servicio, de manera que sean atendidas en forma adecuada por el personal de la CUI.**<br><br>**1.4. La creación, modificación, habilitación/inhabilitación y eliminación de cuentas de Dominio o Sistema, debe ser aprobada por el Administrador de Dominio o el Dueño del Sistema según corresponda. Para lo cual, debe transferirse las solicitudes respectivas para su revisión.**<br><br>1.5. **El Administrador de Accesos debe supervisar la ejecución de los procedimientos de control de acceso, verificando la correcta atención de las solicitudes de usuarios y el cumplimiento de lo establecido en esta política.**<br><br>1.6. **El Administrador de Accesos debe llevar el monitoreo de las cuentas y accesos, verificando que el personal de la Municipalidad de Belén cuente con los permisos establecidos según sus funciones y responsabilidades, así como debe mantener también la revisión de cuentas inhabilitadas/eliminadas debido a vacaciones, despido o renuncia.**<br><br>1.7. **Administrador de Accesos debe transferir al personal de Seguridad de la Información, los informes técnicos de los monitoreos realizados, así como cualquier incidente o hallazgo identificado para su revisión. Además, los informes técnicos deben enviarse al responsable de la Gestión Técnica para el control de las acciones realizadas por el personal.** |

| Código | Descripción de la Política |
|---|---|
| 1. | **1.8. Los sistemas de información que sean desarrollados/adquiridos en la Municipalidad de Belén, deben contar con bitácoras de acceso y pistas de auditoría, que permita llevar un control del acceso.**<br><br>**1.9. Los registros y bitácoras de acceso a los sistemas de información deben estar activos y disponibles para las revisiones a ejecutar, tanto por el personal de Control de Accesos, así como de Seguridad de la Información, en caso de incidentes.**<br><br>**1.10. El personal de Seguridad de la Información, como parte de sus tareas de monitoreo y seguimiento, analiza los informes de monitoreo y atiende los incidentes de seguridad relacionados con accesos no autorizados.**<br><br>**1.11. Es responsabilidad de la Coordinación de Recursos Humano solicitar la habilitación de cuentas para nuevo personal, así como la inhabilitación de las cuentas en caso de vacaciones, permisos, despido o renuncia. De igual forma, el Administrador de Accesos puede generar este tipo de solicitudes, producto del monitoreo realizado.**<br><br>**1.12. Las cuentas de usuario se considerarán como inhabilitadas una vez que un funcionario ha sido despedido o ha renunciado a sus labores en la Municipalidad, o bien, se encuentra en vacaciones o permiso según criterio de la UCRH.** |
| 2. | **Los lineamientos para Definición y Protección Contraseñas dictan las siguientes actividades:**<br><br>**2.1. La longitud de las contraseñas debe ser como mínimo de ocho caracteres.**<br>**2.2. Las contraseñas deben contener al menos un carácter de tres de los siguientes tipos:**<br>• **Letra minúscula.**<br>• **Letra mayúscula.**<br>• **Caracteres Numéricos**<br>• **Caracteres especiales/símbolos (#-!@^:?*).** |

| Código | Descripción de la Política |
|---|---|
| 2 | **2.3. Las contraseñas deben ser renovadas como mínimo en un periodo de 3 meses, para lo cual, el personal de la Unidad de Tecnologías de Información y Comunicación informará a los funcionarios de su respectivo cambio.**<br><br>**2.4. Las cuentas de usuario deben ser bloqueadas después de 3 intentos fallidos por un período de 10 minutos.**<br><br>**2.5. Las contraseñas de usuario son de uso personal, por lo cual, los funcionarios no deben compartirlas con personas internas o externas a la Institución; salvo en casos de atención de incidentes por parte del personal de la Mesa de Servicio o Seguridad de la Información de la Coordinación de la Unidad de Informática**<br><br>**2.6. Las contraseñas de usuario son clasificadas como información restringida, por lo cual, no deben estar visibles en el sitio trabajo o en documentación compartida (física/digital).**<br><br>**2.7. Seguridad de la Información será la unidad encargada de capacitar y concientizar al personal de la Municipalidad de Belén en el uso y establecimiento de contraseñas.**<br><br>**2.8. La información relacionada a los incidentes de accesos no autorizados debe ser comunicada al personal de la Municipalidad de Belén, con el objetivo de prevenir su recurrencia.**<br><br>**2.9. La CUI debe velar por el cambio de contraseñas establecidas por defecto en los sistemas de información que han sido adquiridos.**<br><br>**2.10. La CUI debe establecer controles automatizados para asegurar que las contraseñas de acceso cumplan con los requerimientos de longitud y complejidad establecidos.**<br><br>**2.11. Los funcionarios deben establecer contraseñas complejas, evitando la introducción de su información personal o palabras que puedan ser fácilmente reveladas.**<br><br>**2.12. Cada funcionario es responsable de la protección de su contraseña, así como de las acciones ejecutadas con su usuario en los sistemas de la Municipalidad de Belén.** |

