I. Municipalidad de María Elena

DECRETO EXENTO N°: 1588/2022
MARIA ELENA, 20-06-2022

VISTOS ESTOS ANTECEDENTES

1 La necesidad de regular los procedimientos administrativos que sean desarrollados por el Municipio.

2 POLITICAS DE SEGURIDAD DE LA INFORMACION.

3 Las atribuciones que me confiere el D.F.L. N° 1/19.704 del Ministerio del Interior. Fija el texto refundido, coordinado y sistematizado de la Ley N° 18.695 Orgánica Constitucional de Municipalidades. (Diario Oficial 26.07.06).

D E C R E T O

1- APRUEBASE, POLITICAS DE SEGURIDAD DE LA INFORMACION.

ANOTESE, COMUNIQUESE, PUBLIQUESE Y ARCHIVESE.

MARCELA GARRIDO URIBE
SECRETARIA MUNICIPAL

OMAR NORAMBUENA RIVERA
ALCALDE
MUNICIPALIDAD DE MARIA ELENA

ONR/MGU/lpc.

DISTRIBUCION: Contabilidad y Presupuesto– Adquisiciones IMME Depto Finanzas- Archivo.

I. Municipalidad de María Elena

Políticas de Seguridad de la Información

ILUSTRE MUNICIPALIDAD DE MARIA ELENA
SECRETARIA MUNICIPAL
Nº DECRETO 1588
FECHA 20/06/12
FIRMA

Realizado	Revisado	Visado
Departamento Informática	Iván Soublette Mandiola	Priscila Chamorro Vargas

ILUSTRE MUNICIPALIDAD MARIA ELENA
DIRECTOR DE FINANZAS

I. Municipalidad de María Elena

1. Objetivo

Establecer las políticas, prácticas y lineamientos internos de Seguridad de la Información para Ilustre Municipalidad de María Elena, con el fin de asegurar la protección de los activos de información en todas sus formas y medios contra su modificación accidental o deliberada, utilización no autorizada, divulgación o interrupción, de modo de garantizar su confidencialidad, integridad y disponibilidad.

Ilustre Municipalidad de María Elena establece que ante cualquier presentación legal que se requiera y esté relacionado con los sistemas informáticos o los usuarios internos, se observarán las leyes vigentes mediante el asesoramiento legal respectivo, para asegurar los requisitos regulatorios que apliquen.

2. Alcance

Este documento es de aplicación en todas las fases del ciclo de vida de la información (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción) y de los sistemas que la procesan (análisis, diseño, desarrollo, implementación, explotación y mantenimiento).

Aplica a todos los sectores de Ilustre Municipalidad de María Elena, es decir, a todo el personal, tanto interno como externo; así como a las personas que directa o indirectamente prestan sus servicios profesionales dentro de la misma, y a toda la información obtenida, creada, procesada, almacenada o intercambiada dentro y desde la organización.

3. Vigencia

Su vigencia será a partir del 20/06/2022.

4. Responsabilidades

- El CEO director con responsabilidad general de la seguridad de la información de toda la organización.
- Encargado Depto. Informático es el oficial de protección de datos que va a asesorar en leyes de protección de datos y las mejores prácticas.

5. Revisión y publicación documental

Todos los documentos que se encuentran dentro del alcance del SGSI se revisarán de manera anual o después de cualquier cambio significativo en el alcance, para asegurar su conveniencia, suficiencia, y eficacia continua. Estos documentos deberán ser publicados y comunicados según el Plan de Comunicación del SGSI.

6. Reglas de aplicación

Política General de Seguridad de la Información

La Seguridad de la Información en La Ilustre Municipalidad de María Elena es parte fundamental del negocio para así entregar confianza a los usuarios sobre las tecnologías de la información que operamos. Los datos, con base en nuestra clasificación de la información, es gestionada con los más altos estándares según las mejores prácticas disponibles en el mercado, lo cual es una base para nuestro crecimiento y sustentabilidad organizacional.

La Seguridad de la Información en nuestro municipio es posible dado el compromiso, con herramientas necesarias para proveer el espacio adecuado de trabajo para los empleados.

En este Municipio las políticas y procedimientos en cuanto a la Seguridad de la Información son del conocimiento general para todos los empleados de la organización. En la medida de lo posible y con base al Plan de Comunicación definido, nuestras partes interesadas clave serán informados de nuestros lineamientos y mejores prácticas.

Sólo se clasifica información que sea estrictamente necesaria para el funcionamiento de este Municipio. También se limitan los accesos a los datos sólo para aquellos que lo requieran en el desempeño de sus tareas.

La información se divide en categorías, para asegurar que está protegida de forma adecuada y que se están asignando los recursos de seguridad de forma pertinente.

La organización establece las siguientes categorías de clasificación:

- **No clasificado:** Es información que se puede hacer pública, sin que implique consecuencias negativas para el municipio, como es la información que es de conocimiento público.
- **Confidencial de los empleados:** Esto incluye información como registros médicos, salarios, entre otros.
- **Confidencial del Municipio:** Como contratos, códigos fuente, contraseñas para sistemas críticos de TI, etcétera.
- **Confidencial del usuario:** Esto incluye información de identificación como nombre, dirección, claves de acceso al sistema de clientes, planes de negocio, información de nuevos productos, información sensible del mercado, etcétera.

Saneamiento y destrucción de activos de información

Activo de información	Saneamiento	Destrucción
Papel	N/A	Triturar o incinerar. Nota. Se recomienda la contratación de un proveedor.
Equipos móviles	Borrar manualmente toda la información almacenada: contactos, SMS, etc. Así como restaurar valores predeterminados del proveedor.	El equipo no se destruye sólo se re asigna a otro empleado.
Servidores	Cuando aplique, eliminar la configuración de arreglo de discos. Formateo de disco duro de servidor. Etc.	Si el servidor es arrendado se entrega al proveedor con el formateo efectuado Si el servidor es propiedad del Municipio se Formatea

Equipo	Si aplica • Se respalda la información. • Se realiza formateo de equipo.	El equipo no se destruye sólo se re asigna a otro funcionario.

6.1 Gestión de Riesgos de Seguridad

La Gestión de Riesgos tiene como objetivo ayudar a identificar y medir posibles eventos de pérdida (operativa y tecnológica) futuros y a establecer y priorizar planes de tratamiento sobre los riesgos que desafían sus objetivos estratégicos y prácticas operativas cotidianas de la empresa.

Ayudar a este Municipio a identificar y medir amenazas y vulnerabilidades que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información de la compañía, en especial aquella más crítica para el desarrollo confiable e ininterrumpido de sus actividades, como así también, establecer y priorizar los planes de tratamiento para reducir riesgos.

El CEO deberá establecer un proceso formal que permita:

- Identificar los riesgos estratégicos que pueden afectar negativamente al logro de los objetivos estratégicos de este municipio.
- Definir y aprobar el alcance del proceso de gestión de riesgos y las modificaciones eventuales al mismo.
- Definir el umbral de tolerancia y aceptación de riesgos de la organización.
- Aprobar el nivel de riesgo residual del municipio.
- Identificar activos críticos, amenazas y vulnerabilidades.
- Establecer los criterios de evaluación, tratamiento y medición de riesgos.
- Definir la planificación de los análisis de riesgos.

El análisis y evaluación de riesgos se realizará, como mínimo, **anualmente** o cuando ocurran cambios significativos en el entorno, lo que suceda primero.

6.2 Gestión de Accesos y Perfiles

La Gestión de Accesos y Perfiles tiene como objetivo establecer los lineamientos para un adecuado control de todos los usuarios, perfiles utilizados y que accedan a los activos informáticos.

Como departamento tratamos que la seguridad se cumpla, sin embargo, la intención es compartir la información para ayudar a la gente a realizar su trabajo y no para aumentar las barreras de acceso a la información innecesarias.

Adicionalmente, los privilegios de administrador de los sistemas son restringidos a funcionarios específicos y autorizados, para las siguientes funciones que le permiten desarrollar su trabajo de forma correcta.

Como medidas de precaución para la preservación de la información se adopta los siguientes lineamientos:

- Todo usuario de sistemas o plataformas tecnológicas está asociado a una persona física de manera unívoca y en los casos que se requiera la utilización de usuarios genéricos, estos tengan un responsable asociado.

- Se establece una gestión de las altas y asignación de credenciales de usuarios considerando la identificación de los mismos y las autorizaciones necesarias para su gestión.

- Ante un cambio de funciones se eliminan los accesos relacionados con la función anterior y se asignan los accesos necesarios para la nueva función.

- Toda desvinculación de personal implica el retiro de los accesos otorgados y/o la eliminación **o inhabilitación** de los ID de usuarios asociados a la persona.

- Se asegura la adecuada segregación de funciones (información entregada según jefatura directa), evitando la asignación de permisos incompatibles con las funciones de los usuarios.

- La generación/acceso a los usuarios de privilegios especiales en los sistemas y plataformas se encuentre limitado a personal debidamente identificado y bajo una adecuada justificación de necesidad, como así también que su utilización sea monitoreada y controlada.

- Existe una adecuada custodia de las credenciales de usuarios de privilegios especiales y usuarios genéricos que asegure la identificación del personal que las utilice y el registro de la justificación para su utilización.

- En vista de mantener la asignación de manera correcta, cada vez que un profesional deja el Municipio o uno nuevo ingresa se realiza la **revisión de derechos de accesos** que está a cargo de la jefatura directa y se ejecuta de la siguiente manera:

  Cuando ocurre este tipo de situación es el departamento de Recursos Humanos quien informa al departamento de Informatica de esta Municipio, la baja o alta de algún funcionario.

  Se procede a habilitar o inhabilitar, en su caso, en plataforma reloj control.(se adjunta manual de uso general Qwnatec).

  Se procede a habilitar o inhabilitar, en su caso, en software de gestión Municipal Cas Chile.(se adjunta manual de uso general Caschile).

  Se procede a la eliminación de la casilla en ISP Config. (primero se realiza respaldo de la información).

6.3 Gestión de Seguridad de Entornos, Plataformas y Aplicaciones

La Gestión de Seguridad de Entornos, Plataformas y Aplicaciones tiene como objetivo establecer los lineamientos para la definición, implementación y control de una adecuada seguridad en todos los entornos y plataformas que soportan los servicios de negocio.

Para proteger los datos, sistemas, usuarios y clientes se usan los siguientes sistemas:

- Anti-Virus para computadoras portátiles y de escritorio:
  (Kaspersky- licencia Antivirus Suite).
- Archivos y continuidad de correos electrónicos:
  (Conectiva chile – servidor web).
- Firewall:
  (Movistar Chile)

Adicionalmente, se desarrollan estándares que deberán contemplar como mínimo las definiciones necesarias para las siguientes categorías de entornos, plataformas, sistemas o aplicativos:

- Sistemas operativos.
- Redes y dispositivos de red.
- Estaciones de trabajo y dispositivos móviles.
- Sistemas de almacenamiento.
- Bases de datos.
- Correo electrónico e internet.
- Aplicaciones en general.

Todo cambio de arquitectura, infraestructura o definiciones de seguridad deben ser acordados con el departamento de Informatica Ilustre Municipalidad de María Elena, a fin de no generar problemas de seguridad.

Es por esto, que se deben considerar los siguientes lineamientos:

Gestión de la seguridad de redes

- Las redes deben gestionarse y controlarse adecuadamente para proteger la información en los sistemas y aplicaciones de la Ilustre Municipalidad de María Elena.
- Restringir las conexiones entre redes no confiables y cualquier componente del sistema en los entornos críticos.
- Se prohíbe el acceso público directo entre Internet y todo componente del sistema en los entornos críticos.

6.4 Gestión y Protección del Uso de los Dispositivos

La Gestión y protección del uso de los dispositivos tiene como objetivo establecer los lineamientos para una adecuada utilización de los activos de información de la compañía por parte de los usuarios incluyendo colaboradores, proveedores y terceros contratados.

Por lo que se toman las siguientes medidas recomendadas:

- Eliminar softwares que no se usen o necesiten en los computadores.
- Actualizar el sistema operativo y aplicaciones de forma regular.
- Mantener el firewall del computador encendido, en base a las necesidades del trabajo del profesional.
- Para los usuarios de **Windows**, asegurar la instalación de un software anti-virus o utilizar Windows Defender.

- Mantener encendido el cifrado de disco.
- No compartir bajo ningún concepto las credenciales de acceso a los diferentes sistemas, plataformas y aplicativos como así tampoco escribir las contraseñas en lugares donde otras personas puedan visualizarlas.
- Proceder a cambiar la contraseña en forma inmediata cuando sospeche que se encuentra comprometida.

6.5 Gestión de Claves

La Gestión de Claves tiene como objetivo establecer lineamientos para garantizar una adecuada gestión de las claves de acuerdo a las mejores prácticas de seguridad en el entorno y a los requerimientos normativos que aplican a este Municipio.