## 29. Notas

**Los lineamientos relacionados con el establecimiento y uso de contraseñas de usuario deben ser comunicados (correo electrónico/capacitaciones) por Seguridad de la Información a los funcionarios de la Municipalidad de Belén.**

## 30. Control de Periodicidad de Revisiones

**Los lineamientos de esta política deben ser actualizados a medida que ocurran cambios en los elementos de la Seguridad de la Información.**

# 5. PROCEDIMIENTO DE MANTENIMIENTO DE INFRAESTRUCTURA

**Versión 2.0 – Julio 2017**

## 31. Control de versiones

| Versión | Fecha | Descripción | Autor |
|---|---|---|---|
| 1.0 | 23/12/16 | Política Mantenimiento de Infraestructura (Seguridad). | Defloitte Touche S.A. |
| 2.0 | 18/7/2017 | Ajustes de formato acorde a lo señalado por la Coordinación de Informática | Defloitte Touche S.A. |

## 32. Presentación

**En esta sección, se presenta una lista de las actividades correspondientes a las políticas de la Municipalidad de Belén.**

## 33. Objetivo o Propósito

**Establecer los lineamientos mínimos para el mantenimiento de la infraestructura que soporta los procesos y servicios de la Municipalidad de Belén, contemplando los requerimientos de seguridad de la información.**

## 34. Alcance

**Esta política abarca las actividades de mantenimiento de la infraestructura de la Municipalidad de Belén, gestionada por el personal del sub-proceso de infraestructura de la Coordinación de la Unidad de Informática.**

## 35. Referencia a otros Documentos

**Esta sección contiene la lista de documentos asociados al instructivo.**

| Nombre del Documento |
|---|
| 2.3.1 MB-CUI-Form-01-Plan de Adquisición y Mantenimiento de Infraestructura |
| <Código del Documento> Esquema de Clasificación de la Información |

## 36. Abreviaturas y Definiciones

**En esta sección se describe la lista de conceptos y sus respectivas definiciones.**

| Concepto | Definición |
|---|---|
| CGI | Comité Gerencial de Informática |
| CUI | Coordinación de la Unidad de Informática |

### 37. Política

**El ámbito de aplicación del presente reglamento comprende todos los aspectos relacionados con el uso de la Tecnologías de Información de la Municipalidad de Belén.**

| Código | Descripción de la Política |
|---|---|
| 1. | Las actividades de mantenimiento deben ser ejecutadas según lo establecido en el DGTI-FO 34000501 Formulario Plan de Adquisición y Mantenimiento de Infraestructura, así como los cambios realizados deben verse reflejados en este documento. |
| 2. | Las actividades de mantenimiento y soporte de los componentes de infraestructura deben tomar en cuenta los lineamientos de seguridad física, incluyendo los requerimientos de acceso y monitoreo de las instalaciones restringidas de TI. |
| 3. | La CUI debe procurar que las actividades de mantenimiento sobre los componentes de infraestructura se realicen tomando en cuenta las recomendaciones de los fabricantes. |
| 4. | La renovación y reposición de equipo tecnológico debe tener un visto bueno por la Coordinación de la Unidad de Informática, verificando que éstos cumplan con los requerimientos de seguridad mínimos establecidos en el Marco de Seguridad de la Información de la Unidad de Tecnologías de Información y Comunicación. |
| 5. | La evaluación de adquisiciones de equipo tecnológicas por parte Coordinación de la Unidad de Informática, debe contemplar los requerimientos de seguridad de la información, así como las características de la plataforma tecnológica. |
| 6. | La Coordinación de la Unidad de Informática debe analizar los riesgos asociados a la plataforma tecnológica, e informar sobre éstos al Encargado de Seguridad de la Información y al Gestor de Riesgos, para su conocimiento y control. |