Se recomienda:

- Los funcionarios no deben compartir contraseñas, si un funcionario requiere credenciales para acceder a un servicio, el mismo debe solicitarlo al **Jefe de Área**, el cual solicitara al departamento informático la creación de estas credenciales.
- Las contraseñas son personales e intransferibles, siendo responsabilidad del usuario hacer un buen uso de las mismas.
- Las contraseñas generadas por del funcionario o en su caso por el departamento informático, deben poseer como mínimo una longitud de 8 caracteres Alfanumérica una letra mayúscula.
- No escribir PINs y contraseñas al lado de computadores o teléfonos.
- Cambiar las contraseñas de manera regular y cuando se sospeche compromiso.
- No utilizar la misma contraseña para diferentes sistemas críticos.

6.6 Gestión de Respaldo, Recuperación y Continuidad

La Gestión de Respaldo, Recuperación y Continuidad tiene como objetivo establecer lineamientos tendientes a la preservación de los datos, operatoria y poder asegurar la continuidad del negocio.

Para esto, es necesario:

- Asegurar un inventario de los soportes de resguardo existentes, su contenido y lugar de almacenamiento, así como también fijar los responsables de mantener esos inventarios y mantener una copia actualizada.
- Realizar pruebas periódicas de recuperación de información desde los soportes almacenados con el fin de asegurarse del adecuado funcionamiento de los procesos de generación de las copias y de la disponibilidad de la información en tiempo y forma.
- Realizar un análisis de riesgo para determinar cuáles son las amenazas y escenarios de desastre a las que se encuentran expuestos los procesos críticos, cuál es su probabilidad de ocurrencia y cuál es su impacto económico en caso que ocurra una contingencia.
- Definir, documentar, ejecutar y controlar un plan de pruebas anual para la evaluación de la eficiencia del plan de continuidad del negocio y la detección de mejoras.

6.7 Gestión de Cumplimiento

La Gestión de Cumplimiento tiene como objetivo establecer lineamientos tendientes a estar alineados con las diferentes regulaciones y normativas a las que la empresa esté sujeta.

6.8 Gestión de la Seguridad Física y Ambiental

La Gestión de la seguridad física y ambiental tiene como objetivo identificar y establecer medidas de control para proteger adecuadamente los activos de información y así evitar incidentes o interferencias no deseadas que afecten a la integridad física de la información.

La Ilustre Municipalidad de María Elena contempla para protección física de los activos:

- Perímetro de Seguridad Física del municipio.
- Controles de acceso físico al municipio y salas de servidores.
- Aseguramiento de las oficinas, centro de procesamiento de datos, etc.
- Trabajo en áreas seguras.
- Áreas designadas para la entrega y carga de material.
- Ubicación y protección de equipos y activos de información.
- Monitoreo, evaluación y redundancia en los servicios de apoyo. *Como, por ejemplo: electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado.*
- Seguridad en cableado estructurado.
- Mantenimiento de equipo.
- Retiro de equipos y activos de información.

Ciclo de uso general

A continuación se entregan los pasos que debe seguir para un buen uso de relojcontrol.com:

1 Realizar cambio de contraseña / Activar nuevo usuario

Al momento de contratar el servicio de relojcontrol.com, se le entrega una cuenta de usuario del tipo *Administrador General*, además de la contraseña para ingresar al sistema, vía correo electrónico.

- Al iniciar sesión por primera vez, debe realizar un cambio de contraseña. Vea Perfil (//soporte.relojcontrol.com/article/28-perfil-de-usuario#primer_inicio).

2 Administrar usuarios del sistema

Éste primer usuario *Administrador general* es capaz de realizar cambios de toda la información de la Compañía.

Sin embargo, es posible que necesite de nuevos usuarios, con igual o distintos privilegios.

- Para conocer los tipos de usuarios del sistema, vea Tipos de usuario (//soporte.relojcontrol.com/article/26-usuarios-del-sistema?preview=5473920ce4b0f6394183b9c4#tipos_usuario)
- Para conocer cómo crear y/o modificar usuarios del sistema, vea Usuarios (//soporte.relojcontrol.com/article/26-usuarios-del-sistema?preview=5473920ce4b0f6394183b9c4).

3 Crear sucursales y departamentos

Si la Compañía posee varias sucursales o departamentos, debe registrarlos. Más adelante se podrán asignar los relojes (en caso de más de uno) por sucursal.

Si es un cliente antiguo (antes de relojcontrol, se utilizó el Software *Control de Asistencia QWANTEC*), y los empleados se dividen por departamentos, puede realizar la exportación más adelante.

- Para conocer cómo crear sucursales, vea Sucursales (//soporte.relojcontrol.com/article/3-sucursales#nueva_sucursal).
- Para conocer cómo crear departamentos, vea Departamentos (//soporte.relojcontrol.com/article/5-departamentos#nuevo_departamento).

4 Asignar relojes a las sucursales

Si la compañía posee más de una sucursal, y éstas poseen relojes control instalados, se debe realizar la asignación de cada uno de ellos a su sucursal respectiva. Ésto es necesario si desea configurar el sistema para que los terminales sólo posean las huellas digitales de los empleados en la sucursal a la cual asiste, o en el caso que existan sucursales y relojes fuera de la zona horaria de la sucursal matriz.

- Vea Administración de sucursales (//soporte.relojcontrol.com/article/29-relojes#modificacion).

5 Ajustar zona horaria de las sucursales

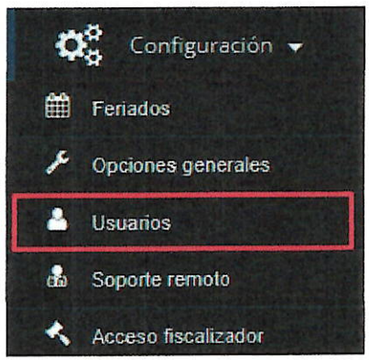
La Compañía puede poseer sucursales fuera de la zona horaria de la sucursal Matriz. La zona horaria es utilizada para que los relojes posean la hora actual en el lugar que se encuentren, además para obtener resultados correctos en los reportes, asistencia actual, etc.

PREVIEW Changes will not be visible to customers until published.