| Código | Descripción de la Política |
|---|---|
| 7 | El personal de la CUI debe procurar que el cableado estructurado sea instalado en ubicaciones seguras, de modo que evite la materialización de daños accidentales o deliberados por terceros. |
| 8. | El personal de la CUI debe resguardar el equipo y los sistemas de la Municipalidad de Belén ante amenazas de seguridad, utilizando mecanismos de protección, tales como antivirus, firewall, entre otros. |
| 9. | El personal de la Municipalidad de Belén debe utilizar de forma segura los dispositivos de comunicación (computadoras, teléfonos, impresoras, escáneres, entre otros), protegiendo la sensibilidad de la información digital transmitida por éstos, en concordancia con lo establecido en el DGTI-EA-0116 Esquema de Clasificación de la Información. |
| 10 | El personal de la Municipalidad de Belén debe mantener un uso seguro de los medios de almacenamiento (discos, dispositivos usb, tarjetas extraíbles, entre otros) protegiendo la información contenida de accesos no autorizados. Estos controles deben ser aplicados tanto a lo interno como externo de la Municipalidad de Belén |
| 11 | Es responsabilidad del personal de la CUI conocer las políticas y directrices relacionadas con el manejo y la protección de los componentes de infraestructura. |
| 12 | El usuario que tenga asignado un componente de tecnología es responsable de su estado, cumpliendo con los requerimientos mínimos de uso y cuidado. |
| 13 | El personal externo (proveedores, consultores, auditores externos, practicantes, entre otros) que haga uso de la plataforma tecnológica de la Municipalidad de Belén, debe cumplir con los requerimientos establecidos en esta política. |

## 38. Notas

**La CUI deberá establecer los mecanismos de comunicación necesarios para que el personal de la Municipalidad de Belén conozca y siga los requerimientos mínimos de seguridad en el uso y mantenimiento de la infraestructura.**

## 39. Control de Periodicidad de Revisiones

**Los lineamientos de esta política deben ser actualizados a medida que ocurran cambios en los elementos de la Seguridad de la Información.**

# 6. POLÍTICA DE CUMPLIMIENTO REGULATORIO DE TI

**Versión 2.0 – Julio 2017**

### 40. Control de versiones

| Versión | Fecha | Descripción | Autor |
|---|---|---|---|
| 1.0 | 22/12/2016 | Política de cumplimiento regulatorio | Deloitte Touche S.A. |
| 2.0 | 18/07/2017 | Ajustes de formato acorde a lo señalado por la Coordinadora de Informática | Deloitte Touche S.A. |

### 41. Presentación

**En esta sección, se presenta una lista de las actividades correspondientes a las políticas de la Municipalidad de Belén.**

### 42. Objetivo o Propósito

**Mantener un proceso de revisión que garantice el cumplimiento de las políticas, leyes, regulaciones y requerimientos contractuales.**

### 43. Alcance

**Aplica para todo el personal de la Unidad de Informática de la Municipalidad de Belén y personal de la institución involucrado en el cumplimiento de las leyes que afecten de forma directa e indirecta la gestión y uso de tecnologías de información.**

### 44. Abreviaturas y Definiciones

**En esta sección se describe la lista de conceptos y sus respectivas definiciones.**

| Concepto | Definición |
|---|---|
| CGI | Comité Gerencial de Informática |
| CUI | Coordinación de la Unidad de Informática |
| | Estado de aprobación, concordancia, aceptación con los aspectos requeridos. |
| Gestor de cumplimiento | Encargado "debe ser una persona asignada dentro de la Unidad de TI, que velará por el cumplimiento de las regulaciones que afecten la gestión de Tecnologías de Información. |
| Marco Jurídica | Se refiere al conjunto de elementos (Documentos, Herramientas) utilizados para velar por el cumplimiento de las obligaciones de la gestión de Tecnología de Información y Comunicación. |

## 45. Referencia a otros Documentos

**Esta sección contiene la lista de documentos asociados al instructivo.**

| Nombre del documento |
|---|
| Cumplimiento de obligaciones relacionadas con la gestión de Tecnología de Información y Comunicación. (1.7.2 MB- CUI-Procedimientol-01-Cumplimiento Regulatorio de TI) |
| Marco jurídico de Tecnología de Información y Comunicación |
| Código de ética institucional. |