Usuarios del sistema

EN ESTE ARTÍCULO

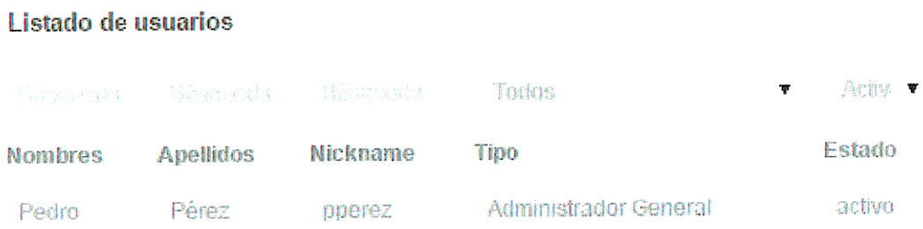
Descripción



Al momento de contratar el servicio de Relojcontrol.com, se le entrega una cuenta de usuario, del tipo *Administrador General.* Éste tipo de usuario es capaz de realizar cambios de toda la información de la Compañía.

Sin embargo, es posible que necesite de nuevos usuarios, con igual o distintos privilegios. En éste artículo se explican los tipos de usuarios, y la forma de administrarlos.

El usuario que actualmente lo está utilizando no puede ser modificado desde el menú de Usuarios. Puede editarlo desde Perfil (//soporte.relojcontrol.com/article/28-perfil-de-usuario).



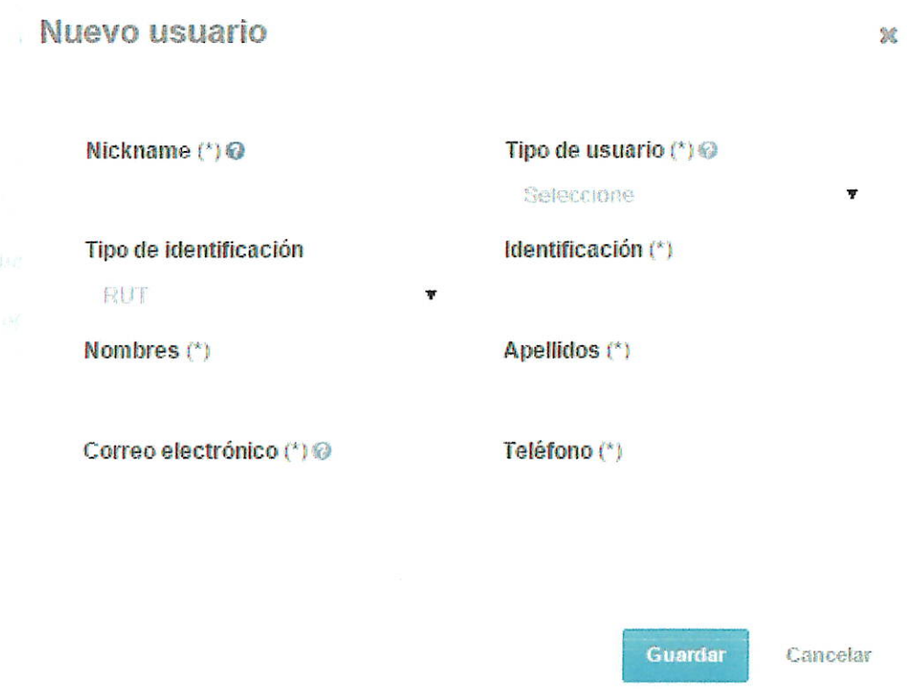
Tipos de usuario

- **Administrador general:** Acceso total. Posee privilegio para modificar toda la información de su Compañía.
- **Administrador de sección:** Acceso parcial, sólo a las sucursales y/o departamentos asignados. Posee privilegios para modificar información de la compañía, pero no puede modificar usuarios, crear sucursales y/o departamentos. Los empleados creados por éste tipo de usuario sólo pueden ser asignados a las sucursales del usuario.
- **Revisor:** Acceso a todo el sistema, pero sólo para visualizar. Sólo puede modificar su perfil.

Registrar nuevo usuario

1 Presione el botón *Nuevo usuario.*

2 Ingrese la información requerida. Debe ingresar el RUT (en caso de poseerlo) o el número de Pasaporte (en caso de ser extranjero, y no poseer RUT chileno aún). Además, debe indicar el correo real del usuario, ya que la contraseña de activación al sistema se enviará dicha dirección.Además, ingrese el tipo de usuario (para el usuario *Administrador de sección,* se deberá asignar sucursales y/o departamentosluego de ser registrado.



3 Presone *Guardar.*

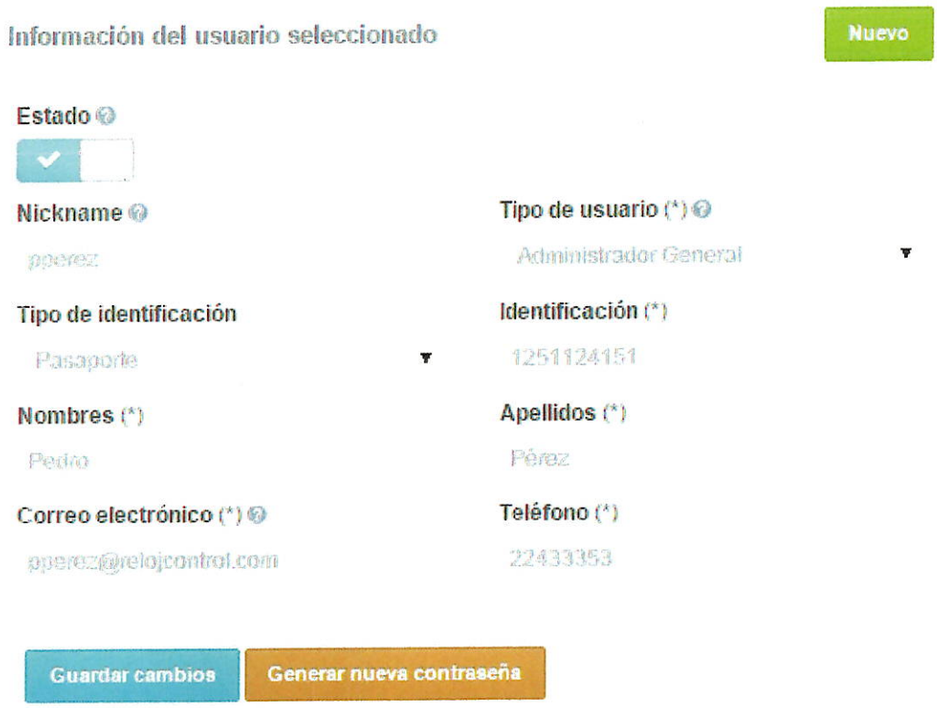
Al momento de registrar el nuevo usuario, se enviará un correo electrónico a la dirección ingresada, con el nombre de usuario y contraseña para ingresar. Además, el usuario debe ingresar al link recibido en dicho correo para realizar una verificación de correo electrónico en la aplicación. Si el usuario se encuentra asociado a un correo electrónico no verificado, no podrá recibir algunos mensajes y alertas de sistema.