## 46. Política

**El ámbito de aplicación del presente reglamento comprende todos los aspectos relacionados con el uso de la Tecnologías de Información y Comunicación de la Municipalidad de Belén.**

| Código | Descripción de la Política |
|---|---|
| 1. | 1.1. El personal designado por la CUI debe de identificar cada 6 meses, cuáles leyes (locales e internacionales), reglamentos, regulaciones y otros requerimientos externos se deben cumplir por parte de la CUI y velar porque los mismos sean incorporados en la normativa correspondiente de manera incorporados en la normativa correspondiente de manera oportuna, para evitar sanciones o incumplimientos que repercutan en la imagen y confianza de la Unidad. |

| Código | Descripción de la Política |
|---|---|
| | **1.2. Todas las leyes, reglamentos, regulaciones y otros requerimientos externos identificados deben de encontrarse disponibles para su consulta por parte de los interesados en el documento Marco Jurídico de TI.**<br><br>**1.3. El personal designado por la CUI debe de reportar el grado de cumplimiento, por medio de reportes de avance y estado, al CUI, para que la información sea integrada en informes a nivel de la organización.**<br><br>**1.4. El personal designado por la CUI debe velar por la alineación entre los requerimientos regulatorios (leyes locales e internacionales, normativas y reglamentos) y la normativa de la CUI, con el objetivo de gestionar las operaciones dentro de la regulación aplicable a TI, en relación con la prestación de servicios de información y los procesos, funciones, infraestructura e información en general.**<br><br>**1.5. El cumplimiento regulatorio debe contemplar aquellas regulaciones que están directamente relacionadas con la gestión de TI y todas aquellas que indirectamente requieren o afectan a TI, que por cumplimiento organizacional deben de acatarse, contempladas en las políticas, estándares y procedimientos en todos los niveles de la CUI.**<br><br>**1.6. El personal designado por la CUI es responsable de velar por el cumplimiento regulatorio y gestionar los recursos necesarios para realizar las evaluaciones de cumplimiento CUI brindará la información correspondiente apoyándose en la experiencia y habilidades técnicas de cada área quela compone.**<br><br>**1.7. La CUI debe mantenerse preparada e informada sobre los cambios y nuevas regulaciones que impactan a TI, para identificar requerimientos nuevos que repercutan en el Marco Jurídico relacionado a TI. La identificación de requerimientos de cumplimiento regulatorio debe realizarse cada seis meses y/o cuando se identifique un cambio en las regulaciones que afectan a TI o cuando se genere una nueva regulación, garantizando de esta manera que el cumplimiento reglamentario, contractual y legal se mantiene actualizado, documentado y comunicado a los interesados.** |

| Código | Descripción de la Política |
|---|---|
| | **1.8. Asimismo, las evaluaciones de cumplimiento también deben ejecutarse cada seis meses y el personal involucrado en la ejecución de estas, debe realizar su labor de forma transparente y legal de acuerdo al código de ética organizacional, sin intereses de por medio que afecten los resultados de las evaluaciones y bajo la supervisión de la CUI y CGI.**<br><br>**1.9. La CUI debe velar por proporcionar una respuesta rápida y eficiente ante nuevas regulaciones o cambios en las mismas, con el objetivo de optimizar la aplicación de estas en la Municipalidad de Belén, cubriendo las políticas, estándares y procedimientos de TI para ejecutar actividades de revisión y ajuste, garantizando así el empleo, dirección y comunicación de los requisitos legales, contractuales y regulatorios.**<br><br>**1.10. Los informes de resultados sobre las evaluaciones de cumplimiento de personal TI deben comunicarse a la CUI.**<br><br>**1.11. Los planes de acción para cualquier incumplimiento identificado deben ser determinados por las jefaturas de las áreas de TI en conjunto con el gestor de cumplimiento, con el fin de asegurar el cumplimiento y alineamiento entre los requerimientos regulatorios y la normativa la CUI.**<br><br>**1.12. La CUI debe implementar los planes de acción definidos para las desviaciones identificadas y analizar la causa raíz del incumplimiento. Además, deben reportar el estado de avance y de cumplimiento de los mismos al personal designado por la CUI-** |

**47. Control de Periodicidad de Revisiones**

**Los lineamientos de esta política deben ser actualizados a medida que ocurran cambios en los elementos de la Cumplimiento Regulatorio.**

**Aprobada en la Sesión Ordinaria N° 39, Artículo 25, del día 02 de julio del 2019**