Una vez ingresado en el sistema, el nuevo usuario debe realizar un cambio de contraseña, y registrar una pregunta y respuesta secreta, ver Perfil (//soporte.relojcontrol.com/article/28-perfil-de-usuario).

Visualizar/Modificar usuarios

1 Seleccione un usuario de la lista. En el caso de reactivar un usuario, selecciónelo del listado, usando el filtro de estado.

2 Modifique los campos que desea actualizar y/o desactivar. El nombre de usuario (nickname) no se puede modificar. En caso de cambiar el tipo de usuario a Administrador de sección, vea el siguiente título. Además, si el usuario posee Pasaporte, puede cambiar el valor por su RUT chileno, en caso de obtenerlo.

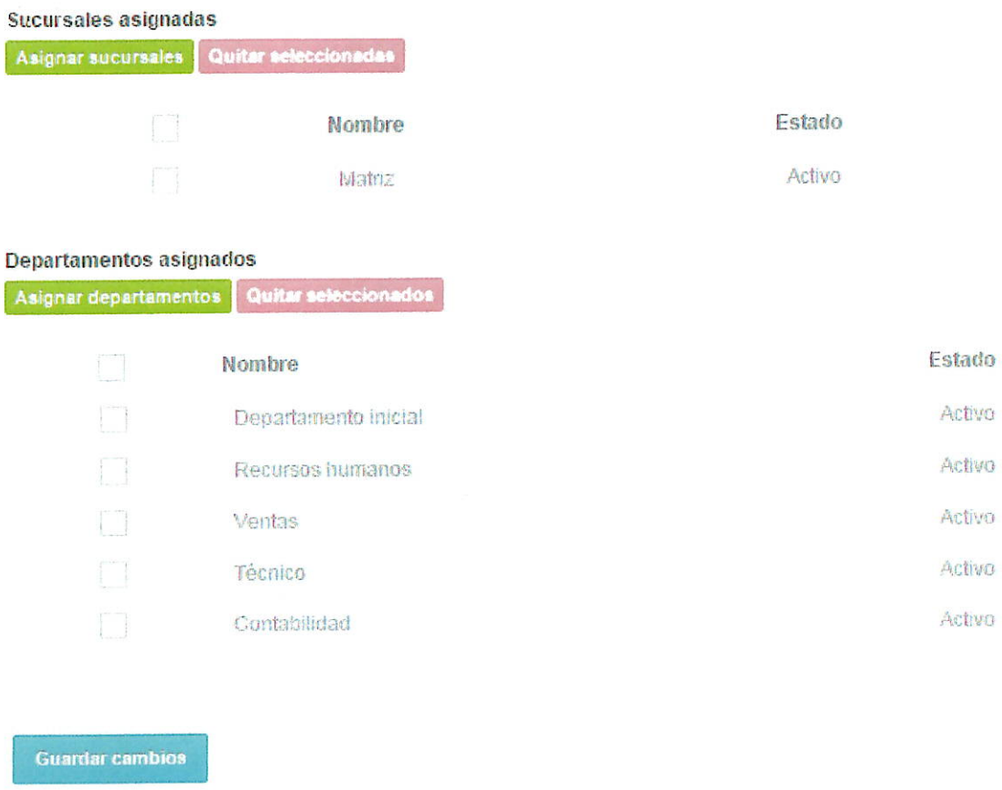


3 Presione *Guardar cambios*.

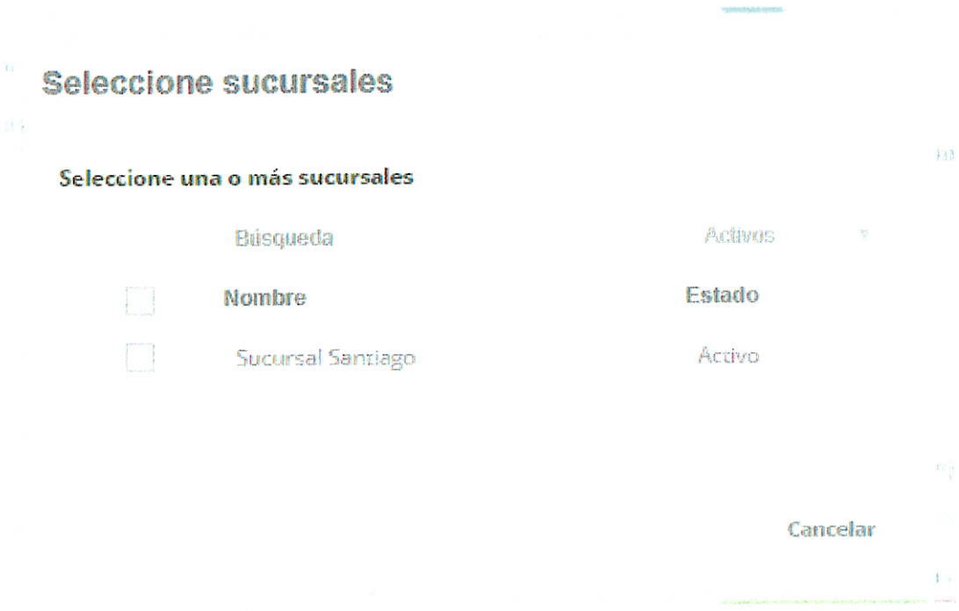
Asignaciones a usuario *Administrador de sección*

El usuario del tipo Administrador de sección sólo puede ver y/o modificar la información correspondiente a las sucursales y/o departamentos asignados. Al momento de crear un usuario de éste tipo, se asigna automáticamente la sucursal *Matriz* y el departamento *Inicial*, con la posibilidad de desasignarlos.

1 Presione el botón correspondiente a lo que desea asignar (sucursal o departamento).



2 Seleccione las sucursales (o departamentos) que desa asignar al usuario.



3 Presione *Seleccionar.*

4 Una vez en la pantalla principal de edición de usuarios, presione *Guardar cambios.*

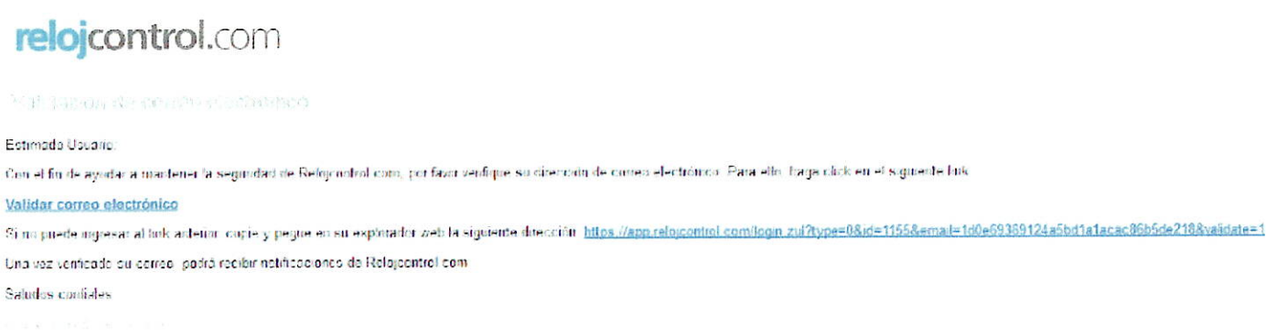
Para quitar elementos, selecciónelos y presione *Quitar seleccionados*. Una vez realizado presione *Guardar cambios.*

Verificación de correo electrónico

Al crear un nuevo usuario, o al modificar el correo electrónico de un usuario existente, se enviará automáticamente un correo de verificación, para comprobar que la dirección de correo electrónico exista y sea válida.

Si no se realiza el proceso de verificación el usuario no podrá recibir correos de mensajes y alertas de sistema, y en cada inicio de sesión recibirá la siguiente información:

Al presionar OK, el sistema volverá a enviar un correo de verificación a la casilla registrada. Recibirá un mensaje de este tipo:



Al presionar Validar correo electrónico, ingresará a Relojcontrol.com, y validará su dirección de correo electrónico.

¿Aún necesitas ayuda? Contáctanos (#) *Última actualicación Julio 20, 2020*

Al momento que se realiza un cambio de hora (adelantar - atrasar / hora verano - invierno) en el país de la sucursal, se debe realizar el cambio de hora desde el menú de sucursal. Una vez realizado, se actualizarán los terminales asociados con la nueva hora. Se debe realizar el cambio de zona horaria para todas las sucursales que posean relojes control.

- Vea Sucursales (//soporte.relojcontrol.com/article/3-sucursales#modificar_timezone).

6 Configurar opciones generales- envío de huellas digitales

Los relojes de la Compañía comparten la información de todos los usuarios,sin importar si se encuentran activos, inactivos, o si no pertenecen a la sucursal del reloj. Sin embargo, se puede configurar el sistema para que los relojes posean las huellas sólo de los empleados de la sucursal perteneciente (las huellas de los empleados que se encuentran en la sucursal matriz, y de los administradores de reloj, permanecerán en todos los relojes de la compañía).

- Vea Opciones generales (//soporte.relojcontrol.com/article/31-reglas-de-asistencia#reloj).

7 Crear empleados desde el sistema

Los empleados se pueden registrar desde el sistema o desde el reloj (no recomendado). En relojcontrol.com, cada empleado debe tener un ID o código en el reloj diferente, sin importar si se encuentra activo/inactivo, o la sucursal a la que pertenesca. Se recomienda utilizar como ID (código en reloj) el Rut del empleado, sin puntos, guión ni dígito verificador.

Para una Compañía que se encuentra migrando desde el Software de Windows *Control de asistencia de Windows*, es posible que pueda realizar una *importación de los empleados registrados*, siempre y cuando todos los empleados posean diferente código en reloj. En caso contrario, se debe realizar un cambio de ID para todos los empleados. Luego de realizar la importación, debe registrar las huellas digitales.

Una vez registrado un empleado, desde relojcontrol.com o desde una terminal, la información se replica a todos los relojes activos de la compañía. Además, debe registrar las huellas digitales de los empleados (si los relojes de la compañía son Biométricos).

- Para crear empleados (compañía nueva o antigua), y registrar huellas, vea Empleados (//soporte.relojcontrol.com/article/7-empleados#nuevo_empleado).
- Para importar empleados (compañía antigua), vea Importación desde Software de Windows (//soporte.relojcontrol.com/article/13-importacion-desde-software-de-windows).

8 Transferir empleados de sucursal / departamento

Es posible que, al crear los empleados o importarlos, los necesite cambiar de sucursal o departamento. Hay una manera que realiza esta operación de manera masiva.

Al momento de realizar una asignación de sucursal, se actualizarán los datos de los empleados seleccionados en los relojes.

- Vea Asignación masiva sucursal / departamento (//soporte.relojcontrol.com/article/7-empleados#asignacion_suc_depto).

9 Sincronizar relojes

Al momento de realizar modificaciones en empleados, sucursales o configuraciones, se envían automáticamente comandos a los relojes. Sin embargo, si adquiere nuevos relojes para la Compañía, es necesario sincronizar los nuevos relojes, mediante Comandos de reloj.

- Vea Comandos de reloj (//soporte.relojcontrol.com/article/32-comandos-de-reloj#enviar).

10 Crear horarios

Luego de crear los empleados, asignarlos a las sucursales/departamentos y enviar la información hacia los relojes de la Compañía, los empleados pueden realizar marcaciones y el sistema las almacenará correctamente.

Ahora debe crear los horarios para asociarlos a los turnos, y así asignarlos a los empleados.

Si el empleado no trabaja con horario (puede entrar o salir del trabajo en cualquier momento), pero tiene que cumplir con horas de trabajo semanal, o el horario a cumplir tiene una duración fuera de lo normal (por ejemplo, médicos que puedan realizar una cirugía por más de 24 horas), puede optar por crear **turnos flexibles (en base a horas de trabajo)**. Estos turnos no poseen horarios.

- Para conocer cómo crear horarios, vea Horarios (//soporte.relojcontrol.com/article/11-horarios#nuevo).
- Si desea no crear horarios, sino que turnos flexibles, vea Turnos (//soporte.relojcontrol.com/article/14-turnos#nuevo).

11 Crear turnos

Luego de crear horarios, debe asignarlos a los turnos correspondiendes. Un horario puede asignarse a varios turnos.

- Para conocer cómo crear turnos, y asignarle horarios a éstos, vea Turnos (//soporte.relojcontrol.com/article/14-turnos#nuevo).

12 Asignar turnos a empleados

Ahora puede asignar turnos a los empleados. Puede asignar turnos individualmente, o utilizar la herramienta de asignación masiva.

- Vea Asignación de turnos (//soporte.relojcontrol.com/article/15-asignacion-de-turnos-a-empleados).

13 Crear feriados

Puede ocurrir que en el mes actual de trabajo, existan días festivos, los cuales todos (o algunos) de los empleados no deban trabajar ese día.

Los empleados que deben trabajar, como horas de trabajo normal o tiempo extra, pueden ser configurados mediante su Turno.
(//soporte.relojcontrol.com/article/14-turnos#info)

- Vea Feriados (//soporte.relojcontrol.com/article/33-feriados#nuevo).

14 Crear tipos de salida especial

Al momento de registrarse su Compañía, se crean automáticamente tipos de salida especial. Los tipos de salida especial identifican a la salida especial asignada a un empleado, comportándose de distinta forma al momento de realizar el cálculo de horas.

- Si desea, puede crear más tipos de salida especial, o modificar el nombre de los ya existentes. Vea Tipos de salida especial (//soporte.relojcontrol.com/article/17-salidas-especiales#tipos_salida).

15 Crear salidas especiales

Si caso que uno o varios empleados presenten salidas, tales como vacaciones, salidas a terreno, etc., es necesario crear sus salidas especiales. Éstas salidas especiales se pueden crear para uno o varios empleados a la vez.

- Para conocer cómo crear salidas especiales, individuales o masivas, vea Salidas especiales (//soporte.relojcontrol.com/article/17-salidas-especiales).

16 Configuración de las opciones del Sistema

Su Compañía ya se encuentra lista para realizar los cálculos de horas para los empleados que poseen turnos asignados. Sin embargo, es posible que necesite cambiar las opciones para el cálculo de horas trabajadas.

- Vea Opciones generales (//soporte.relojcontrol.com/article/31-reglas-de-asistencia#calculo).

17 Realizar cálculo de horas

Para realizar el cálculo de horas correctamente, es necesario realizar los procedimientos mencionados en los puntos anteriores. Los empleados que no posean turnos asignados, no aparecerán en los resultados, previa advertencia.

- Vea Cálculo de horas trabajadas (//soporte.relojcontrol.com/article/22-calculo-de-horas-trabajadas).

18 Generar reportes de asistencia

Una vez realizado el cálculo de asistencia, es posible generar una serie de reportes e informes, siendo el mas importante el **Reporte de asistencia legal**.

- Para conocer los reportes que se pueden generar en relojcontrol.com, vea Reportes (//soporte.relojcontrol.com/article/20-reportes-de-asitencia).
- Para generar los reportes necesarios, vea Cálculo de horas trabajadas (//soporte.relojcontrol.com/article/22-calculo-de-horas-trabajadas#reportes).

19 Solución a los problemas de cálculo

Si al momento de realizar un cálculo de horas, se encuentra algún dato incoherente en el reporte legal de asistencia (horas extra o falta elevadas, falta de licencias médicas), o simplemente el empleado no aparece en el reporte, se debe generalmente a registros o configuraciones incorrectas.

- Si presenta uno de estos problemas, puede dirigirse a Solucion de problemas al cálculo de horas trabajadas (//soporte.relojcontrol.com/article/36-solucion-de-problemas-al-calculo-de-horas-trabajadas).

(//soporte.relojcontrol.com/article/31-reglas-de-asistencia#calculo)

¿Aún necesitas ayuda? Contáctanos (#)

Última actualicación Marzo 6, 2020

Hoy en día las organizaciones deben tener una real preocupación por la Seguridad de la Información, ya que sus sistemas manejan información muy sensible para las empresas, contribuyentes, ciudadanos, etc. Estas organizaciones no pueden darse el lujo de que sus sistemas sean vulnerados por hackers que buscan generar pérdidas y daños.

En el mundo vemos que no existe ninguna organización pública o privada que esté ajena a ataques. Es así como se ha sabido de ataques sufridos por la multinacional Intel, el mayor fabricante de procesadores en el mundo. Se encontraron dos graves vulnerabilidades llamadas MELTDOWN y SPECTRE que afectan a los procesadores que son fabricados por esta compañía.

Las fallas que presentan estos procesadores permiten el acceso a información sensible y con ello al robo de datos de los usuarios como claves y llaves de encriptación . Esto nos confirma que las organizaciones deben estar atentas a ataques informáticos como los RANSOMWARE y tomar las medidas que sean necesarias para disminuir el daño que generan estos ataques . Deben ser capaces de implantar una serie de dispositivos como firewall y generar una política de respaldos, un procedimiento de contingencia que asegure la continuidad operacional. En el caso de la empresa privada, deben implantar la ISO 27001 :2013.

Es un hecho real que constantemente somos atacados y esto va generar incidentes que pueden llevarnos a la suspensión de los servicios entregados, lo que traer á como consecuencia una mala imagen frente a nuestros clientes . los que se molestarán por la suspensión del servicio.

De esta forma. debemos velar en todo momento por la Seguridad de la Información ya que ésta es uno de los principales activos de las organi zaciones. Debemos asegurar la defensa de este activo ya que es una tarea esencial para asegurar la continuidad del negocio y la protección de los datos personales. Cada día debemos seguir implementando medidas que nos permitan disminuir los riesgos de ataques hacia nuestros sistemas.

Sabemos que es imposible asegurar en un 100% nuestros sistemas y redes. Pero si podemos disminuir cada vez más los riesgos que se presentan. Debemos tomar conciencia de lo importante que es la Seguridad de la Información y tratar de concientizar a todos los integrantes de la organización y en mayor medida, a la alta dirección.

Daniel Valdés Gómez

El Peligro de los Insiders al Interior de las Organizaciones

Consejos para prevenir las Amenazas Internas

Las amenazas internas son cada vez más problemáticas para las organizaciones. Un informe arrojó que el 89% de las organizaciones considera que las amenazas se deben al personal interno, ya que manejan información y antecedentes.

Insiders: son personas que están dentro de una empresa u organización, tales como trabajadores, programadores, administrativos, gerentes, etc., que atacan sistemas, redes y comunicaciones desde su interior. Además, son personas que roban información, realizan fraudes, sabotaje, alteran registros y archivos.

Ataques de Insiders

Son ataques y violaciones de seguridad cometidos por los mismos empleados de la organización, ya que una de las formas más eficaces para romper esquemas de seguridad, es desde el interior de la misma. Este tipo de acto se comete con intenciones de obtener beneficios económicos a través de la información que posee valor.

Esto implicaría, por ejemplo, la pérdida de una llave USB portátil o dejando un correo electrónico sobre la mesa para que todos en la oficina lo puedan ver, o realizando el envío accidental de un mail a la persona equivocada .

De esta forma, los tipos de ataques perpetrados por personal interno pueden tomar diferentes formas, como por ejemplo:

- Ataque malicioso.
- Compartir password.
- Exposición accidental.
- Robo de información

Los tipos de datos expuestos por los insiders son variados y dependen del motivo. Algunos lo hacen motivados por razones económicas, otros lo hacen para exponer información por razones sociales o ideológicas (como es el caso de Edward Snowden) o por venganza contra la empresa.

Uno de los principales métodos que contribuyen a la exposición de los datos de información privilegiada es el mal uso de las credenciales que se comparten, usualmente nombre de usuario y password.

Prevenir que alguien dentro de la organización exponga los datos sensibles y personales es una tarea difícil. Pero mitigar este riesgo es parte de la estrategia de seguridad.

Detallamos algunos tips para salvaguardar los datos de la amenaza de los insiders.

- Educación: porque muchas de las amenazas son accidentales y no maliciosas, por lo que la educación puede tomar largo tiempo.
- Reducir el riesgo privilegiando credenciales con autenticación multifactor (MFA en inglés).
- Uso adaptativo de medidas de autenticación.
- Uso de técnicas conocidas para prevenir la infección de código malicioso.
- Uso de una herramienta de análisis de comportamiento, una herramienta de seguridad de la información y una de gestión de eventos .

Par que los insiders no tengan éxito, debemos generar cinco prácticas:

- Controles de seguridad.
- Controles de redes.
- Monitoreo continuo de dispositivos finales.
- Capacitación de los empleados.
- Predecir el comportamiento humano .

Con las medidas correctas a implantar, las organizaciones podemos reducir significativamente los riesgos y el impacto de las amenazas internas .

CAS-CHILE®

LÍDER EN SOFTWARE DE GESTIÓN PÚBLICA

Cas-Chile® Conecta a las **Municipalidades** del País.

Seguridad en Municipios

Marín N° 0586 - Providencia | **Mesa Central:** + 600 570 00 20
Ventas: ventas@caschile.cl | **Comunicaciones:** comunicaciones@caschile.cl

¿Cómo se encuentra hoy en día su Municipalidad en relación a su Seguridad de la Información?

Los municIplos deben conocer el estado actual de su Seguridad de la Información (SI) y para ello, deben realizar una Auditoría Interna sobre las TIC, s. Esta auditoría debe llevar a responder una serie de preguntas que tienen que ver con el estado de la SI en relación a su Integridad, Confidencialidad y Disponibilidad.

A continuación, detallamos algunas consultas que debería realizarse un Municipio para evaluar el estado de su Seguridad de la Información:

- ¿Los sistemas de información garantizan las condiciones mínimas de Seguridad y Confidencialidad de la Información de acuerdo a la normativa vigente? (DS N°83/2004; Nch ISO 27002:2013; Ley 17.336;Nch 2m; DS N°77/2014; DS N°100/2006 y DS N° 93/2006).

- ¿Qué mecanismos de control de acceso existen para los servidores y computadores?

- ¿La sala de servidores cumple con las exigencias establecidas en el Decreto Supremo N°83 de 2004, del Ministerio de la Secretaría General de la Presidencia?

- ¿La Municipalidad ha generado en su interior un Comité de Gestión de Seguridad de la Información?

- ¿Existe un Inventario de los Activos de Información, Software y Servicios TIC?

- ¿Existe un procedimiento de Control de Acceso Lógico a los sistemas?

- ¿Se ha dictado por parte de la Municipalidad una Política de Seguridad de la Información?

- ¿Existen políticas de uso, almacenamiento, acceso y distribución de mensajes electrónicos?

- ¿Se han generado Auditorías Internas de TI?

- ¿Existe una política de Seguridad de la Información en relación al personal de la Municipalidad?

- En relación a los respaldos de información ¿Se cuenta con algún procedimiento que dé cuenta de ello?

- ¿El municipio ha generado una Política de Contraseñas?
- ¿Qué tipo de dispositivos mantiene el municipio para el control del acceso físico?
- ¿El municipio mantiene un Plan de Continuidad del Negocio y un Plan de Recuperación de Desastres?
- ¿Cuenta con un Análisis del Impacto del Negocio (BIA)?
- ¿Cuenta con un SLA (Acuerdo de Niveles de Servicio) para proveedores?
- ¿La Municipalidad cuenta con las licencias de software respectivas?
- ¿Existe un procedimiento sobre Incidentes de Seguridad?
- ¿Tiene su Municipalidad un equipo de respuesta a incidentes?
- ¿Los servidores cuentan con las medidas de seguridad necesarias para evitar los hackeos?
- ¿Qué arquitectura de seguridad mantiene el municipio en relación con el e-commerce?
- ¿El portal web de la Municipalidad cumple con lo indicado en el Decreto N°1 de 2015 del Ministerio de Secretaría General de la Presidencia, que aprueba la norma técnica sobre sistemas y sitios web de los órganos de Administración del Estado?.
- ¿Existe un control de cambios en la configuración?
- ¿Existe un encargado de la Seguridad de la Información?
- ¿Existe un procedimiento de Revisión de Contratos?
- ¿Existen Planes de Capacitación para los empleados municipales en materias de Seguridad de la Información?
- ¿Qué medidas de Seguridad mantiene su Municipalidad en relación al uso de la red interna y el uso de Internet?

Todas estas preguntas tienen por objetivo indicar a las Municipalidades en qué áreas se deben preparar para cumplir con la fiscalización que realiza la Contraloría General de la República. Este organismo revisa y evalúa aspectos relacionados con las políticas, normas, prácticas y procedimientos de control relativos a los sistemas basados en las TIC' s, así como también, de la Seguridad de la Información en conformidad con la Norma Técnica para los órganos de la Administración del Estado, sobre Seguridad y Confidencialidad de los Documentos Electrónicos; DS N°83 de 2004 del Ministerio Secretaría General de la Presidencia; DS N°93 de 2006 y DS N° 181 de 2006, del Ministerio de Economía, Fomento y Turismo.

Daniel P. Valdés Gómez